

ATTI PARLAMENTARI

XIII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **CXXXVI**

N. 3

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 1999)

(Articolo 31, lettera n), della legge 31 dicembre 1996, n. 675)

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

Trasmessa alla Presidenza il 15 giugno 2000

PAGINA BIANCA

INDICE

<i>Elenco delle abbreviazioni</i>	<i>Pag.</i>	7
1. Quadro riassuntivo delle novità sul piano normativo	»	11
1.1 I principali provvedimenti normativi	»	11
1.2 Altre novità rilevanti in materia di trattamento dei dati	»	12
1.3 Lavori parlamentari	»	13
2. Stato di attuazione della legge n. 675/1996 e nodi da affrontare	»	15
2.1 Pubblica amministrazione	»	15
2.1.1 Profili generali	»	15
2.1.2 Tempi e rispetto degli adempimenti	»	15
2.1.3 Trasparenza dell'attività amministrativa	»	18
2.1.4 Diritto di accesso a documenti amministrativi	»	20
2.1.5 Dati sensibili e di carattere giudiziario	»	22
2.1.6 Nuovi archivi e grandi banche dati	»	27
2.1.7 Documenti elettronici e carte magnetiche	»	31
2.1.8 Enti locali	»	33
2.1.9 Documentazione anagrafica	»	35
2.1.10 Attività fiscali e tributarie	»	37
2.2. Sanità	»	38
2.2.1 Profili generali	»	38
2.2.2 Dati genetici	»	41
2.2.3 Ricerca medica ed epidemiologica	»	42
2.2.4 Tessera sanitaria	»	43
2.3. Lavoro e previdenza sociale	»	43
2.3.1 Il rapporto di lavoro	»	43
2.3.2 Conoscibilità dei dati contenuti nei « cedolini » dello stipendio	»	47
2.3.3 Enti previdenziali	»	48
2.4. Statistica, ricerca scientifica e ricerca storica	»	49
2.4.1 Attività di ricerca scientifica	»	49
2.4.2 Trattamento di dati personali per finalità di statistica	»	51
2.4.3 Dati personali e ricerca storica	»	53
2.5. Associazioni, partiti e confessioni religiose	»	55

2.6. Settore del credito e assicurativo	Pag.	57
2.6.1 Accesso alle perizie medico legali in ambito assicurativo	»	57
2.6.2 Semplificazioni dell'informativa nel settore bancario	»	59
2.6.3 Le «centrali rischi» gestite dalla Banca d'Italia e da privati	»	61
2.6.4 C.d. «anagrafe dei conti correnti»	»	63
2.6.5 Anagrafe degli assegni	»	64
2.7. Attività di marketing	»	64
2.8. Giornalismo	»	67
2.8.1 Privacy e attività giornalistica nel quadro della normativa vigente .	»	67
2.8.2 Rispetto del segreto d'ufficio, professionale e investigativo	»	67
2.8.3 Attività giornalistica e principi di cui all'articolo 9 legge n. 675/ 1996	»	68
2.8.4 Protezione di minori e malati	»	69
2.8.5 Misure provvedimenti e procedurali di tutela	»	70
2.9. Attività giudiziarie e di polizia e servizi di sicurezza	»	71
2.9.1 Particolari trattamenti in ambito pubblico	»	71
2.9.2 Trattamenti di dati per finalità di giustizia	»	71
2.9.3 Forze di polizia e C.e.d. del Dipartimento della pubblica sicurezza .	»	73
2.9.4 Trattamenti relativi all'Accordo di Schengen	»	75
2.10 Reti telematiche e servizi di telecomunicazione	»	75
2.10.1 Prima attuazione del decreto legislativo 171/1998	»	75
2.10.2 Fatturazione dettagliata	»	77
2.10.3 Utilizzazione di apparecchi telefonici e accessi ad Internet da parte di lavoratori	»	79
2.10.4 L'avvio in Italia di servizi di telefonate gratuite con spot	»	80
2.10.5 La tutela dei dati nei servizi di accesso gratuito ad internet	»	82
2.11 Commercio elettronico	»	84
2.11.1 Profili generali	»	84
2.11.2 La posizione comune europea e la direttiva sulle firme elettroni- che	»	85
2.12 Flussi transfrontalieri di dati	»	87
2.13 Videosorveglianza	»	90
2.14 La disciplina della sicurezza nel trattamento dei dati	»	94
3. Il garante	»	98
3.1 E ricorsi ex articolo 29: un bilancio d'insieme	»	98
3.1.1 Principali settori e ambiti di trattamento dei dati	»	99
3.1.2 Particolari profili applicativi e considerazioni finali	»	100
3.2 Rapporti con l'ufficio del garante	»	101
3.2.1 Relazioni esterne e rapporti con i media	»	101
3.3 Contabilità, dotazione finanziaria, impegni di spesa e sedi dell'ufficio .	»	105
3.3.1 La gestione finanziaria dell'esercizio 1999	»	105
3.4 Registro generale dei trattamenti	»	107
3.5 Attività ispettive e applicazione di sanzioni amministrative	»	109

3.5.1 Poteri di accertamento	Pag.	109
3.5.2 Controllo dei trattamenti e accertamento delle violazioni	»	110
3.6 Codici di deontologia	»	111
3.7 Informatizzazione e sito web	»	114
3.8 Attività di documentazione	»	117
3.8.1 Servizio studi e documentazione	»	117
3.9 Personale, regolamento e gestione risorse umane	»	118
3.9.1. Il decreto legislativo n. 51/1999	»	118
3.9.2 La gestione delle risorse umane	»	119
3.9.3 Il personale	»	121
3.10 Dati sulle principali attività del garante	»	122
3.11 Indagine conoscitiva sulle autorità indipendenti	»	125
4. Quali prospettive per l'anno 2000	»	126
5. Attività sul piano internazionale e comunitario	»	128
5.1 Profili Generali	»	128
5.2 Direttiva n. 95/46/CE e gruppo di lavoro ex articolo 29	»	128
5.3 Cenni comparativi sul recepimento delle direttive 95/46/CE e 97/66/CE	»	130
5.4 Altri gruppi di lavoro in materia di protezione dei dati	»	133
5.5 Cooperazione europea nel settore giustizia e affari interni	»	135
5.6 Schengen	»	136
5.7 Europol	»	137
5.8 Sistema informativo doganale	»	138
5.9 Eurodac	»	138
5.10 Consiglio d'Europa	»	139
5.11 O.C.S.E.	»	140
5.12 Collaborazione con altre Autorità di garanzia	»	141
6. Allegati	»	142
6.1 Disposizioni normative	»	144
6.1.1 Legge 31 dicembre 1996, n. 675 (testo aggiornato)	»	144
6.1.2 Decreto legislativo 11 maggio 1999, n. 135	»	168
6.1.3 Decreto legislativo 30 luglio 1999, n. 281	»	178
6.1.4 Decreto legislativo 30 luglio 1999, n. 282	»	186
6.1.5 Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 ...	»	190
6.1.6 Autorizzazioni generali al trattamento di dati sensibili	»	194
6.1.6.1 Autorizzazione n. 1/99 (rapporti di lavoro)	»	194
6.1.6.2 Autorizzazione n. 2/99 (stato di salute e vita sessuale)	»	198
6.1.6.3 Autorizzazione n. 3/99 (organismi di tipo associativo)	»	203
6.1.6.4 Autorizzazione n. 4/99 (liberi professionisti)	»	207
6.1.6.5 Autorizzazione n. 5/99 (diverse categorie di titolari)	»	211
6.1.6.6 Autorizzazioni n. 6/99 (investigatori privati)	»	218
6.1.6.7 Autorizzazione n. 7/99 (dati a carattere giudiziario)	»	222
6.2 Provvedimenti del garante	»	228

6.2.1 Provvedimento n. 1 /P/2000 del 30 dicembre 1999-13 gennaio 2000 (attività di rilevante interesse pubblico)	Pag.	228
6.2.2 Provvedimento 10 febbraio 2000 (codici di condotta)	»	231
6.2.3 Deliberazione 29 febbraio 2000, n. 8 (modifica del modello di notificazione)	»	233
6.3 Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali	»	235
6.3.1 Raccomandazione 4/99 sulla Carta europea dei diritti fondata- menti	»	235
6.3.2 Negoziato Europa-USA sul trasferimento di dati: Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione europea e il governo degli Stati Uniti	»	237
Parere 2/99 riguardante l'adeguatezza dei « <i>Safe Harbor Principles</i> » (ver- sione del 19 aprile)	»	239
Parere 4/99 riguardante le FAQ (domande poste frequentemente) relative al « <i>Safe Harbor</i> »	»	244
Documento di lavoro sullo stato delle discussioni in corso tra la Com- missione europea e il governo USA (7 luglio 1999)	»	252
Parere 7/99 sul livello di tutela dei dati offerto dai principi del « <i>Safe Harbor</i> » (versione del 15 e 16 novembre)	»	254
6.3.3 Internet	»	265
Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet	»	265
Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni	»	268
Raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari	»	274
Documento di lavoro del 23 febbraio 1999 relativo al trattamento dei dati personali su Internet	»	279
6.3.4 Informazione nel settore pubblico	»	282
Parere 3/99 sull'informazione nel settore pubblico e la protezione dei dati personali	»	282
6.3.5 Trasferimenti di dati verso Paesi terzi	»	290
Parere 5/99 relativo al livello di tutela dei dati personali in Svizzera	»	290
Parere 6/99 relativo al livello di protezione dei dati personali in Ungheria .	»	293
6.4 Autorità comune di controllo Schengen	»	295
6.4.1 3ª Relazione di attività (marzo 1998-febbraio 1999)	»	295
6.5 Autorità comune di controllo Europol	»	345
6.5.1 Atto 1/99 che stabilisce il regolamento interno	»	345
6.6 Consiglio d'Europa	»	355
6.6.1 Emendamenti alla Convenzione n. 108 del 1981	»	355
6.6.2 Protocollo aggiuntivo alla Convenzione n. 108 del 1981	»	357

La presente relazione è riferita al 1999 e contiene alcune notizie ulteriori, aggiornate al 10 aprile 2000, relative a taluni sviluppi significativi che si è ritenuto opportuno menzionare.

ELENCO DELLE ABBREVIAZIONI

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

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

PAGINA BIANCA

RELAZIONE
SULL'ATTIVITÀ SVOLTA DAL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI
(Anno 1999)

PAGINA BIANCA

1. Quadro riassuntivo delle novità sul piano normativo

1.1 I principali provvedimenti normativi

Il 1999 segna un periodo di rilevante attività normativa nell'integrazione della disciplina in materia di trattamento dei dati personali. In attuazione delle leggi che hanno conferito la delega al Governo scaduta nel mese di luglio (leggi nn. 676/1996 e 344/1998), sono stati infatti emanati alcuni provvedimenti integrativi e correttivi della legge n. 675 del 1996.

Il decreto legislativo 26 febbraio 1999, n. 51 (*"Disposizioni integrative e correttive della legge 31 dicembre 1996 n. 675, concernenti il personale dell'ufficio del Garante per la protezione dei dati personali"*), ha istituito il ruolo organico del personale dell'Autorità ed ha attribuito al Garante il potere di emanare uno o più regolamenti per disciplinare l'inquadramento in ruolo delle unità in servizio, il trattamento giuridico ed economico, il reclutamento del personale e l'organizzazione ed il funzionamento dell'Ufficio anche sotto il profilo contabile e della gestione delle spese (v. oltre, par. 3.9).

Il decreto legislativo 11 maggio 1999, n. 135, (*"Disposizioni integrative della legge n. 675/1996 sul trattamento dei dati sensibili da parte dei soggetti pubblici"*), ha invece integrato la disciplina sul trattamento dei dati sensibili e di carattere giudiziario da parte della pubblica amministrazione ponendo fine al regime transitorio già previsto dall'art. 41, comma 5, della citata legge (e oggetto di alcune proroghe), il quale aveva permesso ai soggetti pubblici di proseguire il trattamento di tali dati, previa comunicazione al Garante, anche in mancanza delle disposizioni di legge aventi le particolari caratteristiche richieste dall'art. 22, comma 3, della medesima legge. Il decreto n. 135 ha così introdotto un nuovo quadro di carattere generale, prescrivendo alcuni principi già operanti e individuando alcune finalità di rilevante interesse pubblico che sono attualmente oggetto di disposizioni integrative promosse dalle amministrazioni (v. oltre, par. 2.1.5).

Con il d.P.R. 28 luglio 1999, n. 318 (*"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675"*), è stato emanato il regolamento che individua le "misure minime" di sicurezza per il trattamento dei dati personali, ai sensi dell'art. 15, comma 2, della legge n. 675/1996, la cui osservanza è obbligatoria anche sul piano penale (art. 36 l. cit.) e che sono graduate a seconda che il trattamento sia effettuato solo con strumenti diversi da quelli elettronici o automatizzati oppure per fini personali ai sensi dell'art. 3 della legge, ovvero (nell'ambito dei trattamenti svolti con strumenti elettronici o automatizzati) riguardi elaboratori accessibili mediante reti disponibili al pubblico. Un disegno di legge in via di definitiva approvazione da parte delle Camere prevede, per la piena attuazione del regolamento già prevista entro il 29 marzo 2000, un differimento al 31 dicembre 2000 per i soggetti pubblici e privati che intenderanno avvalersi della facoltà di adeguarsi in modo più graduale alla nuova disciplina (v. oltre, par. 2.14).

Il decreto legislativo 30 luglio 1999, n. 281 (*"Disposizioni in materia di trattamento di dati personali per finalità storiche, statistiche e di ricerca scientifica"*), ha introdotto le previste norme integrative in tema di trattamento dei dati personali utilizzati per scopi storici, di ricerca scientifica e di statistica tenendo conto dei principi contenuti nelle raccomandazioni del Consiglio d'Europa n. R (83)10, adottata il 23 settembre 1983, e n. R (97) 18 adottata il 30 settembre 1997. Oltre ad alcune modifiche alla legge n. 675/1996 e ad altre norme di settore, il decreto ha individuato alcune ulteriori garanzie per il rispetto dei diritti e delle libertà fondamentali degli interessati, prevedendo

inoltre un ruolo particolare per uno o più codici di deontologia e di buona condotta promossi dal Garante in conformità a quanto previsto dall'art. 31 della medesima legge (cfr. oltre, par.3.1).

Il contestuale decreto legislativo 30 luglio 1999, n. 282 (*"Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario"*) ha invece disciplinato alcuni aspetti del trattamento dei dati sanitari da parte di organismi sanitari pubblici, nonché di organismi sanitari e di esercenti le professioni sanitarie in regime di convenzione o di accreditamento con il servizio sanitario nazionale, anche in riferimento ai dati trattati nell'ambito di ricerche epidemiologiche (cfr. oltre, par. 2.2.3).

1.2 Altre novità rilevanti in materia di trattamento dei dati

Nel 1999, oltre ai predetti provvedimenti riguardanti specificamente la tematica del trattamento dei dati personali, sono stati approvati anche altri atti comunque significativi nella materia tra i quali vanno segnalati, in particolare:

- a) il d.P.R. 22 giugno 1999, n. 250 (*"Regolamento per l'autorizzazione all'installazione ed esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato ai sensi art. 133-bis della legge 15 maggio 1997, n. 127"*), nel disciplinare l'introduzione di sistemi di rilevazione di immagini per determinate finalità collegate alla circolazione stradale, ne regola l'utilizzo in relazione alle finalità perseguite dal regolamento anche in riferimento alle modalità di raccolta e di conservazione dei dati;
- b) il d.P.C.M. 22 ottobre 1999, n. 437 (*"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 legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191"*), prevede l'inserimento di alcuni dati necessari per l'identificazione personale ed altre possibili utilizzazioni;
- c) il d.P.C.M. 8 febbraio 1999, recante regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del d.P.R. 10 novembre 1997, n. 513, il quale stabilisce che il piano per la sicurezza deve essere conforme a quanto previsto dall'articolo 9, comma 2, lettera f) del d.P.R. 10 novembre 1997, n. 513, riguardo alla sicurezza dei dati personali;
- d) il regolamento emanato con il d.P.R. 1 dicembre 1999, n. 503, recante norme per l'istituzione della Carta dell'agricoltore e del pescatore e dell'anagrafe delle aziende agricole, in attuazione dell'articolo 14, comma 3, del d.lg. 30 aprile 1998, n. 173, che all'articolo 6 detta disposizioni per l'accesso alla predetta anagrafe;
- e) la legge 19 ottobre 1999, n. 422, di ratifica, in base all'articolo K3 del Trattato sull'Unione europea, della convenzione relativa alla notificazione negli Stati membri di atti giudiziari ed extra-giudiziari in materia civile o commerciale e del protocollo concernente l'interpretazione della stessa convenzione da parte della Corte di giustizia delle Comunità europee, fatti a Bruxelles il 26 maggio 1997 (articolo 1);
- f) il d.P.C.M. 18 febbraio 1999, contenente l'approvazione del Programma statistico nazionale per il triennio 1999-2001, illustra, in relazione a quanto previsto dall'art. 6-bis del d.lg. n. 322/1989, le finalità perseguite e le garanzie previste dalla legge n. 675/1996 e dal citato d.lg. che è stato di recente modificato e integrato dal d.lg. n. 281/1999; sulla tutela della «riservatezza dei dati individuali», comporta un nuovo atteggiamento degli statistici ufficiali nei confronti dei soggetti e dei dati personali che ad essi si riferiscono;

- g) il decreto legislativo 22 luglio 1999, n. 261, che recepisce la direttiva 97/67/CE concernente regole comuni per lo sviluppo del mercato interno dei servizi postali comunitari e per il miglioramento della qualità del servizio (il decreto, all'articolo 1, pone tra le esigenze essenziali del servizio postale la riservatezza della corrispondenza e la protezione dei dati, comprendendo in tale accezione la protezione dei dati personali, la riservatezza delle informazioni trasmesse o conservate, nonché la tutela della vita privata);
- h) il d.P.R. 16 marzo 1999, n. 14, in tema di gestori dei pubblici servizi, recante il regolamento di attuazione delle direttive nn. 95/18/CE (relativa alle licenze delle imprese ferroviarie) e 95/19/CE (relativa alla ripartizione delle capacità di infrastruttura ferroviaria e alla riscossione dei diritti per l'utilizzo dell'infrastruttura). Il relativo art. 7, comma 8, dispone in particolare che *"il gestore dell'infrastruttura ferroviaria è tenuto a rispettare gli obblighi di riservatezza inerenti alla tutela delle persone o delle imprese su notizie, informazioni e dati in conformità alla normativa in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali"*;
- i) la direttiva della Presidenza del Consiglio dei Ministri 28 ottobre 1999, sulla gestione informatica dei flussi documentali nelle pubbliche amministrazioni, che fa salva la tutela dei dati personali (articolo 6);
- j) il d.m. 13 ottobre 1999 che recepisce la direttiva 98/41/CE del Consiglio del 18 giugno 1998 relativa alla registrazione delle persone a bordo delle navi da passeggeri che effettuano viaggi da e verso i porti degli Stati membri della Comunità (articoli 4 e 7);
- k) il d.m. 28 ottobre 1999 del Ministro delle finanze, contenente l'approvazione, con le relative istruzioni, dello schema di certificazione unica (modello CUD 2000), concernente l'attestazione dei redditi di lavoro dipendente e assimilati;
- l) il d.lg. 23 febbraio 2000, n. 38 (*"Disposizioni in materia di assicurazione contro gli infortuni sul lavoro e le malattie professionali, a norma dell'art. 55, comma 1, della legge 17 maggio 1999, n. 144"*), che prevede all'art. 10, comma 5, la possibilità di accedere al registro nazionale delle malattie causate dal lavoro ovvero ad esso correlate, nel rispetto delle disposizioni della legge n. 675/1996.

1.3 Lavori parlamentari

Nel 1999 è stato inoltre avviato o proseguito l'esame parlamentare di alcuni disegni di legge che hanno attinenza con la protezione dei dati o, comunque, con l'attività del Garante.

Fra questi assume particolare rilevanza il disegno di legge per il rinnovo della delega già prevista dalla citata legge 31 dicembre 1996, n. 676, il cui termine di scadenza era già stato prorogato al 31 luglio 1999 dalla legge 6 ottobre 1998, n. 344.

A decorrere dall'entrata in vigore della legge n. 675 sono stati adottati nove decreti legislativi, ma alcuni dei settori e delle tematiche indicati nei principi e criteri direttivi della citata delega non sono stati ancora oggetto delle previste disposizioni integrative e correttive.

L'ulteriore delega prevista dalla legge comunitaria per il 1998 (l. 5 febbraio 1999, n. 25), che riguardava più specificamente il completamento del recepimento della direttiva comunitaria n. 95/46/CE, non è stata poi esercitata.

In Parlamento si è avvertita quindi l'esigenza di un parziale rinnovo della legge delega n. 676, limitatamente ai settori non affrontati dai citati decreti delegati.

Il disegno di legge, già approvato dalla Commissione giustizia del Senato della Repubblica e ora all'esame dell'aula (A/S n. 4178), fissa il nuovo termine per l'esercizio della delega al 31 marzo 2001 e prevede che entro i successivi dodici mesi il Governo, previo parere delle competenti commissioni parlamentari, adotti un testo unificato in materia di protezione dei dati personali coordinandovi le norme vigenti ed apportando ad esse le integrazioni e modificazioni necessarie per assicurarne la migliore attuazione.

L'approvazione definitiva del provvedimento permetterebbe di completare i complessi interventi normativi previsti dall'originaria legge-delega e di dare in tutti i settori pubblici e privati ivi previsti piena effettività ai principi di tutela della riservatezza (si pensi, in particolare, al *direct marketing*, alla sicurezza sociale e del lavoro, alla circolazione delle informazioni nell'ambito delle reti telematiche, nonché ai trattamenti svolti per fini di giustizia o di polizia che sono, allo stato, soggetti solo ad alcune delle disposizioni della legge n. 675/1996).

Fra gli ulteriori disegni di legge d'interesse si segnalano, inoltre:

- a) il provvedimento che apporterebbe modifiche al sistema delle notificazioni di atti giudiziari e nell'ambito di procedimenti amministrativi, già approvato in un testo unificato dal Senato (A/C 6735);
- b) i disegni di legge che ridisciplinano la trasmissione dei dati contenuti nelle c.d. "schede d'albergo" (testo unificato dell'A/C 5003 e proposte abbinate), nonché la materia delle intercettazioni telefoniche (A/S 3964, già approvato dalla Camera);
- c) il testo unificato in materia di telelavoro (AA/SS 2305, 3123, 3189 e 3489) e il provvedimento in materia di neutralità e trasparenza dell'informazione statistica già approvato dalla Camera (A/S 3774);
- d) i provvedimenti riguardanti l'attività regolamentare delle autorità indipendenti (AA/CC 1665, 4868 e 5151), la normativa processuale ad esse applicabile (A/C 5956 del Governo e proposte abbinate in materia di riforma del processo amministrativo) nonché le incompatibilità dei loro componenti (A/S 3236 del Governo, sul conflitto d'interessi);
- e) le proposte in materia di cancellazione dagli elenchi dei protesti cambiari (AA/SS 4151, già approvato dalla Camera, 233, 647 e 2189).

2. Stato di attuazione della legge 675/1996 e nodi da affrontare

2.1 Pubblica amministrazione

Nel primo periodo della propria attività, il Garante per la protezione dei dati personali si è impegnato particolarmente nel promuovere la conoscenza della legge anche tra le pubbliche amministrazioni, attraverso numerose pronunce e pareri nei vari settori di loro competenza (decisioni che, come noto, vengono tra l'altro pubblicate nel Bollettino dell'Autorità "*Cittadini e Società dell'informazione*", inviato gratuitamente anche ad uffici centrali e periferici della p.a.), nonché mediante la diffusione di comunicati stampa e l'attività di propri funzionari presenti in numerosi convegni, seminari e incontri di lavoro presso regioni, comuni, università ed altri organismi pubblici.

2.1.1
Profili
generali

Anche nel corso del 1999, il Garante ha continuato, però, a riscontrare un perdurante ritardo da parte delle pubbliche amministrazioni nell'adempiere ad alcuni fondamentali obblighi previsti dalla legge, ritardo che non è giustificabile anche in ragione del fatto che sono decorsi ormai tre anni dall'entrata in vigore della legge n. 675/1996.

Sono, infatti, ancora numerosi i settori della pubblica amministrazione che risultano inadempienti nei riguardi delle disposizioni concernenti, ad esempio, la notificazione, l'informativa agli interessati, le misure di sicurezza e la designazione di responsabili e incaricati del trattamento.

La complessiva situazione di alquanto diffuso inadempimento da parte di taluni soggetti pubblici, relativamente ad alcuni obblighi previsti dalla legge sulla privacy, è confermata da varie segnalazioni inviate da cittadini che lamentano l'illiceità o la non integrale correttezza del trattamento di dati ed evidenziano comportamenti difforni dai principi stabiliti in materia.

Il Garante ha perciò sviluppato una larga parte della propria attività in segnalazioni a singole amministrazioni o nella risposta a richieste di chiarimenti di interesse generale (si pensi, ad esempio, alle varie questioni attinenti ai trattamenti di dati presso enti locali o, tra l'altro, ai trattamenti di dati sanitari o comunque riguardanti mutilati e invalidi civili) sensibilizzando anche organismi rappresentativi di enti e funzionari.

Inoltre il Garante, come annunciato durante la presentazione della relazione annuale per il 1998, ha individuato, nel quadro del programma ispettivo per la prima parte del 2000, apposite iniziative ispettive e di controllo nei riguardi di amministrazioni pubbliche centrali e locali. L'Autorità ha inoltre proseguito l'esame di segnalazioni, reclami e ricorsi nei confronti di alcuni enti pubblici attivando, anche in diverse occasioni, apposite richieste di informazioni ai sensi dell'art. 32, comma 1, circa le misure e le modalità osservate per la corretta applicazione della legge.

Nel corso del 1999, sono pervenuti ancora ulteriori e numerosi quesiti provenienti da uffici della pubblica amministrazione circa le procedure da adottare per una puntuale attuazione degli obblighi di legge.

2.1.2
Tempi e risposte
degli
adempimenti

Va constatata, poi, l'esistenza di dubbi circa il pieno rispetto da parte di tutte le amministrazioni dell'obbligo di notificazione previsto dagli artt. 7 e 28 della legge n. 675/1996, che per alcuni trattamenti riguardanti anche dati sensibili o di carattere giudiziario poteva essere eseguito in forma semplificata (art. 7, comma 5-bis e 5-ter, legge cit.). In proposito, il Garante ha evidenziato l'importanza di tale obbligo volto a rendere trasparente il trattamento dei dati e ad agevolare gli

interessati nella verifica dell'esistenza e delle finalità dei trattamenti di dati che li riguardano, importanza che traspare anche dal fatto che, com'è noto, la legge 675 ha previsto per l'omessa o infedele notificazione una sanzione penale (art. 34).

Risulta inoltre indispensabile che tutte le pubbliche amministrazioni conformino pienamente i propri trattamenti ai principi di cui all'art. 9 della legge in ordine alle modalità della raccolta e ai requisiti dei dati personali. Tale disposizione, che si applica anche ai particolari trattamenti effettuati da soggetti pubblici, ai quali la legge n. 675/1996 si applica attualmente solo in parte (art. 4, commi 1 e 2, legge n. 675/1996), impone, fra l'altro, di raccogliere e trattare le sole informazioni personali la cui conoscenza sia, caso per caso, realmente giustificata dagli scopi perseguiti, selezionando i dati effettivamente pertinenti ed escludendo, contestualmente, i dati, le informazioni e le notizie il cui impiego ecceda quanto necessario per perseguire gli scopi medesimi (in senso analogo, v. il provvedimento del Garante del 13 aprile 1999 riguardante il trattamento di dati da parte della polizia giudiziaria, in Bollettino n. 10, pag. 72).

Un'altra questione nuovamente emersa è relativa agli obblighi di informativa. A tale riguardo, l'Autorità ha ribadito che l'art. 10 della legge, il quale disciplina anzitutto l'obbligo di informare l'interessato anche oralmente al momento della raccolta dei dati, non prevede casi di esclusione, ma solo un'eventuale informativa ridotta (cfr. art. 10, comma 2). Il Garante ha richiamato quindi le pubbliche amministrazioni al pieno rispetto di tale adempimento. L'obbligo di informativa (al quale può ottemperarsi in maniera più agevole anche attraverso opportune misure organizzative che portino a ridurre il numero dei singoli adempimenti, sempreché l'informativa sia sostanziale: si pensi, ad esempio, ad idonee forme di affissioni o di avvisi agli sportelli) deve trovare una corretta e puntuale applicazione in modo da rendere il cittadino pienamente consapevole di come sono trattati i propri dati personali. L'importanza di tale strumento di trasparenza è anzi tale da aver indotto il Governo a prevedere che i soggetti pubblici, quando trattano dati sensibili o di carattere giudiziario, debbano indicare nell'informativa anche la normativa che prevede gli obblighi o i compiti in base ai quali è effettuato il trattamento (art. 2, comma 2, d.lg. n. 135/1999).

Da generali riscontri (tra cui anche le informali segnalazioni pervenute al servizio di assistenza telefonica predisposto dall'Ufficio) appare invece, ancora oggi, piuttosto diffusa la mancanza di informative o la presenza di informative complesse e di difficile comprensione, errate o lacunose, come pure di casi nei quali l'amministrazione tende a reiterare superflualmente l'informativa in occasione di ogni operazione o contatto con l'interessato anziché a predisporre una idonea informativa *una tantum* che riguardi il complesso dei rapporti e delle operazioni con l'interessato stesso.

Al riguardo, va osservato che l'eventuale accertamento della violazione dell'obbligo di informativa, oltre a far emergere l'illiceità del trattamento, può comportare l'applicazione da parte dell'Autorità della sanzione amministrativa pecuniaria prevista dall'art. 39 della citata legge.

Importante è sottolineare, poi, le difficoltà incontrate da parte di diverse pubbliche amministrazioni nell'interpretare le disposizioni sul diritto di accesso ai dati personali (art. 13 della legge n. 675/1996) e sul distinto diritto di accesso ai documenti amministrativi (previsto invece dagli artt. 22 ss. della legge n. 241/1990 sul procedimento amministrativo). Si tratta infatti, come ricordato più volte dall'Autorità, di due diversi ed autonomi diritti di accesso che presentano finalità e modalità diverse.

Nel caso dell'esercizio del diritto di accesso ai dati previsto dall'art. 13 della legge n. 675/1996, il titolare o il responsabile del trattamento sono infatti tenuti ad estrapolare dai propri archivi e documenti tutti i dati di carattere personale che riguardano il richiedente, riportati anche su supporto informatico, e a comunicarli a quest'ultimo in forma idonea a renderli facilmente comprensibili.

In più occasioni il Garante ha quindi richiamato l'attenzione delle amministrazioni sulla

necessità di non procrastinare l'attivazione di idonei meccanismi e procedure volti a dare piena attuazione alle disposizioni in tema di accesso ai dati, secondo quanto previsto dall'art. 17 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501. Come si ricorderà, infatti, il comma 9 di tale articolo prevede che i titolari del trattamento debbano agevolare l'accesso ai dati anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad una accurata selezione dei dati che riguardano i singoli soggetti, a semplificare le modalità e a ridurre i tempi per dare riscontro agli interessati anche nell'ambito degli uffici per le relazioni con il pubblico.

Altro grave problema, riscontrato dall'Autorità in ambito pubblico, concerne la non esatta o incompleta individuazione delle figure degli incaricati del trattamento dei dati personali.

L'individuazione di tale figura corrisponde ai dipendenti o ai collaboratori esterni che in ragione del proprio ufficio, servizio o attività, sono legittimati ad accedere a determinati atti e documenti e a trattare dati seguendo le istruzioni del titolare o del responsabile del trattamento e operando sotto la loro autorità (art. 8, comma 5 e 19 della legge n. 675/1996).

Tale individuazione permette quindi di considerare, in generale, legittimo il flusso delle informazioni personali contenute in atti o documenti nell'ambito degli uffici e tra i dipendenti dell'amministrazione titolare del trattamento. In altre parole, senza una formale designazione degli incaricati del trattamento, i soggetti che hanno accesso e trattano dati personali vanno considerati come soggetti estranei all'amministrazione, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e, quindi, per la liceità del trattamento.

Strettamente connessa a tale tema è la problematica dell'individuazione dei responsabili del trattamento acuita dal fatto che i soggetti pubblici si avvalgono per l'adempimento delle proprie finalità istituzionali, anche di organismi privati che devono accedere, quindi, a dati detenuti dalla p.a.

L'amministrazione pubblica deve quindi scegliere se considerare tali soggetti come soggetti esterni che la coadiuvano in un'attività che ricade nell'ambito di titolarità e responsabilità dell'amministrazione stessa o, invece, quali figure del tutto distinte dall'amministrazione che decide, in questo caso, autonomamente in ordine al trattamento delle informazioni e si assume, in concreto, ogni responsabilità in proposito.

Nel primo caso tali figure, designate quali responsabili del trattamento, assumono un ruolo quale parte sostanziale della struttura della pubblica amministrazione e possono quindi trattare i dati detenuti dal soggetto pubblico senza che vi sia necessità di una manifestazione del consenso dell'interessato (indispensabile, invece, se si verificasse la seconda ipotesi e cioè se assumessero la qualità di soggetti "terzi" rispetto all'amministrazione). Tutto ciò è stato ancora una volta ribadito in una pronuncia del Garante, rivolta al Ministero delle finanze, in cui si è chiarito che l'amministrazione finanziaria deve precisare il ruolo assunto dai concessionari della riscossione per poter consentire a questi ultimi l'accesso ai dati detenuti dall'amministrazione (parere del 16 giugno 1999 rilasciato al Ministero delle finanze, in Bollettino n. 9, pag. 19).

Sotto altro profilo, numerose pronunce dell'Autorità hanno ancora una volta ribadito a singole amministrazioni pubbliche che, di norma, esse devono operare senza acquisire il consenso degli interessati al trattamento dei dati personali.

Secondo la legge n. 675, infatti, i soggetti pubblici non operano, di regola, sulla base del consenso dell'interessato, mentre possono effettuare solo i trattamenti connessi all'esercizio delle proprie funzioni istituzionali rispondenti, in caso di comunicazione e diffusione dei dati, a puntuali previsioni di legge o di regolamento (art. 27).

Per quanto riguarda la comunicazione e la diffusione, l'Autorità, dopo aver ricordato nuovamente che la legge n. 675/1996 regola diversamente la comunicazione e diffusione tra soggetti

pubblici (ammesse se previste da norme di legge o di regolamento o qualora risultino comunque necessarie per lo svolgimento di finalità istituzionali) dalla divulgazione di dati da amministrazioni pubbliche nei confronti di soggetti privati, ha analizzato vari casi valutando la loro conformità non solo ai parametri dell'art. 27 della legge n. 675/1996, ma anche al quadro generale delineato dalla normativa relativa ai singoli settori interessati. Ad esempio, il Garante ha constatato che una provincia poteva acquisire dati dai comuni e da altre amministrazioni pubbliche nel rispetto della specifica disciplina applicabile alle singole amministrazioni (parere reso alla provincia di Modena il 14 gennaio 1999, pubblicato in Bollettino n. 7, pag. 53).

Il Garante ha inoltre ribadito più volte la predetta necessità che, qualora la comunicazione e la diffusione dei dati avvengano da parte di soggetti pubblici a soggetti privati o enti pubblici economici, tali operazioni siano previste da norme di legge o di regolamento. La comunicazione e la diffusione dei dati personali può infatti avvenire quando ciò sia previsto da una disposizione normativa di rango primario o secondario; al contrario, la previsione contenuta nel regolamento interno di un ente pubblico economico non può considerarsi fonte idonea a legittimare una comunicazione e diffusione dei dati (cfr. parere rilasciato all'A.C.I. il 16 giugno, 1999, pubblicato in Bollettino n. 9, pag. 61).

Fondamentali sono, infine, le novità apportate dal decreto legislativo n. 135/1999 (di cui si tratterà ampiamente più avanti) concernente il trattamento dei dati sensibili da parte dei soggetti pubblici, che definisce i principi generali in base ai quali questi ultimi sono autorizzati a trattare tali dati e quelli attinenti a particolari provvedimenti giudiziari e individua alcune finalità di rilevante interesse pubblico per il cui perseguimento è consentito tale trattamento.

Da ultimo, per quanto concerne l'adozione delle misure minime di sicurezza da parte delle pubbliche amministrazioni, previste all'art. 15 della legge 675/1996 e individuate nel d.P.R. 318/1999 (*"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15, comma 2 della legge 31 dicembre 1996, n. 675"*) si rinvia al capitolo n. 2.14.

2.1.3
Trasparenza
dell'attività
amministrativa

Il processo di profondo rinnovamento che, come è noto, ha interessato le pubbliche amministrazioni nell'ultimo decennio grazie all'entrata in vigore di provvedimenti normativi innovativi rispetto a quelli precedenti, ha come linee-guida i principi di pubblicità, efficienza ed economicità dell'azione pubblica.

L'intenzione di fare dell'amministrazione una "casa di vetro" si è tradotta, infatti, negli istituti di partecipazione al procedimento, introdotti in via generale dalla legge 7 agosto 1990, n. 241 (la comunicazione di avvio del procedimento, il diritto di intervento, la predeterminazione dei criteri per ausili economici, ecc.) e, ancora, negli ulteriori strumenti apprestati al fine di garantire il massimo della trasparenza nell'agire pubblico (l'obbligo di provvedere, la motivazione obbligatoria, la previa individuazione del termine conclusivo e del responsabile del procedimento, gli accordi sostitutivi e procedurali) fra i quali, in particolare, il diritto di accesso ai documenti amministrativi ai sensi dell'art. 22 della citata legge.

Nella non facile transizione da un'amministrazione "chiusa" ad una "trasparente" rispetto ai cittadini ed alle istanze da essi rappresentate, un ruolo fondamentale è svolto dalla progressiva informatizzazione dei sistemi pubblici che, quotidianamente, sono in grado di trattare e scambiare fra loro migliaia di dati personali.

Così il valore della trasparenza sembrerebbe poter confliggere con il diritto degli interessati di tutelare la riservatezza e di esercitare un controllo sulle informazioni trattate, in particolare, dai

soggetti pubblici. Al contrario, la stessa legge n. 241/1990 individua nella riservatezza di terzi un limite al diritto di accesso (art. 24, comma 2, lettera d), mentre, dall'altro lato, la legge sulla privacy ammette la comunicazione e la diffusione dei dati personali da parte dei soggetti pubblici a privati o ad enti pubblici economici solo se previste da norme di legge o di regolamento (art. 27, comma 3, legge n. 675/1996).

Contrariamente all'opinione secondo la quale questo regime particolarmente severo avrebbe ripristinato la prevalenza della segretezza sulla trasparenza dell'agire pubblico, fornendo alle amministrazioni un comodo pretesto per negare ai cittadini la conoscenza di documenti che li riguardano, il Garante ha proseguito sulla strada intrapresa in materia sin dalla sua istituzione, della quale si è fornito ampio riscontro nelle due precedenti relazioni per il 1997 e per il 1998.

Infatti, il richiamo ad una precisa disposizione normativa operato dall'articolo 27, comma 3, della legge n. 675 è riferito a tutte le disposizioni vigenti che la legge sulla privacy non ha abrogato e che presuppone, anzi, come limiti legali al trattamento dei dati effettuato dalle amministrazioni pubbliche.

In un parere reso il 16 giugno 1999 (in Bollettino n. 9, pag. 61), in relazione alla possibilità per l'ACI di rendere pubblico l'elenco dei soggetti e dei centri autorizzati alla demolizione di veicoli e rimorchi, il Garante ha ricordato che *"la legge n. 675/1996 non ha introdotto alcun divieto di dare conoscibilità a questi dati, ma in un quadro di maggiore trasparenza stabilisce che le amministrazioni e gli enti pubblici possono diffondere i dati personali quando ciò sia previsto"* da un'apposita disposizione di rango normativo primario o secondario. Di conseguenza, come già accennato, la previsione contenuta in un regolamento meramente interno dell'ente non poteva considerarsi fonte idonea a consentire la diffusione dei dati personali.

Ad analoghe conclusioni è possibile arrivare anche in applicazione del generale principio di legalità, da cui l'attività amministrativa è retta, poiché essa deve svolgersi, in ogni caso, nel rispetto dei limiti previsti dalle leggi.

A questo proposito, in difetto di una specifica disciplina di settore, mentre il trattamento di dati personali "interno" alle singole amministrazioni può comunque avvenire qualora sia necessario per lo svolgimento delle funzioni istituzionali dell'amministrazione (articolo 27, comma 1, legge n. 675/1996), la mancanza di tale disciplina porta a ritenere vietata la comunicazione dei dati stessi a privati (art. 27, comma 3), come precisato in occasione del chiarimento in merito al regime di pubblicità dell'albo professionale degli iscritti all'Ordine degli assistenti sociali, fornito con provvedimento del 29 marzo 1999 (in Bollettino n. 8, pag. 50). Con ciò, tuttavia, il Garante non ha inteso escludere una volta per tutte la possibilità per il soggetto pubblico di divulgare a privati o ad enti pubblici economici i dati personali oggetto di trattamento, ma, al contrario, ha suggerito di integrare la normativa specifica con idonee previsioni, nel senso di rendere maggiormente trasparente l'attività svolta.

Affrontando nuovamente la questione, già trattata nel periodo precedente di attività (cfr. Relazione per l'anno 1998, pag. 14), relativamente al regime di pubblicità delle deliberazioni comunali, il Garante ha preso in considerazione il rapporto della precedente normativa con il d.lg. 11 maggio 1999, n. 135. In particolare, riferendosi all'ipotesi in cui i dati contenuti nelle deliberazioni dell'ente locale abbiano natura sensibile, ai sensi dell'articolo 22 della legge sulla privacy, nel parere del 2 settembre 1999 (in Bollettino n. 9, pag. 9) si è fatto presente che il trattamento di tali informazioni risulta ora espressamente autorizzato dal citato decreto, il quale, tra l'altro, ha riconosciuto la rilevanza a livello di interesse pubblico dei trattamenti di dati personali:

- diretti all'applicazione della disciplina in materia di documentazione dell'attività istituzionale di organi pubblici (art. 8 d.lg. cit.), facendo salvo, anche in questo caso, il divieto di diffusione dei dati idonei a rivelare lo stato di salute previsto in termini generali dall'art. 23, comma 4, della legge n. 675/1996;

- effettuati in conformità alle leggi e ai regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi (art. 16, comma 1, lett. c) d.lg. cit.).

All'amministrazione, pertanto, non rimane che identificare i tipi di dati e le operazioni strettamente necessarie e pertinenti in relazione alle specifiche attività svolte, secondo la disposizione dell'art. 22, comma 3-bis, della legge n. 675/1996, poiché *"non vi è alcuna incompatibilità di fondo tra le disposizioni in materia di dati personali e le disposizioni anche previgenti alla legge n. 675/1996 in tema di trasparenza dell'attività della pubblica amministrazione, di accesso ai documenti amministrativi e di pubblicità di taluni atti"*.

Ulteriore applicazione della normativa sui dati sensibili è stata fatta nel parere reso in data 9 giugno 1999 (in Bollettino n. 9, pag. 71) in merito al rilascio dell'elenco dei sottoscrittori di una lista elettorale, rilascio di cui è stata riconosciuta la liceità, dovendosi ritenere ricompreso nelle attività in materia di elettorato e di altri diritti politici indicate nell'articolo 8, comma 4, del d.lg. n. 135/1999. Tale norma, infatti, consente la diffusione dei dati per le finalità individuate *"con riguardo alle sottoscrizioni di liste, alle presentazioni delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti"*. In ogni caso, però, il Garante ha sottolineato che i trattamenti in questione devono essere effettuati nel rispetto dei principi fissati dalla legge n. 675/1996 e dal citato decreto legislativo e, in particolare, di quelli di pertinenza e di essenzialità dei dati trattati e del rispetto della finalità perseguita (art. 9, legge n. 675 e artt. 1-4 del d.lg. n. 135). In tal senso è apparso legittimo il rilascio dell'elenco esclusivamente a soggetti che intendano servirsi per l'esercizio dei diritti politici, come nel caso in cui la richiesta pervenga da candidati di liste concorrenti.

Nel corso dell'anno è stato risolto anche il problema della comunicazione e della diffusione da parte delle scuole e degli istituti scolastici, anche a privati e per via telematica, dei dati relativi agli esiti scolastici degli studenti, nonché di altri dati personali diversi da quelli sensibili. L'articolo 17 del d.lg. n. 281/1999, intervenuto a modificare, fra le altre, le disposizioni del testo unico approvato con d.lg. n. 297/1994, ha reso legittima, facendola oggetto di espressa previsione normativa ai sensi dell'art. 27, comma 3, della legge sulla privacy, la divulgazione di dati personali degli studenti a soggetti diversi da quelli pubblici, al fine di agevolarne l'orientamento, la formazione e l'inserimento professionale, come sottolineato dal Garante in un parere del 27 ottobre 1999. La comunicazione e la diffusione non riguardano, comunque, dati sensibili o di carattere giudiziario e sono subordinate alla richiesta dell'interessato. Rispetto ai dati personali raccolti prima dell'entrata in vigore del d.lg. n. 281/1999, il comma 2 del nuovo articolo 330-bis del d.lg. n. 297/1994 riconosce poi, espressamente, il diritto degli interessati di opporsi alla loro divulgazione.

2.1.4
Diritto di accesso
a documenti
amministrativi

Con riferimento al rapporto tra la legge n. 241 del 1990 e la legge n. 675 del 1996 ed in particolare al problema se le due normative interferiscano tra loro, nel 1999 è rimasto confermato il principio secondo cui la legge n. 675 non ha modificato presupposti e ambito di applicazione della citata legge n. 241.

L'Autorità ha, in particolare, ribadito che non v'è alcuna incompatibilità di fondo tra le due normative e che spetta all'amministrazione destinataria della richiesta di accesso il compito di valutare la sussistenza dell'interesse giuridicamente rilevante e degli altri presupposti per accedere ai documenti amministrativi.

L'accesso ai documenti è pur sempre riconosciuto a chiunque abbia un interesse personale e concreto in relazione alla tutela di situazioni giuridicamente rilevanti (art. 22 legge n. 241/1990; art. 2 d.P.R. n. 352/1992) anche dopo l'entrata in vigore della legge n. 675, come testualmente stabilito dall'articolo 43 della stessa legge.

Deve anzi ricordarsi, sotto altro profilo, che, a norma dell'articolo 13 della legge n. 675, l'accesso, in questo caso ai propri dati personali, è uno dei mezzi di tutela della riservatezza, atteso che l'interessato ha diritto di accesso ai dati che lo riguardano per verificarne la correttezza ed il trattamento effettuato.

Sempre relativamente al rapporto tra diritto di accesso e tutela della riservatezza ed all'insussistenza di un rapporto di contraddizione tra i due istituti, non va dimenticato che già la legge n. 241 del 1990, all'articolo 24, comma 2, lettera d), prevede una limitazione al diritto di accesso in relazione alla riservatezza di terzi. E tale limitazione, ovviamente non contrastata dalla legge n. 675 del 1990, trova ora, nella stessa legge, parametri più precisi ai quali ancorarsi.

Con un parere del 4 novembre 1999 sulla richiesta del Ministero delle finanze, volta a conoscere se contrasti con la normativa sulla protezione dei dati personali la richiesta di accesso - avanzata da alcuni concorrenti di un concorso pubblico - alle certificazioni prodotte da altri concorrenti, il Garante ha ribadito quanto già chiarito in precedenti pareri e cioè che le pubbliche amministrazioni, a fronte di domande di accesso agli atti, non devono chiedere il consenso degli interessati alle operazioni di comunicazione dei dati personali, ma devono semplicemente valutare se vi è nel caso concreto l'esigenza di tutelare la specifica posizione di riservatezza di terzi, tenendo presente che la comunicazione che si realizza attraverso l'accesso ai documenti amministrativi è da ritenersi "autorizzata" per legge (in conformità al generale principio di cui all'art. 27, comma 3, della legge n. 675), stante il disposto della legge n. 241/1990.

Nella richiamata occasione, il Garante ha, quindi, nuovamente riconosciuto la possibilità per l'amministrazione di esibire o di consegnare copia di documenti amministrativi a seguito dell'esercizio del diritto di accesso ai sensi dell'art. 22 della legge n. 241/1990 e degli artt. 1 e 2 del d.P.R. n. 352/1992.

Il principio della compatibilità tra l'accesso ai documenti amministrativi e la legge sulla tutela dei dati personali è stato poi ribadito a seguito dell'emanazione del d.lg. n. 135 del 1999 che, all'art. 16, comma 1, lettera c), superando alcuni dubbi emersi tra vari commentatori, consente esplicitamente di applicare la normativa sull'accesso ai documenti amministrativi anche quando questi contengano dati sensibili o riguardanti determinati provvedimenti di carattere giudiziario. Tale principio è stato di seguito ribadito in risposta a diversi quesiti, ad esempio, con il parere del 29 novembre 1999 in riferimento ad una richiesta formulata dal Ministero delle finanze-Dipartimento delle dogane e delle imposte indirette, circa il rapporto tra le due leggi.

L'ordinamento, poi, riconosce uno speciale e più ampio diritto di accesso ai consiglieri comunali e provinciali nei confronti degli atti detenuti dalle rispettive amministrazioni per l'espletamento del proprio mandato (articolo 31, comma 5, della legge n. 142 del 1990).

Con riferimento a tale disposizione, l'Autorità garante ha, però, avuto modo di chiarire che anche questo diritto di accesso può trovare alcuni limiti nella riservatezza di alcuni dati personali contenuti negli atti cui l'accesso stesso è rivolto (ad esempio, in riferimento alla possibile presenza nel cedolino dello stipendio di un dirigente di determinati dati personali ed informazioni di natura sensibile).

Nel parere dell'8 giugno 1999 (Bollettino n. 9 del 1999, pag. 7), reso in risposta ad un quesito del Comune di Viterbo, è stato ribadito che l'accesso ai documenti dell'amministrazione da parte dei consiglieri comunali e provinciali è più ampio di quello previsto dalla legge n. 241, posto che, se detto accesso attiene all'esercizio delle funzioni istituzionali del consigliere medesimo e ne costituisce modalità di espletamento, non è richiesta la sussistenza di un interesse giuridicamente rilevante per l'accesso medesimo.

È stato altresì chiarito, nella medesima circostanza, che il diritto del consigliere comunale di verificare, nell'esercizio delle funzioni consiliari, con piena cognizione di causa, ivi compreso l'accesso ai documenti, la correttezza e l'efficacia dell'operato dell'amministrazione, può essere soddisfatto anche attraverso il regime di pubblicità della situazione patrimoniale dei dirigenti (l. n. 441/1992 e l. n. 127/1997), l'esame dei contratti collettivi, l'accesso alle deliberazioni adottate dalla stessa amministrazione in materia di indennità ed emolumenti ai dipendenti.

2.1.5
Dati sensibili
e di carattere
giudiziario

Il 1999 ha rappresentato un anno particolarmente significativo per la definizione di una disciplina tendenzialmente organica in materia di trattamento dei dati personali più "delicati" da parte dei soggetti pubblici. Dopo i diversi rinvii che avevano comportato la proroga del regime transitorio previsto dalla legge 675/1996, è stato infatti finalmente approvato il decreto legislativo 11 maggio 1999, n. 135, contenente una serie di disposizioni integrative e modificative della legge n. 675/1996 sul trattamento dei dati sensibili da parte dei soggetti pubblici.

Durante la complessa fase di elaborazione di tale provvedimento, si è realizzata, più di quanto non fosse accaduto in passato, un'effettiva e concreta consultazione del Garante che ha in tal modo potuto formulare diverse osservazioni tendenti a rendere il testo maggiormente conforme ai principi dettati in materia di riservatezza (Comunicato n. 43 del 3 maggio 1999, in Bollettino n. 8, pag. 88).

Il decreto, pur non potendo esaurire la regolamentazione della materia, ha avuto il merito di fissare alcuni principi generali sull'uso di tali informazioni da parte degli enti pubblici, nonché quella di fornire una prima elencazione dei settori all'interno dei quali la pubblica amministrazione può fare uso dei dati sensibili, fissandone al contempo le modalità ed i limiti.

Giova ricordare che i soggetti pubblici, a differenza dei privati, generalmente non sono tenuti a richiedere il consenso degli interessati e fondano invece la loro legittimazione a trattare i dati personali unicamente su disposizioni normative. A causa di ciò, il cittadino non ha il potere di intervenire con una propria manifestazione di volontà per acconsentire o negare l'autorizzazione all'utilizzo dei propri dati da parte della pubblica amministrazione. Da qui l'importanza delle disposizioni che regolano la materia, le quali devono contenere già in sé quel bilanciamento di valori perseguiti e interessi tutelati che, nei rapporti fra privati, scaturisce dal confronto intersoggettivo alla base della manifestazione del consenso. Da qui, anche, l'attenzione che è necessario porre alle specifiche e concrete determinazioni assunte in materia dalle singole amministrazioni, le quali, come si vedrà fra breve, sono spesso chiamate a disciplinare nel dettaglio tali ipotesi.

Si deve tuttavia evidenziare che anche il d.lg. n. 135/1999 è espressione di un'impostazione - propria di gran parte delle disposizioni della legge 675 - basata su una netta separazione di disciplina fra pubblico e privato. In molti casi, essa appare giustificata, oltre che dalla diversità del soggetto agente, da un'innegabile differenza di fini perseguiti e di mezzi utilizzati. Altre volte, però, tale netta separazione potrebbe, in certi casi, essere suscettibile di determinare alcune disparità a causa del sempre più frequente utilizzo di strumenti ed istituti privatistici da parte dei soggetti pubblici, nonché dell'accrescersi della pratica di affidare ai privati la realizzazione di attività svolte fino a ieri da enti pubblici. Per questo, appaiono meritevoli di approfondimento e suscettibili di eventuali sviluppi le tecniche regolative adottate per taluni ambiti di attività, nei quali il trattamento dei dati sensibili viene disciplinato senza assegnare unica rilevanza alla natura pubblica o privata del titolare (il riferimento è, in particolare, ai trattamenti svolti in ambito sanitario e di ricerca scientifica per i quali si rinvia alle apposite sezioni di questa relazione).

Al fine di cogliere le novità introdotte dalla nuova disciplina, ed insieme capirne il significato complessivo, è necessario ricordare che la legge n. 675, sulla scorta di quanto disposto in sede

comunitaria, aveva previsto specifiche garanzie per l'utilizzo da parte delle pubbliche amministrazioni dei dati sensibili, nonché di alcune delle informazioni relative a determinati provvedimenti di carattere giudiziario (artt. 22 e 24, l. n. 675/1996).

Si era infatti stabilito che i soggetti pubblici potessero trattare queste informazioni esclusivamente dietro un'espressa "autorizzazione" di legge, nella quale fossero specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite (art. 22, comma 3). Poiché, nel nostro ordinamento, le leggi in grado di rispondere a tali caratteristiche erano e sono un numero molto esiguo, lo stesso legislatore del '96 aveva previsto un regime transitorio.

Sulla base di esso, questo tipo di trattamenti sono potuti proseguire anche in assenza delle leggi indicate con l'unico onere, per i soggetti pubblici interessati, di dare una preventiva comunicazione sugli stessi al Garante (art. 41, comma 5). Una disciplina in molti aspetti analoga era stata disposta anche per i predetti dati di carattere giudiziario (art. 686, commi 1, lett. a), d), 2 e 3), prevedendosi però che i trattamenti potessero essere autorizzati, oltre che dalle leggi particolarmente dettagliate cui si è fatto riferimento, anche da un provvedimento del Garante con il medesimo livello di specificazione (art. 24, l. 675).

Fin da subito, è però apparso evidente che tale disciplina, dettata esclusivamente per sopperire ad una carenza normativa presente al momento dell'entrata in vigore della legge n. 675/1996, non poteva offrire garanzie pienamente sufficienti per i cittadini e doveva essere integrata in tempi rapidi da una normativa più rispettosa dei diritti delle persone. Tuttavia, anche a causa delle innegabili difficoltà incontrate nell'affrontare le complesse problematiche ad essa legate, la disciplina transitoria è stata prorogata più volte (art. 1 del d.l.g. n. 135/1998; e art. 1 del d.l.g. 6 novembre 1998, n. 389), fino all'approvazione del decreto legislativo n. 135/1999.

Quest'ultimo - come accennato - da una parte ha voluto fissare alcuni principi generali ai quali devono attenersi i soggetti pubblici che trattano le delicatissime informazioni personali di cui si è detto (capo I) e, dall'altra, ha invece individuato numerose rilevanti finalità di interesse pubblico al fine di autorizzare i trattamenti svolti per il loro perseguimento (capo II). In considerazione della loro particolare posizione nell'ambito dell'ordinamento costituzionale, il legislatore delegato ha invece ritenuto di escludere dall'ambito di applicabilità di tale decreto, oltre ad alcuni trattamenti svolti in ambito pubblico per i quali era già prevista una disciplina differenziata - art. 4, l. 675/1996, art. 1 comma 1, lett. i), l. 676/1996 - anche quelli che divengano oggetto di una nuova disciplina ad opera della Presidenza della Repubblica, del Senato della Repubblica, della Camera dei deputati, nonché della Corte costituzionale.

Molte delle disposizioni di cui al capo I del d.l.g., comuni a tutti i trattamenti, costituiscono poi uno sviluppo ed un rafforzamento di alcuni principi generali già sanciti dalla legge n. 675/1996. Si è così previsto, in generale, che i soggetti pubblici devono trattare i dati in discorso con modalità atte ad assicurare il rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, adottando le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 13 della legge 675/1996.

Al fine di garantire al cittadino una conoscenza adeguata sull'uso che sarà fatto dei propri dati personali, nonché di consentire un più immediato ed efficace controllo sulla legittimità dei trattamenti, è stato altresì stabilito che i soggetti pubblici, nell'informare gli interessati secondo quanto previsto in generale dalla legge (art. 10 l. 675/1996), debbano fare riferimento espresso alla normativa in cui sono previsti gli obblighi o i compiti in base alla quale è effettuato il trattamento.

La particolare delicatezza dei trattamenti disciplinati dal decreto ha inoltre indotto ad un rafforzamento di alcuni principi generali già sanciti dalla legge 675/1996 ed in particolare dal suo art. 9. I soggetti pubblici sono stati infatti autorizzati a trattare esclusivamente i dati essenziali per

svolgere le attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. Gli stessi soggetti sono, inoltre, chiamati a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

Per assicurare che i dati siano strettamente pertinenti e non eccedenti rispetto agli obblighi ed ai compiti loro attribuiti, i soggetti pubblici devono valutare specificamente il rapporto fra le informazioni personali e gli adempimenti. Nel caso in cui da tali verifiche risulti che alcuni dei dati detenuti o comunque utilizzati sono eccedenti, non pertinenti o non necessari, il loro utilizzo è vietato, fatta salva l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Un'attenzione specifica è infine richiesta nella verifica dell'essenzialità delle informazioni riguardanti soggetti diversi da quelli a cui si riferiscono direttamente le prestazioni o gli adempimenti.

L'uso di mezzi elettronici e di quelli comunque automatizzati per creare elenchi, registri o banche dati, consente il trattamento di quantità molto elevate di informazioni personali con il conseguente aumento dei rischi ad esso connessi. Per tale ragione, in tali ipotesi, i soggetti pubblici debbono ricorrere a tecniche di cifratura ed all'utilizzazione di codici identificativi o di altri sistemi che, considerati il numero e la natura dei dati, consentano di identificare gli interessati solamente in caso di necessità.

In considerazione della particolare delicatezza dei dati idonei a rivelare lo stato di salute e la vita sessuale, il loro trattamento è sempre soggetto al rispetto di quest'ultimo obbligo, indipendentemente dall'uso dei mezzi elettronici o automatizzati a cui si è appena fatto riferimento. Tali informazioni personali devono, inoltre, essere sempre conservate separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo. In ogni caso, infine, è fatto divieto di usare i dati sensibili nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato.

Anche con riguardo alle operazioni di trattamento consentite, si è disposto che i soggetti pubblici debbano svolgere unicamente quelle strettamente necessarie al perseguimento delle finalità per le quali il trattamento è permesso. Inoltre, per accrescere il grado di trasparenza sulle operazioni di raffronto, e così anche consentire un più efficace controllo da parte degli interessati, si è previsto che queste debbano essere sempre accompagnate dall'indicazione scritta dei motivi che le giustificano.

Le novità introdotte dal d.lg. n. 135/1999 sono particolarmente rilevanti soprattutto per le modifiche apportate all'art. 22 della legge n. 675/1996, attraverso le quali si è in gran parte ridisegnato il sistema attraverso cui devono essere regolati i trattamenti di dati sensibili da parte dei soggetti pubblici.

Come si è accennato, la legge generale sulla protezione dei dati personali consentiva tali trattamenti solo se autorizzati da una legge particolarmente dettagliata che indicasse, oltre alle finalità di interesse pubblico perseguite ed alle operazioni eseguibili, anche i dati trattati. In seguito alla modifica, tesa anche ad uniformare la disciplina sui dati sensibili a quella dettata per le informazioni di tipo giudiziario, per rendere possibile il trattamento sarà sufficiente che la legge si limiti ad individuare il genere di dati trattati.

Tuttavia, le modifiche sicuramente più rilevanti attengono al fatto che la legge, pur continuando a costituire la base necessaria per ogni trattamento delle delicate informazioni in questione, non rappresenta più l'unica fonte chiamata a disciplinare, fin nei particolari, i trattamenti medesimi. Si è infatti stabilito che tali trattamenti possano avvenire attraverso due nuovi percorsi procedurali.

Il primo richiede una pronuncia del Garante, chiamato ad intervenire in attesa di una successiva specificazione legislativa. Esso riguarda sia i casi in cui manca un'espressa disposizione di legge del tipo prima indicato, sia quelli non previsti dai decreti legislativi di modificazione ed integrazione della legge 675/1996, emanati in attuazione della legge delega n. 676/1996. In queste ipotesi, i soggetti pubblici possono richiedere all'Autorità l'individuazione delle attività -tra quelle demandate ai medesimi soggetti dalla legge- che perseguono rilevanti finalità di interesse pubblico e per le quali è conseguentemente autorizzato il trattamento.

Anche in questo caso, dunque, il legislatore delegato ha voluto uniformare la disciplina sui dati sensibili a quella in vigore per le informazioni di tipo giudiziario rifacendosi anche all'impostazione della direttiva n. 95/46/CE. Si è in tal modo creata una procedura particolarmente flessibile, tesa soprattutto ad evitare ogni rischio di paralisi nell'attività delle amministrazioni pubbliche fino all'adozione dei provvedimenti normativi diretti a dare regolamentazione definitiva ai trattamenti in discorso.

Il d.lg. n. 135/1999 aveva infine previsto che, per le richieste presentate entro la fine del 1999, l'Autorità avesse novanta giorni di tempo per pronunciarsi, stabilendosi altresì che durante tale termine e fino alla sua decisione fosse possibile proseguire i trattamenti in corso.

Tutto ciò ha dunque rappresentato anche un riconoscimento per il ruolo del Garante che in tale quadro ha contribuito, da un lato, a garantire il perdurante rispetto dei diritti della persona legati alla protezione dei dati e, dall'altro, ad individuare le vie attraverso le quali sia comunque possibile perseguire con efficacia e celerità le finalità dei soggetti pubblici di volta in volta interessati.

La seconda nuova via, attraverso cui i soggetti pubblici possono trarre legittimazione per effettuare trattamenti di dati sensibili, trova applicazione nei casi in cui siano state determinate -secondo il disposto del già citato comma 3 dell'art. 22 della legge 675/1996- le finalità di rilevante interesse pubblico, ma non siano stati specificati i tipi di dati e le operazioni eseguibili.

In tali ipotesi, i soggetti pubblici sono chiamati ad identificare e rendere pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando periodicamente tale identificazione.

Il Garante è intervenuto più volte per chiarire che tale "identificazione" deve essere effettuata attraverso atti di rango regolamentare da parte dei soggetti dotati della relativa potestà. Tali atti dovranno intervenire su profili che prima dell'entrata in vigore del decreto erano disciplinati per legge. Si tratta, poi, di atti che assumono una funzione concretamente normativa in una materia delicata, data la natura delle situazioni soggettive coinvolte, e che svolgono una funzione non meramente ricognitiva di operazioni di trattamento e di tipi di dati (Comunicato del 15 dicembre 1999, in Bollettino n. 10, pag. 112).

Al fine di evitare che le modifiche apportate da tale decreto si risolvano -anche contro lo spirito con cui il Governo stesso ha proceduto alla sua approvazione- in un'attenuazione delle garanzie inizialmente previste dalla legge n. 675/1996, il Garante si è impegnato a vigilare affinché le regole in via di introduzione da parte delle pubbliche amministrazioni assicurino anche il rigoroso rispetto dei principi sopra richiamati. Ciò in considerazione del fatto che -come si è detto- tale regolamentazione deve farsi carico di contemperare in maniera adeguata gli interessi delle singole amministrazioni con i diritti fondamentali dei singoli e di organismi collettivi in ordine alla tutela dei propri dati "particolari".

Si deve infine ricordare che il 31 dicembre 1999 ha segnato il termine entro cui tutte le amministrazioni pubbliche, centrali e locali, dovevano quantomeno avviare l'adeguamento dei propri ordinamenti alle disposizioni prima richiamate. I soggetti pubblici sono stati dunque chiamati ad un'attenta disamina dei trattamenti svolti alla luce dei principi che si sono prima ricordati, veri-

ficando in che misura la disciplina relativa alla loro azione fosse adeguata e sufficiente per assicurare le garanzie oggi richieste. Si è già ricordato, in proposito, il regime più favorevole previsto per le pubbliche amministrazioni che hanno presentato al Garante entro la fine del 1999 una richiesta di autorizzazione allo svolgimento dei trattamenti privi della necessaria copertura normativa. Tali enti hanno potuto infatti proseguire gli stessi trattamenti fino alla decisione dell'Autorità, per la quale era previsto un termine di novanta giorni dalla domanda stessa.

Il d.lg. 135/1999 ha anche provveduto ad individuare un numero considerevole di rilevanti finalità di interesse pubblico, autorizzando i trattamenti ad esse legati. Rinviamo al testo del decreto legislativo per la completa elencazione di tali settori, nonché per le disposizioni dettate in relazione a ciascuno di essi, in questa sede è sufficiente sottolineare l'ampiezza di tale individuazione, capace di coprire diversi importanti trattamenti di dati sensibili svolti dalla pubblica amministrazione. Essi interessano, in particolare, lo stato civile, l'anagrafe, le liste elettorali, la cittadinanza, l'immigrazione, la condizione dello straniero, l'esercizio dei diritti politici, la pubblicità degli organi rappresentativi. Ed ancora: i rapporti di lavoro, i tributi, le dogane, le verifiche, le ispezioni, i controlli, l'istruzione, i benefici economici, le abilitazioni, le onorificenze, le ricompense, i riconoscimenti, il volontariato, l'obiezione di coscienza, la tutela della salute, l'interruzione volontaria della gravidanza, le tossicodipendenze, l'handicap, le sanzioni, la tutela in sede amministrativa e giurisdizionale, i rapporti con gli enti di culto, la statistica, la ricerca storica e gli archivi.

Dunque, un insieme di settori assai ampio che tuttavia non esaurisce tutte le materie in cui opera la pubblica amministrazione, sia in ragione del fatto che altri trattamenti svolti dalle pubbliche amministrazioni possono essere — ed in linea di fatto sono — autorizzati attraverso le altre procedure che si sono prima evidenziate; sia perché alcuni dei settori appena elencati hanno successivamente ricevuto un'ulteriore regolamentazione attraverso i decreti delegati previsti dalla legge n. 676/1996 (si rinvia, in particolare, alle sezioni di questa relazione dedicate alla sanità, alla statistica, alla ricerca scientifica e storica).

Come si è detto, il decreto n. 135 non aveva, però, individuato un numero di finalità di rilevante interesse pubblico tale da coprire tutte le innumerevoli attività realizzate dalla pubblica amministrazione, trascurando, in particolare, alcuni importanti trattamenti svolti in sede locale. Per tale ragione, il Garante ha autorizzato le amministrazioni pubbliche e gli enti locali, su loro richiesta, ad utilizzare i dati sensibili per una cospicua serie di specifiche attività che non erano state appunto previste dal d.lg. n. 135/1999 (autorizzazione pubblicata in *Gazzetta Ufficiale* n. 26 del 2 febbraio 2000).

L'autorizzazione ha carattere generale e trova pertanto applicazione anche per gli enti che non avevano presentato apposita richiesta. Essa assume particolare importanza per il rilevante interesse dei trattamenti autorizzati: essi attengono infatti, fra l'altro, al collocamento ed all'avviamento al lavoro, alle attività relative alla gestione degli asili nido e delle mense scolastiche, a quelle degli uffici leva presso i comuni, ai servizi in materia di edilizia abitativa pubblica, nonché alle attività ricreative, di promozione della cultura e dello sport.

Col medesimo provvedimento sono state altresì autorizzate diverse attività socio-assistenziali, quali gli interventi di sostegno psico-sociale e di formazione a favore dei giovani e degli altri soggetti che versano in condizioni di disagio sociale, economico o familiare; gli interventi, anche di rilievo sanitario, in favore dei soggetti bisognosi, non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto. Sempre in tale ambito, sono state autorizzate l'assistenza nei confronti di minori, anche in relazione a vicende giudiziarie, le indagini psico-sociali relative ai provvedimenti di adozione, nonché le iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi.

Oggetto di autorizzazione sono state infine le attività di polizia amministrativa locale, quelle in materia di protezione civile, le attività dei difensori civici regionali e locali, con particolare rife-

rimento alla trattazione di petizioni e segnalazioni, nonché quelle svolte dagli uffici per le relazioni con il pubblico.

Per concludere su tali problematiche, sembra doversi rilevare che le numerose novità introdotte nel corso del 1999 in materia di trattamento di dati sensibili e di carattere giudiziario da parte dei soggetti pubblici vanno nella direzione di una maggiore responsabilizzazione di questi ultimi. Essi sono infatti ora chiamati, in molti casi, ad una vera e propria auto-regolamentazione.

Si tratta di una scommessa e di una sfida per le pubbliche amministrazioni alle quali è data un'occasione unica per instaurare un rapporto nuovo con i cittadini, più rispettoso dei loro diritti e conseguentemente più ricco e suscettibile di ulteriori proficui sviluppi. Tutto ciò non comporterà effetti negativi sull'efficienza dell'azione amministrativa che potrà, anzi, esplicarsi con maggiore efficacia grazie al quadro di trasparenza che viene ad introdursi.

Ed è proprio questo lo spirito che ha animato il Garante nei contributi forniti nella fase di elaborazione delle possibili soluzioni normative, nonché in sede di risposta ai sempre numerosi quesiti e segnalazioni che quotidianamente pervengono in relazione alle problematiche sopra evindenziate. Solo partendo dalla piena e rigorosa tutela dei diritti legati alla sfera privata ed alla protezione delle informazioni personali, le amministrazioni potranno migliorare i loro rapporti con i consociati, contribuendo al rafforzamento dello spirito civico e, così, a far nascere una cittadinanza più matura e consapevole.

Si deve però purtroppo registrare che non tutte le amministrazioni sembrano aver compreso l'importanza di tale sfida e, quindi, operato con la necessaria solerzia nella direzione sperata. Si riscontrano infatti casi di enti pubblici che continuano a considerare l'adeguamento alle disposizioni sulla protezione dei dati come un onere sgradito da cui tenersi lontani, almeno ove ciò sia possibile (Comunicato del 15 dicembre 1999, in Bollettino n. 10, pag. 112).

Anche prescindendo da tutti gli aspetti di illegittimità di tali comportamenti -sui quali il Garante è impegnato ad esercitare un controllo rigoroso- resta comunque da sottolineare l'esigenza di un maggiore spirito di collaborazione anche da parte delle amministrazioni che si sono adeguate o si stanno adeguando alla normativa citata. Questa Autorità si è a tal fine dedicata con energia ad un'opera di informazione e formazione degli operatori del settore. Ciò, oltre che per far conoscere meglio il contenuto delle singole disposizioni, soprattutto per diffondere una cultura della privacy e, in tal modo, fare apprezzare il suo significato profondo e le sue potenzialità nel miglioramento delle relazioni reciproche fra cittadini e istituzioni.

L'attuale grande e continua evoluzione tecnologica apre sempre nuove possibilità di creazione di archivi e banche dati in grado di contenere un numero crescente di informazioni personali che possono essere poste in relazione fra loro per le finalità più diverse. Tutto questo offre certamente un'opportunità per i cittadini e le imprese, che possono così disporre di nuovi servizi in maniera più efficiente e rapida. E costituisce, altresì, una facilitazione per le pubbliche amministrazioni che possono ridurre i costi della loro azione e rendere più efficaci i controlli.

2.1.6
Nuovi archivi
e grandi
banche dati

Tuttavia, questo comporta anche un aumento dei rischi intrinsecamente connessi con tali operazioni, le quali moltiplicano le possibilità che i dati vengano impropriamente comunicati o comunque utilizzati per finalità differenti da quelle consentite o autorizzate. Per tale ragione, il Garante è impegnato in un'opera di attenta vigilanza sulle iniziative relative a nuove banche dati, al fine di verificare il rispetto delle disposizioni in materia di riservatezza.

Le possibilità offerte dalla tecnica, se correttamente utilizzate in questo ambito, possono costituire un'importante risorsa anche per accrescere il livello di partecipazione dei cittadini alla

vita sociale ed alle scelte collettive, innalzando in tal modo lo stesso grado di democraticità del sistema. Al contrario, però, un uso delle grandi potenzialità tecniche che fosse poco rispettoso dei diritti delle persone potrebbe condurre rapidamente ad una pericolosa regressione verso un restringimento degli spazi di libertà individuale e collettiva.

Se veramente si vuole che la società attuale, caratterizzata anche dalla necessità di molteplici flussi informativi e di conoscenza, non si trasformi in una società della sorveglianza e della classificazione, è necessario che tutti i soggetti operanti nei diversi contesti sociali maturino la piena consapevolezza dei rischi legati ad un uso non selezionato o non corretto delle informazioni personali ed insieme delle stesse opportunità di sviluppo e crescita civile legate al rispetto dei diritti connessi alla tutela della riservatezza personale.

Per questo motivo, le rapide trasformazioni in cui siamo immersi non possono essere lasciate alla loro più o meno naturale evoluzione, ma devono essere accompagnate da un'attenta riflessione sulle conseguenze legate ad ogni diversa opzione. Così, il moltiplicarsi degli archivi e delle interconnessioni fra banche dati non può derivare quasi meccanicamente dall'aprirsi di nuove potenzialità tecniche, ma deve presentarsi come il risultato di un cammino consapevole e comunque rispettoso dei diritti personali.

Naturalmente, nel governo di questi incessanti cambiamenti, i soggetti pubblici hanno un ruolo determinante sia per le decisioni di carattere normativo che sono chiamati a prendere, direttamente destinate a regolare il comportamento altrui, sia per le scelte compiute all'interno, attraverso l'organizzazione delle proprie attività.

Negli anni più recenti le pubbliche amministrazioni, impegnate in un meritevole sforzo per ammodernarsi e rendersi più efficienti, hanno mostrato un interesse crescente per tali sviluppi e hanno compiuto passi avanti verso un migliore utilizzo di tali strumenti. Specialmente intorno al progetto per la realizzazione della rete unitaria della pubblica amministrazione, si assiste ad un fiorire di iniziative destinate a creare entro breve tempo una più ampia automatizzazione dei servizi ed una progressiva informatizzazione degli uffici. Tutto ciò grazie in particolare ad un numero accresciuto di interconnessioni fra le diverse banche dati, con però il conseguente grave rischio che possa pensarsi che la mera esistenza dei collegamenti fra le tante e diverse banche dati delle pubbliche amministrazioni possa far prescindere dal rispetto dell'essenziale principio di finalizzazione che caratterizza la legislazione sulla tutela dei dati personali, secondo il quale i dati possono essere raccolti e successivamente trattati per i soli fini determinati dalle diverse normative o con essi compatibili. Normative che possono prevedere la comunicazione ed anche la diffusione dei diversi dati, ma nel rispetto di quanto prescritto dalle disposizioni della legge 675/1996 relative alle diverse categorie di dati personali (si vedano in particolare l'art. 27, comma secondo, l'art. 22, comma 3 e 3 bis, l'art. 24).

Il Garante ha avuto modo di occuparsi di tali banche dati in più occasioni durante l'anno trascorso, specie in occasione delle richieste di parere sugli schemi di disposizioni normative predisposte dal Governo.

Limitandosi in questa sede ad un sintetico richiamo ad alcune delle maggiori iniziative intraprese da soggetti pubblici e privati e rinviando, per una loro più puntuale disamina alle altre parti di questa relazione, è qui sufficiente richiamare anzitutto la previsione dell'anagrafe degli assegni bancari prevista dall'art. 36 del decreto legislativo n. 507 del 1999 (su cui cfr. par. 2.6.5) e lo schema di regolamento governativo che istituisce un archivio dei rapporti di conto e deposito, previsto dalla legge n. 413 del 1999 sul potenziamento degli accertamenti fiscali e sulla riforma del contenzioso, sul quale si è espresso criticamente il Garante il 17 novembre 1999 (cfr. par. 2.6.3).

L'Autorità ha altresì partecipato alle attività del Comitato di coordinamento per l'indirizzo ed il controllo della fase di avvio e sperimentazione del Sistema di accesso e interscambio anagrafi-

co - SAIA (art. 8 della Convenzione stipulata in data 4 novembre 1999 tra il Ministero dell'interno e l'Associazione nazionale comuni italiani - A.N.C.I.). Tale Sistema è stato previsto dal Ministero dell'interno in vista del conseguimento della semplificazione burocratica, della riduzione dei costi dei servizi pubblici e del rilascio della carta di identità elettronica (d.P.C.M. 22 ottobre 1999, n. 437), sulla base di un progetto intersettoriale dell'Autorità per l'informatica nella pubblica amministrazione. Il Ministero dell'interno ha posto anche l'esigenza di realizzare, nell'ambito del medesimo Sistema, un Indice nazionale delle anagrafi per l'immediata individuazione del Comune che detiene i dati personali contenuti nelle anagrafi della popolazione di ciascun cittadino, nonché per facilitare l'esercizio dei compiti di vigilanza attribuiti sulla tenuta delle anagrafi comunali.

La rilevante incidenza di quest'ultima progettata innovazione sull'ordinamento anagrafico ed un'assai ampia individuazione dei soggetti legittimati ad accedere all'Indice, hanno originato una prima presa di posizione del Garante, il 2 novembre 1999, nei riguardi del Ministro dell'interno ed una successiva, l'8 marzo 2000, nei riguardi di una pluralità di organi governativi, facendosi presente che la materia sembra esigere un intervento a livello legislativo, che permetta anche di definire con chiarezza le finalità di utilizzo, i soggetti aventi accesso e il contenuto stesso di questo Indice, che comunque non può certo prefigurare la creazione di una vera e propria anagrafe nazionale. Successivamente a questi interventi, sembra che sia in fase di predisposizione un apposito disegno di legge (su tutta la vicenda cfr. par. 2.1.9).

L'Autorità è stata altresì chiamata ad occuparsi delle diverse banche dati costituite nell'ambito del sistema creditizio e finanziario.

Come è noto, presso la Banca d'Italia opera la Centrale dei rischi alla quale sono tenuti a partecipare le banche iscritte all'albo di cui all'art. 13, le società finanziarie di cui all'art. 65, comma 1, lett. a) e b), nonché gli intermediari finanziari iscritti nell'elenco speciale di cui all'art. 107 del testo unico delle leggi in materia bancaria e creditizia, i quali esercitano, in via esclusiva o prevalente, l'attività di finanziamento sotto qualsiasi forma.

Recentemente l'Associazione bancaria italiana (ABI) si è espressa a favore della realizzazione di un sistema di rilevazione degli affidamenti di importo inferiore alla soglia di rilevazione della Centrale di cui sopra. Ciò al fine di ricavare una completa valutazione di tutti i rischi assunti nei confronti della clientela del sistema creditizio e finanziario. Il C.I.C.R., ritenendo che tale iniziativa si iscriva nella logica di sana e prudente gestione e sia coerente con le finalità di vigilanza, ha stabilito l'obbligo, per tutti gli intermediari finanziari che partecipano alla Centrale dei rischi prima citata, di comunicare ad un sistema centralizzato di rilevazione tutti i dati relativi alle esposizioni creditizie di importo inferiore al limite minimo del censimento previsto per la medesima Centrale e superiore al limite massimo stabilito per le operazioni di credito al consumo (attualmente pari a sessanta milioni di lire).

Alla Banca d'Italia è stato affidato il compito di emanare le istruzioni di carattere generale necessarie all'attuazione della delibera del C.I.C.R., prevedendo però che prima essa consulti il Garante per gli aspetti relativi al trattamento dei dati personali e che, successivamente, verifichi il rispetto della relativa disciplina (cfr. par. 2.6.3).

Al fine di offrire un'idea della vastità del fenomeno a cui si è fatto riferimento, può essere utile ricordare altresì alcune altre banche dati di più recente costituzione.

All'interno del Sistema informativo agricolo nazionale (SIAN), integrato con i sistemi informativi regionali, è stata costituita un'anagrafe delle aziende agricole. Essa raccoglie le notizie relative ai soggetti pubblici e privati esercenti attività agricola, agroalimentare, forestale e della pesca, che intrattengano a qualsiasi titolo rapporti con la pubblica amministrazione centrale o locale (art. 1, d.P.R. 1 dicembre 1999, n. 503).

Nell'ambito del riordino delle procedure di collocamento pubblico dei lavoratori dipen-

denti si prevede poi l'istituzione di un Sistema informativo lavoro e di una carta elettronica personale del lavoratore (cfr. par. 2.3.1 di questa relazione).

Più di recente, presso la banca dati dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro e le malattie professionali (INAIL), è stato istituito il registro nazionale delle malattie causate dal lavoro ovvero ad esso correlate. Per ciò che specificamente attiene alla protezione dei dati personali, la disciplina di tale registro richiama la necessità di rispettare quanto disposto dalla legge n. 675/1996, specificando inoltre le categorie di soggetti che possono avervi accesso (art. 10, comma 5, d.lg. 23 febbraio 2000, n. 38).

Con lo stesso provvedimento normativo, si è altresì proceduto al riordino dei compiti e della gestione del Casellario centrale infortuni. Quest'ultimo, posto sotto la vigilanza del Ministero del lavoro e della previdenza sociale, è titolare di una banca dati relativa agli infortuni professionali e non professionali ed alle malattie professionali. Essa viene alimentata e può essere consultata dagli istituti che esercitano l'assicurazione obbligatoria contro gli infortuni sul lavoro, nonché dagli enti che provvedono all'assicurazione contro i rischi di infortunio e contro i rischi derivanti dalla circolazione di automezzi.

Il Casellario dovrà archiviare, conservare e comunicare agli utenti i dati relativi ai casi di infortunio e di malattia professionale che importino invalidità permanente o morte, anche a prescindere da uno specifico evento lesivo. Esso dovrà inoltre elaborare i dati mediante procedure informatiche che consentano l'ottimizzazione del loro uso anche in forma aggregata da parte dei soggetti autorizzati. Suo compito è, infine, quello di favorire l'integrazione ed il raccordo della propria banca dati con altre analoghe a livello nazionale e sovranazionale, nonché con quelle a carattere previdenziale (artt. 15-17, d.lg. 23 febbraio 2000, n. 38).

Da quanto detto e dagli esempi fatti, si desume con chiarezza che l'obiettivo di consentire, attraverso la gestione informatica dei flussi documentali, un più ampio interscambio di dati tra le diverse amministrazioni e fra queste ed i cittadini può svilupparsi solo se viene inserito all'interno di un preciso quadro di garanzie sul rispetto dei diritti fondamentali della persona.

A tal fine, è innanzi tutto necessario avere sempre presenti gli sviluppi complessivi del sistema, così da poterne valutare in modo corretto i rischi e le opportunità, calibrando conseguentemente le misure atte a tutelare i diritti eventualmente messi in pericolo. In tal modo, è anche possibile evitare i pur troppo frequenti casi di duplicazioni e sovrapposizioni fra diversi trattamenti, di impropria diffusione delle informazioni personali o anche solo la costituzione di pericolose concentrazioni di dati, intrinsecamente portatrici di un accrescimento dei rischi.

Occorre evitare poi la creazione di grandi banche la cui disciplina, benché inclusiva di generiche clausole di richiamo della legge n. 675, sia in realtà lacunosa e priva di adeguate garanzie per ciò che riguarda le finalità perseguite, le modalità del trattamento, i flussi di dati e i soggetti legittimati ad utilizzarli.

È in ogni caso necessario che il fiorire non sempre ordinato di disposizioni legislative sulla creazione di nuovi archivi o sulla concentrazione di quelli esistenti rispetti i principi dettati dalla legge 675/1996, essendo questi in gran parte una trasposizione dei contenuti della direttiva 95/46/CE, alla quale il nostro ordinamento è vincolato ad adeguarsi. Tale rilievo assume evidentemente un carattere ancora più pressante per i casi in cui la regolamentazione dei diversi settori avviene attraverso norme di rango regolamentare o, addirittura, mediante circolari ed altri atti amministrativi, comunque privi di carattere normativo (Comunicato del 18 ottobre 1999, in Bollettino n. 10 pag. 88).

Nel corso del 1999, il Garante si è in più occasioni adoperato per sensibilizzare le pubbliche amministrazioni ed i cittadini in ordine a tali problematiche ed ha nel contempo compiuto uno sforzo per far riscoprire le ragioni profonde di quella parte della normativa relativa alla tutela della

riservatezza dalla quale è scaturito il primo nucleo delle leggi più avanzate oggi vigenti. Normativa, che era appunto incentrata sulla regolazione delle banche dati e sui trattamenti realizzati mediante strumenti elettronici.

L'evoluzione normativa e la pratica amministrativa mettono in luce una tendenza sempre più diffusa all'utilizzo da parte delle pubbliche amministrazioni di documenti elettronici, di carte magnetiche con funzioni identificative dei cittadini ma anche finalizzate a consentire una più celere erogazione di taluni servizi. Tali strumenti offrono indubbi vantaggi per i cittadini, che in tal modo hanno l'opportunità di ridurre gli oneri di carattere burocratico a cui spesso sono sottoposti e di ottenere con maggiore celerità quanto loro dovuto. Essi comportano anche notevoli risparmi per gli uffici pubblici, che possono contenere i costi sia per la maggiore celerità delle procedure, sia per la possibilità di evitare inutili duplicazioni di documenti ed archivi.

2.1.7
Documenti
elettronici
e carte
magnetiche

Tutto questo non deve però andare a detrimento della tutela dei diritti delle persone e, in particolare, della riservatezza di ciascuno. Per tale motivo, nel disciplinarne l'utilizzo, è indispensabile porre particolare attenzione al tipo di informazioni che vengono inserite al loro interno, alle operazioni che è possibile fare su di essi ed ai soggetti che hanno accesso alle diverse categorie di dati. È inoltre necessario inquadrare gli interventi diretti alla creazione di nuovi documenti elettronici e carte magnetiche all'interno di un progetto organico, evitando che si creino — come, purtroppo, a volte si verifica — duplicazioni e sovrapposizioni di informazioni ed archivi.

Nella regolamentazione di tali strumenti assume infine particolare rilievo il grado di libertà lasciato agli interessati in ordine alla possibilità di inserire o meno alcuni dati. Al fine di consentire una scelta realmente consapevole, è necessario che siano prospettati in maniera chiara ed esaustiva non solo i trattamenti a cui saranno soggetti in via ordinaria i dati, ma anche tutti i possibili ulteriori usi degli stessi, nonché i rischi legati alla conservazione di tali informazioni all'interno del supporto elettronico (per il parere sulla carta di identità elettronica cfr. par. 2.1.9).

Sotto tutti questi profili, le previsioni relative alle carte sanitarie elettroniche contenute nell'art. 6 del d.lg. n. 282/1999 possono certamente essere considerate un primo importante risultato, frutto anche di un proficuo confronto instaurato fra l'amministrazione interessata ed il Garante. Rinviano per una più approfondita analisi della disposizione in parola al par. 2.2.4 di questa relazione, si deve qui ricordare che, sulla base di esso, gli interessati possono opporsi all'inserimento nelle carte sanitarie dei dati idonei a rivelare lo stato di salute che li riguardano e che eccedono le informazioni relative alla gestione amministrativa e alle situazioni di interventi di urgenza, quali definiti a livello internazionale. Tali disposizioni prevedono inoltre che un decreto ministeriale determini le categorie di incaricati delle aziende sanitarie locali e di operatori che possono accedere ai diversi tipi di dati contenuti nelle carte, le categorie professionali tenute ad inserire i dati, nonché il periodo massimo di conservazione (art. 6, commi 2 e 3).

Conviene, infine, richiamare l'attenzione sulla necessità che i progetti relativi all'introduzione dei documenti elettronici e delle carte magnetiche tengano conto degli sviluppi che si stanno registrando in sede comunitaria. Attualmente, infatti, è in corso un ricco dibattito che mira ad individuare standard tecnici uniformi e regolamentazioni analoghe a livello dell'Unione europea. Regolamentazione, questa, all'interno della quale la tutela della riservatezza rappresenta uno dei capitoli di maggiore rilievo. In tale percorso elaborativo confluiscono perciò le diverse esperienze nazionali in materia, che, fondandosi sulla base comune della citata direttiva n. 95/46/CE, possono condurre a migliori tutele dei diritti della persona, ampliando nel contempo l'ambito di utilizzabilità dei documenti e delle carte in discorso.

In alcuni casi, invece, proprio l'utilizzo delle tecnologie elettroniche può consentire una maggiore tutela della riservatezza, ad esempio permettendo di selezionare le persone che possono avere accesso alle diverse categorie di dati, o facilitando la conservazione separata dei dati fino a che sorga l'effettiva necessità di una loro riunione. Su questo versante si può ricordare il caso inte-

ressante sorto con la proposta di istituire una tessera elettorale cartacea destinata a svolgere la funzione di certificato elettorale per diciotto consultazioni, in attesa di adottare una tessera magnetica (art. 13, l. 30 aprile 1999, n. 120).

La proposta, contenuta in uno schema di regolamento sottoposto al parere del Garante, avrebbe avuto il vantaggio di ridurre le spese per le operazioni di voto, in quanto il costo della distribuzione su tutto il territorio nazionale dei certificati elettorali, ora sostenuto per ogni consultazione, sarebbe stato sostituito dai minori oneri legati alla distribuzione della tessera una sola volta per tutti gli appuntamenti elettorali in essa registrabili. Essa avrebbe inoltre consentito di ridurre il rischio - di fatto ineliminabile col sistema attuale - che qualche persona appartenente alle categorie abilitate a votare anche in sezioni diverse da quelle di iscrizione possa tentare di esprimere un voto doppio o plurimo (la tessera elettorale, avrebbe dovuto contenere, fra le altre informazioni, anche la certificazione dell'avvenuta votazione).

Proprio quest'ultimo dato assume però una particolare delicatezza in quanto - specie in alcune consultazioni quali i referendum abrogativi o votazioni di ballottaggio -, la partecipazione o la mancata partecipazione al voto possono di per sé manifestare una particolare opzione politica dell'elettore. Ed è dunque evidente che la conservazione in un unico documento cartaceo della storia della partecipazione al voto di un elettore espone quest'ultimo al rischio di pressioni di vario genere, che potrebbero ridurre la sua sfera di libertà. Sono, infatti, numerose le persone che potrebbero trovarsi nella condizione di verificare il contenuto di tale documento, sia per ragioni legate al proprio ufficio (è, ad esempio, il caso del personale addetto ai seggi), sia, soprattutto, in conseguenza dei rapporti intrattenuti con l'interessato (si pensi alla famiglia, alle associazioni politiche, all'ambiente di lavoro).

Proprio la considerazione del fatto che lo strumento cartaceo era in ogni caso destinato ad essere superato in tempi rapidi da tessere elettroniche in grado di garantire un più elevato livello di riservatezza, il Garante con il parere del 17 novembre 1999 (in Bollettino n. 10, pag. 19) ha suggerito al Ministero dell'interno di attendere che tali più moderni strumenti possano essere introdotti. Ciò, anche in considerazione delle analoghe iniziative che si stanno sperimentando in ambito comunitario.

In alternativa a ciò, l'Autorità ha comunque segnalato la necessità che fossero adottati accorgimenti atti a ridurre i rischi sopra evidenziati, quali la conservazione separata dei dati identificativi da quelli relativi alla partecipazione al voto, consentendo la loro riunione solo quando questa sia effettivamente necessaria. Il Garante ha inoltre avuto modo di richiamare la necessità di un più attento vaglio della pertinenza dei dati contenuti nella tessera rispetto alle finalità che con essa si intendono perseguire, nonché l'obbligo di adottare le ordinarie misure di sicurezza previste dal nostro ordinamento.

Con particolare riguardo alla possibilità che nella tessera venisse inserito anche un codice di identificazione personale, ed al di là di ogni considerazione sulla pertinenza dello stesso, il Garante ha inoltre voluto ribadire le considerazioni già espresse in un precedente parere relativo alla carta di identità elettronica (parere del 26 febbraio 1998 sullo schema di regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica), relative alla necessità che l'attribuzione ed il trattamento di dati connessi a numeri di identificazione personale siano accompagnati da precise garanzie sui presupposti e sulle condizioni per il loro utilizzo. Garanzie, queste, che devono essere affidate a norme di carattere primario (art. 8, par. 7, direttiva n. 95/46/CE).

Una parte rilevante dell'attività del Garante nei riguardi del settore pubblico è stata rivolta alla soddisfazione di numerose richieste di chiarimenti avanzate da enti locali, con riferimento alla disciplina parzialmente diversa applicabile nei loro confronti in relazione alle loro specifiche funzioni e caratteristiche, pur nella uniformità di fondo della disciplina relativa a tutti i soggetti pubblici, salvo gli enti pubblici economici.

2.1.8
Enti
locali

Per quanto attiene in particolare ai temi della trasparenza dell'attività amministrativa e del diritto di accesso agli atti e ai documenti abbiamo già visto ai par. n. 2.1.3 e 2.1.4 alcune specificità degli enti locali.

Con riferimento alla disciplina normativa concernente il trattamento dei dati personali da parte degli enti locali, una serie di interventi del Garante hanno riguardato problemi relativi alla comunicazione e alla diffusione dei dati nell'ambito delle norme riguardanti lo stato civile e gli atti anagrafici.

Una decisione del 9 dicembre 1999 ha dichiarato conforme alla legge n. 675/1996 la possibile consultazione per via telematica degli atti anagrafici da parte delle forze dell'ordine, dal momento che la normativa sugli atti anagrafici (d.P.R. 223 del 1989) regola in modo specifico la consultabilità dei medesimi atti da parte degli appartenenti alle forze dell'ordine, consentendo a queste ultime di accedere direttamente agli uffici anagrafici ai soli fini della consultazione, anche mediante terminali collegati con gli uffici stessi. Indicazioni specifiche fornite rispetto a talune concrete modalità previste.

Il tema ha richiesto un'ulteriore precisazione per quanto riguarda la possibilità di convenzioni fra archivi anagrafici, altre amministrazioni pubbliche e gestori o esercenti di pubblici servizi: il Comune di Novara, infatti, ha chiesto un parere su una bozza di convenzione in attuazione della facoltà prevista dall'art. 2, comma 5, della l. 127/1997, di trasmissione di dati o documenti tra gli archivi anagrafici e dello stato civile "garantendo il diritto alla riservatezza delle persone": il Garante nel parere in data 31 dicembre 1999 ha chiarito che questa disposizione agevola semplicemente la possibilità di trasmissione di dati e documenti a cui i diversi soggetti possono già accedere sulla base della legislazione vigente, mentre una nuova forma di gestione ed accesso ai dati anagrafici "potrebbe essere invece introdotta solo da apposite norme modificative".

Sulla base di quanto previsto dal primo e dal secondo comma dell'art. 27 della l. 675/1996, il Garante con il provvedimento del 14 gennaio 1999 (in Bollettino n. 7, p. 53), ha ritenuto pienamente conforme alla legge in materia di protezione dei dati personali l'acquisizione da parte di una provincia di una serie di dati personali comuni (ad es., dati anagrafici) in possesso di altre amministrazioni pubbliche per adempiere ai propri compiti, tra cui rientra l'attività di controllo sulla manutenzione e sull'esercizio degli impianti termici. Ove la provincia operi sulla base di una convenzione, affidando quindi a soggetti esterni il trattamento dei dati, occorre peraltro che provveda a designarli formalmente come responsabili o incaricati del trattamento.

Per quanto riguarda invece il rilascio da parte dell'ufficiale dello stato civile degli estratti dei certificati di matrimonio, è stato evidenziato, con il provvedimento del 29 marzo 1999 (in Bollettino n. 9, p. 115), che al fine di accertare il regime patrimoniale esistente tra una persona sottoposta ad un esproprio immobiliare e il suo coniuge, è sufficiente richiedere un estratto per riassunto, senza necessità di acquisire l'atto di matrimonio in copia integrale, che può essere invece rilasciato solo dietro autorizzazione del procuratore della Repubblica.

Un tema ricorrente ha riguardato la possibilità per i Comuni di conoscere dalle imprese che partecipano a gare pubbliche i dati relativi agli importi e ai destinatari di analoghi servizi prestati in precedenti occasioni, al fine di soddisfare l'esigenza della stazione appaltante di verificare la capacità tecnica delle imprese concorrenti.

Sull'argomento l'Autorità ha risposto con provvedimento del 16 febbraio 1999 (in Bollettino n. 7, p. 7) sottolineando che i Comuni, ai fini dello svolgimento dei compiti istituziona-

vizi sia di forniture, possono legittimamente richiedere alle imprese concorrenti di dimostrare le proprie capacità tecniche mediante la produzione di informazioni riguardanti i servizi o le forniture prestati, con le indicazioni degli importi, delle date e dei destinatari, fermo restando il rispetto del segreto aziendale ed industriale.

Con riferimento poi alle problematiche attinenti alle misure di sicurezza presso gli enti comunali, un provvedimento del 28 ottobre 1999 (in Bollettino n. 10, p. 93) ha riguardato la necessaria verifica della rispondenza delle misure di sicurezza adottate dopo un furto di alcuni tagliandi contenenti dati anagrafici e foto identificative, corrispondenti alle carte di identità rilasciate ai cittadini. Nel ricordare in tale circostanza che anche i soggetti pubblici, al pari dei privati che trattano dati personali, devono osservare modalità di conservazione e di controllo dei dati tali da ridurre al minimo i rischi di eventuale distruzione o perdita degli stessi (art. 15 l. 675/1996), il Garante ha sottolineato, fra l'altro, che il regolamento sulle misure minime di sicurezza (d.P.R. 14 settembre 1999, n. 318) imponeva, anche per quanto riguarda i trattamenti cartacei, l'adozione di accorgimenti e cautele minime (misure organizzative, conservazione in archivi ad accesso selezionato, ecc.) entro il 29 marzo 2000, la cui mancata osservanza comporta sanzioni di carattere penale anche solo di tipo colposo.

In altra occasione il Garante si è occupato dell'attività dei consigli provinciali per quanto attiene al trattamento dei dati connessi alla nomina degli organi di enti, società, comitati e altri organismi, sia in caso di nomina diretta, sia nel caso che le persone vengano previamente indicate da singoli consiglieri o da gruppi consiliari.

Con un provvedimento del 15 luglio 1999 (in Bollettino n. 9, pag. 69) è stato chiarito preliminarmente che nella prima ipotesi i dati personali trattati ai fini della nomina sono per lo più comuni, riguardando, ad esempio, le generalità dei candidati, l'eventuale posizione di lavoro, ecc. Nelle altre ipotesi, invece, la circostanza che l'indicazione dei nominativi sia effettuata dai singoli consiglieri, o da gruppi consiliari, potrebbe far ritenere che si tratti anche di dati "sensibili", idonei a rivelare le opinioni politiche dell'interessato, potendosi presumere che i soggetti indicati appartengano, più o meno direttamente, all'area politica del consigliere o del gruppo che li propone.

In entrambi i casi, il trattamento di tali dati da parte del consiglio provinciale è peraltro legittimo, ferma restando la necessità di rispettare gli obblighi concernenti l'informativa all'interessato, le misure da adottare per garantire la sicurezza degli archivi e il principio di pertinenza, in base al quale possono essere trattati solo i dati strettamente necessari alle finalità per le quali sono raccolti. In tal senso è stato precisato che i dati relativi ai soggetti, la cui proposta non sia seguita da una effettiva nomina o designazione, siano cancellati non appena terminate le operazioni di vaglio delle candidature, mentre i dati delle persone nominate dovranno essere conservati per il tempo strettamente necessario al loro uso.

Un aspetto delicato, trattandosi di dati sensibili, è stato affrontato con il provvedimento del 9 giugno 1999 (in Bollettino n. 9, p. 71) con riferimento al regime di conoscibilità dell'elenco dei sottoscrittori di una lista elettorale. La disciplina del trattamento dei dati sensibili da parte dei soggetti pubblici, prevista dal decreto legislativo n. 135/1999, consente, nell'ambito delle attività in materia di elettorato e altri diritti politici, solo i trattamenti finalizzati all'esecuzione di specifici compiti previsti da leggi o regolamenti. Fra tali compiti deve ritenersi ricompresa la comunicazione a soggetti determinati dei dati e delle informazioni in possesso delle amministrazioni pubbliche ai sensi della normativa sul diritto di accesso, nei limiti e alle condizioni ivi previsti, nonché nel rispetto dei principi fissati dalla legge n. 675/1996 e dallo stesso decreto legislativo n. 135/1999, e, in particolare, di quelli di pertinenza e di essenzialità dei dati trattati e del rispetto della finalità perseguita (art. 9 legge n. 675 e artt. 1-4, d.l.g. n. 135). In tal senso deve quindi ritenersi legittimo il rilascio di questo elenco ai soggetti che intendano servirsene per l'esercizio dei diritti politici, come nel caso in cui la richiesta pervenga da candidati appartenenti a liste concorrenti.

Come già si è accennato al par. 2.1.6, la realizzazione del progetto relativo alla rete unitaria della pubblica amministrazione non prevede soltanto una semplice costruzione di infrastrutture, ma lo sviluppo di un insieme coordinato e coerente di progetti utili a garantire a qualunque utente, purché autorizzato, di poter accedere ai dati e alle procedure residenti nei sistemi informativi automatizzati delle altre amministrazioni, indipendentemente dalle reti attraversate e dalle tecnologie adottate dai singoli sistemi.

In questo quadro, la funzione anagrafica riveste indubbiamente un ruolo centrale, in quanto essa è la fonte principale di informazioni di base e quindi indispensabile per l'attività di tutte le amministrazioni pubbliche e di molti settori privati. In tal senso il Sistema di accesso e interscambio anagrafico (SAIA), che si inserisce nel più vasto ambito della rete unitaria della pubblica amministrazione, è stato studiato in vista del conseguimento della semplificazione amministrativa e della riduzione dei costi dei servizi pubblici. Anche la carta di identità elettronica, come la gestione ed il controllo dell'immigrazione, farebbe perno sul Sistema di accesso e integrazione anagrafica.

Naturalmente, tale gestione informatica dei flussi documentali potrà svilupparsi nell'ambito del processo di trasformazione dell'apparato statale soltanto se verrà delineato un preciso quadro di garanzie che riguardi, in primo luogo, la compatibilità tra le finalità perseguite dalle amministrazioni interessate e la pertinenza e la non eccedenza dei dati raccolti tramite questo sistema. In particolare la comunicazione di dati tra pubbliche amministrazioni è lecita solo nel rispetto delle prescrizioni, a seconda delle categorie di dati interessati, degli artt. 27, 22 commi 3 e 3 bis, 24 della legge 675/1996.

In proposito, l'Autorità garante ha sviluppato diversi spunti di riflessione nell'ambito dell'attività consultiva ai sensi dell'art. 31, comma 2, della legge n. 675, con particolare riferimento allo schema di regolamento per il rilascio della carta d'identità elettronica e del documento d'identità elettronico (provvedimento del 26 febbraio 1999, in Bollettino n. 7, p. 27), fissando il principio che le informazioni relative al cittadino da inserire nella carta d'identità elettronica devono essere delimitate e individuate in modo specifico, evitando riferimenti generici suscettibili di porsi in contrasto con i principi espressi dalla legge n. 675.

Sempre in questo parere è stata ribadita l'esigenza che l'attribuzione generalizzata ai cittadini di numeri di identificazione personale, ivi compreso il codice fiscale, debba essere accompagnata da precise garanzie sulle condizioni del loro utilizzo (garanzie che sono demandate dalla legge delega 676/1996 a disposizioni di carattere primario, da adottare allo scopo di completare il recepimento della direttiva comunitaria sulla riservatezza dei dati).

Già nella precedente Relazione per l'anno 1998 (pag. 22), il Garante aveva riferito in merito alle problematiche scaturite dall'emanazione della circolare del Ministero dell'interno 1° dicembre 1998, Miacel n. 20, in relazione alla quale l'Autorità ha anche dovuto manifestare il proprio disappunto per la mancata consultazione relativamente ad una importante iniziativa destinata ad incidere profondamente sul sistema di comunicazione ad altri enti pubblici dei dati personali contenuti nelle anagrafi comunali.

L'Autorità ha continuato a seguire attentamente le attività e i progressi che si registrano nell'ambito della realizzazione della rete unitaria della pubblica amministrazione partecipando anche presso il Ministero dell'interno alle riunioni del Gruppo di lavoro incaricato del coordinamento, controllo e valutazione della fase di avvio del progetto S.A.I.A., e formulando in questa sede alcune prime indicazioni utili per la redazione di una normativa da adottarsi su iniziativa del Ministero dell'interno, per la realizzazione dell'Indice nazionale delle anagrafi (INA) e per la disciplina dell'accesso all'indice medesimo. L'introduzione di tale Indice, in cui dovrebbero essere contenuti nome, cognome, codice fiscale e comune di residenza, avrebbe lo scopo di consentire agli enti collegati di individuare rapidamente il comune presso il quale rivolgersi per ottenere le informazioni di interesse.

Al riguardo, deve darsi atto degli sforzi compiuti dall'amministrazione dell'interno per recepire i suggerimenti che il Garante ha formulato riguardo alla costituzione del S.A.I.A. nonché alla convenzione con l'ANCI con provvedimento del 2 novembre 1999 per lo scambio di dati relativi alle variazioni anagrafiche, tra comuni ed altri enti pubblici.

Peraltro, con particolare riguardo alla costituzione dell'Indice delle anagrafi, previsto dalla citata convenzione con l'ANCI e da realizzarsi mediante decreto del Ministero dell'interno, il Garante ha constatato che detto Indice, pur non costituendo un'«Anagrafe delle anagrafi», introdurrebbe inevitabilmente tali ed importanti innovazioni nell'ambito della vigente legislazione anagrafica da rendere necessaria una disciplina legislativa di tale istituto, che lo preveda espressamente e che ne determini le caratteristiche fondamentali. Come si è detto al par. 2.1.6, il Garante ha fatto presenti questi rilievi mediante una lettera dell'8 marzo 2000 al Presidente del Consiglio dei Ministri e ad alcuni Ministri; successivamente sembra che sia in fase di adozione un apposito disegno di legge. ...

In seno ad un Gruppo di lavoro presso il Ministero dell'interno, il Garante partecipa altresì ai lavori per la predisposizione dell'apposito decreto ministeriale, previsto dal d.P.R. 31 agosto 1999, n. 394, per determinare, nell'ambito della più generale disciplina delle iscrizioni e variazioni anagrafiche dei cittadini stranieri che regolarmente soggiornano nel territorio nazionale, le modalità di comunicazione dei dati concernenti i cittadini stranieri fra gli uffici di anagrafe dei comuni, gli archivi dei lavoratori extracomunitari e gli archivi degli organi centrali e periferici del Ministero dell'interno. Già in merito allo schema di regolamento per l'attuazione del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e la condizione dello straniero (ora d.P.R. n. 394/1999), il Garante (provvedimento del 2 febbraio 1999, in Bollettino n. 7, p. 21) aveva segnalato al competente Ministero, l'opportunità di inserire precisi riferimenti ai principi espressi dalla legge n. 675/1996 con particolare riguardo alla pertinenza delle informazioni trasmissibili fra diverse amministrazioni ed alla compatibilità tra le finalità perseguite da ciascuna amministrazione. Tali indicazioni sono state puntualmente recepite nel citato provvedimento regolamentare.

Sempre nell'ambito dell'attività consultiva, il Garante è intervenuto con il provvedimento del 16 giugno 1999 (in Bollettino n. 9, p. 19) in merito allo schema di decreto ministeriale recante norme per stabilire i casi, i limiti e le modalità di esercizio delle facoltà di accesso dei concessionari della riscossione alle banche dati degli uffici pubblici, come previsto dal d.lg. n. 112/1999, esprimendo alcune osservazioni volte a garantire che i trattamenti effettuati dai concessionari riguardino le finalità e i dati strettamente collegati all'espletamento delle procedure esecutive, secondo modalità connesse a tale scopo e con un generale divieto di divulgazione dei dati fuori dei casi espressamente previsti.

L'Autorità ha inoltre fornito indicazioni al Governo (parere del 21 luglio 1999, in Bollettino n. 9, p. 27) con riguardo allo schema di regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile, formulando alcune osservazioni in merito all'archivio nazionale informatico dello stato civile che si intende istituire. È stato così suggerito di adottare tutte le misure idonee per garantire la riservatezza di terzi, auspicando l'adozione di una gestione informatica separata, per ciascun comune, dei dati relativi agli atti dello stato civile, al fine di evitare che la condivisibile esigenza di evitare la dispersione dei dati in caso di eventi dolosi o di calamità naturali comporti, però, un'eccessiva concentrazione di dati, soprattutto quando questi riguardino profili particolarmente delicati relativi alla vita privata delle persone o possano permettere, anche attraverso agevoli collegamenti tra diversi tipi di informazioni, di utilizzare i dati anche per finalità diverse da quelle indicate dalla legislazione.

Nel formulare le proprie osservazioni (parere del 5 maggio 1999, in Bollettino n. 8, p. 18) in merito allo schema di regolamento che istituisce l'anagrafe delle aziende agricole e la carta dell'agricoltore, il Garante ha ribadito l'esigenza di chiarire con precisione, anzitutto, il regime di pubblicità delle informazioni contenute nell'istituenda anagrafe.

In tale circostanza, infatti, ferme restando le condivisibili finalità di interesse pubblico connesse all'istituzione dell'anagrafe delle aziende agricole, si è ritenuto necessario, per un corretto bilanciamento di tali finalità con i diritti fondamentali degli interessati, siano essi persone fisiche o persone giuridiche, che l'utilizzazione dei dati che si intende raccogliere avvenga sulla base di un più preciso quadro di riferimento, anche relativamente all'attivazione dei flussi di dati tra amministrazioni ed altri enti pubblici, e la possibilità di accedere e di interconnettere informazioni contenute in altri archivi, pubblici e privati (ad es., sistema informativo dell'Amministrazione delle finanze, sistema informativo delle camere di commercio; sistemi informativi di utenti esterni interconnessi ecc.).

Un interessante aspetto è stato inoltre affrontato dall'Autorità, in occasione dello svolgimento delle elezioni per il rinnovo del Parlamento europeo (provvedimento del 18 maggio 1999, in Bollettino n. 8, p. 21) con riguardo al regime di conoscibilità degli elenchi degli elettori italiani residenti all'estero per il rinnovo del Parlamento europeo: la piena conoscibilità di questi elenchi a fini di propaganda elettorale può essere dedotta dalla disciplina sulla tenuta e sulla pubblicità delle liste elettorali, ma è praticamente contraddetta dal fatto che questi elenchi sono disponibili presso le sedi consolari solo pochi giorni prima delle elezioni.

Una più tempestiva predisposizione di questi elenchi è tanto più necessaria in quanto non si può supplire alla conoscenza dei cittadini residenti all'estero mediante un indiscriminato accesso agli schedari che costituiscono l'anagrafe consolare, che sono invece disciplinati secondo l'ordinaria normativa anagrafica. Semmai si può in parte ovviare a questa situazione mediante la piena conoscibilità degli elenchi predisposti in precedenza per le elezioni dei componenti dei Comitati degli italiani all'estero (*Comites*), elenchi pubblici per espressa disposizione di legge e di cui, pertanto, è possibile favorire un'ampia conoscenza da parte dei terzi, sia pubblici sia privati, analogamente a quanto previsto dalla disciplina sulla tenuta delle liste elettorali.

È proseguita anche per il 1999 la collaborazione con il Ministero delle finanze per la predisposizione dei modelli delle dichiarazioni da presentarsi nel 2000 da parte dei contribuenti e dei sostituti d'imposta.

2.1.10
Attività
fiscali e
tributarie

In particolare, il Garante è stato chiamato a dare il proprio parere in ordine ad alcune modifiche apportate alle informative inserite nei modelli 730, 770, CUD ed Unico a seguito dell'abrogazione, da parte dell'art. 7 della legge 3 giugno 1999, n. 157, della norma che consentiva ai contribuenti di destinare la quota del 4 per mille dell'Irpef al finanziamento dei partiti e dei movimenti politici (art. 1, l. n. 2/1997).

Rispetto ai modelli dell'anno precedente, il testo completo dell'informativa è stato poi collocato nelle istruzioni in appendice, lasciando ad una nota sintetica sul frontespizio il compito di fornire una prima informazione e di operare il necessario rinvio.

L'Autorità ha fornito, in data 3 febbraio 2000, il proprio parere positivo su tali modifiche, formulando solo alcune osservazioni di secondario rilievo. Con l'occasione, il Ministero ha informato il Garante della scelta di utilizzare per le dichiarazioni da presentarsi nel 2000 lo stesso modello di busta impiegato nell'anno precedente; anche in questa circostanza l'Autorità ha preso atto delle assicurazioni fornite dall'Amministrazione finanziaria circa la non estraibilità delle dichiarazioni dalle aperture praticate su tale busta, assicurazioni che sarebbero peraltro confermate dall'assenza di segnalazioni pervenute durante l'anno passato.

2.2 Sanità

2.2.1
Profili
generali

A distanza di circa tre anni dall'entrata in vigore della legge n. 675/1996, il quadro normativo in materia di protezione dei dati personali idonei a rivelare lo stato di salute può dirsi notevolmente mutato, anche se l'efficacia di buona parte dei mutamenti dipenderà dalla prossima e doverosa adozione di alcuni atti.

La disciplina generale contenuta negli artt. 22 e 23 della legge n. 675 è stata infatti modificata a seguito dell'emanazione dei due decreti legislativi: 11 maggio 1999, n. 135 recante *"disposizioni integrative della legge n. 675 sul trattamento dei dati sensibili da parte dei soggetti pubblici"* e 30 luglio 1999, n. 282, che detta *"disposizioni per garantire la riservatezza dei dati personali in ambito sanitario"*.

Mentre il primo ha posto fine al regime transitorio che ha consentito ai soggetti pubblici di proseguire — da ultimo fino all'8 maggio 1999, previa comunicazione al Garante — il trattamento dei dati sensibili 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"* (artt. 22, comma 3 e 41, comma 5, l. n. 675/1996), con il secondo, in attuazione della delega contenuta nelle leggi n. 676/1996 e n. 344/1998, il legislatore ha integrato e modificato le disposizioni dell'art. 23 della l. n. 675, prevedendo innanzitutto una disciplina uniforme per il trattamento dei dati sulla salute da parte degli organismi sanitari pubblici nonché degli organismi sanitari e degli esercenti le professioni sanitarie in regime di convenzione o di accreditamento con il S.S.N. Al di fuori di questa disciplina restano esclusi solo gli esercenti le professioni sanitarie ed i soggetti privati estranei al S.S.N. Ciò mentre in precedenza, come ben noto, si distingueva nettamente la disciplina fra i *"soggetti pubblici"* (art. 22, comma 3), *"gli esercenti le professioni sanitarie e gli organismi sanitari pubblici"* (art. 23) e gli altri soggetti (art. 22).

Ai soggetti, pubblici o privati, operanti nell'ambito del S.S.N. si applica la disciplina di cui all'art. 23, primo comma della legge 675/1996, integrata da quanto previsto dai nuovi commi 1 bis, ter e quater dell'art. 23.

Ai soggetti estranei al S.S.N., sino all'adozione del codice di deontologia e di buona condotta di cui all'art. 17, comma 3, del d.lg. n. 135/1999 come modificato dall'art. 3 del d.lg. n. 282/1999, continua ad applicarsi rispettivamente la regola generale della doppia condizione del consenso scritto dell'interessato e dell'autorizzazione del Garante, ovvero la disciplina speciale prevista dall'art. 23, comma 1, della legge n. 675/1996.

Al riguardo si rammenta che l'Autorità, con provvedimento del 29 settembre 1999, ha rinnovato l'autorizzazione generale per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, la quale avrà efficacia fino al 30 settembre 2000 (autorizzazione n. 2/1999, pubblicata sulla *"Gazzetta Ufficiale"* n. 232 del 2 ottobre 1999). Il nuovo testo non contiene mutamenti di carattere sostanziale rispetto all'autorizzazione precedente, se non nelle parti in cui era necessario tener conto delle modificazioni intervenute a seguito dell'emanazione dei due decreti legislativi sopra menzionati.

Si segnala inoltre che, sulla base di una specifica richiesta, il Garante ha ritenuto di dover espressamente autorizzare il trattamento dei dati sulla salute anche per scopi di trapianto, *"limitatamente ai dati dei donatori e dei beneficiari e alle operazioni indispensabili all'effettuazione di trapianti di organi e tessuti, nonché di donazioni di sangue"* (capo 1.2, lett. g), autorizzazione n. 2/1999).

Tornando invece alla recente disciplina più innovativa e al decreto legislativo n. 135/1999 (per la cui compiuta trattazione si rinvia al par. 2.1.5), si nota che il suo nucleo centrale consiste nell'individuazione di alcune rilevanti finalità di interesse pubblico per il cui perseguimento è ora con-

sentito il trattamento dei dati sensibili da parte dei soggetti pubblici, purché nel rispetto di alcuni principi generali in materia di modalità del trattamento e di informativa agli interessati, di dati trattati e di operazioni eseguibili (artt. 2, 3 e 4 d.lg. n. 135).

I diversi soggetti pubblici sono vincolati ad effettuare i trattamenti di dati personali in materia sanitaria nel rispetto di alcune specifiche garanzie di riservatezza. Anzitutto l'art. 17 prevede che, in ciascun ambito di attività, l'interessato possa essere identificato dai soli soggetti che perseguono direttamente le finalità individuate nel comma 1 e che l'accesso ai dati sia consentito ai soli "incaricati" del trattamento preposti alle specifiche fasi delle diverse attività, secondo il principio della pertinenza dei dati di volta in volta trattati (art. 17, comma 2, d.lg. n. 135/1999).

Al riguardo il Garante, in più pareri resi al Ministero della sanità nell'esercizio della sua funzione consultiva (art. 31, comma 2, della legge n. 675), ha segnalato la necessità di provvedere al più presto, ove non si sia già provveduto, alla nomina dei "responsabili" e degli "incaricati" del trattamento ai sensi degli articoli 8 e 19 della legge n. 675; ciò anche al fine di assicurare il rispetto delle disposizioni del regolamento in materia di sicurezza, le quali prevedono, per l'accesso alle operazioni di trattamento dei dati c.d. "particolari", che siano rilasciate agli incaricati del trattamento o della manutenzione specifiche autorizzazioni da parte del titolare o, se designato, del responsabile (art. 5, d.P.R. 28 luglio 1999, n. 318).

Nella stessa ottica di garanzia, i principi generali contenuti nel capo I del d.lg. n. 135/1999 stabiliscono che "i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo" e che il trattamento di tali dati deve sempre avvenire con "tecniche di cifratura o codici identificativi che consentano di identificare gli interessati solo in caso di necessità" (art. 3, comma 5, d.lg. n. 135/1999).

Quest'ultima garanzia è peraltro estesa al trattamento di tutti i dati sensibili, qualora essi siano contenuti in elenchi, registri o banche dati gestite con l'ausilio di mezzi elettronici o comunque automatizzati (art. 3, comma 4, d.lg. n. 135/1999).

In relazione a tali principi il Garante, nel corso di questo anno di attività, si è trovato più volte a dover sottolineare che si tratta di disposizioni immediatamente efficaci, la cui osservanza è quindi obbligatoria per tutti i soggetti pubblici sin dal maggio 1999 (si veda, ad esempio, il provvedimento del 1° dicembre 1999).

In particolare, per quanto attiene l'ambito sanitario, nel capo II del suddetto decreto, l'articolo 17, specificamente dedicato alla "tutela della salute", riconoscendo la rilevante finalità di interesse pubblico di una serie di attività rientranti nei compiti del servizio sanitario nazionale e degli altri organismi sanitari pubblici, ha sancito la legittimità di ogni trattamento di dati sulla salute che si svolga nell'ambito di tali attività nel rispetto dell'art. 23, comma 1, della l. n. 675.

Allo stesso modo i successivi articoli 18, 19 e 20 considerano di rilevante interesse pubblico i trattamenti dei dati volti all'applicazione della disciplina relativa all'interruzione volontaria della gravidanza, alla cura e riabilitazione dei tossicodipendenti e all'assistenza dei portatori di handicap.

Come si è detto, l'impianto delineato dall'art. 17 del d.lg. n. 135 è stato successivamente integrato dal d.lg. 30 luglio 1999, n. 282, il quale è stato emanato in attuazione della delega contenuta nelle leggi nn. 676/1996 e 344/1998, per la disciplina della riservatezza dei dati personali in ambito sanitario.

Con esso, in particolare, il legislatore ha fissato i criteri direttivi cui dovrà uniformarsi il decreto del Ministro della sanità nell'individuare modalità semplificate per le informative e per la prestazione del consenso nei confronti di organismi sanitari pubblici, di organismi sanitari e di eser-

centi le professioni sanitarie convenzionati o accreditati dal S.S.N., nonché per il trattamento dei dati da parte dei medesimi soggetti (art. 23 l. n. 675/1996, come integrato dall'art. 2, comma 1, d.lg. n. 282/1999).

La novità sostanziale di tale decreto delegato sta infatti nell'aver integrato per i soggetti surrichiamati l'art. 23 della legge n. 675, prevedendo rilevanti semplificazioni in materia di informativa e di consenso.

Mentre la prima potrà essere effettuata anche da un unico soggetto, in particolare dal medico di medicina generale scelto dall'interessato, per conto di più titolari del trattamento, il consenso, non più necessariamente scritto, ma anche semplicemente documentato per iscritto, potrà essere validamente prestato nei confronti di tutti gli operatori della "catena sanitaria" previsti nell'informativa (art. 23, comma 1bis, lett. a) e b) l. n. 675/1996).

Infine, recependo le istanze degli operatori sanitari che, nella prima fase di applicazione della legge, avevano rappresentato la difficoltà di acquisire il consenso in alcune situazioni particolari, il d.lg. n. 282, da un lato, ha disposto che nel caso in cui la persona bisognosa di cure si trovi in stato di incapacità di agire, ovvero di impossibilità fisica o di incapacità di intendere o di volere, il consenso può essere validamente manifestato da altri soggetti, ovvero da chi esercita la potestà genitoriale o di tutela, da un familiare, da un prossimo congiunto, da un convivente o, in loro assenza, dal responsabile della struttura presso cui l'interessato dimora; d'altra parte, lo stesso decreto legislativo ha rimesso al decreto del Ministro della sanità il compito di identificare quelle situazioni d'urgenza nelle quali l'informativa e il consenso dell'interessato possono intervenire successivamente alla raccolta ed al trattamento dei dati (art. 23, commi 1bis, lett. c) e 1quater, l. n. 675/1996).

Le semplificazioni previste dal decreto legislativo n. 282 - che in larga parte troveranno precisa definizione ed attuazione nel regolamento ministeriale che sarà emanato previo parere della Conferenza permanente Stato-regioni e del Garante - dovranno coordinarsi, se non essere analoghe, con quanto stabilito nei codici di deontologia e di buona condotta, adottati dalle rappresentanze dei soggetti privati e degli esercenti le professioni sanitarie estranei al S.S.N., ai sensi dell'art. 31, comma 1, lett. h) della legge n. 675 (si veda, in proposito, il par. 3.6, relativo all'avvio dei codici deontologici).

L'art. 17 del d.lg. n. 135 stabilisce infatti che, per quanto non previsto dal regolamento ministeriale, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale è fatto oggetto di appositi codici deontologici. Questi devono prevedere modalità semplificate per l'informativa e per la prestazione del consenso, nonché regole di condotta analoghe al segreto professionale per quegli incaricati del trattamento che non sono tenuti per legge al vincolo del segreto (art. 17 comma 3, d.lg. n. 135/1999 come modificato dall'art. 3 d.lg. n. 282/1999).

Un ulteriore aspetto che dovrà essere oggetto di disciplina da parte del regolamento ministeriale e dei codici deontologici è la previsione di modalità che consentano anche ai professionisti sanitari diversi dai medici, che intrattengono rapporti diretti con i pazienti, di comunicare all'interessato (o agli altri soggetti individuati nell'art. 23, comma 1quater) le informazioni relative al suo stato di salute (v. art. 23, comma 2, l. n. 675/1996; art. 17, comma 3, lett. b) d.lg. n. 135/1999; art. 2, comma 1, lett. d) d.lg. n. 282/1999).

Il decreto legislativo recante "disposizioni per garantire la riservatezza dei dati personali in ambito sanitario" non poteva inoltre tralasciare la complessa problematica relativa alle prescrizioni mediche, già oggetto di ampi dibattiti in occasione del c.d. "decreto Di Bella" (per il quale si rinvia alla Relazione annuale per l'anno 1997, pagg. 38 e 81).

In particolare, l'art. 4, dopo aver fatto salvi i casi in cui norme speciali prevedono che le ricette siano rilasciate in forma anonima o con particolari annotazioni (ovvero quelli indicati dal c.d.

decreto Di Bella), rinvia anch'esso ad un decreto del Ministro della sanità per l'individuazione dei medicinali la cui prescrizione non necessita dell'indicazione delle generalità dell'interessato (art. 4, comma 1, d.lg. n. 282/1999).

D'altra parte il medesimo decreto, per la cui adozione sarebbe stato fissato il termine del 1° aprile 2000, dovrà prevedere un apposito modello per la prescrizione di medicinali a carico, anche parziale, del servizio sanitario nazionale. Tale modello, la cui utilizzazione sarà obbligatoria decorso diciotto mesi dall'entrata in vigore del decreto che lo disciplina, deve essere configurato in modo da permettere di risalire all'identità dell'interessato solo ove ciò sia necessario per controllare la correttezza della prescrizione, per effettuare verifiche amministrative ovvero per scopi epidemiologici e di ricerca (art. 4, comma 2).

Laddove invece, come ai sensi del testo unico in materia di tossicodipendenze, è fatto obbligo di accertare l'identità dell'interessato, le ricette sono conservate separatamente da ogni altro documento che non ne richieda l'utilizzazione.

Un'ultima disposizione riguarda la conservazione e la distruzione delle ricette da parte del farmacista: sono conservate per il periodo prescritto e successivamente distrutte con modalità che escludono l'accesso di terzi ai dati contenuti nelle stesse (art. 4, comma 5).

Il trattamento dei dati genetici è stato oggetto di particolare attenzione da parte del Garante sin dall'emanazione della prima autorizzazione generale al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/1997, punto 2, lett. b).

2.2.2
Dati
genetici

Tale provvedimento (come i successivi rinnovi), con alcune esclusioni soggettive e limitazioni nelle finalità, ma soprattutto nel presupposto del consenso scritto dell'interessato, autorizza il trattamento dei 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"*. È invece necessaria un'apposita autorizzazione del Garante nel caso in cui il trattamento sia finalizzato alla tutela della salute di un terzo o della collettività e l'interessato non abbia prestato il proprio consenso.

Il quadro normativo è parzialmente mutato con i decreti delegati 135 e 281 del 1999, che prevedono un'apposita e speciale autorizzazione per il solo trattamento dei dati genetici, *"da chiunque effettuato"* (art. 17, comma 5, del d.lg. n. 135/1999, come integrato e modificato dall'art. 16 del d.lg. 30 luglio 1999, n. 281), con anche la prescrizione di uno speciale procedimento (*"sentito il Ministro della sanità, che acquisisce a tal fine il parere del Consiglio superiore di sanità"*).

Nelle more di questa autorizzazione, che dovrà essere rilasciata dal Garante entro il maggio 2000, i trattamenti di dati genetici possono essere iniziati o proseguiti nel rispetto delle prescrizioni contenute nell'autorizzazione n. 2/1999, tra cui in particolare il divieto della loro comunicazione a terzi.

Questi erano i riferimenti normativi entro i quali si è mossa l'Autorità nel decidere in merito alla richiesta di autorizzazione presentata da due coniugi che intendevano acquisire i dati sanitari contenuti nella cartella clinica del padre della richiedente, anche in assenza del consenso di quest'ultimo.

In tale occasione il Garante, ai sensi dell'art. 23 della legge n. 675, ha autorizzato l'ospedale universitario - presso il quale era in corso un'indagine genetica a scopo procreativo - ad acquisire i dati suddetti, sulla base della considerazione che il diritto al benessere psico-fisico della donna, ovvero ad una sua scelta riproduttiva consapevole ed informata, dovesse prevalere sul diritto alla assoluta riservatezza dell'interessato (provvedimento del 22 maggio 1999, in Bollettino n. 8, p. 13).

2.2.3
Ricerca medica
ed
epidemiologica

La peculiarità delle problematiche poste dalla ricerca medica ed epidemiologica rispetto alla ricerca scientifica in genere spiega la scelta di disciplinare tale materia in modo più specifico nell'ambito del d.lg. n. 282, piuttosto che solo in quello recante *"disposizioni in materia di trattamento di dati personali per finalità storiche, statistiche e di ricerca scientifica"* (d.lg. 30 luglio 1999, n. 281), al quale comunque deve farsi riferimento per la disciplina degli aspetti generali della ricerca e del ruolo del codice di deontologia e di buona condotta, il cui rispetto anche in quest'ambito "costituisce condizione essenziale per la liceità del trattamento dei dati" (si vedano i par. 2.4 e 3.6 di questa relazione).

Con l'art. 5 del d.lg. n. 282 il legislatore delegato ha introdotto un'importante semplificazione: il trattamento dei dati idonei a rivelare lo stato di salute per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico può essere effettuato senza il consenso dell'interessato, a condizione che la ricerca sia prevista da un'espressa disposizione di legge o rientri nel programma di ricerca biomedica o sanitaria contemplata dall'art. 12 bis della legge 30 dicembre 1992, n. 502.

In tutti gli altri casi devono essere osservate le prescrizioni contenute e richiamate nel capo 1.2 dell'autorizzazione n. 2/1999, in attesa di eventuali modificazioni conseguenti all'adozione del regolamento ministeriale di cui al comma 1 bis dell'art. 23 della legge 675/1996, quale introdotto dall'art. 2 del d.lg. n. 282.

La previsione dell'art. 5 sopra citato, che consente di prescindere dal consenso dell'interessato, ha destato l'allarme della Lega italiana per la lotta all'AIDS, la quale ha chiesto al Garante di chiarire se essa debba considerarsi applicabile anche in materia di sorveglianza epidemiologica dei casi di infezione da HIV.

A tale riguardo, con provvedimento del 16 febbraio 2000, l'Autorità ha precisato che il d.lg. n. 282/1999, in quanto reca disposizioni di modifica ed integrazione della legge n. 675/1996 in relazione al trattamento dei dati personali in ambito sanitario, non può ritenersi in contraddizione con il principio generale che fa salve le disposizioni di legge che prevedono limiti più restrittivi, tra cui in particolare la normativa contenuta nella legge 5 giugno 1990, n. 135, la quale impone il mantenimento di un rigoroso rispetto della riservatezza delle persone affette da AIDS (art. 43, comma 2, l. n. 675). Pertanto — ha chiarito il Garante — benché non espressamente richiamate nel testo del d.lg. n. 282, restano ferme le disposizioni della legge n. 135/1990 le quali prevedono, da un lato, che *"nessuno può essere sottoposto, senza il suo consenso, ad analisi tendenti ad accertare l'infezione da HIV, salvo che per motivi di necessità clinica e nel proprio interesse"* e, dall'altro, che *"la rilevazione statistica della infezione da HIV deve essere comunque effettuata con modalità che non consentano l'identificazione della persona"* (art. 5, commi 2 e 3, l. n. 135/1990).

Per completezza di esposizione si segnala che, sempre con riferimento al rapporto tra le disposizioni della legge n. 675/1996 e quelle della normativa in materia di prevenzione e lotta contro l'AIDS, il Garante ha esaminato la questione relativa alla legittimità della comunicazione al tribunale per i minorenni che decide circa l'affidamento preadottivo, dei dati relativi alla sieropositività degli aspiranti genitori adottivi (si veda il provvedimento del 15 luglio 1999, in Bollettino n. 9, p. 77).

Anche in questa occasione, confermando la piena vigenza delle disposizioni della legge n. 135/1990 (in particolare, art. 5, commi 1 e 4), l'Autorità ha ritenuto che il medico del servizio di medicina legale che compie i dovuti accertamenti (tra cui quello per l'infezione HIV, sulla base del consenso scritto degli interessati), possa comunicare il risultato diagnostico direttamente ed esclusivamente all'interessato e debba invece trasmettere al tribunale per i minorenni una relazione medica da cui si evinca soltanto un giudizio complessivo circa la sussistenza di eventuali condizioni di rischio o patologiche che possono minacciare l'interesse del minore.

D'altra parte, valutando l'eventuale necessità che il tribunale, in virtù di specifici vincoli

derivanti da obblighi internazionali ratificati con legge, debba acquisire il risultato dell'accertamento dell'AIDS o dell'infezione HIV, l'Autorità ha suggerito di adottare una prassi secondo la quale ciascuno dei coniugi, informato dal medico in ordine alle proprie condizioni di salute, provveda personalmente a produrre la documentazione al tribunale dei minorenni. Questa soluzione infatti, pur non ostacolando in nessun modo lo svolgimento dei procedimenti per le adozioni, realizzerebbe un adeguato bilanciamento tra l'interesse dei minori "ad un ambiente familiare stabile ed armonioso, nel quale essi possano crescere sviluppando la loro personalità in un sano ed equilibrato contesto di vita, affettivo ed educativo" (Corte Cost. 24 luglio 1995, n. 361) e il diritto degli adottanti al rispetto della propria dignità e riservatezza.

La previsione di sperimentazioni della carta sanitaria elettronica, contenuta nell'art. 59, comma 50, lett. i), della legge 27 dicembre 1997, n. 449 e nel decreto-legge 28 dicembre 1998, n. 450 convertito, con modificazioni, dalla legge 26 febbraio 1999, n. 39, risultava priva di una normativa a tutela della riservatezza degli interessati ed idonea a delimitare il possibile contenuto della stessa tessera, nonché a definire i livelli di accesso ai dati memorizzati. Il legislatore delegato è quindi intervenuto a fissare alcuni principi fondamentali in materia di protezione dei dati sanitari ed a stabilire alcune garanzie nelle fasi di formazione e di corretta utilizzazione delle carte sanitarie elettroniche.

2.2.4
Tessera
sanitaria

L'art. 6 del d.lg. n. 282/1999 infatti, da un lato dispone che gli interessati, ai quali sia stata preventivamente fornita l'informativa prevista dall'art. 10 della legge n. 675, possono opporsi all'inserimento nella tessera sanitaria elettronica di quei dati sulla salute che "eccedano i dati relativi alla gestione amministrativa e alle situazioni di urgenza, quali definite a livello internazionale"; dall'altro prevede espressamente che il decreto del Ministro della sanità previsto dall'art. 2, comma 1, del d.l. n. 450/1998, convertito con modificazioni dalla legge n. 39/1999, determini anche le categorie di incaricati delle aziende sanitarie locali e di operatori sanitari che possono accedere ai diversi dati inseriti nelle carte, nonché le categorie professionali tenute ad inserirli e il periodo massimo entro il quale i dati devono essere aggiornati.

2.3 Lavoro e previdenza sociale

La complessa disciplina normativa concernente il trattamento dei dati personali nell'ambito del rapporto di lavoro, specie per quanto riguarda la tenuta delle liste degli iscritti al collocamento da parte del Ministero del lavoro e della previdenza sociale e, ora, delle Regioni, ha reso necessario uno specifico intervento dell'Autorità (provvedimento del 17 febbraio 1999, in Bollettino n. 7, p. 59). In tale occasione è stato suggerito al Ministero di valutare l'esistenza delle condizioni per una modifica delle attuali norme sul collocamento in modo tale da consentire il rilascio, ai datori di lavoro privati che ne facciano richiesta, dell'elenco degli iscritti al collocamento a fini di assunzione. Il Garante ha dunque richiamato l'attenzione del Ministero sulla opportunità di intervenire sulla normativa allo scopo di ampliare il regime di pubblicità delle liste di collocamento tenuto conto che nell'attuale legislazione, anche dopo l'introduzione del Sistema informativo lavoro (SIL) che naturalmente incide sulla conoscibilità dei dati relativi ai lavoratori, è esclusa espressamente la pubblicità di tali liste di collocamento in favore di privati che non siano società autorizzate ad operare nel campo della mediazione di manodopera.

2.3.1
il rapporto
di lavoro

In proposito, nell'ambito dell'attività consultiva prevista dall'art. 31, comma 2, della legge n. 675/1996, il Garante ha espresso un parere in data 30 novembre 1999 (in Bollettino n. 10, p. 27) in merito allo schema di regolamento riguardante il riordino di alcune procedure per il collocamento pubblico. Detto schema di provvedimento ha lo scopo di facilitare l'incontro della domanda e dell'offerta di lavoro nel rispetto della competenza delle regioni, garantendo l'efficace attivazione sul territorio nazionale del Sistema Informativo Lavoro (SIL). In proposito il Garante ha ritenuto necessario specificare, in via generale, che l'intento di ampliare il regime di pubblicità delle liste di collocamento deve prevedere, in conformità ai principi fissati dalla legge n. 675, l'introduzione di un quadro di maggiore precisione dei flussi di informazioni in cui siano specificati i vari ambiti di divulgazione dei dati.

In tale occasione l'Autorità ha formulato forti perplessità in merito alla possibilità di istituire una *"scheda professionale"* del lavoratore senza preventivamente chiarire la concreta funzione di tale strumento, né le modalità del trattamento dei dati in essa riportati, tenuto conto che tali informazioni riguarderebbero anche le esperienze formative e professionali del lavoratore. Analoghe riserve sono state formulate anche in ordine alla possibilità che le regioni possano autonomamente disciplinare il rilascio di una *"carta elettronica personale"* del lavoratore, in mancanza di un quadro normativo d'insieme che tenga conto della recente disciplina della carta d'identità elettronica introdotta dal d.P.C.M. n. 437 del 1999.

Sempre nell'ambito dell'attività consultiva, il Garante, con parere del 9 novembre 1999, si è espresso in merito alla legge approvata dal Consiglio regionale del Friuli Venezia Giulia per le semplificazioni dei procedimenti in materia di lavoro, cooperazione ed artigianato. In tale occasione l'Autorità ha evidenziato che qualsiasi disposizione normativa, anche di rango regionale, concernente il trattamento dei dati personali nell'ambito del rapporto di lavoro deve ritenersi superflua, in quanto le varie rilevanti finalità di interesse pubblico connesse alla gestione di rapporti di lavoro sono già individuate, per la globalità delle amministrazioni pubbliche, dall'art. 9 del d.lg. 11 maggio 1999, n. 135. È stato così ricordato che le amministrazioni interessate devono soltanto promuovere l'adozione di apposite fonti normative secondarie in cui vengano identificati e resi pubblici i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite.

Sotto altro profilo, l'originaria mancanza di una specifica normativa concernente il trattamento dei dati personali degli studenti da parte di istituti scolastici che abbiano intenzione di agevolare l'inserimento professionale comunicandone gli esiti scolastici, ha reso necessario nell'aprile 1999 uno specifico intervento dell'Autorità (non pubblicato nel Bollettino) per suggerire al Ministero della pubblica istruzione di promuovere l'adozione di un'apposita disposizione legislativa o regolamentare, per disciplinare in modo omogeneo i presupposti, le finalità e le garanzie dell'eventuale rilascio degli elenchi dei diplomati nei confronti di aziende e di altri soggetti, anche per scopi diversi da quelli di assunzione, ma ugualmente meritevoli di considerazione. Una previsione normativa in tal senso è stata successivamente introdotta dal legislatore delegato con il d.lg. 30 luglio 1999, n. 281 (cfr. par. 2.1.3 di questa relazione).

Il provvedimento del Garante del 29 settembre 1999 (in Bollettino n. 9, p. 144) contiene l'autorizzazione al trattamento dei dati a carattere giudiziario da parte di privati e di enti pubblici economici. In particolare, alla stregua del precetto contenuto nell'art. 24 della legge n. 675, 1996, il Garante ha predisposto un'autorizzazione a carattere generale con riguardo ai dati idonei a rivelare i provvedimenti che sono oggetto di iscrizione al casellario giudiziale, riguardanti le condanne in materia penale e gli altri provvedimenti di restrizione della libertà personale (art. 686 del codice di procedura penale).

Tale autorizzazione coinvolge anche il rapporto di lavoro, nel senso che autorizza il trattamento dei dati riguardanti il lavoratore (o il soggetto in procinto di stipulare il contratto di lavoro),

trattamento che può essere effettuato dal datore di lavoro ovvero da soggetti i quali svolgano un'attività di composizione delle controversie.

Per quanto attiene alle finalità del trattamento, l'autorizzazione riproduce, in gran parte, quella generale in materia di rapporti di lavoro (autorizzazione n. 1/1999 rinnovata il 29 settembre 1999 e pubblicata nel Bollettino n. 9, p. 115), per cui il trattamento deve essere strettamente necessario per l'adempimento degli obblighi previsti da leggi, regolamenti, contratti collettivi, normativa comunitaria e ai soli fini della gestione del rapporto di lavoro (una disamina approfondita delle autorizzazioni generali al trattamento dei dati sensibili è stata svolta nella Relazione per l'anno 1998, p. 95). Tale previsione - la quale si iscrive, peraltro, all'interno del generale criterio di finalità che caratterizza l'intera normativa sul trattamento dei dati (art. 9 della legge n. 675 del 1996) - limita la possibilità di trattare tali dati al solo caso in cui il disposto legale o contrattuale consenta il predetto trattamento.

Nell'ambito della disciplina del rapporto di lavoro, il datore di lavoro viene necessariamente a conoscenza di numerosi dati personali dei lavoratori, sia per la costituzione sia per lo svolgimento del rapporto lavorativo.

In tale contesto la legge n. 675 del 1996 prevede che si rispetti il principio di non eccedenza dei dati rispetto alle finalità per le quali sono raccolti e successivamente trattati (art. 9, primo comma, lett. d)). Sotto quest'ultimo profilo, assume particolare significato il principio della finalità del trattamento, il quale costituisce il vincolo che autorizza la raccolta e il trattamento dei dati solo con riguardo allo scopo attinente all'esecuzione della prestazione lavorativa.

Con riguardo a tale aspetto, occorre considerare che molto spesso il trattamento può essere imposto dalla legge (si pensi agli obblighi di documentazione e di informazione in riferimento all'assunzione del lavoratore e alle caratteristiche del rapporto di lavoro), ovvero è funzionale all'esecuzione della prestazione lavorativa (in materia di retribuzione, di assegnazione a mansioni, di trasferimenti, di sospensione del rapporto, di mobilità o di licenziamento, ecc.).

In tale contesto, quindi, i pronunciamenti dell'Autorità hanno consentito di chiarire alcuni dubbi o incertezze interpretative in ordine alla liceità di alcuni trattamenti di dati personali svolti da soggetti pubblici e privati nell'ambito del rapporto di lavoro.

Un particolare rilievo deve attribuirsi alla decisione del Garante adottata il 2 giugno 1999 (in Bollettino n. 9, p. 34) relativa alle valutazioni che contribuiscono a formare il giudizio annuale sul rendimento di un dipendente, le cosiddette "note di qualifica", stabilendo che esse sono dati personali e devono essere messe a disposizione del dipendente che ne faccia richiesta.

L'importante principio stabilito si fonda sull'ampia nozione di dato personale contenuta nella legge n. 675 del 1996, dal momento che le note di qualifica forniscono un contributo aggiuntivo di valutazione rispetto ad un soggetto identificato. E questo in riferimento sia ad informazioni oggettive, sia a descrizioni, giudizi, analisi o ricostruzioni di profili personali (riguardanti attitudini, qualità, requisiti o comportamenti professionali) che danno origine a valutazioni complessive del soggetto interessato. In tal senso, quindi, deve ritenersi legittima la richiesta di accesso ai giudizi espressi in sede di formulazione delle note di qualifica, anche in considerazione del fatto che solo una piena conoscenza di tali elementi informativi permette al dipendente di poter attivare i meccanismi di ricorso interno o di eventuale tutela giurisdizionale.

Tra gli elementi che concorrono alla formazione del giudizio ve ne sono alcuni che hanno carattere obiettivo (il numero delle pratiche svolte, i giorni di assenza, ecc.) rispetto ai quali può certamente essere esercitato il diritto di correzione. Non si potrà, invece, chiedere la correzione dei giudizi espressi nell'ambito dell'attività di valutazione della prestazione lavorativa. Questi dati potranno semmai essere oggetto soltanto di un'eventuale richiesta di integrazione (attraverso l'inserimento di note o precisazioni a margine), diritto ugualmente previsto dall'art. 13 della legge n. 675.

L'esercizio del diritto di accesso è, comunque, subordinato al completamento della procedura di valutazione, e quindi non può essere fatto valere nelle fasi di preparazione delle schede di valutazione e delle finali note di qualifica. L'intervento del Garante è stato anche un'occasione per precisare che il datore di lavoro può prevedere misure idonee al fine di tutelare l'anonimato dell'autore delle valutazioni stesse.

Altrettanto importante è la risposta del 25 ottobre 1999 fornita ad un'associazione di categoria nella quale il Garante ha affermato che i dipendenti possono anche dare un consenso solo parziale al trattamento dei propri dati personali, fermo però restando che questa possibilità non deve portare ad un appesantimento degli adempimenti previsti dalla legge sulla protezione dei dati personali, né ad un suo uso strumentale.

Nel sancire questo principio è stato ricordato che la legge n. 675 del 1996 mira a garantire all'interessato il controllo sui flussi delle informazioni che lo riguardano. Uno degli strumenti perché ciò possa avvenire è appunto quello del consenso informato, posto come condizione affinché i trattamenti possano essere effettuati, fatti salvi alcuni casi specifici per il trattamento di categorie particolari di dati. La legge prevede esplicitamente che il consenso possa riguardare l'intero trattamento, oppure una o più operazioni (raccolta, elaborazione, conservazione, comunicazione, diffusione ecc.). È possibile, infatti, che, all'interno di un medesimo trattamento, siano considerate anche operazioni non strettamente necessarie al perseguimento della finalità principale per la quale esso viene svolto, oppure operazioni che comportino l'utilizzo di dati particolarmente delicati, per i quali, a tutela dell'interessato, sia necessaria la manifestazione di un consenso differenziato.

Tuttavia, la necessità di semplificare quanto più possibile gli adempimenti e di garantire la correttezza nei rapporti negoziali, rende auspicabile una considerazione unitaria delle operazioni relative ad un trattamento.

Si dovrà, quindi, evitare, sia da parte del datore di lavoro, sia del dipendente, di utilizzare in maniera strumentale le norme sulla riservatezza allo scopo di danneggiare o rendere più onerosa e difficile l'attività della controparte. In tal senso quindi dovrebbe ricorrersi ad una manifestazione di consenso differenziata solo nel caso in cui il datore di lavoro intenda effettuare trattamenti non rientranti nell'ordinaria gestione del rapporto stesso o caratterizzati da una marcata specificità. Il consenso non pregiudica, comunque, in alcun modo il diritto del lavoratore di verificare l'uso fatto dei suoi dati o di opporsi a specifiche forme di utilizzazione degli stessi ritenute non corrette o non giustificate.

Con il provvedimento del 4 giugno 1999 (in Bollettino n. 9, pag. 81) si è stabilito che le rilevazioni effettuate mediante "badge" magnetico e conservate in un archivio informatico costituiscono dati personali e possono essere quindi oggetto di una richiesta di accesso.

L'affermazione di tale principio discende dalla circostanza che la legge n. 675 definisce il concetto di dato personale in maniera particolarmente ampia, comprendendovi qualunque informazione che possa scaturire da dati alfanumerici, immagini, suoni, a prescindere dal supporto che contiene i dati e dalla forma in cui essi sono trattati. In tal senso sono quindi da considerarsi dati personali anche le registrazioni informatiche degli accessi.

Un altro intervento del Garante del 5 giugno 1999 ha riguardato il riconoscimento all'interessato del diritto di ottenere l'integrazione dei propri dati, in quanto può esistere un legittimo interesse della persona ad ottenere che i dati riguardanti il proprio stato di salute (nel caso specifico quelli risultanti dal foglio matricolare) siano esatti, aggiornati e completi.

Nel fornire un parere al Ministero del Lavoro e della previdenza sociale con provvedimento del 5 luglio 1999, con riferimento al trattamento di dati svolto da un soggetto privato per conto dello stesso Ministero in relazione ai tirocini avviati nell'ambito di progetti di formazione profes-

sionale (legge n. 845 del 1978), il Garante ha precisato che l'affidamento a privati di attività per fini istituzionali da parte di un'amministrazione pubblica è pienamente compatibile con le norme in materia di riservatezza. È stato infatti chiarito che il privato che svolga determinate attività per organismi pubblici, attraverso concessioni, appalti o convenzioni, può essere formalmente designato responsabile del trattamento o, in mancanza di tale designazione, va considerato come soggetto autonomo che tratta i dati.

Per quanto riguarda invece la possibilità per gli istituti di assistenza sociale di visionare le denunce di infortunio sul lavoro che i datori di lavoro segnalano al sindaco in quanto autorità locale di pubblica sicurezza, il Garante ha fatto presente (provvedimento del 21 ottobre 1999, in Bollettino n. 10, p. 76) che questi, annoverabili fra i soggetti di diritto privato, possano conoscere soltanto gli elenchi delle denunce di infortunio sul lavoro relative agli assistiti che abbiano loro conferito un mandato.

Il Garante con provvedimento del 12 luglio 1999 (in Bollettino n. 9, p. 51) ha affermato il principio che le amministrazioni pubbliche possono utilizzare i dati relativi a sentenze penali emesse nei confronti dei propri dipendenti al fine dello svolgimento dei procedimenti disciplinari. In tale circostanza è stato ricordato che il decreto legislativo n. 135/1999 rende ammissibili la raccolta e l'utilizzazione di questi dati da parte della pubblica amministrazione nell'ambito del rapporto di lavoro e, in particolare, per svolgere attività dirette all'accertamento della responsabilità disciplinare.

Un'interessante problematica sottoposta al Garante riguarda la compatibilità con la legge n. 675/1996 della decisione del datore di lavoro di effettuare alcune riprese televisive nelle varie fasi di lavorazione riguardanti un'attività artigianale, con il conseguente coinvolgimento in tali riprese anche di parte del personale dipendente. In tale circostanza il Garante con il provvedimento del 21 ottobre 1999 (in Bollettino n. 10, p. 91) ha ritenuto che il trattamento dei dati personali dei dipendenti possa ritenersi un trattamento temporaneo analogo a quello finalizzato alla pubblicazione occasionale di articoli o saggi, al quale si applicano le disposizioni della legge sulla riservatezza riguardo all'attività giornalistica, con la necessaria osservanza delle specifiche disposizioni della legge 675 e del codice deontologico dei giornalisti, con quindi anche il diritto del lavoratore di opporsi, per motivi legittimi, alla diffusione delle immagini raccolte. Ciò al di là del permanente divieto che riprese televisive siano finalizzate al controllo a distanza dell'attività dei lavoratori, di cui all'art. 4 dello Statuto dei lavoratori (legge n. 300/1970).

Le particolari garanzie previste dalla legge n. 675/1996 hanno trovato un risvolto applicativo anche con riferimento al regime di conoscibilità delle informazioni contenute nei c.d. "cedolini" dello stipendio. Si deve osservare, infatti, che alcune delle informazioni contenute in tale documento possono avere natura "sensibile" (sussidi di cura, indennità missione handicappati, iscrizione al sindacato, ecc.) o comunque richiederebbero particolari cautele nel trattamento (multe disciplinari, pignoramenti per alimenti o tasse, ecc.).

In tal senso quindi il Garante, con il provvedimento del 31 dicembre 1998 (in Bollettino n. 6, p. 100) ha precisato che per i dati la cui inclusione nel cedolino dello stipendio appaia necessaria nell'interesse del dipendente, andrebbero adottate opportune cautele a tutela della riservatezza, individuabili, ad esempio, nel suo inserimento in una busta, nel piegare e spillare il cedolino, nell'apportarvi una copertura delle parti che non riguardino dati di comune conoscenza (generalità, ufficio di appartenenza, ecc.), ovvero nell'introdurre una cd. "distanza di cortesia" agli sportelli.

In merito al più generale tema del regime di pubblicità della situazione patrimoniale relativa ai titolari di alcune cariche elettive o direttive, il Garante, nel provvedimento dell'8 giugno 1999

2.3.2
Conoscibilità
dei dati
contenuti
nei cedolini
dello stipendio

(in Bollettino n. 9, p. 7) ha evidenziato che le vigenti norme in materia non rendono in generale obbligatorio pubblicare i dati patrimoniali relativi a tali soggetti, né comunque comportano il diritto di conoscere, neanche da parte dei consiglieri comunali nell'esercizio del loro mandato, il contenuto dei "cedolini" dello stipendio. L'esigenza quindi dei consiglieri comunali di valutare con piena cognizione di causa la correttezza e l'efficacia dell'operato dell'ente locale, e di accedere, a tale scopo, ai documenti e a qualsiasi notizia o informazione utili ai fini dell'esercizio delle funzioni consiliari, può essere soddisfatto attraverso altre modalità, quali, ad esempio, la pubblicità della situazione patrimoniale dei dirigenti; l'esame dei contratti collettivi, destinati per loro natura ad un regime di diffusa conoscibilità; l'accesso alle deliberazioni e alle determinazioni riguardanti indennità e altri emolumenti corrisposti, adottate dall'amministrazione a favore dei dipendenti.

Sempre in tema di "cedolini" dello stipendio, il Garante (provvedimento del 9 giugno 1999 non pubblicato nel Bollettino) è intervenuto presso il Dipartimento della pubblica sicurezza del Ministero dell'Interno, a seguito di una circostanziata segnalazione, chiedendo di conoscere quali misure si intendessero adottare per adeguare alle norme sulla protezione dei dati personali le procedure attualmente in uso presso alcune Questure riguardo al trattamento dei dati contenuti nei cedolini dello stipendio dei dipendenti. Proprio in relazione a tale richiesta di informazioni, il Ministero dell'Interno ha comunicato all'Autorità (nota del 25 febbraio 2000) che avrebbe proceduto immediatamente ad adottare idonee procedure per garantire la riservatezza dei dati contenuti nei cedolini degli stipendi del personale.

2.2.3

Enti
previdenziali

Il problema della tutela dell'interessato di fronte al trattamento di dati personali si pone, naturalmente, anche con riguardo all'attività degli enti previdenziali.

In particolare, in relazione all'iniziativa assunta dal Ministro del lavoro e della previdenza sociale di pubblicare gli atti relativi alla dismissione del patrimonio immobiliare residenziale degli enti previdenziali, il Garante con provvedimento del 6 settembre 1999 (non pubblicato nel Bollettino) ha stabilito che è possibile rendere pubblici i dati degli inquilini, con l'accortezza di scegliere le relative modalità e di individuare quali informazioni, tra quelle che sono nella disponibilità degli enti, siano pertinenti e opportunamente divulgabili in rapporto anche alla finalità di trasparenza perseguita.

In proposito l'Autorità, già in diverse occasioni, menzionate anche nella Relazione al Parlamento per l'anno 1998, aveva evidenziato che la legge n. 675/1996 non pregiudica affatto le esigenze di trasparenza dell'attività amministrativa, specie quando sussista un interesse pubblico a verificare i criteri di utilizzazione di beni pubblici o la correttezza dell'operato di organi.

Questa compatibilità trova conferma nelle disposizioni del recente decreto legislativo n. 135/1999 che si riferiscono al buon andamento e all'imparzialità dell'azione amministrativa, alla pubblicità dell'attività istituzionale degli enti pubblici e alla trasparenza in materia di incarichi dei dipendenti pubblici.

In questo contesto, andrebbero osservate solo alcune cautele per evitare la diffusione di dati di cui risulti superflua la pubblicità, come quelli che possono riguardare, ad esempio, particolari situazioni personali e familiari o, eventualmente, il preciso indirizzo degli interessati, fatta salva comunque la possibilità di identificare la zona urbana e le caratteristiche dell'immobile.

La possibilità quindi per il Ministero di procedere alla stessa diffusione al pubblico dei suddetti dati non è preclusa, in linea generale, ferma restando la necessità che tale circostanza sia specificamente prevista da una norma di legge o da un regolamento (art. 27, comma 3, legge n. 675/1996).

2.4 Statistica, ricerca scientifica e ricerca storica

Nel testo originale della legge n. 675 non vi erano specifiche disposizioni che riguardassero i trattamenti aventi le finalità di ricerca scientifica, storica e statistica: gli unici riferimenti erano anzi di dubbia efficacia, essendo relativi alla previsione dell'esonero dalla preventiva acquisizione del consenso dell'interessato nel caso in cui il trattamento per fini di ricerca scientifica o di statistica riguardava dati anonimi (artt. 12, comma 1, lett. d) e 21, 4° comma lett. a)), nonché al rinvio, in quanto compatibile, alla normativa sulla statistica pubblica (art. 43, comma 2).

2.4.1
Attività
di ricerca
scientifica

Da queste iniziali previsioni si è opportunamente giunti ad una apposita disciplina di settore con l'emanazione del decreto legislativo 30 luglio 1999, n. 281, ("Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica"), con cui il Governo ha dato attuazione ad uno dei criteri di delega previsti dalla legge 31 dicembre 1996, n. 676, il cui termine di scadenza era stato prorogato dalla legge 6 ottobre 1998, n. 344.

Il riconoscimento di questa peculiarità trova fondamento nell'importante lavoro di elaborazione svolto a livello internazionale ed in particolare nella direttiva n. 95/46/CE che prevede discipline speciali rispetto ai principi generali in materia di trattamento dei dati personali per le attività svolte a fini storici, di ricerca e di statistica (si vedano i "considerando" nn. 29 e 40, nonché gli artt. 6, comma 1, e 32, comma 3). Coerentemente la legge delega n. 676/1996 ha richiamato il legislatore delegato al rispetto dei principi contenuti in alcune raccomandazioni del Consiglio d'Europa e tra queste la n. R. (83) 10, relativa alla protezione dei dati personali utilizzati a fini di ricerca scientifica e statistica, adottata il 23 settembre 1983 dal Consiglio d'Europa, e nelle loro "successive modificazioni", al chiaro scopo di permettere al legislatore delegato di tenere conto della Raccomandazione, all'epoca ancora in corso di adozione, n. R. (97) 18 del 30 settembre 1997 in materia di statistica.

Il decreto legislativo n. 281 fa propri i principi richiamati nella legge delega e definisce le procedure relative all'utilizzazione di dati personali a fini storici, di ricerca e di statistica in modo compatibile con la necessaria tutela del singolo, semplificando notevolmente gli adempimenti previsti dalla legge n. 675/1996 a tutela dei dati personali. A tal fine il testo interviene su tre direzioni:

- contiene disposizioni integrative alla legge n. 675/1996, a cominciare dalla fondamentale previsione dell'art. 3 del d. lg. n. 281 che, per questi tipi di trattamento, deroga alle disposizioni sulle finalità e sulla temporaneità della conservazione dei dati personali (art. 9, comma 1 bis, l. 675). Inoltre si prevede la possibilità di effettuare la notificazione in forma semplificata o in alcuni casi addirittura di prescindere, purché questi trattamenti siano effettuati nel rispetto delle normative nazionali e comunitarie e dei codici di deontologia e di buona condotta (art. 2 d.lg. 281). Infine, l'art. 4 del d. lg. n. 281 esclude che questi trattamenti necessitino di forme di consenso per il trattamento, per la comunicazione e per il trasferimento all'estero di dati comuni, sempre se ciò viene effettuato "nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'art. 31";
- introduce alcune modifiche alla normativa vigente nei diversi settori coinvolti ed in particolare al d.lg. 6 settembre 1989, n. 322 ("Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica") ed al decreto legislativo 20 settembre 1963, n. 1409 ("Norme relative all'ordinamento e al personale degli Archivi di Stato");
- riconosce un ruolo molto rilevante ai codici di deontologia, la cui adozione diviene sostanzialmente obbligatoria in tali settori di attività e la cui adozione è stata promossa dal Garante entro sei mesi dall'entrata in vigore del decreto legislativo; inoltre, una volta che il Garante ne abbia

verificato positivamente la legalità, verranno pubblicati sulla Gazzetta ufficiale (sui codici di deontologia in generale si veda il par. 3.6 di questa relazione). Tali codici non sono quindi da intendere come un insieme di norme di etica professionale idonee a tracciare principi o regole di comportamento affidati alla sola eventuale reattività disciplinare dei soggetti professionali interessati, ma assumono uno specifico rilievo giuridico, in quanto il loro rispetto, per l'art. 6, comma 2, del d.lg. n. 281, diviene "condizione essenziale per la liceità del trattamento dei dati". Inoltre, come abbiamo appena visto, solo il rispetto delle disposizioni dei codici di deontologia e di buona condotta permette di ridurre fortemente una serie di vincoli nel trattamento dei dati personali. Ed infine le specifiche disposizioni che prevedono i codici di deontologia nel settore della ricerca storica, della statistica e della ricerca medica, attribuiscono solo a questi atti la possibilità di introdurre ulteriori deroghe alla legislazione generale sulla tutela dei dati personali (cfr. artt. 7 e 10 d.lg. 281/1999; art. 17, comma 3, modificato dall'art. 3 del d.lg. 282/1999).

In attesa dell'entrata in funzione delle nuove disposizioni, largamente dipendenti dall'adozione dei codici di deontologia e, per il settore dei dati medici, di alcune disposizioni normative del Ministero della sanità, continuano a svolgere un ruolo fondamentale le autorizzazioni generali emanate dal Garante ai sensi dell'art. 41, comma 7, della legge n. 675 nel corso del 1999, al fine di permettere il trattamento da parte dei soggetti privati dei dati sensibili.

Nella autorizzazione n. 2 del 29 settembre 1999, relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale, si confermano sostanzialmente le indicazioni già presenti nei provvedimenti autorizzativi degli anni passati, valevoli per i trattamenti effettuati *"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 relazioni 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..."* (punto 1.2, lett. a)).

Nel provvedimento sono rinvenibili alcuni dei più importanti principi su cui si basa la disciplina a protezione dei dati personali e che possono essere così riassunti:

- il trattamento dei dati personali è consentito qualora la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi;
- 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;
- è necessario acquisire il consenso scritto nel caso in cui si trattino dati sensibili o attinenti a provvedimenti giudiziari;
- il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

La medesima autorizzazione, inoltre, come abbiamo accennato al par. 2.2.2, continua a disciplinare provvisoriamente anche il trattamento dei dati genetici.

Altri provvedimenti autorizzativi generali considerano nel loro testo le finalità in esame. Anche l'autorizzazione numero 3/1999 al *"trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni"*, richiama al punto 1, lett. c), tra le finalità del trattamento quelle relative alla ricerca scientifica.

L'autorizzazione n. 7/1999, relativa al trattamento di dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici, si riferisce ad attività di ricerca allorché disciplina le condizioni dell'attività di documentazione, studio e ricerca in campo giuridico (come

è noto, questa particolare autorizzazione che riguarda i dati indicati all'art. 24 della legge n. 675 è configurata dal legislatore come alternativa alla stessa disciplina legislativa). In particolare, questa autorizzazione permette la diffusione di dati relativi a precedenti giurisprudenziali in ragione sia dell'affinità che tali attività presentano con quelle di manifestazione del pensiero, già disciplinate dagli articoli 12, 20 e 25 della legge n. 675/1996, sia della possibile adozione di norme volte a favorire lo sviluppo dell'informatica giuridica.

Il trattamento di dati personali per finalità di statistica è stato considerato nel corso del 1999 in vari provvedimenti legislativi.

È anzitutto il caso del decreto legislativo 11 maggio 1999, n. 135 (vedi par. 2.1.5) che, nel dettare le regole al trattamento di dati sensibili effettuato da soggetti pubblici, individua alcune rilevanti finalità di interesse pubblico e tra queste vi comprende anche i trattamenti effettuati a fini di "statistica" (art. 22) e quelli di "ricerca storica e archivi" (art. 23).

Inoltre, come evidenziato nel paragrafo precedente, la disciplina del trattamento di dati personali per finalità di ricerca contenuta nel decreto legislativo 281/1999, si riferisce espressamente anche all'attività svolta per fini statistici.

In questo decreto delegato, infatti, viene delineato l'ambito del trattamento dei dati personali per finalità statistiche, mediante l'individuazione dei requisiti e delle modalità di trattamento, di conservazione e di comunicazione dei dati personali utilizzati a tali fini.

Il testo, nel tenere in debito conto l'attuale dibattito in materia di statistica, contiene una disciplina flessibile applicabile sia alla statistica pubblica, sia alla statistica privata non compresa nel Sistema statistico nazionale, e prevede oltre alle disposizioni integrative e correttive alla legge n. 675/1996, alcune modifiche al decreto legislativo n. 322 del 1989 relativo a norme sul "Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica".

In particolare è prevista un'importante disposizione che riguarda la possibilità che il consenso relativo ai dati di carattere sensibile possa essere prestato con le modalità semplificate che saranno determinate dal codice deontologici (art. 10, comma 4, d.lg. n. 281).

Inoltre, come già visto nel precedente paragrafo, vengono ampliati i casi di esclusione dal consenso anche nel caso del trattamento di dati comuni finalizzato a scopi statistici effettuato nel rispetto dei codici di deontologia e buona condotta (artt. 12, 21 e 28 della legge n. 675).

Oltre ai decreti legislativi appena citati, la statistica è stata oggetto di considerazione anche nelle autorizzazioni al trattamento dei dati sensibili da parte dei soggetti privati che sono state adottate dal Garante in data 29 settembre 1999.

In tal senso l'autorizzazione n. 5/1999, relativa al "trattamento dei dati sensibili da parte di diverse categorie di titolari", dedica l'intero Capo II alla attività di sondaggi e ricerche.

In quest'ultima autorizzazione è precisato che il trattamento dei dati sensibili per tali scopi deve riguardare i dati attinenti ai soggetti che abbiano manifestato il proprio consenso informato, manifestato in ogni caso per iscritto, 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.

Anche in questo provvedimento il Garante ha richiamato l'attenzione su diversi principi che governano la normativa a tutela dei dati personali:

- 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;

2.4.2
Trattamento
di dati
personali
per finalità
di statistica

- 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;
- 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;
- 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, sempreché non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili;
- vi è l'obbligo di informare l'interessato, ai sensi dell'art. 10, commi 1 e 3, della legge n. 675/1996, anche quando i dati sono raccolti presso terzi;
- i dati 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.

Il Garante nel corso del 1999, oltre ad aver seguito con attenzione l'elaborazione dei decreti delegati prima citati e ad aver adottato le autorizzazioni generali a cui ci si è riferiti nel presente paragrafo ed in quello precedente, ha fornito pareri su una serie di richieste specifiche.

In tal senso appaiono interessanti le indicazioni fornite all'I.S.T.A.T. nel provvedimento del 2 agosto 1999 (in Bollettino n. 9, pag. 13) relativamente a una comunicazione di dati da effettuare verso un soggetto pubblico facente parte del Sistema statistico nazionale: anzitutto si ricorda che l'art. 27, comma 2, della legge n. 675 considera lecito lo scambio di dati tra soggetti pubblici in presenza di una norma di legge o di regolamento che preveda detta comunicazione, o in via del tutto subordinata, ove ciò sia necessario per lo svolgimento di funzioni istituzionali (in questo caso, previa apposita comunicazione al Garante).

Ulteriori argomentazioni sono state dedotte dal decreto legislativo 281: ci si è, infatti, riferiti all'art. 4, comma 9 del d.lg. n. 322/1989, parzialmente modificato dall'art. 12, comma 4, del d.lg. n. 281, secondo cui tra i dati tutelati dal segreto statistico *"non rientrano gli estremi identificativi di persone o di beni provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque"*; inoltre è stata richiamata l'attenzione su un'ulteriore disposizione in base alla quale i dati raccolti per uno scopo statistico possono essere trattati dai soggetti che fanno parte o partecipano al Sistema statistico nazionale e che operano per altri scopi statistici di interesse pubblico (art. 6-bis, comma 4, del d.lg. n. 322 introdotto dall'art. 11 del d.lg. n. 281).

Il Garante ha inoltre espresso il 21 febbraio 2000 il parere previsto all'art. 6-bis, comma 2, del d.lg. n. 322/1989 sul programma statistico nazionale 2000-2002. Pur nella valutazione positiva delle tutele relative al trattamento dei dati sensibili, l'Autorità ha richiamato la necessità di porre una maggiore attenzione sulle modalità per l'esercizio dei diritti di cui all'art. 13 da parte degli interessati.

Degno di considerazione appare anche il parere positivo formulato dal Garante il 21 febbraio 2000 sullo schema di *"Regolamento per la definizione dei criteri e delle procedure per la individuazione dei soggetti privati partecipanti al Sistan"*, ai sensi dell'art. 2, comma 1, della legge 28 aprile 1998, n. 125". In detto parere, espresso ai sensi dell'art. 31, comma 2, della legge n. 675/1996, il Garante ha rilevato che il regolamento reca gli opportuni richiami alle garanzie previste sia dalla legge n. 675, sia dal decreto legislativo n. 322/1989, ed ha richiamato l'attenzione sulla eventuale opportunità di menzionare e considerare anche il recente d.lg. n. 281/1999.

Inoltre, in occasione della recente richiesta di un parere sullo schema di regolamento formulata dall'I.S.T.A.T. in merito al censimento dell'agricoltura, il Garante ha rilevato il 28 febbraio 2000 che alcuni organi periferici dell'Amministrazione statale avevano chiesto se fosse possibile, per i soggetti appartenenti al SISTAN, semplificare le operazioni del censimento, raccogliendo alcuni dati direttamente dalle associazioni di categoria del settore. Il Garante ha osservato che mentre non si rinvergono ragioni ostative di fondo alla raccolta di questo genere di dati, in considerazione della nozione assai vasta di dato sensibile contenuta nell'art. 22 della legge 675/1996 potrebbero essere considerati come dati sensibili le stesse appartenenze di talune aziende a determinate associazioni di categoria.

Il Garante ha segnalato pertanto l'opportunità all'Amministrazione che propone il regolamento di inserire nello stesso una disposizione che preveda l'ipotizzata forma di raccolta delle informazioni direttamente dalle associazioni di categoria (anche in eventuale collegamento all'obbligo di fornire dati statistici di cui all'art. 7 del d.lg. n.322/1989), in quanto altrimenti le associazioni di agricoltori non sarebbero tenute a fornire gli estremi delle aziende agricole iscritte. Il Garante ha inoltre osservato che le associazioni restano comunque soggette agli obblighi previsti all'art. 22 della legge n. 675 (acquisizione del consenso scritto degli interessati e rispetto delle prescrizioni contenute nelle autorizzazioni del Garante). In tal caso il consenso non deve essere necessariamente richiesto in forma specifica, potendo derivare anche dal più generale consenso manifestato una tantum dagli interessati in riferimento al perseguimento, da parte delle associazioni, delle finalità previste statutariamente.

Infine, nel parere del 1° marzo 2000 sullo schema di decreto ministeriale relativo al certificato di assistenza al parto, il Garante ha segnalato al Ministero della sanità la necessità di integrare la previsione che la trasmissione all'I.S.T.A.T. delle informazioni rilevate attraverso i suddetti certificati devono essere prive di elementi identificativi diretti, con la analoga previsione che anche la trasmissione semestrale di tali informazioni da parte delle Regioni al Ministero della sanità avvenga in modo che non possa risalirsi all'identità delle persone interessate.

Da tempo era avvertita da parte di studiosi e giuristi l'esigenza di armonizzare la disciplina della ricerca storica alla mutata realtà sociale con particolare riferimento alla riservatezza e alla consultabilità dei documenti rilevanti ai fini storici.

2.4.3
Dati
personali e
ricerca storica

Questa attività di aggiornamento non poteva prescindere dall'attenta valutazione delle opposte esigenze che caratterizzano la materia. Basti pensare alle necessità della ricerca storica, che richiede la conservazione permanente dei documenti d'interesse, in apparente contrasto con alcuni dei principi che emergono dalla legge n. 675/1996 per il corretto trattamento dei dati personali ed in particolare con quello che prevede la loro conservazione per un tempo limitato (il cosiddetto "diritto all'oblio"). Ma, come abbiamo visto al par. 2.4.1, il bilanciamento fra le diverse esigenze era già previsto nella direttiva europea ed il decreto legislativo n. 281 lo ha risolto nelle sue linee di fondo soprattutto attraverso il nuovo comma 1 bis dell'art. 9 della legge 675/1996.

Inoltre lo stesso decreto legislativo n. 281 ha introdotto tutta una serie di importanti modifiche alla normativa previgente ed in particolare al decreto legislativo 30 settembre 1963, n. 1409, la cosiddetta legge archivistica.

Tra queste merita un rilievo particolare quella operata sui limiti alla consultabilità dei documenti, con le modificazioni all'art. 21 della legge archivistica e l'introduzione del nuovo art. 21 bis. Sono stati riconsiderati in tale ottica sia i termini necessari alla libera consultabilità dei documenti contenenti dati personali, sia le stesse categorie di dati personali particolarmente tutelati, fermo restando il principio generale della libera consultabilità dei documenti conservati negli Archivi di Stato. Né è stato trascurato il problema dell'armonizzazione della disciplina dell'accesso ai docu-

menti a fini storici con la normativa in tema di accesso ai documenti amministrativi.

La modifica fondamentale ha riguardato l'accesso alla documentazione contenente dati personali: mentre in generale il termine per gli stessi dati sensibili è stato determinato in quaranta anni (corrispondente al termine ordinario di versamento dei documenti), esso sale a settanta anni per i soli dati che siano "idonei a rivelare lo stato di salute o la vita sessuale o rapporti riservati di tipo familiare" (come è noto, la precedente legislazione si riferiva all'indeterminata categoria delle "situazioni puramente private" ed alla documentazione relativa ai processi penali). Per scopi di ricerca storica il termine può essere ridotto dal Ministro dell'interno "previo parere del direttore dell'Archivio di Stato competente e udita la Commissione per le questioni inerenti la consultabilità degli atti di archivio riservati" (organo collegiale in parte riformato dallo stesso decreto delegato). È significativo che si preveda espressamente che la concessione di un'autorizzazione ad accedere ai dati riservati prima della scadenza deve essere "rilasciata, a parità di condizioni, ad ogni altro richiedente".

Anche per il trattamento dei dati a scopi storici è prevista l'adozione di un codice deontologico che deve individuare le specifiche cautele cui dovranno attenersi non solo gli archivisti ma, ai fini della comunicazione e diffusione dei dati personali, anche gli utenti degli archivi di Stato e degli archivi privati dichiarati di notevole interesse storico (sui codici di deontologia in generale si veda il par. 3.6 di questa relazione). Va rilevato che gli utenti degli archivi non si inquadrano in una specifica categoria professionale, ma ricomprendono, oltre ai ricercatori di professione e agli studenti universitari, una vasta gamma di persone che si rivolgono alle fonti documentarie per le finalità più diverse.

Un importante risultato raggiunto dal decreto legislativo in argomento è l'aver risolto il nodo apparentemente spinoso, dato dalla coesistenza della possibilità di esercitare i diritti riconosciuti dall'art. 13 della legge 31 dicembre 1996, n. 675 con la conservazione dei documenti per fini storici.

Da una parte, infatti, non si poteva certo negare l'esercizio anche in questo settore dei diritti riconosciuti in generale dalla legge 675, dal momento che lo stesso art. 9 della direttiva 95/46/CE, nel momento in cui prevede che si possano introdurre speciali deroghe alla disciplina generale di tutela dei dati personali per favorire la ricerca storica, tuttavia esige che si assicurino "garanzie adeguate" a tutela dei diretti interessati. Dall'altra non è sottovalutabile il rischio che potrebbe derivare alla ricerca storica da un esercizio di questi diritti da parte degli interessati e dei loro eredi tale da impedire praticamente l'utilizzazione di molti dati e documenti.

Il punto di equilibrio individuato dal decreto legislativo da una parte si concreta nel fatto che i diritti di cui all'art. 13 possono essere esercitati non solo dal diretto interessato ma, se riferiti a dati personali inerenti persone decedute, "da chiunque vi abbia interesse"; inoltre il codice deontologico dovrà prevedere che "l'interessato o chi vi abbia interesse" sia informato dall'utente della prevista diffusione di dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare". Peraltro di norma l'esercizio dei diritti di cui all'art. 13 non può alterare la documentazione a cui si è avuto accesso, ma può portare solo alla sua eventuale integrazione tramite l'allegazione ad essa di un'altra documentazione correttiva o integrativa. La stessa misura più incisiva, consistente nel blocco dei dati personali, è possibile soltanto in casi rarissimi e cioè qualora il loro trattamento comporti un "concreto pericolo di lesione della dignità, della riservatezza o dell'identità personale degli interessati e i dati non siano di rilevante interesse pubblico" (art. 21-bis, comma 2, del d.P.R. 20 settembre 1963, n. 1409, introdotto dall'art. 9, comma 1 del d.lg. n. 281).

Da ultimo, il Garante ha ravvisato l'esigenza di una sollecita integrazione e modifica del recente testo unico in materia di beni culturali e ambientali, approvato con d.lg. n. 490/1999. Tale testo ha tra l'altro abrogato e riformulato alcune disposizioni del d.P.R. n. 409/1963 in materia di archivi e ricerca a fini storici, senza però tener conto delle modifiche ed integrazioni apportate nel luglio del 1999 al d.P.R. stesso (in particolare, artt. 21 e 21-bis), che vanno ora rapidamente riprodotte nel d.lg. anche per evitare errori applicativi).

2.5 Associazioni, partiti e confessioni religiose

L'art. 8, comma 2, lett. d) della direttiva n. 95/46 CE, prevede che la legislazione nazionale di recepimento possa stabilire che le fondazioni, le associazioni o qualsiasi altro organismo che non persegua scopo di lucro ed abbia carattere politico, filosofico, religioso o sindacale, trattino i dati sensibili connessi all'adesione associativa degli aderenti e delle persone che hanno contatti regolari con i medesimi organismi, anche senza il consenso degli interessati, purché siano previste adeguate garanzie ed i dati non vengano comunicati a terzi.

La legge n. 675, com'è noto, non ha considerato tale possibilità ed ha sottoposto i predetti organismi alla disciplina comune, basata sul consenso degli interessati e sull'autorizzazione del Garante.

La materia è stata in parte innovata dal decreto legislativo n. 135/1999, il cui art. 5, comma 1, ha aggiunto all'art. 22 della legge n. 675 il comma 1-bis, stabilendo che la rigida disciplina prevista per i dati sensibili non si applica ai trattamenti effettuati dagli organi o dagli enti civilmente riconosciuti della Chiesa cattolica e delle confessioni religiose che hanno stipulato un'intesa con lo Stato ai sensi dell'art. 8 della Costituzione, relativamente ai dati dei loro aderenti e dei soggetti che, con riferimento a finalità di carattere esclusivamente religioso, hanno contatti regolari con le medesime confessioni, purché detti dati non siano comunicati o diffusi all'esterno.

Questa innovazione, com'è agevole comprendere, è di carattere parziale e, come peraltro annunciato dalla stessa relazione di accompagnamento al d. lg. n. 135/1999, dovrà essere completata con riferimento agli altri e più numerosi organismi contemplati dal citato art. 8 della direttiva.

Nelle more di tale regolamentazione complessiva, questi ultimi soggetti devono continuare a gestire i dati sensibili richiedendo il consenso agli interessati e l'autorizzazione al Garante. Quest'ultima, già rilasciata con il provvedimento generale n. 3 nel 1997 e nel 1998, è stata rinnovata, con poche modifiche, anche nel 1999 con scadenza al 30 settembre 2000.

La Congregazione cristiana dei Testimoni di Geova, non potendo avvalersi del regime introdotto dall'art. 5 del d. lg. n. 135/1999 fino a quando non sarà stata approvata l'intesa con lo Stato, ha chiesto al Garante, anche in deroga al ricordato provvedimento generale n. 3/1999, di essere autorizzata a procedere al trattamento dei dati sensibili dei propri aderenti senza richiedere il loro consenso scritto. Tale istanza, però, sollecitando il rilascio di un provvedimento che aveva un contenuto non previsto dalla legge n. 675 ed anzi contrastante con la modifica introdotta dal d. lg. n. 135, è stata rigettata dal Garante con provvedimento dell'11 gennaio 2000.

Contestualmente, la stessa Congregazione ha impugnato, con un ricorso al Tribunale amministrativo del Lazio, la citata autorizzazione n. 3/1999 per *"violazione e falsa applicazione"* dell'art. 22 della legge n. 675, ritenuto in contrasto con gli artt. 3, 7, 8 e 19 della Costituzione. L'Autorità, nel rappresentare le proprie osservazioni all'Avvocatura dello Stato, ha prioritariamente eccepito il difetto di giurisdizione, considerato che l'art. 29, comma 8, della legge n. 675 affida le controversie relative a tali autorizzazioni al giudice ordinario, ed ha poi esplicitato ulteriori elementi (obbligo per l'Autorità di uniformarsi al chiaro dettato normativo, funzione "anticipatrice" e non di privilegio del comma 1 bis dell'art. 22 nell'ambito del pieno recepimento della direttiva comunitaria, ecc.) a conforto della correttezza del proprio agire.

Contemporaneamente, un'aderente alla Congregazione ha citato quest'ultima in giudizio, con ricorso ai sensi dell'art. 700 c.p.c., affinché fosse accertato che la medesima, in quanto membro della confessione religiosa, non era tenuta a prestare il consenso scritto per il trattamento dei propri dati personali. Il giudice adito ha ritenuto sussistere la rilevanza e la non manifesta infondatezza della questione di costituzionalità ed ha pertanto sollevato la questione di legittimità costituzionale con ordinanza del 14 febbraio 2000.

Il fenomeno associativo, nel corso dell'anno, è stato poi interessato da diversi provvedimenti dell'Autorità. Con riferimento a quelli di maggior rilievo, va ricordata anzitutto la pronuncia del 1° dicembre 1999 relativa alla comunicazione da parte di alcune pubbliche amministrazioni ad alcune associazioni di categoria di dati concernenti persone invalide.

L'entrata in vigore del d. lg. n. 135/1999, infatti, ha chiaramente reso impossibile la prosecuzione di tali procedure, considerato che i soggetti pubblici, nel predisporre le necessarie norme regolamentari, devono preoccuparsi di verificare che l'eventuale comunicazione di dati sia strettamente necessaria al perseguimento delle rilevanti finalità individuate dalla normativa primaria o dal provvedimento del Garante.

In una successiva occasione (decisione del 29 settembre 1999, in Bollettino n. 10, pag. 35) l'Autorità ha affrontato il tema dell'utilizzo dei dati degli iscritti ad un'associazione per finalità diverse da quelle loro indicate nell'informativa; nel caso specifico, erano state inviate agli aderenti messaggi di propaganda da parte del presidente dell'associazione, candidatosi ad una consultazione elettorale. Il Garante ha valutato come illegittimo il comportamento, in quanto non riconducibile alle finalità dell'associazione così come risultanti dall'informativa rilasciata agli interessati ed ha quindi segnalato all'associazione semmai la necessità di integrare l'informativa originariamente fornita, specificando meglio i trattamenti legati alle finalità istituzionali dell'associazione e distinguendo, eventualmente, come trattamento "facoltativo" e "non essenziale" la comunicazione dei dati a fini elettorali.

Va infine ricordata, anche per il risalto che la vicenda ha avuto sulla stampa quotidiana, la decisione sul ricorso di una persona che aveva chiesto la cancellazione dei propri dati personali contenuti nei registri dei battezzati (vedi il provvedimento del 13.9.1999, in Bollettino n. 9, pag. 54).

I responsabili ecclesiastici, ai quali l'interessato si era rivolto motivando la richiesta con le proprie convinzioni di ateo, pur assicurando di aver allegato la richiesta di cancellazione all'atto di battesimo, avevano risposto di non poter dar corso alla materiale cancellazione dei dati, considerato che questi attestavano un fatto realmente verificatosi.

Il collegio del Garante, nel dichiarare infondato il ricorso sotto diversi profili, ha evidenziato che, effettivamente, la registrazione dei dati in questione, rappresentando "l'ingresso" della persona in un determinato organismo, non costituisce solo un dato relativo all'aderente, ma rappresenta un aspetto della vita dell'organismo stesso. In altre parole, la Chiesa, al pari di quanto può avvenire per vari altri organismi di tipo associativo (partiti, sindacati, associazioni, ecc.), non può cancellare la traccia di un avvenimento che storicamente l'ha riguardata, se non a costo di modificare la stessa rappresentazione della propria realtà.

L'aspirazione degli interessati, comunque, a vedere correttamente riferita la propria immagine attuale, può essere adeguatamente soddisfatta da misure diverse dalla pura e semplice cancellazione (ad. es., attraverso un'annotazione, ovvero, tramite allegazione di atti, ecc.). Il Garante ha inoltre posto in evidenza che dalla volontà dell'interessato di abbandonare una determinata comunità discende l'impossibilità di continuare a considerare la persona in questione come appartenente al gruppo, all'associazione o, nel caso specifico, alla confessione religiosa. In questa prospettiva, risulta altresì impedita la possibilità di continuare a considerare la persona fra gli aderenti alla comunità in caso, ad esempio, di eventuali attività, anche di tipo statistico, che debbano essere compiute successivamente a detta manifestazione di volontà.

Poco tempo dopo l'emanazione di tale pronuncia, la Conferenza episcopale italiana (CEI) ha annunciato l'approvazione di un decreto relativo alla tutela dei dati personali conservati nei registri e negli archivi degli enti ecclesiastici "Disposizioni per la tutela del diritto alla buona forma e alla riservatezza", stabilendo, fra l'altro, rigide regole per la loro consultabilità da parte di estranei e la

possibilità per l'interessato che chieda di non essere più considerato aderente alla confessione, di ottenere in luogo della cancellazione del dato —che non è mai consentita— l'annotazione della sua richiesta sul registro dei sacramenti.

Nel ribadire i concetti già espressi nella sopra ricordata pronuncia, l'Autorità, con una decisione del 17.11.1999, ha precisato che l'adesione ad una associazione, pur costituendo anche un dato del soggetto associativo, non può sottrarre all'interessato il diritto di far valere prerogative così tipicamente personali come quelle previste dall'art. 13 della legge n. 675, trasferendone la disponibilità in capo all'associazione. Tale precisazione si è resa necessaria a seguito del ricorso presentato all'Autorità dal presidente di un'associazione, in nome e per conto degli iscritti all'organismo stesso, non già in veste di loro delegato, ma in quanto "organo espressivo della volontà di un'associazione".

L'attenzione nei confronti del mondo associativo, in senso lato, non si è però manifestata esclusivamente all'atto dell'emanazione di alcuni provvedimenti, ma anzi, conformemente ad una prassi avviata fin dalla sua istituzione, il Garante ha cercato anche nel 1999 di instaurare proficui rapporti di collaborazione con alcuni organismi.

In quest'ottica si situa, ad esempio, l'incontro, avvenuto nel mese di settembre, con le associazioni dei consumatori facenti parte del Consiglio nazionale dei consumatori e degli utenti. In tale occasione sono stati approfonditi diversi temi di rilievo: dall'uso non corretto o strumentale della legge sulla *privacy* (tanto da parte delle pubbliche amministrazioni, quanto del mondo delle imprese), al *marketing* diretto; dalle indagini di mercato ai rapporti con il sistema bancario; dal diritto alla trasparenza al mondo delle telecomunicazioni, a Internet e al commercio elettronico, anche alla luce del dibattito che si sta svolgendo tra Europa e Stati Uniti sui flussi di dati transfrontalieri.

Particolare attenzione è stata posta, inoltre, all'elaborazione dei codici di condotta previsti per diversi settori dalla legge n. 675, in merito ai quali Autorità ed associazioni hanno concordato sulla necessità di assicurare ai consumatori e agli utenti alcune garanzie, anche mediante un loro coinvolgimento in quanto "soggetti interessati" nei procedimenti di valutazione dei codici nei settori che li interessano direttamente.

2.6 Settore del credito e assicurativo

Fin dalla prima fase di applicazione della legge n. 675, il settore assicurativo si è rivelato come un campo nel quale le nuove disposizioni sulla protezione dei dati personali hanno avuto una forte incidenza sul rapporto fra clienti e imprese di assicurazione già caratterizzato, tra l'altro, da un diffuso contenzioso.

In particolare, diversi contraenti hanno esercitato il diritto di accedere ai propri dati personali detenuti dalle imprese, innestando poi alcuni ricorsi al Garante ai sensi dell'art. 29 della legge n. 675 per la tutela dei diritti di cui all'art. 13.

Il principale denominatore comune di tali ricorsi è stato rappresentato dalle richieste di accesso da parte degli interessati alle perizie medico-legali redatte dai sanitari di fiducia delle imprese.

Le richieste si sono innestate a margine di una specifica fase del rapporto assicurativo che si verifica in rapporto ad una richiesta di risarcimento a seguito di un sinistro. La persona che in conseguenza di incidenti di qualsiasi tipo ha riportato danni specie fisici viene invitata dall'impresa a sottoporsi ad una visita medica presso lo studio di un medico di sua fiducia. Quest'ultimo, com-

2.6.1
Accesso
alle perizie
medico legali
in ambito
assicurativo

più un'anamnesi del soggetto visitato, esprime le proprie valutazioni (alla stregua di giudizio peritale) in ordine all'entità del danno sofferto, al rapporto di causalità fra il danno ed il sinistro, alla percentuale di invalidità che residua, ecc... Non di rado il medico esprime all'impresa alcune valutazioni personali e suggerimenti in ordine alla condotta da osservare sia in rapporto agli esiti di eventuali perizie di parte già effettuate, sia in relazione alla perizia tecnica d'ufficio che potrebbe essere richiesta nel corso dell'eventuale controversia civile.

Si tratta, come è evidente, di un momento molto delicato nella gestione delle richieste di risarcimento, nel quale l'impresa di assicurazione acquisisce elementi di valutazione e di giudizio che possono ispirare e condizionare la sua condotta successiva, inducendola, ad esempio, a resistere in giudizio alle richieste della controparte, a formulare proposte transattive, ad accogliere le richieste del sinistrato, ecc.

In casi particolari la valutazione peritale si inserisce anche in un momento in cui la società di assicurazione può acquisire elementi in ordine alla veridicità del fatto denunciato e apprestare quindi idonee misure a tutela della propria posizione anche attraverso ulteriori investigazioni o tramite denunce penali. Si tratta di situazioni di particolare delicatezza, specie in presenza del fenomeno delle truffe assicurative.

È però evidente come un diritto eguale e contrapposto esista in capo all'interessato (cioè alla persona i cui dati, ordinari e sensibili, siano stati appunto trattati nell'ambito della visita medica) per conoscere, in base alla legge n. 675, dati personali a sé riferiti e caratterizzati da così delicati profili.

La situazione evidenziata dà luogo ad uno dei confronti fra situazioni soggettive che frequentemente si manifestano nell'ambito della disciplina sulla protezione dei dati personali. Di questa evenienza si è fatta carico la stessa legge n. 675, la quale, nell'art. 14, comma 1, lettera e), ha previsto che i diritti di cui all'art. 13, comma 1, lettere c) e d) non possano essere esercitati nei confronti dei trattamenti di dati personali raccolti ai sensi dell'art. 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)".

La legge ha quindi previsto che possano esistere situazioni nelle quali, in ragione della specifica esigenza di salvaguardare il diritto di difesa del titolare del trattamento, possa essere consentito il temporaneo differimento dell'esercizio del diritto di accesso e di eventuale rettifica.

I recenti ricorsi presentati al Garante in materia di accesso ai dati contenuti nelle perizie medico/legali hanno appunto messo in luce la necessità di precisare limiti e portata della citata disposizione dell'art. 14.

Al riguardo sono emersi due profili specifici sui quali il Garante ha avuto modo di pronunciarsi più volte:

- la ricomprensione di larga parte delle informazioni contenute nelle predette perizie medico-legali nel novero dei "dati personali";

- i limiti di applicabilità della disposizione sul differimento del diritto di accesso di cui all'art. 14, comma 1, lettera e).

Fin dalla sua prima decisione in proposito, risalente al 21 giugno 1999, il Garante ha avuto modo di precisare che le valutazioni espresse dal medico in sede di perizia (e relative al giudizio formulato in ordine all'entità del danno subito dalla vittima del sinistro e alla quantificazione del periodo di inattività della stessa) rientrano pienamente nel concetto di dato personale di cui all'art. 1, comma 2, lettera c) della legge.

Le perizie in questione contengono anche valutazioni e giudizi di tipo soggettivo del medico fiduciario della società di assicurazione. Ma, come il Garante ha constatato fin dalla decisione del

2 giugno 1999 (relativa al diverso tema dell'accesso alle note di qualifica dei lavoratori dipendenti, in Bollettino n. 9, pag. n. 34) anche i rilievi, i giudizi, le valutazioni di tipo soggettivo rientrano nell'ambito di applicazione della legge. L'espressione "dato personale" comprende infatti ogni notizia, informazione o elemento che abbia un'efficacia informativa tale da fornire un contributo di conoscenza rispetto ad un soggetto identificato o identificabile.

Così chiarita la natura di dato personale delle informazioni contenute nelle perizie, il Garante ha affrontato il problema dell'applicabilità della citata disposizione dell'art. 14 relativa al temporaneo differimento del diritto di accesso. Al riguardo si è precisato (vedi, in particolare, le decisioni del 13 ottobre e del 9 dicembre 1999) che tale disposizione è di carattere eccezionale e impone pertanto di effettuare caso per caso una valutazione attenta dell'effettivo pregiudizio che potrebbe derivare al titolare del trattamento, nell'immediato, a seguito dell'ostensione dei dati personali richiesti. Inoltre, di tale pregiudizio il titolare medesimo deve sempre fornire all'interessato adeguata motivazione, comprovando le esigenze difensive che giustificerebbero tale differimento.

Come è stato ribadito in più occasioni, la mera pendenza di un giudizio non è, infatti, di per sé sufficiente per rendere applicabile la norma, dovendo l'impresa titolare del trattamento dimostrare i riflessi che l'immediata disponibilità dei dati accordata all'interessato avrebbe sulla posizione difensiva del titolare. In concreto, nei numerosi casi esaminati in sede di ricorso, è stata ravvisata più volte l'esistenza delle ragioni di tutela di cui al predetto art. 14, anche con riferimento a situazioni pre/contenziose nelle quali vi era ad esempio la temporanea necessità di non pregiudicare l'attività delle parti in ordine ad un determinato accertamento probatorio (riguardo, ad esempio, all'espletamento di perizie contrattuali previste nella polizza o alla determinazione delle modalità di svolgimento di una consulenza tecnica d'ufficio).

Va però precisato che il Garante, nel riconoscere in più occasioni la legittimità del differimento del diritto di accesso, ha però circoscritto rigorosamente questa parziale e temporanea limitazione dei diritti dell'art. 13, anzitutto in relazione alle parti propriamente valutative delle perizie medico-legali, statuendo che tali diritti sono comunque pienamente operanti per i dati personali dell'interessato di tipo meramente identificativo o aventi carattere oggettivo o comunque non incidenti sulle specifiche ragioni di tutela prospettate dal titolare del trattamento.

Inoltre, è stato rimarcato che la limitazione in parola del diritto di accesso è temporanea. Cessate infatti le esigenze di tutela cui l'art. 14 fa riferimento, il diritto di accesso può riespandersi e i dati devono essere comunicati integralmente all'interessato che li richieda.

Il Garante ha reso noto, nel maggio del 1999, uno schema di un nuovo modello semplificato di informativa e per il consenso che potrebbe essere opportunamente fornito ai clienti di istituti di credito.

2.6.2
Semplificazione
dell'informazione
nel settore
bancario

Una prima bozza era stata messa a punto nel mese di febbraio (e proposta alla riflessione e ai contributi di tutti i cittadini e delle categorie coinvolte: v. *Relazione per l'anno 1998*, par. 2.10, pag. 66), a seguito di un'indagine conoscitiva condotta presso diversi istituti di credito, da cui era emerso che una parte consistente della clientela non aveva ancora risposto alle comunicazioni inviate dalle banche, anche a causa della loro non agevole comprensibilità.

In tali, assai numerosi, casi di mancato riscontro alle informative bancarie, altre prestazioni richieste dall'utenza (quali, ad esempio, un bonifico o un assegno) erano state finora considerate come provvisorie manifestazioni di consenso implicito. Anche per uscire da questa situazione di anomalia rispetto al dettato legislativo (in base al quale è, per diversi casi, richiesta invece la raccolta di un consenso espresso per determinate operazioni di trattamento quale la comunicazione), l'Autorità ha ritenuto opportuno suggerire agli operatori del settore un nuovo modello

che, pur mantenendo ferme le garanzie sancite dalla legge sulla privacy, renda più snello e chiaro l'adempimento "burocratico" nei confronti del pubblico, armonizzando peraltro i diversi modelli già in circolazione (analizzati nell'ambito della verifica di oltre ottocento esemplari utilizzati dai diversi istituti).

Il nuovo modello suggerito dal Garante è il risultato dello sforzo volto a sintetizzare al massimo le informazioni da fornire agli interessati e a dare alle stesse una veste meno giuridica e più vicina al c.d. "uomo della strada" (con eliminazione di ripetizioni inutili, passaggi generici e "tautologici", nonché di complicati riferimenti e di citazioni normative allorché superflue). Tale modulo può rappresentare, per alcuni aspetti, una svolta significativa rispetto ai moduli già in circolazione, nella direzione di un'attuazione più sostanziale e meno formalistica dei principi di lealtà e correttezza stabiliti dalla legge n. 675.

Si ricordano qui di seguito alcune delle maggiori innovazioni che verrebbero introdotte dal modello:

- la significativa riduzione delle firme che il cliente deve apporre per la manifestazione del consenso (da cinque o più, ad una o, al massimo, due);
- l'indicazione a parte di alcune caselle da barrare per i trattamenti di dati non strettamente collegati ai servizi attivati dalla clientela (per lo più, iniziative promozionali e di marketing);
- la possibilità per gli istituti di credito di predisporre a parte, di aggiornare e di mettere a disposizione degli interessati, in modo agevole e gratuito (attraverso anche un numero verde od un sito web), il lungo elenco delle società di fiducia che svolgono per conto della banche compiti di natura tecnica od organizzativa (ad eccezione, quindi, di taluni soggetti come, ad es., le centrali rischi private che effettuano stabilmente complessi trattamenti dei dati: v. il prossimo paragrafo);
- l'analoga facoltà di indicare ai clienti il servizio o la persona responsabile del trattamento a cui rivolgere eventualmente le proprie richieste di conoscenza, cancellazione o rettificazione dei dati, accedendo poi alla lista completa ed aggiornata di tutti gli altri responsabili (lista che le banche possono comunque rendere disponibile mediante numero verde o sito web);
- il sostanziale rinvio ad una ulteriore e specifica richiesta di consenso, manifestato volta per volta, per servizi che comportano la conoscenza e il trattamento da parte della banca di dati sensibili (mutui assistiti da assicurazione, polizze vita, ecc.), ferma restando, invece, l'idoneità dell'attuale modulo a "coprire" anche situazioni relative a versamenti che riguardano sindacati, forze politiche e determinate associazioni e ad accreditamenti di alcune pensioni o di speciali rimborsi assicurativi.

Nell'ambito delle iniziative assunte e dei chiarimenti forniti con riferimento alla semplificazione degli adempimenti per la tutela della privacy nel settore bancario, va poi segnalato un provvedimento del 5 giugno 1999, con il quale, in relazione ad un'operazione di cartolarizzazione relativa all'acquisto in blocco di migliaia di posizioni creditizie tra alcuni istituti di credito, il Garante ha autorizzato la Paribas-succursale di Milano ad effettuare l'informativa ai debitori ceduti nelle stesse forme previste dal testo unico delle leggi in materia bancaria e creditizia per l'annuncio della cessione dei rapporti giuridici in blocco (art. 58 d.lg. n. 385/1993), ovvero mediante pubblicazione della medesima informativa, per classi di operazioni, nella Gazzetta Ufficiale.

Nel richiamare una propria precedente pronuncia sugli esoneri dall'obbligo dell'informativa rispetto ai dati raccolti presso terzi e sulla possibilità di adottare modalità di informazione sostitutive (provvedimento del 26 novembre 1998, in *Relazione per l'anno 1998*, pag. 33), l'Autorità ha ritenuto infatti che, in considerazione anche del quadro normativo sulla cessione del credito, la singola informativa da parte della banca fiduciaria a ciascun interessato avrebbe comportato un impiego

di mezzi sproporzionato rispetto al diritto tutelato e allo specifico contesto in cui esso si colloca, pur essendo necessario assicurare un'informativa generale adeguata.

Per questo motivo, la banca è stata autorizzata a ricorrere alle modalità già utilizzate per informare gli interessati in base al citato testo unico bancario, purché siano garantite forme concorrenti di informazione volte ad assicurare l'effettiva conoscibilità dell'inserzione nella Gazzetta Ufficiale. Ciò attraverso la comunicazione della data di pubblicazione nell'estratto conto degli interessati e la messa a disposizione dell'informativa nelle filiali che intrattengono rapporti con gli stessi, mediante opportuni accorgimenti che la rendano agevolmente visibile.

Nel settore bancario e finanziario, si è registrata in questi ultimi anni una crescente proliferazione di iniziative di privati volte a realizzare, soprattutto per le attività di credito al consumo, sistemi di rilevazione del rischio creditizio. Tali sistemi, che sono meglio noti al pubblico con la denominazione di "centrali rischi", permettono alle banche e alle società finanziarie di segnalare e di conoscere la situazione debitoria di nuovi potenziali clienti e rispondono, più in generale ad un'esigenza di circolazione delle informazioni nel mercato creditizio, nonché di sana e prudente gestione delle proprie attività.

2.6.3
Le "centrali rischi" gestite dalla Banca d'Italia e dai privati

Le centrali rischi private sono in qualche misura complementari al servizio di centralizzazione dei rischi gestito dalla Banca d'Italia, disciplinato da alcune disposizioni del t.u. bancario (artt. 53, comma 1, lett. b), 67, comma 1, lett. b) e 107, secondo comma), che attribuiscono a tale Autorità, nello svolgimento della funzione di vigilanza regolamentare, il compito di emanare, in conformità alle deliberazioni del Comitato interministeriale per il credito ed il risparmio, disposizioni per il contenimento del rischio nelle sue diverse configurazioni (v. la delibera Cicr del 29 marzo 1994 e le norme attuative adottate dalla Banca d'Italia). Tale servizio fornisce, appunto, a banche ed intermediari finanziari informazioni sull'indebitamento della clientela verso il sistema creditizio e finanziario, allo scopo di contenere i rischi derivanti dalla presenza di alcune condizioni derivanti, in particolare, dal cumulo di finanziamenti di importo pari o superiore ai 150 milioni o comunque in sofferenza.

La legge sulla privacy non ha posto particolari ostacoli al trattamento dei dati personali effettuato nell'ambito della centrale dei rischi gestita dalla Banca d'Italia, ferma restando, più in generale, l'esigenza di un'integrazione normativa sotto il profilo della tutela dei dati. Tale trattamento è, infatti:

- assoggettato alla particolare disciplina prevista per i soggetti pubblici (che consente a questi ultimi di operare senza il consenso dell'interessato, per lo svolgimento delle funzioni istituzionali e in base a quanto stabilito dalla legge e dai regolamenti: v. l'art. 27 legge n. 675/1996);
- oggetto di una specifica deroga per quanto riguarda le modalità di esercizio da parte degli interessati dei diritti di cui all'art. 13, rientrando nell'ambito dei trattamenti dei dati raccolti "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" (art. 14, comma 1, lett. d) legge n. 675/1996: v. il provvedimento del 9 gennaio 1999, in Bollettino n. 7/1999, pag. 42, con cui è stato dichiarato inammissibile un ricorso per la cancellazione dei dati dalla centrale rischi della Banca d'Italia).

Anche per quanto concerne la comunicazione alla centrale dei dati relativi ai clienti, appare evidente che le previsioni del citato testo unico in materia bancaria, in base alle quali gli istituti di credito e finanziari sono obbligati a fornire all'autorità di vigilanza del settore le informazioni sugli indebitamenti della propria clientela, rendono superflua l'acquisizione da parte dei medesimi istituti di un preventivo consenso degli interessati (art. 20, comma 1, lett. c), legge n. 675/1996).

Le disposizioni introdotte dalla legge n. 675/1996 hanno fatto invece emergere alcuni pro-

blemi per i complessi e delicati trattamenti di dati personali svolti nell'ambito delle centrali rischi gestite da società. Per queste ultime, dopo l'entrata in vigore della legge n. 675, si è posta la questione dei presupposti di liceità del relativo trattamento dei dati, con particolare riguardo agli adempimenti dell'informativa e del consenso, nonché ai diritti degli interessati di accesso ai dati che li riguardano e di loro eventuale rettificazione o cancellazione.

Sono, infatti, in rapida crescita le segnalazioni, i reclami e i ricorsi presentati al Garante circa le attività e i connessi trattamenti di dati effettuati dalle centrali rischi gestite da privati. Ciò evidenzia la particolare delicatezza che tali attività rivestono nei riguardi dei diritti e delle libertà degli interessati, rendendo necessaria una riflessione più generale da parte degli operatori del settore bancario e finanziario (in particolare, delle società che gestiscono le centrali rischi), del Garante e dello stesso legislatore per trovare un giusto equilibrio tra le esigenze di tutela del credito e di salvaguardia della riservatezza.

Nei diversi provvedimenti adottati nel corso del 1999 (v. i provvedimenti del 9 gennaio 1999 e del 29 settembre 1999, pubblicati, rispettivamente, nei bollettini del 1999 nn. 7, p. 44, e 10, pag. 45), il Garante ha comunque sottolineato che non è di per sé illecita la comunicazione alle centrali rischi private dei dati personali inerenti ai finanziamenti richiesti dagli interessati, ferma restando l'esigenza che nei relativi contratti sia presente una clausola per la manifestazione del consenso informato.

L'Autorità ha, infatti, esaminato numerosi casi di cittadini che chiedevano la cancellazione dei dati contenuti negli archivi di società finanziarie ritenute responsabili di aver comunicato a società di rilevazione dei rischi finanziari, senza il loro previo consenso, informazioni circa l'insolvenza e l'inaffidabilità patrimoniale (i ricorrenti hanno fatto invocare la norma che consente la cancellazione dei dati quando questi sono trattati in violazione di legge: v. anche il provvedimento del 9 dicembre 1999, pubblicato nel Bollettino n. 10/1999, pag. 48).

Il Garante ha però constatato che alcune doglianze non erano fondate. In taluni casi la manifestazione di consenso di cui l'interessato invocava la necessità non era, in realtà, un presupposto indefettibile del trattamento dei dati da parte della società finanziaria, in quanto quest'ultimo era stato effettuato prima dell'entrata in vigore della legge n. 675 del 1996. Per quanto riguarda, in secondo luogo, la divulgazione dei dati a terzi, il Garante ha evidenziato che nei contratti era presente un'apposita clausola di autorizzazione che, pur non essendo perfettamente conforme alle indicazioni contenute nella legge n. 675, perché redatta prima della sua entrata in vigore, poteva essere considerata come una manifestazione sostanziale di consenso alla comunicazione dei dati alle categorie di soggetti ivi indicati, e cioè alle società di rilevazione dei rischi creditizi.

Poiché tali clausole di trasmissione dei dati alle centrali rischi erano contemplate specificamente dai contratti di finanziamento ed espressamente accettate dagli interessati, è apparsa corretta la registrazione dei dati in questione presso le centrali rischi per un certo periodo (in genere, cinque anni), allo scadere del quale essi vengono di regola cancellati.

Recentemente, peraltro, nel sistema bancario è stata avvertita l'esigenza di rilevare in maniera più capillare, attraverso un'unica struttura centralizzata (anziché mediante più "centrali rischi" gestite da diversi soggetti privati), anche gli indebitamenti di importo inferiore a quelli censiti presso la Banca d'Italia, allo scopo di ridurre il più possibile il rischio creditizio e di salvaguardare la stabilità finanziaria degli istituti di credito e finanziari.

Con deliberazione del 3 maggio 1999 (pubblicata sulla G.U. n. 158 dell'8/7/99), il Cici ha quindi previsto l'istituzione di un sistema centralizzato dei rischi riguardanti affidamenti di importo inferiore a quelli rilevati dalla Banca d'Italia. Tale sistema prevede per le banche e le società finanziarie, in analogia e secondo le procedure previste per la centrale rischi già gestita presso la Banca d'Italia, sia l'obbligo di comunicare i dati relativi alle esposizioni creditizie della clientela, sia la pos-

sibilità di ricevere i dati relativi alla situazione complessiva di ogni cliente segnalato. Per gli aspetti inerenti al trattamento dei dati personali, la stessa Banca d'Italia dovrà quindi emanare, sentito il Garante, le istruzioni necessarie per l'attuazione della deliberazione Cidr, verificandone poi il rispetto.

Con provvedimento in data 17 novembre 1999 (in Bollettino n. 10, pag. 22), il Garante ha espresso, ai sensi dell'art. 31 della legge n. 675, il richiesto parere in ordine allo schema di regolamento concernente l'istituzione della c.d. "anagrafe dei rapporti di conto e di deposito".

2.6.4
C.d.
"anagrafe
dei conti
correnti"

La legge n. 413 del 1991 ha previsto un regolamento per stabilire "la destinazione e le modalità delle comunicazioni da parte delle aziende ed istituti di credito e dell'amministrazione postale nonché delle società fiduciarie e di ogni altro intermediario finanziario dei dati identificativi, compreso il codice fiscale, di ogni soggetto che intrattienga con loro rapporti di conto o deposito o che comunque possa disporre del medesimo, nonché i criteri per le relative utilizzazioni".

La finalità è quindi quella di creare uno strumento che, data la natura dei dati conservati, riguarderebbe pressoché tutti i cittadini e potrebbe agevolare le indagini investigative e fiscali.

L'estensione ed il rilievo dello strumento pongono però rilevanti problemi di protezione dei dati personali trattati, che già erano stati percepiti dal legislatore del 1991 (quindi in un momento precedente l'adozione della stessa legge n. 675), il quale ha stabilito (art. 20) che l'emanando regolamento dovesse essere caratterizzato da una assai rigorosa disciplina dei vari profili di riservatezza.

Più specificamente il modello proposto con lo schema vedrebbe la costituzione di un apposito "centro operativo" presso il Ministero del tesoro, del bilancio e della programmazione economica. A tale centro una serie di soggetti (autorità giudiziaria, UIC, SECIT, funzionari degli uffici delle entrate del Ministero delle finanze, ufficiali della Guardia di Finanza) potrebbe richiedere "con riferimento a persone fisiche o giuridiche specificamente individuate, l'eventuale esistenza di rapporti di conto o di deposito alle medesime intestati...o relativamente ai quali esse agiscono in nome e per conto o ne possono disporre nell'ambito dell'archivio unico informatico tenuto dagli intermediari creditizi o finanziari e dalle Poste italiane S.p.A. ai sensi della legge 5 luglio 1991, n. 197".

Il centro operativo presso il Ministero, ai fini dell'acquisizione dei predetti elementi informativi, si dovrebbe avvalere poi del servizio fornito da una società attraverso la rete telematica da questa gestita.

Nell'esprimere il prescritto parere su tale schema di regolamento, il Garante ha messo in luce una serie di carenze dell'articolato, che richiedono significative modifiche per assicurare il pieno rispetto dei principi della legge n. 675.

In primo luogo è stato messo in luce che lo schema non disciplina, come necessario, tutti i profili relativi alla destinazione e alle modalità di comunicazione dei dati, effettuando anzi una subdelega a distinte fonti di disciplina.

Il Garante ha inoltre messo in luce la necessità di precisare con maggiore chiarezza le finalità che giustificano l'accesso all'archivio che si intende costituire, evitando formule generiche. In questo quadro la previsione, ad esempio, di un accesso ai dati per "l'espletamento di attività di prevenzione" è apparsa formula senza dubbio equivoca da circoscrivere con riferimento alle attività di prevenzione puntualmente previste da norme (ad esempio in materia tributaria).

Si è evidenziato infine come il regolamento debba prevedere espressamente che le richieste di accesso siano accompagnate dall'indicazione delle finalità e del procedimento di riferimento. In caso contrario non sarebbe infatti possibile verificare la legittimità della richiesta e, all'occorrenza, del successivo utilizzo dei dati.

Si è sottolineata poi la necessità di contenere il numero degli "incaricati" che avranno accesso ai dati ed ai quali andranno impartite precise istruzioni, nonché la necessità di evitare la conservazione dei dati relativi a rapporti ormai cessati, coerentemente con il disposto di cui all'art. 9 della legge n. 675 che prevede la conservazione dei dati per un periodo non superiore a quello necessario per gli scopi per i quali i dati stessi sono raccolti o successivamente trattati.

Le osservazioni relative al predetto schema regolamentare non riguardavano, invece, le disposizioni del decreto 9 dicembre 1999 del Ministero delle finanze (sul quale peraltro non è stato richiesto il previo parere di questa Autorità ai sensi dell'art. 31 della legge) con il quale è stata invece semplicemente approvata la nuova modulistica che potrà essere impiegata dagli uffici e dai servizi preposti agli accertamenti tributari per richiedere alle banche e a Poste italiane S.p.A. "dati, notizie e documenti di carattere specifico relativi ai conti intrattenuti con il contribuente".

2.6.5.
Anagrafe
degli assegni

L'art. 36 del decreto legislativo n. 507 del 1999 concernente la depenalizzazione di alcuni reati minori (che ha introdotto nella legge 15 novembre 1990, n. 386, il nuovo art. 10 bis), ha previsto l'istituzione di un archivio informatizzato.

La disposizione, al fine di assicurare il regolare funzionamento dei sistemi di pagamento, mira a creare un archivio unico informatizzato nel quale saranno inseriti i nominativi dei soggetti traenti degli assegni bancari o postali emessi senza autorizzazione o senza provvista, nonché gli elementi identificativi degli assegni emessi nelle medesime circostanze e l'indicazione delle sanzioni amministrative e penali comminate per la violazione della relativa disciplina. Nell'archivio confluiranno altresì l'indicazione delle carte di pagamento e degli assegni di cui sia stato denunciato il furto o la smarrimento.

I commi 2, 3 e 4 del citato art. 36 contengono significativi richiami alla disciplina sul trattamento dei dati personali, prevedendo la possibilità per la Banca d'Italia di avvalersi di un ente esterno per la gestione dell'archivio, da nominarsi responsabile ai sensi dell'art. 8 della legge n. 675, nonché il diritto per ogni soggetto interessato di accedere alle informazioni che lo riguardano e di esercitare anche gli altri diritti di cui all'art. 13 della medesima legge.

Con successivo regolamento in corso di emanazione su iniziativa del Ministro della giustizia, sentita la Banca d'Italia ed il Garante per la protezione dei dati personali, saranno individuate le norme necessarie per disciplinare la trasmissione, l'iscrizione, la raccolta, la conservazione e la consultazione dei dati.

2.7 Attività di marketing

La raccolta e l'utilizzazione dei dati personali costituiscono un aspetto rilevante delle attività di marketing che, in passato, non erano state oggetto di una dettagliata disciplina e sulle quali, quindi, l'introduzione di nuove regole per la tutela dei diritti fondamentali della persona ha prodotto significativi effetti. Dopo l'entrata in vigore della legge sulla privacy, i consumatori hanno infatti acquisito nuovi strumenti di difesa nei confronti del trattamento dei dati per finalità promozionali, pubblicitari e commerciali, avendo ora il diritto di consentire, in piena consapevolezza, o di opporsi ad un uso per questi scopi delle informazioni che li riguardano.

Il Garante, sin dall'inizio della propria attività, è stato particolarmente vigile su questo settore ed ha fornito diverse indicazioni per il rispetto da parte delle imprese degli obblighi di trasparenza, lealtà e correttezza che la legge sulla privacy prevede nei confronti dei cittadini, promuovendo attivamente, anche tra questi ultimi, una maggiore conoscenza dei principi affermati dalla

normativa italiana e comunitaria in materia di protezione dei dati personali.

In particolare, alla fine del 1999, l'Autorità è intervenuta sul diffuso fenomeno delle raccolte di dati effettuate a fini promozionali e commerciali attraverso *coupon*, inseriti nelle pubblicità delle aziende, con cui si chiede ai consumatori (interessati, per esempio, ad un determinato prodotto, servizio o regalo) di fornire alcuni dati anagrafici, recapiti telefonici e telematici, informazioni sull'attività svolta, sul nucleo familiare o su gusti e preferenze (v. il provvedimento del 13 gennaio 2000).

Si tratta di un fenomeno che era da tempo sotto il monitoraggio dell'Autorità, la quale, anche su segnalazione di molti cittadini, ha inoltre acquisito un considerevole numero di tagliandi e coupon offerti da negozi e supermercati, benzinai e società di servizi, di depliant, lettere e annunci pubblicitari per partecipare a lotterie, estrazioni di premi e offerte di regali, di schede per abbonamenti a riviste e periodici, di questionari per ricerche di mercato o collegati a tessere per clienti affezionati, nonché di lettere di adesione ad associazioni e di annunci di offerte di lavoro sui giornali. In diversi casi, tale materiale si è rivelato del tutto inadeguato rispetto ai requisiti richiesti dalla legge sulla protezione dei dati personali.

Il Garante ha quindi effettuato un esame complessivo del tema, esprimendo rilievi, da valutare poi, più approfonditamente, nei singoli casi, e fornendo anche alcuni suggerimenti "operativi", in modo da consentire alle aziende di rispettare meglio gli obblighi legati all'informativa ed al consenso degli interessati, pur mantenendo ferme le esigenze di semplificazione e di chiarezza di tali adempimenti.

Sulla base dei predetti rilievi di carattere generale, l'Autorità ha pertanto deciso di avviare i necessari accertamenti per l'applicazione delle sanzioni amministrative pecuniarie previste dalla legge n. 675 e si è anche riservata, nei casi più gravi, di informare l'autorità giudiziaria circa le eventuali violazioni penali da parte delle società e degli organismi che utilizzano i dati senza aver acquisito il necessario consenso degli interessati. Verranno inoltre effettuate, dall'Ufficio, verifiche caso per caso, anche ai fini dell'adozione di eventuali provvedimenti di blocco o di divieto del trattamento dei dati, o della segnalazione ai titolari e responsabili del trattamento delle modifiche indispensabili per renderlo pienamente conforme ai principi affermati dalla legge.

In primo luogo, molti dei coupon esaminati sono risultati privi di qualsiasi informativa o degli altri elementi dai quali gli interessati possano ricavare informazioni sul trattamento dei dati che li riguardano. Al riguardo, l'Autorità ha chiarito che la ricezione del *coupon* compilato concreta un trattamento di dati il quale presuppone che la società "titolare" abbia fornito già al consumatore interessato le informazioni previste dalla legge n. 675 (art. 10). Nessuna importanza assume al riguardo la circostanza che il titolare del trattamento rinunci o non proceda immediatamente alla registrazione dei dati contenuti nel *coupon* in un elenco, archivio o banca dati; né hanno rilievo le modalità con le quali il "titolare" intenda trattare successivamente i dati. L'informativa è dovuta poi in ogni caso, anche quando il consenso non sia per legge indispensabile.

Il Garante ha fatto presente, quindi, che il titolare deve dapprima fornire l'informativa (anziché contattare successivamente gli interessati dopo aver ricevuto i dati e l'eventuale generica manifestazione di consenso), inserendo nel coupon o nel più ampio documento nel quale quest'ultimo è collocato un messaggio chiaro e sintetico, basato su un opportuno stile colloquiale che permetta di comprendere, anzitutto, quali effetti comporta la spedizione del coupon (es.: mero invio del solo materiale esplicativo richiesto, oppure di riviste e libri inviati in abbonamento anche a seguito dell'adesione a determinati circoli o *club*; contatti periodici telefonici o per corrispondenza; cessione dei dati a terzi, ecc.).

Omettendo, anche per ragioni di spazio, superflue assicurazioni circa il rispetto della normativa (che a volte rappresentano l'esclusivo contenuto del messaggio, senza però indicare nulla di quanto richiesto dall'art. 10), i *coupon* devono riportare un'indicazione, sia pure succinta, che per-

metta di comprendere l'insieme delle altre notizie previste dalla legge (nonché la formula di manifestazione del consenso, ove sia necessario in base alla legge n. 675).

Nei casi sopra menzionati, come per le altre numerose ipotesi riscontrate di informative approssimative o incomplete, è inoltre necessario:

- specificare gli scopi per i quali i dati sono raccolti ed utilizzati (soprattutto quelli non strettamente collegati all'iniziativa promozionale), l'obbligatorietà o meno del loro conferimento e le conseguenze di una compilazione solo parziale dei *coupon* (in termini di benefici di cui l'interessato potrebbe non fruire);
- chiarire se i dati verranno anche ceduti a terzi e, in questo caso, indicare le categorie dei destinatari, anche a grandi linee, evitando però generici riferimenti ad "aziende di fiducia";
- indicare se vi sono particolari modalità di organizzazione, di raffronto e di elaborazione dei dati (per età, sesso, profilo professionale o di altro tipo, aree geografiche, ecc.);
- operare un richiamo all'esercizio dei diritti previsti per gli interessati dall'art. 13 della legge sulla privacy (accesso ai dati, rettificazione, cancellazione, ecc.) e fornire l'indicazione dei riferimenti, nonché dei recapiti telefonici dell'ufficio o del servizio presso cui esercitare tali diritti;
- collocare l'informativa in spazi o riquadri ben visibili e facilmente leggibili, evitando un'eccessiva frammentazione dei vari elementi in essa contenuti.

Il Garante ha poi rilevato che, di frequente, nei casi in cui è indispensabile, non viene invece chiesto agli interessati di acconsentire al trattamento dei dati raccolti con il *coupon*. In tali ipotesi, la raccolta e l'utilizzazione dei dati risultano quindi illecite e possono integrare anche gli estremi di un reato. Spesso, inoltre, la formula di consenso non appare conforme ai principi stabiliti dalla legge n. 675, in quanto non è supportata da un'adeguata informativa che consenta la manifestazione libera e consapevole del consenso; oppure risulta espressa e documentata in forma negativa, come mera possibilità di esprimere un dissenso o di barrare una casella per la rinuncia o l'opposizione ad ulteriori contatti o comunicazioni commerciali; o ancora riguarda una prestazione che non richiede consenso (come, ad esempio, l'invio di un regalo) o non è stata prevista per una serie di finalità per le quali è invece obbligatoria (uso da parte di terzi).

Sul punto, l'Autorità ha ricordato che le formule di consenso devono essere precedute da una corretta informativa e devono permettere agli interessati di esprimere o di negare il consenso attraverso opzioni di tipo "positivo", in quanto l'art. 11, comma 3, della legge 675 richiede che il consenso, per essere valido, sia "espresso liberamente" e "in forma specifica".

Le indicazioni fornite dall'Autorità per l'ampia casistica di *coupon* con finalità promozionali valgono anche per le offerte di lavoro riportate su quotidiani e periodici. Anche in questo settore, il Garante ha riscontrato analoghi casi di assenza di idonee informative e richieste di consenso. Infatti, viene chiesto spesso ai candidati interessati a partecipare ad una selezione di personale, di inviare un *curriculum*, la cui ricezione comporta una raccolta di dati, come avviene per i *coupon*.

È necessario quindi che anche le offerte di lavoro rechino la prevista informativa (che, peraltro, potrebbe essere fornita agevolmente attraverso i bandi o gli annunci che le contengono, indicando i requisiti per l'assunzione). La mancanza di tali informative rende non valide le dichiarazioni di consenso che sono spesso richieste per l'utilizzazione del *curriculum*.

In conclusione del provvedimento, il Garante ha richiamato l'attenzione di tutti gli operatori interessati al rispetto dei principi in esso evidenziati, facendo presente che l'utilizzazione dei dati raccolti in contrasto con tali principi può risultare illecita. Per questo motivo, ha inoltre disposto che il provvedimento sia trasmesso anche agli organismi, alle istituzioni ed alle organizzazioni dei settori coinvolti, affinché contribuiscano a sensibilizzare gli operatori interessati nei rispettivi ambiti.

L'Autorità ha annunciato, altresì, che avvierà altri accertamenti su ulteriori casi, analoghi alle tipologie in questione, per assicurare il rispetto delle norme sulla privacy. In particolare, saranno oggetto di specifici provvedimenti alcuni casi segnalati all'Autorità, riguardanti questionari di indagine sui consumi o il rilascio di tessere per clienti affezionati (c.d. "fidelizzazione").

2.8 Giornalismo

Tra gli altri profili di interesse, nel corso del 1999 ha assunto particolare rilievo il processo di sviluppo di un equilibrio più corretto tra le legittime esigenze di tutela della riservatezza dei singoli e le libertà di stampa e di manifestazione del pensiero, alle quali è attribuito rango costituzionale.

Ciò non già per l'assetto del quadro normativo di settore, rimasto immutato dopo il completamento dell'essenziale opera di revisione realizzata, nel corso del 1998 (sia per effetto della modifica dell'art. 25 della l. n. 675/1996, sia in virtù dell'adozione del codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica: cfr. Relazione per l'anno 1998, p. 36 ss.), bensì, soprattutto, per effetto di una maggiore consapevolezza di alcuni diritti e limiti ai diritti di cronaca rilevante in tema di privacy e trattamento dei Dati.

L'attento esame delle numerosissime richieste di intervento ricevute consente, infatti, di individuare taluni profili che, nell'ovvio presupposto della pari dignità di tutti gli altri parimenti rientranti nelle competenze dell'Autorità, sono tra quelli in relazione ai quali si avverte una più forte domanda sociale di protezione giuridica.

Sulla base dell'esperienza precorsa, in particolare, è un dato di fatto che tale domanda assai spesso si formi in relazione: a) al momento e ai modi di acquisizione delle informazioni poi utilizzate dalla stampa; b) ai principi cui si deve ispirare il trattamento dei dati da parte del giornalista; c) alla tutela dei minori e degli altri soggetti "deboli" coinvolti nelle vicende di cui la stampa dà notizia; d) all'individuazione delle misure di tutela funzionalmente più efficaci in rapporto agli interessi esposti a pregiudizio.

Diverse segnalazioni pervenute attengono al rispetto dei principi contenuti nella legge n. 675/1996 in ambiti istituzionali deputati a svolgere compiti in materia di giustizia (uffici giudiziari), nonché presso organismi che operano a supporto dei primi (forze di polizia in genere).

In particolare sono stato segnalati alcuni casi di mancato rispetto del segreto d'ufficio o del segreto d'indagine, a volte anche in riferimento a particolari dati sensibili oggetto anche di segreto professionale (cfr. comunicato stampa n. 7 dell'8 marzo 1999 relativo ad un omicidio a Gravina di Puglia, in Bollettino n. 8, pag. 67).

Per quanto riguarda il diritto di cronaca, sono stati portati all'esame dell'Autorità alcuni casi nei quali poteva darsi lecitamente notizia dell'esistenza di alcuni provvedimenti di ordine giudiziario attinenti anche a procedimenti in corso (cfr. nota del 16 giugno 1999, relativa all'avvenuta presentazione di una richiesta di rinvio a giudizio, notizia diffusa unitamente ad altri dati relativi ad un imprenditore vittima di minacce estorsive, divulgati però dal giornalista nell'ambito di un corretto esercizio del diritto di cronaca, in quanto acquisiti in occasione di una conferenza stampa

2.8.1
Privacy e attività
giornalistica
quadro della
normativa
vigente

2.8.2
Rispetto del
segreto d'ufficio
professionale
investigativo

tenuta dalle autorità inquirenti e di polizia). Casi che sono stati invece distinti da quella area più ristretta nella quale il codice di procedura penale prevede invece determinate ipotesi temporanee di segreto in relazione a specifiche situazioni.

La problematica ha però portato ad evidenza non solo la dialettica cronaca-segreto, ma anche ipotesi di indebite "fughe" di notizie che possono derivare a volte dalla rivelazione di notizie e documenti da taluna delle parti del procedimento, altre dal non corretto comportamento di coloro che hanno accesso agli atti in ragione del proprio servizio o ufficio. In altri casi, gli episodi segnalati presuppongono invece la verifica della correttezza della raccolta dei dati da parte di operatori nel campo dell'informazione, il che rende più articolata la questione, risultando spesso non agevole stabilire dove terminino le responsabilità che si radicano negli uffici dai quali le notizie fuoriescono e dove inizino, invece, quelle di coloro che sono interessati all'acquisizione di una data informazione (v. la lettera del 5/3/1999 indirizzata dal Garante all'Osservatore Romano, riportata in Bollettino n. 8, pag. n. 102, e il provvedimento del 16/2/2000 relativo alla diffusione di dati relativi allo stato di salute di un automobilista invalido civile e del relativo coniuge affetto da una grave patologia).

Segnatamente sulle modalità in base alle quali si realizza la raccolta da parte degli organi di informazione di dati attinenti a procedimenti giudiziari in corso, appare pertanto necessario, per far fronte alla domanda sociale di cui si è detto, mantenere alto il grado di attenzione, sì da promuovere anche nell'ambito che qui interessa la piena affermazione della cultura del rispetto della sfera privata, e in particolare della riservatezza e della dignità delle persone coinvolte.

2.8.3
Attività
giornalistica
e principi
di cui
all'art. 9 legge
n. 675/1996

Premesso che, come più volte ribadito dall'Autorità (v. provvedimento del 16/2/2000), la legge n. 675/1996 e il citato codice deontologico riconoscono piena possibilità di esplicazione al diritto di cronaca, anche in riferimento ai dati sensibili (art. 25 della legge) e nei casi in cui l'informazione assuma carattere dettagliato (art. 6 del codice), è chiaro, però, che ciò deve aver luogo nel rispetto di alcune garanzie di fondo che l'ordinamento ha inteso apprestare a tutela dei cittadini.

Da questo punto di vista, con riguardo ai principi cui deve essere ispirato il trattamento dei dati da parte del giornalista (come pure di pubblicisti e praticanti e di chiunque, in base all'art. 25 della legge, tratta i dati per finalità di pubblicazione o di pubblicazioni di saggi e articoli), l'Autorità ha avuto modo di constatare che in un certo numero di casi le segnalazioni pervenute attengono a vicende nelle quali si configurano profili di mancato rispetto da parte degli organi di informazione dei criteri (di liceità, correttezza, esattezza, e così via) fissati nell'art. 9 l. n. 675/1996.

Al riguardo, pertanto, appare opportuno richiamare quanto è stato puntualizzato nel ricorso incidentale per cassazione proposto dall'Autorità avverso il decreto del Tribunale di Milano che, in accoglimento di un ricorso in opposizione ex art. 29, comma 6, l. n. 675/1996, ha annullato una decisione adottata dal Garante il 19 aprile 1999 (in Bollettino n. 8, pag. 31) all'esito di una procedura di ricorso regolata dalla norma sopraindicata (nel caso di specie, l'interessata aveva lamentato la lesione della propria identità personale nell'ambito della cronaca giornalistica, in relazione all'utilizzazione del cognome del coniuge defunto). Nel ricorso incidentale, l'Autorità ha infatti precisato che talune previsioni contenute nel codice deontologico, e segnatamente quelle rinvenibili nel relativo art. 4 ("il giornalista corregge senza ritardo errori ed inesattezze, anche in conformità al dovere di rettifica nei casi e nei modi stabiliti dalla legge"), recano precetti coerenti con quelli di cui all'art. 9 l. n. 675/1996, e che ne rafforzano l'efficacia.

La rilevanza dei principi sanciti dal citato art. 9 spiega effetto, in particolare, per quanto attiene ai canoni di pertinenza e non eccedenza (v. comunicato stampa del 7/4/1999, in Bollettino n. 9, pag. 81), dei quali coloro che esercitano l'attività giornalistica devono tenere conto. Detti prin-

cipi, infatti, operano anche nei casi in cui talune categorie di soggetti risultano autorizzate dalla legge ad operare il trattamento dei dati personali prescindendo dal consenso dell'interessato, sicché il loro eventuale mancato rispetto è circostanza di per sé idonea ad esporre gli autori delle eventuali violazioni alle conseguenti responsabilità.

D'altra parte, la necessità che nell'esercizio dell'attività giornalistica venga assicurato costantemente il rispetto dei principi sopraindicati assume carattere di priorità segnatamente con riguardo al trattamento di dati relativi a minori, considerata anche la delicatezza del quadro psicologico che contraddistingue l'adolescente in formazione.

2.8.4
Protezione
di minori e
malati

Da questo punto di vista, il flusso delle richieste di intervento pervenute all'Autorità evidenzia una situazione che richiede attenta considerazione, soprattutto in riferimento alle ipotesi nelle quali è riscontrabile l'utilizzazione di elementi che, specie se posti in combinazione tra di loro (v. provvedimento del 29/3/1999 relativo alla pubblicazione di alcune delicate notizie su una minore avviata alla prostituzione e vittima di atti di violenza e possibili ritorsioni da parte di un'organizzazione criminale), possono portare con facilità all'identificazione del minore interessato, in particolare laddove il contesto territoriale di riferimento sia per qualche ragione limitato (v. provvedimento del 16/6/1999, in Bollettino n. 9, pag. n. 63). Al riguardo, infatti, è noto che l'art. 7, comma 1, del citato codice deontologico vieta in modo espresso, relativamente ai soggetti di minore età, di fornire "particolari in grado di condurre alla loro identificazione", con l'unica eccezione delle ipotesi nelle quali ciò si riveli necessario o opportuno al fine di salvaguardare l'"interesse oggettivo del minore, secondo i principi e i limiti stabiliti dalla Carta di Treviso" (v. il citato provvedimento del 29/3/1999).

E giova aggiungere che, come l'Autorità ha avuto più volte occasione di puntualizzare, eventuali violazioni di questo tipo sono da considerare tanto più gravi quanto più si rivelino inconferenti, come talvolta accade, in rapporto all'attuazione del primario principio dell'essenzialità dell'informazione.

Da ultimo, giova puntualizzare che, in ogni caso, non devono sussistere dubbi circa il fatto che il sistema normativo vigente mira, per quanto qui interessa, a offrire la protezione più ampia al minore. In particolare, è da escludere che l'art. 7, comma 2, del codice deontologico ("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"), possa essere interpretato in senso restrittivo, e in particolare come diretto a vietare la pubblicazione di dati personali di minorenni quasi esclusivamente nei casi in cui questi risultino coinvolti in fatti criminosi, con esclusione degli altri.

Non soltanto, infatti, resta fermo il principio secondo il quale "il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca" (art. 7, comma 3, del codice deontologico in questione), ma anche il senso dell'art. 7, comma 2, quale fatto palese dal suo tenore letterale, impone di estendere l'ambito di applicazione del divieto anzidetto anche ai fatti privi di rilevanza penale (v. provvedimento del 7 ottobre 1999).

Sul piano dei dati idonei a rivelare lo stato di salute, alcuni provvedimenti del Garante hanno dato applicazione all'art. 25 della legge e agli artt. 6 e 10 del codice di deontologia (cfr., ad esempio, il provvedimento del 28 gennaio 2000 relativo alla diffusione di specifiche notizie sulla patologia da cui è affetto un parlamentare, in corso di pubblicazione), chiarendo che anche nel caso di persone note e che esercitano pubbliche funzioni, l'informazione sullo stato di salute deve mantenersi in limiti essenziali e che comunque occorre astenersi dal pubblicare dati analitici di interesse strettamente clinico.

2.8.5
Misure
provvedimentali
e
procedimentali
di tutela

Da ultimo, occorre esaminare le questioni attinenti alle concrete misure provvedimentali e procedimentali adottabili, dalle quali dipende, in definitiva, la stessa efficacia complessiva del sistema di tutela apprestato dal legislatore in materia di trattamento dei dati personali.

Da questo punto di vista, è opportuno aver riguardo innanzitutto alle misure provvedimentali, relativamente alle quali l'Autorità, anche sulla scorta dell'esperienza applicativa maturata a partire dal 1997, ha inteso dare piena attuazione all'intera gamma dei rimedi previsti dalla l. n. 675/1996 che si discostano in parte da quelli tradizionali. Al riguardo, a titolo meramente esemplificativo, appare sufficiente evidenziare che l'Autorità, in alcune decisioni che hanno riconosciuto la fondatezza delle doglianze degli interessati, ha ritenuto, in accoglimento delle richieste di parte, di disporre il blocco (art. 1, comma 1, lett. l), l. n. 675/1996) dei dati volta per volta rilevanti, obbligando il titolare e il responsabile a sospendere ogni ulteriore operazione di trattamento diversa dalla mera conservazione delle informazioni già raccolte (v. il citato provvedimento del 16/2/2000).

Contrariamente all'inibitoria, che per sua natura mira a impedire il compimento dell'atto dal quale si teme possa derivare un pregiudizio, oppure a interdirne la reiterazione, l'istituto del blocco assolve ad una funzione di maggior garanzia, precludendo in radice qualsivoglia trattamento diverso dalla mera conservazione del dato personale non più utilizzabile. E con specifico riguardo all'attività giornalistica questa circostanza assume evidentemente particolare rilevanza perché vincola l'organo di informazione, ove le circostanze lo richiedano, ad astenersi dal diffondere nuovamente i dati in questione anche in modo indiretto, ovvero attraverso la pubblicazione di una o più parti del provvedimento decisorio emanato dall'Autorità.

Ancora, in tema di rettifica dei dati personali (e segnatamente con riguardo ad un caso di lesione del diritto all'identità personale per inesatto riferimento di un certo cognome e dello status di vedova a persona diversa dall'ultima moglie del defunto: cfr. par. 2.8), l'Autorità ha provveduto a ordinare ai responsabili dell'accertata violazione anche di attestare all'interessata che la rettifica era stata portata a conoscenza di coloro ai quali erano stati diffusi i dati in questione (dandosi applicazione all'art. 13, comma 1, lett. c), n. 4, l. n. 675/1996), attraverso la pubblicazione sullo stesso quotidiano, entro una certa data, di un comunicato volto ad informare i lettori che le notizie riportate, erroneamente riferite ad una data persona, riguardavano in realtà un soggetto differente (v. provvedimento del 19/4/1999, in Bollettino n. 8, pag. 31). Un simile obbligo di attestazione, che esula dalla previsione dell'art. 8 l. n. 47/1948, appare di indubbia utilità, perché non soltanto agevola l'esercizio da parte dell'interessato del potere di controllare, secondo la filosofia ispiratrice dell'intera l. n. 675/1996, che l'adempimento degli obblighi di rettificazione gravanti sul titolare o sul responsabile vi sia stato, ma consente conseguentemente al primo di apprestare una pronta reazione di fronte a eventuali irregolarità della rettifica in questione, facendo valere tempestivamente i propri diritti nelle sedi competenti.

Più in generale, è da dire che anche con riguardo all'attività giornalistica l'interessato può esercitare tutti i diritti previsti dall'art. 13 della legge n. 675/1996, in presenza delle relative condizioni, ivi compreso l'istituto dell'opposizione per motivi legittimi al trattamento dei dati di cui al comma 1, lett. d) di tale articolo. Come è stato di recente chiarito (v. provvedimento del 7/3/2000), perché sia ravvisabile la ricorrenza di detti "motivi legittimi" è infatti sufficiente, ad esempio, il preannunciato proposito di procedere ad una ulteriore divulgazione dei dati, idonei a consentire l'agevole identificazione dell'interessato, eventualmente in concorso con altre circostanze, che si assumono lesivi dei diritti di quest'ultimo.

2.9 Attività giudiziarie e di polizia e servizi di sicurezza

L'articolo 4 della legge n. 675/1996, sulla falsariga di quanto previsto circa l'ambito di applicazione della normativa comunitaria, individua alcuni particolari trattamenti svolti in ambito pubblico che, per la specificità e delicatezza delle funzioni perseguite, sono soggetti solo in parte alla generale applicazione della disciplina in materia di protezione dei dati personali introdotta dalla legge stessa.

2.9.1
Particolari
trattamenti
in ambito
pubblico

L'integrale applicazione della disciplina comune è esclusa, in particolare, per i trattamenti effettuati per ragioni di giustizia, per quelli relativi a dati contenuti o destinati a confluire nel Centro elaborazione dati del Dipartimento della pubblica sicurezza o trattati per finalità di prevenzione e repressione dei reati, nonché per i trattamenti effettuati dai servizi di informazione e di sicurezza.

Lo stesso articolo 4, tuttavia, fa salva l'applicabilità a tali trattamenti di alcune disposizioni della medesima legge (richiamate espressamente nel comma 2) riguardanti, in particolare, le modalità e la sicurezza del trattamento, nonché gli accertamenti e i controlli del Garante. Ci si riferisce, in particolare, alle norme che prevedono il dovere di rispettare i principi di correttezza e di "pertinenza" nel trattamento dei dati e l'obbligo di adottare tutte le cautele necessarie a garantire la sicurezza dei dati trattati.

In applicazione di tali principi, anche gli uffici giudiziari o di polizia, come ogni altro soggetto pubblico e privato cui si applica la legge n. 675, possono trattare solo i dati "pertinenti ... e non eccedenti" rispetto alle finalità istituzionali (art. 9, l. n. 675). Devono, inoltre, rispettare le disposizioni in materia di sicurezza dei dati, adottando "idonee e preventive misure di sicurezza" "in modo da ridurre al minimo" i rischi di distruzione dei dati e di accessi non autorizzati agli stessi (art. 15, commi 1 e 2, l. n. 675/1996), ferma restando l'osservanza delle misure minime di sicurezza previste dal d.P.R. n. 318/1999.

Anche nell'anno appena trascorso, il Garante ha pertanto dedicato particolare attenzione all'individuazione dei limiti in cui tali disposizioni attualmente si applicano ai trattamenti "parzialmente esclusi", in attesa che la materia sia disciplinata compiutamente. Scaduta, infatti, la delega al Governo per la piena attuazione dei principi previsti dalla legge n. 675 nell'ambito di specifici settori, già attribuita dalle leggi n. 676/1996 e n. 344/1998, attualmente è in discussione al Senato un disegno di legge (AS 4178) che mira a rinnovare tale delega per consentire al Governo di completare gli interventi normativi richiesti.

L'Autorità garante ha infine proseguito, in conformità alla legge n. 675/1996, l'attività di verifica su specifici trattamenti di dati personali effettuati presso il SISMI, il SISDE e il CESIS, effettuando accertamenti in riferimento alle segnalazioni pervenute all'Autorità dai soggetti interessati. I controlli sono stati eseguiti secondo le modalità già osservate nel corso del precedente anno, anche in questo caso con piena collaborazione da parte dei predetti organismi.

Per quanto riguarda i trattamenti di dati personali svolti "per ragioni di giustizia" nell'ambito di uffici giudiziari, del Consiglio superiore della magistratura o del Ministero della giustizia (art. 4, comma 1, lett. d), l. n. 675) i principi descritti sono direttamente applicabili benché le norme di settore, specie processuali, antecedenti alla legge n. 675/1996 non siano state più ampiamente integrate e arricchite alla luce dei nuovi principi in materia di trattamento dei dati personali introdotti dalla legge stessa, come previsto dalla citata legge delega n. 676.

2.9.2
Trattamenti
di dati per
finalità di
giustizia

È quanto il Garante ha ad esempio ribadito nel provvedimento adottato il 29 febbraio 2000

in ordine ai trattamenti effettuati nell'ambito di un giudizio per il risarcimento dei danni subiti da persone affette da sindromi contratte a seguito della somministrazione di emoderivati infetti, nel quale un legale aveva rappresentato l'esigenza che fossero adottate dal tribunale misure a tutela della riservatezza dell'identità dei ricorrenti.

Il Garante ha precisato che la circostanza che i suddetti principi della legge n. 675 non sono stati ancora ulteriormente sviluppati sul piano normativo nell'ambito di specifiche norme processuali non deve far ritenere inoperanti i principi stessi, i quali dovrebbero essere già oggi tradotti in concrete misure attuative anche di carattere organizzativo, opportunamente modulate in rapporto alle diverse vicende processuali, tenendo conto della specificità delle prerogative riconosciute all'autorità giudiziaria.

Diversamente, la mancata adozione durante le varie fasi processuali di più efficaci cautele condizionerebbe, nei fatti, il diritto di difesa costituzionalmente tutelato potendo addirittura comportare, nei casi più gravi, la rinuncia della parte lesa a chiedere il risarcimento dei danni per il timore dell'ampia conoscibilità delle patologie sofferte.

Nell'occasione, il Garante ha segnalato al Governo e al Parlamento l'opportunità che siano introdotte al più presto alcune norme processuali che contemperino meglio le esigenze di accertamento dei fatti nel processo con quella di garantire la riservatezza dei soggetti coinvolti in alcune vicende giudiziarie, nelle quali siano esposti ad ulteriore rischio aspetti particolarmente delicati della persona.

Per quanto attiene ai controlli esercitabili sui trattamenti svolti "per ragioni di giustizia", il Garante, con un provvedimento del 4 maggio 1999, ha precisato che, mentre in applicazione delle disposizioni richiamate nel citato articolo 4, comma 2, è possibile inviare al Garante una segnalazione o un reclamo ai sensi dell'articolo 31, comma 1, lett. d), per sollecitare un controllo sulla liceità dei trattamenti, non è invece consentito esercitare i diritti previsti dall'articolo 13 della legge n. 675 rivolgendosi direttamente all'ufficio giudiziario (titolare del trattamento) ed eventualmente con ricorso al Garante in base all'articolo 29 della stessa legge n. 675.

Anche sotto questo aspetto, peraltro, la legge-delega permetterà di valutare la possibilità di sperimentare altri strumenti di garanzia e di trasparenza in favore degli interessati, volti ad esempio a permettere loro di poter esercitare in modo più diretto i diritti di cui all'art. 13 della legge n. 675, tenendo conto della specificità dei trattamenti in questione, senza necessità, quindi, di dover presentare necessariamente una segnalazione o un reclamo.

Il Garante, da ultimo con un provvedimento del 27 ottobre 1999 in risposta ad un quesito presentato dal Consiglio di Stato (in Bollettino n. 10, pag. 78), ha nuovamente precisato che fra le disposizioni non abrogate dalla legge n. 675 vi rientrano anche le norme riguardanti la conoscibilità del calendario dei processi, della pubblicità delle udienze e degli esiti dei giudizi, nonché quelle concernenti l'accesso ai registri giudiziari e l'estrazione di copia di atti processuali, vertendosi in una materia che resta prevalentemente regolata dai codici e dalle altre norme processuali. Trattandosi, peraltro, di attività svolte "per ragioni di giustizia", anche questi aspetti potrebbero essere oggetto di intervento da parte del legislatore, ferma restando, sempre, la loro attuale assoggettabilità al principio di pertinenza.

Infine, in una nota del 26 ottobre 1999, l'Autorità ha chiarito che sono da ritenersi applicabili anche al processo contabile ed amministrativo le cautele richieste nella notifica degli atti del processo a garanzia della riservatezza della persona interessata e, in particolare, nei confronti del terzo cui venga notificato l'atto (ad es. busta chiusa), cui il Garante ha fatto riferimento nel noto provvedimento del 22 ottobre 1998 (v. *Relazione per l'anno 1998*, pag. 23). Al riguardo, il Garante ha rilevato con soddisfazione che è stato recentemente approvato da un ramo del Parlamento un disegno di legge (AC 6735) che recepisce le indicazioni fornite in quest'ultimo provvedimento, non solo rispetto alle notificazioni degli atti del processo (si prevede infatti la modifica di alcune disposizioni dei codici di rito e della normativa sulle notifiche a mezzo posta), ma anche nell'ambito di procedimenti amministrativi.

Sono da segnalare infine, nel quadro delle diverse iniziative dell'Autorità garante sul tema dei trattamenti di dati personali a fin di giustizia.

- a) il parere espresso dall'Autorità stessa sul regolamento di disciplina della Commissione per le adozioni internazionali di cui all'art. 7 della legge 31 dicembre 1998, n. 476 (regolamento approvato con d.P.R. 1 dicembre 1999, n. 492);
- b) la deliberazione adottata il 20 ottobre 1999 dal Consiglio Superiore della magistratura in riferimento al più generale problema della tutela della riservatezza in occasione delle notificazioni e comunicazioni di atti giudiziari e amministrativi già oggetto del provvedimento del Garante del 22 ottobre 1998. Il Consiglio, con la deliberazione, si è occupato della prassi seguita per l'attività della Sezione disciplinare e per i procedimenti delle commissioni consiliari;
- c) il provvedimento adottato il 30 novembre 1999 dal Garante in riferimento ad una segnalazione con la quale un magistrato aveva lamentato le modalità con le quali il dirigente dell'ufficio giudiziario aveva disposto la sua sostituzione in una udienza preliminare, includendo in un avviso al pubblico il referto della certificazione medica. L'Autorità ha constatato che la sostituzione rientra tra i provvedimenti adottati per «ragioni di giustizia», ai quali l'art. 22 della legge in materia di dati sensibili non è attualmente applicabile; ha però constatato l'eccessività dell'indicazione nel provvedimento di sostituzione della diagnosi medica dell'accertamento dell'impedimento del magistrato, segnalando all'ufficio giudiziario l'esigenza di apportare le modifiche opportune ai trattamenti di dati in questione.

Con riferimento ai trattamenti svolti per finalità di polizia, il Garante ha chiarito alcuni importanti aspetti applicativi della disciplina in materia di protezione dei dati personali, ad esempio in occasione di una risposta fornita ad una compagnia aerea circa le modalità di acquisizione da parte delle forze di polizia di dati relativi a passeggeri dei voli (provvedimento del 6 ottobre 1999, in Bollettino n. 10, pag. 69).

Nella circostanza, il Garante ha sottolineato la necessità di distinguere fra le richieste di informazioni formulate nell'ambito di attività di indagine di polizia giudiziaria e le richieste avanzate da pubbliche autorità per altre finalità istituzionali.

Le prime possono infatti ricondursi ai trattamenti di cui al citato articolo 4 e in particolare:

- a quelli svolti per *“ragioni di giustizia”*, quando le richieste di informazioni sono effettuate su delega dell'autorità giudiziaria (art. 4, comma 1, lett. d), l. n. 675; v. par. precedente);
- ai trattamenti effettuati *“per finalità di ...prevenzione, accertamento o repressione di reati in base ad espresse disposizioni di legge”*, quando derivano da un'attività investigativa o d'indagine di iniziativa degli organi di polizia (art. 4, comma 1, lett. e), l. n. 675).

A tali richieste, purché sia chiaro il riferimento ad una attività di polizia giudiziaria, deve quindi darsi corso in base al codice di procedura penale, non ostandovi l'applicabilità della legge n. 675. Esse, però, essendo parimenti soggette al principio di pertinenza, dovranno, nei limiti del possibile, essere circostanziate sotto il profilo oggettivo e temporale (ad es. circostanze di luogo, linee e numero dei voli).

Quando, invece, le richieste avanzate da forze di polizia o da altre pubbliche autorità non sono riconducibili all'esercizio di poteri di polizia giudiziaria (o, comunque, alle altre funzioni specificamente indicate nell'articolo 4), ad esse si applica pienamente la disciplina generale della legge n. 675 e, in particolare, quella prevista per i flussi informativi fra soggetti pubblici e privati (artt. 27

2.9.3
Forze
di polizia e
C.e.d del
Dipartimento
della pubblica
sicurezza

e 20, l. n. 675), in base alla quale un soggetto privato può dare comunicazione di dati personali *“in adempimento di un obbligo legale”* oppure, in mancanza di uno degli altri presupposti di cui all'art. 20, in presenza del necessario consenso dell'interessato. Il Garante ha pertanto richiamato l'attenzione delle pubbliche autorità sulla necessità di indicare nella richiesta la normativa in base alla quale è fatto obbligo di fornire all'autorità le informazioni richieste, al fine di fugare ogni eventuale dubbio circa l'obbligatorietà della risposta.

Per quanto attiene al profilo dei controlli sui trattamenti effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza, il Garante, su segnalazione di un cittadino non soddisfatto del riscontro ottenuto dagli uffici del Dipartimento circa la sua istanza di verifica dei dati, con nota del 16 febbraio 1999, ha richiamato ulteriormente l'attenzione di tali uffici — nel quadro anche del rapporto di collaborazione già avviato — sulla necessità di definire al più presto i limiti temporali entro i quali possono essere conservati i dati inseriti nei vari archivi di polizia. La verifica deve essere effettuata alla stregua della previsione dell'articolo 9, comma 1, lett. e) della legge n. 675, applicabile anche a tali trattamenti, che tutela il c.d. *diritto all'oblio* su determinate vicende della propria vita quando sia ormai raggiunto lo scopo per il quale i dati sono stati a suo tempo raccolti o successivamente trattati (si pensi, ad es., ad una sentenza di assoluzione, ecc). Sarà quindi oggetto di ampi approfondimenti in rapporto alla conformità a tale disposizione — e alla sufficienza della misura — la possibilità rappresentata dal Dipartimento di procedere ad una completa ristrutturazione degli schedari del Centro e di individuare alcune categorie di provvedimenti e di informazioni che, trascorso un certo periodo di tempo, si ipotizza di poter in futuro escludere dai primi livelli di accesso e rendere eventualmente accessibili solo ad un livello *“superiore”* di consultazione.

Il Garante ha segnalato inoltre al Dipartimento, in termini più generali, la necessità che, anche attraverso nuove istruzioni ai competenti uffici centrali e periferici, in caso di esercizio del diritto di accesso e di rettifica ai sensi dell'articolo 10 della legge 1 aprile 1981, n. 121, sia assicurata una risposta agli interessati esauriente e tempestiva.

Sul punto, il Garante ha pure chiarito, con una decisione del 7 ottobre 1999, che per i trattamenti effettuati dal predetto C.e.d. l'interessato può esercitare i suoi diritti di verifica e di rettifica direttamente nei confronti del Dipartimento (Ufficio per il coordinamento e la pianificazione delle forze di polizia), e che tale *“accesso diretto”* è da considerarsi la procedura più *“naturale”* per verificare già in via amministrativa i dati oggetto di trattamento (ferma restando la possibilità di rivolgersi al Garante con eventuali segnalazioni o reclami o all'autorità giudiziaria in base al citato articolo 10), non operando, del resto, la diversa procedura per ricorso al Garante ai sensi dell'articolo 29 della legge n. 675 e 18 e ss. del d.P.R. n. 501/1998.

Ferma restando, quindi, l'inammissibilità dei ricorsi eventualmente presentati, la loro erronea proposizione non pregiudica l'instaurazione da parte del Garante di un autonomo procedimento di verifica su quanto comunque segnalato dall'interessato in ordine ai dati che lo riguardano, in particolare ai sensi dell'articolo 31, comma 1, lett. d) e p).

Resta comunque condivisa l'esigenza che anche attraverso i decreti delegati che potranno essere adottati in base al disegno di legge attualmente in discussione al Senato, siano introdotte modifiche sostanziali alle procedure in atto in modo da rendere più snelle, ma al tempo stesso più efficaci e trasparenti le necessarie verifiche.

Al Garante, quale Autorità di controllo sulla sezione nazionale del Sistema d'Informazione Schengen (SIS), sono state sottoposte n. 59 (al 10 aprile 2000) richieste di verifiche da effettuare presso l'archivio nazionale N.SIS ai sensi dell'articolo 11 della legge 30 settembre 1993, n. 388, di ratifica dell'Accordo e della relativa Convenzione applicativa, al fine di accertare l'eventuale registrazione di dati personali dei soggetti interessati e la legittimità dei relativi trattamenti alla stregua dei principi contenuti nella Convenzione medesima e nella legge n. 675.

Circa 21 casi si riferiscono a richieste presentate presso omologhe autorità di garanzia degli altri Paesi aderenti all'Accordo, le quali, ai sensi dell'art. 114, comma 2, della Convenzione, hanno chiesto al Garante di effettuare accertamenti in relazione a segnalazioni inserite nel SIS da organi del nostro Paese (18 richieste provenienti dall'autorità di controllo francese; 2 dall'autorità tedesca e 1 da quella belga). Le rimanenti richieste di accesso sono state presentate direttamente dagli interessati o per il tramite di uffici diplomatico-consolari.

Nella prevalenza dei casi, le istanze sono volte a conoscere le cause dei provvedimenti amministrativi sfavorevoli adottati nei confronti degli interessati in materia di ingresso e soggiorno nel nostro Paese; in alcuni casi attengono invece al diniego del rilascio di visti.

Nel corso di un incontro di lavoro con l'ufficio SIRENE del Dipartimento della pubblica sicurezza, nel quale sono stati discussi alcuni aspetti applicativi della materia, si è peraltro rappresentata la necessità che, anche attraverso nuove istruzioni ai competenti uffici periferici, sia assicurata la massima speditezza alle procedure per il riscontro delle verifiche effettuate dal Garante.

L'incremento del numero delle richieste pervenute al Garante rispetto all'anno precedente (appena 5), soprattutto nel secondo semestre del 1999 (numero, peraltro, superiore a quello delle richieste ricevute dalla gran parte delle omologhe autorità nazionali degli altri Paesi) è probabilmente da ascrivere anche al buon esito, anche nel nostro Paese, della campagna informativa sui diritti del cittadino nei confronti del Sistema d'Informazione Schengen, deliberata lo scorso anno dall'Autorità comune di controllo Schengen (ACC) in tutti i Paesi aderenti all'Accordo.

In Italia, l'iniziativa dal titolo *"Il Sistema d'informazione Schengen vi riguarda"* è stata attuata dal Garante attraverso la stampa e la distribuzione presso valichi di frontiera esterni, rappresentanze diplomatiche e uffici consolari di centinaia di manifesti e migliaia di opuscoli plurilingue sui diritti dei cittadini segnalati nel SIS, basati su modelli identici per tutti i Paesi e recanti anche l'indicazione delle autorità di garanzia cui rivolgersi per informazioni e richieste d'intervento.

2.10 Reti telematiche e servizi di telecomunicazione

L'evoluzione delle tecnologie nel settore delle telecomunicazioni favorisce il moltiplicarsi di nuovi servizi e funzioni di grande utilità ed interesse per i cittadini, rendendo sempre più rapido lo sviluppo della Società dell'Informazione (con l'abbattimento di ogni limite geografico o confine nazionale) e, nel contempo, più evidenti le contraddizioni tipiche di tale società, in particolare sotto la duplice forma della possibilità di raccolta massiccia di dati e dell'offerta agli utenti di prestazioni gratuite in cambio del loro uso.

Si pone, quindi, il delicato problema delle garanzie da assicurare ai cittadini, soprattutto nelle fasce più deboli, al fine di tutelare la loro vita privata, identità e dignità, anche in relazione alla possibilità di utilizzare le informazioni raccolte presso i consumatori per delineare i loro profili e per classificare i loro comportamenti. L'espandersi di avanzati servizi di telecomunicazione e di reti tele-

2.9.4
Trattamenti
relativi
all'Accordo
di
Schengen

2.10.1
Prima
attuazione del
d.lg. 171/1998

matiche ha fatto pertanto emergere il ruolo centrale assunto in tale campo dalle normative a tutela del diritto alla riservatezza, intesa non più come mera esigenza di riserbo od isolamento dalla curiosità altrui, ma come necessità di proteggere in modo più organico e sostanziale il bene primario della Società dell'Informazione, i dati personali, utilizzati ormai come vera e propria merce di scambio.

In base alle recenti disposizioni comunitarie e nazionali in materia, i cittadini devono essere messi in grado di esercitare consapevolmente le proprie scelte in ordine al trattamento dei dati che li riguardano, ferma restando la loro piena libertà di aderire ai nuovi servizi di telecomunicazione e di fornire i propri dati, ovvero di permettere un libero accesso nella propria sfera privata, personale o familiare.

Come riportato nella *Relazione per l'anno 1998*, alcune importanti norme sulla tutela dei dati personali nel settore delle telecomunicazioni sono state introdotte in Italia con il decreto legislativo 13 maggio 1998, n. 171, con il quale è stata data attuazione, nel quadro dei principi generali stabiliti dalla legge n. 675/1996, al primo corpo di disposizioni comunitarie adottate su questo tema (contenute nella direttiva comunitaria n. 97/66/CE: cfr. *Relazione per l'anno 1998*, pagg. 69 ss.).

Si tratta di norme particolarmente innovative e complesse, anche per la specificità e il continuo evolversi degli aspetti tecnici presi in considerazione, rispetto alle quali sono emersi, nel corso di quest'anno, diversi problemi interpretativi ed applicativi, con particolare riguardo alla correttezza dei comportamenti finora tenuti e delle procedure successivamente attivate dai fornitori dei servizi di telecomunicazioni nei confronti degli utenti.

In particolare, il Garante è intervenuto, d'ufficio o su istanza di singoli cittadini, imprese od altri organismi, nei confronti dell'attivazione e dello svolgimento di diversi servizi di telecomunicazione, per verificarne la conformità alle norme sulla protezione dei dati, avviando così procedimenti di indagine e di segnalazione delle necessarie modifiche, nonché fornendo talune prime indicazioni di carattere generale, utili anche per tutti gli altri operatori che offrono servizi analoghi.

Oltre ai casi più rilevanti che saranno esaminati nei successivi paragrafi, va ricordato che sono stati avviati nel 1999 anche alcuni accertamenti relativi al delicato tema della c.d. "localizzazione" degli apparecchi di telefonia mobile, con richiesta ai tre gestori di telecomunicazioni mobili nazionali di dettagliate informazioni, anche sulla base di una puntuale relazione tecnica, su: a) precise modalità di raccolta ed eventuale registrazione dei dati relativi ai luoghi nei quali si trovano gli apparecchi, specificando se i dati stessi sono acquisiti solo in occasione delle conversazioni; b) tipi di dati raccolti e periodo di eventuale conservazione; c) categorie di incaricati aventi accesso a tali dati all'interno delle strutture societarie; d) possibilità che le predette operazioni di trattamento dei dati riguardino solo gli abbonati o anche carte ricaricabili. L'Autorità si è infatti riservata di effettuare una valutazione complessiva del problema alla luce dei chiarimenti, anche tecnici, forniti dai gestori, in modo da verificare la presenza di eventuali irregolarità rispetto alla legge sulla privacy e prospettare idonee misure ed accorgimenti per la tutela dei diritti degli interessati.

A seguito di numerose segnalazioni pervenute in proposito, il Garante ha, altresì, iniziato un'apposita indagine nei confronti di alcune società di telefonia fissa e mobile allo scopo di valutare compiutamente le modalità di attuazione del decreto legislativo n. 171/1998 relativamente ai servizi inerenti all'identificazione della linea chiamante e alle chiamate di disturbo (v. artt. 6 e 7 del d.lg. n. 171 cit.). In proposito, l'Autorità intende approfondire gli aspetti riguardanti: le modalità di attivazione e funzionamento di tali servizi, delle relative funzioni e delle altre prestazioni connesse; le reti e gli apparecchi per i quali gli stessi servizi sono disponibili, nonché il quadro analitico dei costi addebitati agli abbonati, inclusi quelli relativi all'installazione di eventuali ulteriori dispositivi; le misure previste per la presentazione dell'identificazione della linea chiamante, per la sua eliminazione e per il rifiuto delle chiamate entranti. I gestori telefonici richiesti hanno reso già disponibili i servizi di identificazione della linea chiamante e di disabilitazione o restrizione della presentazione di tale linea, con modalità pressoché analoghe nel campo della telefonia mobile (ove pos-

sono essere attivati gratuitamente dagli utenti), a differenza della telefonia fissa (in cui sono onerose e possono richiedere l'impiego di apparecchi necessari per la visualizzazione dei dati). Vi sono invece alcune difficoltà di applicazione delle disposizioni concernenti il rifiuto delle chiamate entranti e le chiamate di disturbo, rispetto alle quali le società hanno evidenziato la carenza, allo stato, di idonee misure e parametri tecnici per l'attivazione e l'erogazione di tali servizi. Nell'ambito di questo procedimento, il Garante sarà pertanto chiamato ad indicare ai fornitori alcune linee guida per la corretta attuazione delle richiamate norme del d.lg. n. 171/1998.

Ulteriori problemi relativi all'applicazione delle disposizioni del decreto n. 171, che sono sorti nel corso del 1999, riguardano, in particolare, i temi degli elenchi degli abbonati ai servizi telefonici (art. 9) e delle chiamate indesiderate (art. 10). Nel primo tema sono sostanzialmente comprese anche due questioni, tra loro collegate, relative alle utenze telefoniche riservate e all'utilizzabilità degli elenchi a fini di *marketing*. Al riguardo, il Garante ha chiarito che, secondo l'art. 9 del d.lg. n. 171/1998, l'abbonato, gratuitamente e con richiesta documentata per iscritto, ha diritto di non essere incluso negli elenchi (sia cartacei, sia su supporto ottico o magnetico), di ottenere che il suo indirizzo sia omissso anche in parte e, se fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso (v. anche il comunicato stampa n. 22 del 25 marzo 1999, pubblicato sul Bollettino n. 8 del 1999, pag. 75).

In ordine al tema delle chiamate indesiderate, ossia dell'invio in forma automatizzata di pubblicità sugli apparecchi degli utenti, sono poi all'esame dell'Autorità alcune segnalazioni circa il rispetto da parte di alcune società degli adempimenti di informativa agli interessati e, ove necessario, della richiesta del loro consenso in virtù di quanto previsto sia dalla legge n. 675/1996, sia dal d.lg. n. 171 e, ora, anche dal decreto legislativo n. 185 del 1999 sui contratti a distanza. Il tema viene comunque ripreso, più approfonditamente, nei successivi paragrafi relativi ai servizi di telefonate gratuite con spot e di accesso gratuito ad Internet.

Il Garante è tornato ad occuparsi, anche nel corso del 1999, del problema della tutela della riservatezza nelle fatture, le c.d. "bollette", inviate dai fornitori con il dettaglio degli addebiti relativi alle telefonate effettuate dagli abbonati e, in particolare, della corretta attuazione della misura del "mascheramento" delle ultime tre cifre dei numeri chiamati, introdotta dal decreto legislativo n. 171 del 1998 (art. 5).

2.10.2
Fatturazione
dettagliata

L'occasione per il nuovo esame dell'argomento è stata offerta da alcune osservazioni della D.G. XIII della Commissione europea sulle quali il Ministero delle comunicazioni ha chiesto il parere del Garante, concernenti la citata disposizione del d.lg. n. 171 che, obbligando i gestori ad oscurare gli ultimi tre numeri delle chiamate, avrebbe recepito, in modo ritenuto dalla D.G. troppo restrittivo, le norme comunitarie che disciplinano la materia (ossia la direttiva n. 97/66/CE richiamata nel paragrafo precedente). Secondo la D.G., le norme comunitarie sulla telefonia avrebbero individuato la misura del "mascheramento" in alternativa alla previsione di altre misure, quale il pagamento di singole chiamate con modalità diverse dalla "bolletta", imponendo agli operatori di telecomunicazioni (sempre nel rispetto delle norme sulla privacy) l'obbligo di fornire gratuitamente un livello base di dettaglio nelle fatture telefoniche sufficiente a permettere la verifica dei costi sostenuti dall'abbonato. La D.G. ha pertanto suggerito una modifica del decreto legislativo n. 171/1998, in modo da consentire il "mascheramento" delle ultime tre cifre solo su esplicita richiesta dell'abbonato.

L'Autorità, come illustrato nella *Relazione del 1998* (pag. 71 ss.), era intervenuta già sulla questione nell'ottobre del 1998, con un provvedimento con il quale aveva chiarito che il meccanismo del "mascheramento" delle ultime tre cifre già oggi non preclude agevoli accertamenti da parte

degli abbonati in caso di loro contestazioni degli addebiti o di serie necessità di verifica, senza con ciò violare le disposizioni sulla privacy. In queste ultime ipotesi, infatti, il fornitore non dovrebbe opporre un rifiuto e può comunicare anzi per intero i numeri relativi alle chiamate contestate o controverse, qualora l'abbonato chieda di identificare puntualmente alcune chiamate effettuate non per mera curiosità, ma al fine di verificare la correttezza degli importi addebitati e di tutelare i propri diritti in sede giudiziaria. Sotto questo profilo, la legge n. 675 non ostacola l'esercizio dei diritti degli abbonati, rappresentando piuttosto la fonte normativa che permette ai fornitori di servizi di evidenziare anche le cifre mascherate laddove, appunto, emergano serie e concrete esigenze di controllare le fatturazioni e di far valere, anche per via legale, le proprie pretese al corretto adempimento del contratto telefonico.

Nella risposta al Ministero delle comunicazioni (v. il provvedimento del 5 ottobre 1999, pubblicato sul Bollettino n. 10/1999, pag. n. 51), il Garante ha rilevato anzitutto che nella nota della D.G. non si contesta la conformità del d. lg. n. 171 al diritto comunitario, ma si pone una questione di ragionevolezza e funzionalità della norma. La direttiva europea in materia di telecomunicazioni non individua precise misure per conciliare i diritti degli abbonati con il diritto alla vita privata degli utenti chiamanti e degli abbonati chiamati, ma indica unicamente alcune possibili soluzioni esemplificative utilizzabili a discrezione degli Stati membri. Tra gli esempi prospettati figurano sia le modalità di pagamento diverse dall'addebito nella fatturazione (carte di credito, carte telefoniche prepagate anche anonime ecc.), sia, in alternativa, il mascheramento di alcune cifre.

Il decreto legislativo n. 171 del 1998, ha sottolineato il Garante, ha previsto entrambe queste misure, in quanto ha introdotto sia il "mascheramento" obbligatorio delle ultime tre cifre, sia l'obbligo, per i fornitori, di far sì che *"i servizi richiesti e le chiamate effettuate da qualsiasi terminale possano essere pagate con modalità alternative alla fatturazione anche anonime"* (art. 5, comma 1). Infatti, secondo l'Autorità, il sistema prospettato dalle norme comunitarie mira a temperare il diritto dell'abbonato pagante di verificare la correttezza degli addebiti e il diritto alla riservatezza degli utenti chiamanti e degli abbonati chiamati. In generale, l'istituto del "mascheramento" di alcune cifre può risultare utile, in quanto riduce il numero dei dati personali in circolazione, specie nell'attuale fase di evoluzione delle telecomunicazioni in Italia, caratterizzato da un ritardo nell'attuazione delle innovazioni tecnologiche che avrebbero dovuto già rendere facilmente accessibili al pubblico alcune modalità alternative di pagamento.

Il "mascheramento", tuttavia, non soddisfa pienamente diverse tipologie di abbonati e il Garante stesso ha segnalato, oltre ai casi indicati dalla D.G. (numeri brevi di sei cifre e traffico locale), l'ipotesi dell'abbonato unico utente dell'apparecchio e quella di un'utenza affari presso la quale si debbano distinguere determinati tipi di chiamata.

Per ovviare a queste possibili insoddisfazioni della clientela, è apparsa quindi opportuna, ad avviso del Garante (che, del resto, l'aveva già indicata nel citato provvedimento del 5 ottobre 1998), una riflessione a livello normativo sul "mascheramento" delle ultime tre cifre, che deve però essere affiancata dal contestuale rispetto, da parte dei fornitori, dell'obbligo di introdurre le predette modalità alternative di pagamento, anche al fine di assicurare un accesso anonimo o rigorosamente privato ai servizi di telecomunicazione offerti al pubblico, quali carte telefoniche, oppure possibilità di pagamento con carta di credito. Solo l'effettiva introduzione di tali strumenti renderebbe infatti possibile la modifica dell'istituto del "mascheramento".

Alla luce di queste considerazioni, la soluzione proposta dalla D.G. di demandare all'abbonato pagante la scelta se usufruire o meno di una fatturazione "mascherata", è apparsa in via di principio praticabile, ma non attuabile concretamente se non si renderanno contestualmente effettive le modalità alternative di pagamento. Altrimenti, infatti, si affiderebbe alla volontà di una sola parte (l'abbonato pagante) il bilanciamento tra diritti che sono riconosciuti anche ad utenti chiamanti e abbonati chiamati.

Considerato che la questione sollevata dalla D.G. non può essere valutata in relazione ad un solo contesto nazionale, ma verificata all'interno dell'Unione europea (dove, peraltro, la direttiva in materia di telecomunicazioni e privacy non è stata integralmente recepita), il Garante ha evidenziato l'esigenza che la problematica sia discussa nella sede più appropriata e cioè in seno al Gruppo di lavoro delle autorità garanti europee, istituito a Bruxelles in attuazione dell'art. 29 della direttiva n. 95/46/CE e della direttiva n. 97/66/CE, con il compito di verificare l'attuazione del diritto comunitario in tema di protezione dei dati anche nel settore delle telecomunicazioni, analizzarne le eventuali disarmonie ed individuare le modalità più opportune per favorire il suo recepimento.

Per quanto riguarda, poi, il possibile riesame delle disposizioni in materia da parte del legislatore nazionale, l'Autorità ha ritenuto opportuno avviare un'indagine per verificare presso i fornitori italiani di servizi di telecomunicazioni sia lo stato di attuazione del decreto legislativo n. 171 in tema di modalità alternative alla fatturazione, sia il rispetto da parte di questi ultimi delle indicazioni contenute nel richiamato provvedimento dell'ottobre 1998, anche relativamente all'aggiornamento, alle modalità e ai limiti delle procedure concernenti la contestazione delle fatture telefoniche e la "messa in chiaro" dei numeri relativi alle telefonate controverse.

Con tale indagine, nell'ambito della quale sono stati già ascoltati diversi fornitori di telefonia sia fissa, sia mobile, il Garante intende acquisire gli elementi necessari per accertare il grado complessivo di adeguamento delle società operanti in Italia alle novità normative e tecniche sulle modalità di pagamento dei servizi di telecomunicazioni e sulle misure adottate per tutelare la vita privata di abbonati ed utenti, prima di segnalare al Parlamento ed al Governo, anche alla luce degli ulteriori chiarimenti in sede comunitaria, l'opportunità di una revisione delle attuali disposizioni normative.

Va comunque ricordato che, come è emerso in diversi provvedimenti del Garante (cfr., in particolare, due dichiarazioni di non luogo a provvedere su alcuni ricorsi di cui all'art. 29 della legge n. 675, adottate in data 1 e 9 dicembre 1999), che i diritti di accesso ai dati personali previsti dalla legge sulla privacy (art. 13) permettono agli abbonati di accedere ai dati di traffico relativi alle proprie utenze telefoniche, come a qualsiasi altra informazione che li riguardi (anche con riferimento alle chiamate in entrata, come, da ultimo, evidenziato in un parere del 29 novembre, (cfr. comunicato riportato nel Bollettino n. 10 del 1999, pag. 107) concernente un cittadino che, dovendosi difendere in sede giudiziaria, aveva chiesto invano ad un gestore telefonico il rilascio di tali informazioni). Non è legittimo, invece, l'accesso diretto a dati relativi a utenze intestate a terzi, i quali restano conoscibili esclusivamente tramite provvedimento giudiziario.

Occorre fare infine un breve accenno ad un'altra problematica strettamente collegata al tema appena esaminato della verifica dei numeri chiamati nelle fatture dettagliate inviate dalle società telefoniche: il c.d. controllo delle utenze telefoniche da parte dei datori di lavoro, privati e pubblici, nei confronti del proprio personale.

L'Autorità ha, infatti, ricevuto numerosi quesiti e segnalazioni in ordine alla legittimità dell'installazione sul luogo di lavoro di impianti di misurazione del traffico per esigenze di contenimento delle spese o di fatturazione dei costi alla clientela. Tale questione, che il Garante si accinge ad affrontare in una pronuncia di carattere generale, appare particolarmente delicata anche in relazione alle garanzie, ulteriori rispetto agli obblighi previsti dalla legge sulla privacy (relativi, ad es., all'informativa agli interessati), poste dallo "Statuto dei lavoratori" in materia di controllo a distanza dei lavoratori (cfr. l'art. 4 della legge n. 300/1970).

Il tema è direttamente connesso con un altro aspetto di recente emersione che riguarda l'analogica tendenza, consentita da *software* di recente distribuzione, a monitorare o limitare l'accesso a determinati siti Internet da parte del personale dipendente di imprese e pubbliche amministrazioni,

2.10.3
Utilizzazione
di apparecchi
telefonici e
accessi ad
Internet da parte
di lavoratori

come pure dell'effettiva utilizzazione della posta elettronica per esclusive ragioni di ufficio o di servizio. Anche a seguito delle notizie comparse da ultimo sulla stampa, il Garante ha quindi avviato il 13 aprile 2000 un procedimento per verificare la corretta utilizzazione da parte di alcune imprese e pubbliche amministrazioni di programmi per elaboratore utili a fini di filtro o di monitoraggio, anche in riferimento alla segretezza della corrispondenza e alle predette garanzie previste dallo "Statuto".

2.10.4
L'avvio in
Italia
di servizi di
telefonate
gratuite con
spot

La prevista attivazione in Italia di servizi di telefonate gratuite con spot (e in particolare di quello denominato *GratisTel*), ha suscitato particolare interesse e curiosità nell'opinione pubblica, sollevando però alcune questioni relative sia all'offerta di prestazioni gratuite in cambio dell'uso di dati relativi, ad esempio, a proprietà, preferenze e gusti degli utenti, sia all'ascolto dei messaggi pubblicitari da parte degli abbonati chiamati non aderenti al servizio medesimo.

Al fine di verificare la conformità di questi nuovi servizi -e, in specie, di quello citato- alla normativa sulla privacy, l'Autorità ha avviato d'ufficio una approfondita indagine riguardo alle relative modalità e ai connessi trattamenti di dati, sin dal momento dell'annuncio da parte di alcuni organi di stampa (avvenuto nel febbraio del 1999) del loro futuro lancio.

La complessità del problema ha reso necessari ulteriori accertamenti sulle precise modalità tecniche di funzionamento del servizio e sui conseguenti accorgimenti per la tutela dei diritti degli utenti, anche attraverso un'apposita audizione presso l'Ufficio del Garante dei rappresentanti della società che lo gestisce (*GratisT Italia s.r.l.*), nonché mediante una successiva verifica a Milano presso i locali ove sono ubicate alcune apparecchiature utilizzate dalla società.

A conclusione di tale procedimento di indagine, il Garante ha segnalato alla *GratisT Italia s.r.l.* in data 13 novembre 1999 (cfr. Bollettino n. 10/1999, pag. 54) le modifiche necessarie per poter avviare e svolgere il servizio in piena conformità alle garanzie richieste dalla normativa sulla protezione dei dati personali (legge n. 675 del 1996) e anche dalla legislazione sulla tutela della privacy nel settore delle comunicazioni (decreto legislativo n. 171 del 1998).

Il provvedimento adottato dall'Autorità è volto, da una parte, a tutelare pienamente i diritti dei cittadini che si accingono a sottoscrivere questo tipo di contratti e che, in cambio di prestazioni gratuite, prevedono la cessione di dati personali; dall'altra, a garantire il pieno rispetto dei diritti delle persone che ricevono le chiamate destinate ad essere interrotte da spot pubblicitari.

Dalla ricostruzione delle modalità di attivazione e funzionamento del servizio, è emersa anzitutto la necessità di una maggiore attenzione nei riguardi della raccolta e del successivo trattamento dei dati dei sottoscrittori, con particolare riferimento alla chiarezza dell'informativa e alla specificità del consenso, tenuto anche conto dell'intenzione della società di utilizzare i dati per determinare i profili dei consumatori su cui "calibrare" la pubblicità trasmessa durante le conversazioni telefoniche.

Il Garante ha, infatti, evidenziato che il modulo di adesione al servizio *GratisTel* doveva essere perfezionato sotto diversi profili. Le clausole presenti nel modulo dovevano, infatti:

- indicare se il conferimento di alcuni dati è obbligatorio o facoltativo;
- eliminare la richiesta di alcune informazioni non essenziali, come il codice fiscale;
- specificare che l'assenso a ricevere al proprio domicilio materiale pubblicitario, manifestato dal sottoscrittore durante l'ascolto di uno spot (ad esempio con la pressione di un tasto dell'apparecchio telefonico) è espresso in favore della sola società di cui è trasmesso lo spot;
- individuare, riguardo alla cessione dei dati a scopi pubblicitari nei confronti di altre società non direttamente collegate al circuito *GratisTel*, le categorie delle società destinatarie.

L'Autorità ha pertanto invitato la *GratisT Italia s.r.l.* a modificare i moduli del contratto prima dell'attivazione del servizio e a comunicare ai sottoscrittori che avevano aderito già al servizio le clausole modificate, anche al fine di ottenere nuovamente il consenso dei sottoscrittori alla cessione dei loro dati ad altre società.

Tuttavia, il Garante ha osservato che, anche per quanto riguarda gli abbonati ed utenti chiamati che ascoltano anch'essi messaggi pubblicitari, il servizio *GratisTel* è soggetto alla disciplina in materia di dati personali e di riservatezza nelle telecomunicazioni.

I dati relativi alle utenze chiamate sono, infatti, oggetto di trattamento da parte della società che li raccoglie. Pertanto, anche queste ultime devono essere informate e messe in grado di esprimere consapevolmente le proprie scelte in ordine all'utilizzazione dei loro dati a fini pubblicitari.

L'Autorità non ha ritenuto ammissibile un meccanismo che trasferisca sui sottoscrittori l'obbligo di informare le persone chiamate, il cui onere spetta alla società fornitrice del servizio, la quale è stata invitata a predisporre un messaggio chiaro per permettere al chiamato di non ricevere inconsapevolmente una chiamata con spot o di ascoltare messaggi pubblicitari senza un'informativa anche sintetica e l'espressione di un consenso. La manifestazione di volontà da parte del chiamato, si è rilevato, potrebbe essere espressa anche esercitando, tramite l'apparecchio telefonico, un'opzione per l'instaurazione della chiamata o per l'inserimento dei messaggi pubblicitari, sempre sulla base di una preventiva e idonea informativa.

È rimasto, comunque, aperto il problema più in generale della libertà di comunicazione, che potrebbe essere limitata da un'alternativa circoscritta all'accettazione della pubblicità o all'interruzione della telefonata. Per questo motivo, il Garante ha trasmesso il provvedimento all'Autorità per le garanzie nelle comunicazioni; ciò anche perché quest'ultima potesse valutare, per i profili di sua competenza, la natura del servizio offerto.

Successivamente, a seguito della trasmissione da parte della società degli elementi richiesti con il provvedimento del 13 novembre 1999 circa le misure e gli accorgimenti assunti per rendere conforme il servizio alle norme sulla privacy, nonché per consentire l'attivazione nel pieno rispetto dei diritti dei cittadini, il Garante ha inviato una nuova segnalazione a *GratisT Italia s.r.l.* perché, dall'esame della predetta documentazione, in vista dell'annunciato avvio del servizio per il 18 dicembre 1999, era emerso che le modifiche richieste non erano state tutte apportate (v. l'ulteriore segnalazione del 14 dicembre 1999, pubblicata nel Bollettino n. 10/1999, pag. 61).

In particolare, per quanto riguarda i sottoscrittori del contratto, si è ritenuto necessario che la società provvedesse a:

- chiarire quali fossero i dati che i sottoscrittori devono necessariamente fornire nel modulo di iscrizione affinché venga loro erogato il servizio e quali, invece, le informazioni facoltative, anche per quanto riguarda il codice fiscale (la società aveva sino ad allora comunicato ai sottoscrittori di utilizzarlo per imprecisati "scopi interni");
- far presente ai sottoscrittori, dal momento che veniva prevista anche la possibilità per l'utente di ricevere a casa ulteriori informazioni sui prodotti (attraverso i c.d. "spot interattivi"), che è già previsto nel contratto un elenco aggiornato degli inserzionisti dal quale possono essere ricavate le coordinate per esercitare i diritti sanciti dall'art. 13 della legge n. 675 del 1996 (accesso ai dati, loro aggiornamento, rettifica, cancellazione, ecc.);
- specificare meglio, nel modulo di sottoscrizione, le categorie di società e di imprese destinatarie dei dati degli interessati, elencando le principali tipologie di operatori.

Per quanto riguarda invece le persone chiamate attraverso il servizio *GratisTel*, la società aveva previsto, all'inizio della telefonata, un messaggio in base al quale si poteva rifiutare la chiamata interrotta dalla pubblicità. Al riguardo, il Garante ha, però, richiesto che la persona chiamata

fosse messa in grado di esprimere in modo positivo la sua volontà attraverso la digitazione di un tasto, acconsentendo in piena consapevolezza all'instaurazione della telefonata (facendo sì che se il chiamato non accetta la telefonata attraverso la digitazione del tasto indicato, cada la linea).

L'Autorità ha sottolineato inoltre che tale meccanismo serve solo per consentire lo svolgimento della telefonata, ma non per ogni altra utilizzazione dei dati, ad esempio a seguito di "spot interattivi". L'utilizzazione delle informazioni del chiamato a tale scopo può avvenire solo sulla base di una più articolata informativa e dell'acquisizione di un nuovo consenso.

A seguito della seconda segnalazione del Garante, la GratisT Italia s.r.l. ha inviato all'Autorità, prima dell'avvio del servizio, copia dei documenti riformulati secondo le indicazioni fornite dal Garante, impegnandosi a conformare il trattamento dei dati ai principi in tema di tutela della riservatezza.

2.10.5
La tutela dei dati
nei servizi di
accesso gratuito
ad Internet

Nel luglio del 1999, il Garante ha avviato un procedimento di indagine nei riguardi del servizio "Libero" di Infostrada, in seguito ad alcune segnalazioni concernenti il lancio di questo nuovo servizio di accesso gratuito ad Internet, che prevede sia l'acquisizione, al momento della sua attivazione, di diverse informazioni personali relative anche ai propri gusti ed interessi, sia il successivo monitoraggio delle connessioni ai siti visitati dagli abbonati, svolto per individuare le loro preferenze (attraverso la determinazione dei loro profili di consumatori, la cosiddetta "profilazione"), nonché per programmare l'invio di messaggi pubblicitari via e-mail.

In occasione di tale procedimento, l'Autorità ha così affrontato il tema della raccolta e dell'utilizzazione di dati personali nell'ambito dei servizi di accesso gratuito ad Internet offerti dagli operatori nel settore delle telecomunicazioni, indicando alcune modalità necessarie a garantire la liceità e la correttezza dei loro comportamenti nei confronti degli utenti (provvedimento del 13 gennaio 2000).

Il Garante ha chiarito che, fermo restando il rispetto della volontà dei cittadini e dei consumatori di accettare la cessione di dati identificativi o attinenti a gusti, preferenze ed interessi, per ottenere gratuitamente determinati servizi, gli interessati devono, però, essere messi in grado di esprimere le proprie scelte sull'uso dei dati che li riguardano in maniera consapevole e libera. Per questo è necessario che, anzitutto, ricevano tutte le informazioni necessarie per comprendere appieno le finalità e le modalità del trattamento dei dati, compresi quelli che vengano acquisiti successivamente (tali informazioni ai clienti vanno date sempre, anche quando non venga chiesto loro alcun consenso), verificando con attenzione se alcuni dati, richiesti come "obbligatori" dalle società del settore, siano realmente indispensabili per attivare il servizio.

In particolare, le segnalazioni pervenute all'Autorità hanno prospettato un contrasto con la disciplina sulla privacy, con particolare riguardo all'insufficienza delle informazioni fornite agli interessati, alla possibilità di raccogliere i dati sui siti frequentati (con eventuale conoscenza di informazioni relative, ad es., a salute, vita sessuale, opinioni politiche o sindacali, convinzioni religiose o filosofiche) e di controllare se i messaggi pubblicitari inviati dalla società vengano effettivamente letti dagli abbonati.

Durante la fase istruttoria, la società ha eliminato alcune anomalie ed incongruenze presenti nei documenti sottoposti al potenziale cliente al momento dell'iscrizione e ha specificato che l'analisi degli accessi ai siti verrà svolta su un catalogo predefinito dalla stessa società (che non comprenderebbe siti nei quali sono trattati argomenti da cui sono ricavabili dati "sensibili"). Non verrebbe, invece, effettuata alcuna verifica circa il ricevimento e la visualizzazione dei messaggi pubblicitari da parte dei clienti.

Il Garante, tuttavia, ha ritenuto necessario che alcuni profili relativi alle informazioni e ai

documenti, sottoposti al cliente al momento della richiesta del servizio, venissero rivisti e ha fornito, al riguardo, alcune indicazioni da ritenersi valide anche per tutti gli altri operatori che offrono servizi analoghi, in via di rapida espansione.

In particolare, l'Autorità ha sottolineato che l'informativa ai clienti deve essere:

- collocata prima della richiesta di registrazione dei propri dati;
- riferita a tutti gli aspetti del complessivo trattamento svolto dal fornitore nell'ambito del servizio (anziché ai soli profili relativi a finalità commerciali o di marketing), riepilogando in maniera chiara e sintetica le notizie magari disseminate nel contratto;
- integrata con un richiamo, anche sintetico, ai diritti di accesso attribuiti agli interessati dalla legge 675 (art. 13) e con l'indicazione dell'ufficio o servizio presso cui esercitare tali diritti.

Occorre poi precisare meglio tutte le categorie di ulteriori aziende alle quali verranno eventualmente comunicate le informazioni. Tali aziende, a loro volta, dovranno acquisire il consenso degli interessati (oppure la società dovrebbe richiedere il consenso dei clienti anche per conto delle altre aziende, fornendone precisa indicazione, anche in un elenco a parte da rendere agevolmente disponibile agli interessati).

Inoltre, la richiesta del consenso nei confronti degli abbonati che abbiano accettato le condizioni contrattuali e, in particolare, "autorizzato" l'invio di messaggi pubblicitari sulla propria casella di posta elettronica, pur potendo essere limitata alle sole operazioni di utilizzazione dei dati per finalità commerciali non collegate al servizio e di loro divulgazione all'esterno, deve essere riferita anche alle disposizioni in tema di pubblicità e di chiamate indesiderate, introdotte dalle recenti normative sulla privacy nelle telecomunicazioni e sui contratti a distanza.

Riguardo all'acquisizione dei dati con i moduli di adesione al servizio, come già detto, vi è poi la necessità di chiarire agli interessati che le informazioni sono raccolte non per specifici obblighi normativi (che non possono essere ravvisati nella mera opportunità di rendere disponibili alcune informazioni sugli abbonati nel caso in cui organi o autorità preposte ad indagini siano interessate in futuro a raccoglierle), ma perché il fornitore intende raccoglierle sulla base di una propria, autonoma, scelta di caratterizzazione del servizio, anche quando l'abbonato non presti il consenso a trattamenti e comunicazioni per finalità commerciali. La valutazione circa le informazioni non essenziali o eccedenti rispetto alle finalità del servizio (il quale si incentra sull'utilizzo dei codici personali d'accesso ad *Internet* e delle caselle di posta elettronica degli interessati) deve essere quindi accompagnata da una migliore specificazione agli interessati delle ragioni della loro raccolta.

In relazione ad altri aspetti, connessi ai dati relativi ai siti consultati dagli abbonati, nel confermare la necessità che la società assuma tutte le misure idonee ad evitare una raccolta di informazioni sensibili, il Garante si è, nel caso concreto, riservato di verificare il catalogo dei siti predisposto dalla società, non appena disponibile, e le attività ad esso collegate, una volta rese operative.

Nel fornire le predette indicazioni, il Garante ha, peraltro, segnalato a Infostrada S.p.a. la necessità di fornire a ciascun utente già abbonato al servizio il nuovo testo di informativa messo a punto per i futuri clienti, assicurando ai vecchi abbonati la possibilità di esprimere nuovamente il consenso e, tramite un meccanismo agevole, revocare le precedenti manifestazioni di volontà.

L'Autorità ha, infine, disposto che copia del provvedimento fosse trasmesso anche ad altri operatori che offrono servizi analoghi, allo scopo di sensibilizzarli ad un maggiore rispetto della normativa sulla protezione dei dati personali.

2.11 Commercio elettronico

2.11.1 Profili generali

Il tema del commercio elettronico è tra i più attuali nel dibattito che concerne, in verità, non solo la tutela della riservatezza dell'individuo di fronte ai trattamenti in rete, ma anche aspetti che potremmo definire prodromici alla stessa promovibilità del commercio on-line quale alternativa ai tradizionali canali di scambio.

Il crescente sviluppo delle attività commerciali in rete potrà realmente incrementarsi solo se, contestualmente, le imprese osserveranno una efficace prassi di tutela dei diritti fondamentali della personalità di utenti e consumatori, adottando politiche e procedure trasparenti nei riguardi dei tipi di dati raccolti, delle modalità della loro concreta elaborazione ed utilizzazione, nonché dell'eventuale comunicazione, così da alimentare la fiducia degli interessati anche in termini di sicurezza dei dati e delle transazioni.

Un'idonea politica di tutela della riservatezza e della sicurezza non è, quindi, un freno all'*e-commerce*, ma, al contrario, un fattore essenziale per la sua crescita, non potendosi del resto concepire il contesto delle reti telematiche come un'area nella quale i diritti della personalità perdono efficacia o divengono puramente "virtuali".

Di fronte alla chiara evidenza che nessun effettivo incremento dell'uso per fini commerciali delle reti, ed in particolare di Internet, si potrà avere, se non sarà offerto un contesto che si presenti al sicuro anche dai pericoli che possono derivare da fronti diversi (come la raccolta occulta o non informata di dati personali, l'uso non garantito di sistemi di pagamento elettronici o, ancora, le possibili vie di elusione della legislazione di tutela della proprietà intellettuale), lo sforzo iniziale dei lavori in atto sul piano internazionale e comunitario e in particolare presso l'Unione Europea, ai quali questa Autorità partecipa attivamente, è stato nel senso di proporre, anche tramite lo strumento della direttiva comunitaria, una sistemazione completa ed organica di tutte le problematiche connesse, e creare un quadro giuridico coerente per lo sviluppo del commercio elettronico sul piano mondiale e nell'ambito del mercato unico europeo.

L'attività complessivamente svolta nel corso del 1999 presso l'OCSE, il Consiglio d'Europa e il Gruppo di lavoro di cui all'art. 29 della direttiva n. 95/46/CE, è sfociata anche in una "posizione comune" comunitaria, destinata a concretarsi a breve in una direttiva del Parlamento europeo e del Consiglio che è sintetizzata nel successivo paragrafo della presente relazione.

Le tematiche di maggior rilievo sul tema privacy-commercio *on line* sono state portate, poi, sempre a livello internazionale, in seno ai lavori dell'OCSE e al forum dell'OCSE che si è svolto a Parigi il 12 e 13 ottobre 1999, dopo la Conferenza di Ottawa dello scorso anno.

Una parallela attività di sensibilizzazione e di intervento è stata inoltre svolta dal Garante anche in seno all'Osservatorio sul commercio elettronico costituito presso il Ministero del Commercio, dell'industria e dell'artigianato, ove è stato dato ampio spazio alla discussione sui temi che più strettamente riguardano l'armonizzazione della disciplina sul commercio con le disposizioni a tutela della privacy.

Sotto il profilo del tema dei servizi *on line* offerti ai cittadini, e quindi del commercio elettronico inteso quale strumento di attuazione e miglioramento dell'efficacia e produttività dei servizi della pubblica amministrazione, vanno ricordati infine i contributi dell'Autorità in numerosi convegni e seminari e, in particolare, al Forum della p.a. 1999, che si è svolto a Roma dal 4 all'8 maggio 1999, anche sulla tematica "Call center, riconoscimento vocale e servizi ai cittadini", nonché al COMPA tenutosi a Bologna il 15, 16 e 17 settembre 1999.

Parimenti curata è stata poi la partecipazione di questa Autorità ai lavori che hanno portato all'adozione della direttiva n. 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche, diretta a creare uno standard europeo comune e affidabile quanto alle caratteristiche tecniche e agli effetti giuridici della firma digitale.

La direttiva relativa ad un quadro comune sulle firme elettroniche, è stata adottata il 13 dicembre 1999 ed è stata pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* del 19 gennaio 2000.

Gli Stati membri dovranno attuare i principi della direttiva entro il 19 luglio 2001. La direttiva, come già evidenziato nella precedente relazione, è finalizzata ad introdurre una cornice di regole armonizzate tra gli Stati membri 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, nel 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 forme di discriminazione delle firme elettroniche sulla sola base dell'essere espresse sotto forma elettronica, assicurando, in presenza di precisi requisiti di sicurezza, che le stesse siano considerate equivalenti alle firme apposte manualmente.

I principi su cui si basa la direttiva sono, quindi, quelli della neutralità tecnologica, cercando di evitare il collegamento della direttiva ad uno o più prodotti in commercio e tenendo anzi conto del rapido evolversi delle tecnologie, della libertà d'impresa e della libera circolazione. È pertanto escluso che gli Stati membri possano introdurre o mantenere regimi di autorizzazione preventiva, pur avendo la facoltà di conservare o introdurre regimi di accreditamento facoltativi per garantire un più alto livello di sicurezza e di affidabilità dei prestatori di servizi di certificazione e dei certificati da questi emessi.

Durante la discussione i rappresentanti italiani, anche dell'Ufficio del Garante, hanno insistito a lungo per far introdurre nel testo principi di rigore riguardo alla valenza giuridica della firma elettronica, per una identificazione più chiara degli elementi necessari a poter fondare una presunzione di equivalenza con le firme manoscritte e per prevedere specifiche garanzie e sistemi di verifica. Il testo inizialmente proposto dalla Commissione è risultato poi largamente modificato nel corso delle riunioni fino alla posizione comune definita dal Consiglio dei Ministri delle telecomunicazioni dell'Unione europea il 22 aprile 1999, che ha sancito l'ingresso nello stesso di specifici riferimenti, anche nelle definizioni, alle firme elettroniche avanzate ed ai dispositivi "sicuri" di creazione e verifica delle firme stesse.

Di particolare importanza risultano ora gli artt. 6 (relativo alla definizione delle responsabilità), 7 (che disciplina gli aspetti internazionali anche in tema di equivalenza dei certificati rilasciati da prestatori di servizi di certificazione stabiliti in Paesi terzi) e 8 (relativo alla protezione dei dati personali, incluso l'uso dello pseudonimo).

L'art. 8 della direttiva ha previsto infatti una serie di garanzie per la protezione degli aspetti connessi al trattamento dei dati personali, fra cui alcuni obblighi gravanti sul "certificatore" (tra essi, l'obbligo di effettuare la raccolta dei dati direttamente dai soggetti interessati alla certificazione della firma o previo loro esplicito consenso e l'obbligo di rispettare il principio di pertinenza, secondo quanto sostanzialmente disposto all'art. 6 della direttiva comunitaria n. 95/46/CE), nonché facoltà spettanti al soggetto utilizzatore della firma elettronica.

Tra queste ultime, appare rilevante la necessità della prestazione del consenso in merito alla raccolta o all'elaborazione dei dati per fini diversi da quelli necessari per il rilascio e il mantenimento del certificato. Significativo è, anche, il limite posto agli Stati membri ai quali viene preclusa la possibilità di vietare al prestatore di servizi di certificazione di riportare sul certificato uno pseu-

2.11.2

La posizione
comune europea
e la direttiva
sulle firme
elettroniche

donimo in luogo del nome del firmatario (art. 8, par. 3). L'uso dello pseudonimo, peraltro, è stato disciplinato con l'obiettivo di garantire l'equilibrio tra il rispetto della privacy (e dunque la facoltà di riservarsi l'anonimato nell'ambito degli scambi commerciali) e la possibilità (che rimane aperta per gli Stati membri ai sensi del considerando n. 25 della direttiva), di chiedere l'identificazione delle persone in base alla normativa comunitaria o alla legislazione, fermi restando poi, gli effetti giuridici che la legislazione nazionale attribuisce agli pseudonimi (art. 8, par. 3).

Accanto alla direttiva sinora commentata, per consentire un maggiore sviluppo del commercio elettronico (prevedendo una cornice di regole armonizzate in cui dette attività si svolgano e che serva a dare fiducia ad utenti e consumatori), si colloca la proposta di direttiva del Parlamento europeo e del Consiglio relativa a taluni aspetti del commercio elettronico nel mercato interno.

La proposta, presentata nel novembre del 1998, è stata oggetto di lunga e complessa discussione ed è stata sottoposta al Consiglio Mercato interno il 7 dicembre per la definizione di un accordo politico. Il 28 febbraio 2000 il Consiglio Ecofin ha adottato una posizione comune.

Si tratta di una proposta di tipo orizzontale in quanto si aggiunge alle direttive che già disciplinano i diversi settori interessati, dettando norme solo per la parte che rileva ai fini del commercio elettronico.

La proposta intende armonizzare il quadro di riferimento per evitare che gli Stati membri adottino in materia legislazioni divergenti, creando ostacoli e turbative al mercato interno. Il provvedimento ha però destato varie perplessità sia nelle riunioni di coordinamento interministeriali, sia in seno al gruppo di lavoro del Consiglio dell'Unione che la sta discutendo.

Nelle discussioni è stato possibile superare conflitti e contraddizioni presenti nel testo originario, in particolare riguardo alla definizione del luogo di stabilimento del prestatore di servizi, alla stipulazione di contratti *on-line*; alla responsabilità degli intermediari, alla definizione della nozione di comunicazione commerciale e alle misure per incoraggiarne l'uso; alla previsione di sistemi volti a favorire l'effettiva attuazione delle norme comunitarie; ai principi di mutuo riconoscimento.

I lavori hanno mostrato una certa preferenza della Commissione europea verso la limitazione dell'oggetto della direttiva ad aspetti non specificatamente disciplinati da altre normative di settore, ed in particolare a taluni aspetti giuridici (concernenti specificatamente le comunicazioni commerciali, la conclusione di contratti *on line*, la responsabilità degli intermediari), nel dichiarato intento di rimuovere gli ostacoli risultanti dalla divergenza o dalla sovrapposizione di normative negli Stati membri per garantire, oltre all'*acquis* esistente, la libera circolazione dei servizi *on line* all'interno della Comunità.

L'Autorità è più specificamente interessata alle parti che attengono alla tutela dei dati personali, per le quali ha fornito un contributo attivo partecipando alle riunioni di coordinamento interministeriali e a quelle che si sono tenute nel gruppo di lavoro del Consiglio.

Nel corso dei lavori a Bruxelles, l'Autorità si è adoperata al meglio per ridurre il rischio che le problematiche emergenti dal raffronto tra diritti fondamentali e attività commerciali potessero rimanere irrisolte, attraverso una mera formula di deroga quale quella adottata, in quanto la proposta di direttiva reca disposizioni non sempre convergenti con quelle in materia di dati personali. Basti pensare, sotto altri profili, all'art. 7 relativo alle comunicazioni commerciali non sollecitate, agli articoli inerenti alle informazioni da fornire ai fini della conclusione del contratto e alla disciplina della responsabilità degli intermediari, temi che avrebbero richiesto un più preciso chiarimento di raccordo con la disciplina della privacy, sia al fine di dirimere possibili dubbi applicativi, sia per evitare duplicazioni di oneri informativi a carico delle parti, comunque richiesti, su base nazionale, anche ai sensi dell'art. 10 della legge 31 dicembre 1996, n. 675.

Le considerazioni formulate in relazione all'esclusione della protezione dei dati personali

secondo l'originaria previsione dell'articolo 22 della proposta, sono state accolte dal gruppo di lavoro e dalla Commissione ed hanno consentito di modificare parzialmente il testo, inserendo all'articolo 1 (relativo al campo di applicazione) una specifica esclusione per "le questioni relative alla società dell'informazione che sono coperte dalle direttive 95/46/CE e 97/66/CE". È stato del pari introdotto un nuovo considerando che spiega come la protezione dei dati personali sia disciplinata esclusivamente dalle citate direttive, le quali, avendo introdotto una disciplina più armonizzata nella materia, restano pienamente applicabili alla Società dell'Informazione.

Tale soluzione è soddisfacente nella misura in cui demanda alle direttive nn. 95/46/CE e 97/66/CE il compito di continuare a disciplinare il bilanciamento dei diritti coinvolti in materia di tutela della riservatezza. Nonostante i miglioramenti apportati, però, appare ancora non del tutto ottimale, in ragione del fatto che gli operatori a livello comunitario dovranno pur sempre verificare in più fonti normative i parametri per verificare la liceità e la correttezza dei diversi comportamenti in rete, con qualche rischio anche in termini di immediata chiarezza del dettato di varie disposizioni, a volte parzialmente sovrapposte e riportate in più testi comunitari.

2.12 Flussi transfrontalieri di dati

In materia di trasferimento di dati all'estero, non vi sono particolari deliberazioni del Garante di cui dare conto oltre a quelle già riassunte nelle precedenti relazioni (v. Relazione per l'anno 1997, p. 103-105, e Relazione per l'anno 1998, p. 80-82).

Di notevole rilievo è, invece, l'attività svolta dall'Autorità in seno ad organismi comunitari ed internazionali relativamente ai trasferimenti di dati verso Paesi terzi. Per darne conto, sia pur brevemente, è opportuno schematizzare il quadro delle disposizioni rilevanti contenute nella direttiva.

In base all'art. 25 della direttiva n. 95/46/CE è necessario, per trasferire dati in Paese terzo, che questo presenti un livello di protezione "adeguata", da valutarsi con riferimento a tutte le circostanze e, segnatamente, alla natura dei dati. Qualora la Commissione europea constati che un Paese non presenta tale livello di protezione, gli Stati membri adottano tutte le misure per impedire il trasferimento di dati della stessa natura verso tale Paese.

Per constatare su base comunitaria l'adeguatezza della protezione offerta da un Paese terzo possono essere considerati sia la legislazione nazionale, sia, dopo che sia stata accertata la situazione di inadeguatezza, gli impegni internazionali assunti con la Commissione in negoziati volti a porvi rimedio.

L'art. 26 della direttiva prevede inoltre che il trasferimento possa avvenire in determinate circostanze anche verso Paesi la cui legislazione non presenti un livello adeguato di protezione, ad esempio quando l'interessato abbia manifestato il proprio consenso o quando il trasferimento sia accompagnato da clausole contrattuali idonee ad assicurare tale protezione.

Sul piano federale, a differenza di quanto avviene a livello statale, l'ordinamento federale statunitense in materia di protezione della riservatezza non è basato su un organico strumento normativo come invece accade nell'Unione europea, essendo tale protezione affidata, per vari aspetti, ad eventuali sistemi di autoregolamentazione.

Esperti e associazioni di consumatori hanno perciò auspicato l'introduzione di maggiori garanzie, mentre alcuni organismi imprenditoriali hanno manifestato incertezze circa l'impatto che il requisito dell'adeguatezza richiesto dalla disciplina comunitaria potrebbe avere sul flusso di dati tra Europa e Stati Uniti.

Il Governo Usa (e in particolare il Dipartimento del commercio) ha promosso l'elaborazione - ancora in corso - di alcuni "International Safe Harbor Privacy Principles" nonché di una guida per la loro attuazione, articolata in una serie di risposte alle domande che più frequentemente si pongono in materia (FAQ).

In sostanza, alla luce di tali principi, come determinati in un negoziato preliminare tra la parte statunitense e la Commissione europea, quest'ultima, con apposita decisione da adottarsi ai sensi dell'art. 25, par. 2, della direttiva (sulla base del parere del Comitato di seguito citato), introdurrebbe la presunzione che i principi (applicati conformemente alla guida) garantiscono un livello adeguato di protezione dei dati trasferiti dalla Comunità ad organizzazioni insediate negli Usa, purché queste si impegnino a rispettare i principi contenuti nel "Safe Harbor".

L'importanza che una simile decisione avrebbe è evidente in riferimento, anzitutto, al principio di non discriminazione nei confronti di altri Paesi terzi presso, alcuni dei quali si registra al riguardo un atteggiamento di attesa.

Da un lato, i Paesi terzi avrebbero interesse ad evitare nei loro riguardi interpretazioni ed applicazioni della normativa comunitaria più rigorose di quelle praticate in seno alla Comunità. Dall'altro, per quanto riguarda i Paesi terzi, definire "adeguato" il livello di protezione adottato negli Usa significa indicare il livello oltre il quale difficilmente la parte europea potrebbe chiedere adeguamenti ad altri Stati.

Inoltre, se si tiene conto dei diritti fondamentali e degli interessi economici in materia, risulta chiaro che una simile decisione sarebbe di rilevante importanza anche per l'attività di revisione della direttiva n. 95/46/CE, prevista dal relativo art. 33 decorsi tre anni dalla scadenza del termine per la sua attuazione.

In questo quadro, la parte europea (e al suo interno diversi Paesi membri ed autorità di garanzia tra cui quella italiana), ha costantemente sottolineato, nel corso del negoziato, l'importanza dell'effettività degli strumenti di tutela posti in essere. Infatti, senza adeguati ed efficaci strumenti di attuazione, volti a consentire l'effettiva realizzazione dei diritti riconosciuti agli interessati, ovvero agevoli e idonee forme di soddisfazione in caso di loro violazione, i diritti sanciti dalle norme comunitarie rimarrebbero solo sulla carta, e il trasferimento dei dati in Paesi terzi diventerebbe in molti casi lo strumento per eludere le norme stesse.

Il negoziato ha avuto però fasi alterne e una bozza completa e consolidata di accordo si è inoltre resa disponibile solo da ultimo.

In questo quadro si colloca l'intensa attività svolta dal Garante, sia in incontri di studio o comunque non ufficiali, sia, soprattutto, in seno agli organismi a livello comunitario previsti dalla citata direttiva n. 95/46/CE. Si allude, in particolare, al Gruppo di lavoro di cui all'art. 29 della medesima direttiva (composto da rappresentanti di ciascuna autorità nazionale e da un rappresentante della Commissione), al quale spetta, tra l'altro, il compito di formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei Paesi terzi; nonché al Comitato di cui all'art. 31 (composto da rappresentanti degli Stati membri e presieduto da un rappresentante della Commissione).

Nell'ambito di quest'ultimo il Garante ha operato in costante e proficuo raccordo con il Ministero della giustizia, che rappresenta il Governo, e ciò ha consentito l'espressione di un orientamento comune.

Oggetto della valutazione di tali organismi, con riferimento ad una complessa attività di negoziazione svolta dalla Commissione, è stata principalmente la situazione statunitense.

L'ingente attività dei predetti organismi su tale argomento è diffusamente documentata negli allegati della presente relazione, dai quali si evince l'efficace ruolo di impulso svolto in par-

ticolare dal Gruppo di cui all'art. 29 che, in generale sintonia con il Comitato, ha sollecitato, a più riprese, l'introduzione di un livello più elevato di garanzie rispetto ai diversi principi del *Safe Harbor* (informativa, consenso, diritto di accesso, ulteriori trasferimenti e utilizzazioni di dati, *enforcement*).

Grazie a questa attività, i principi del *Safe Harbor* (inizialmente assai vaghi e vanificati da alcune interpretazioni restrittive inserite nelle FAQ) sono stati oggetto di un certo miglioramento, sia pure assai graduale. Il loro adeguamento è tuttora in corso e la posizione definitiva dei medesimi organismi non è ancora definita, essendo prevista nell'ambito delle riunioni che si terranno, in particolare, nel mese di maggio del 2000.

Il proficuo contributo offerto dall'Autorità italiana (che nella persona del prof. Rodotà ha svolto le funzioni di vice presidenza del Gruppo di cui all'art. 29 e, dal marzo del 2000, di presidenza), è testimoniato, tra l'altro, dall'incontro avuto con il sottosegretario di Stato americano Aaron in visita al Garante nel gennaio del 1999, dalla recente audizione del presidente del Garante avvenuta il 22 febbraio 2000 dinanzi al Parlamento europeo, dalla partecipazione alla visita ufficiale a Washington del 18-20 gennaio 2000 del Comitato di cui all'art. 31 (cui ha partecipato, per il Garante, il segretario generale), da alcuni comunicati stampa del Garante, nonché dai diversi contributi, chiarimenti e prese di posizione anche sulla stampa dei rappresentanti del collegio del Garante e del segretario generale.

In proposito il Garante ha segnalato anche l'esigenza di valutare con maggiore attenzione le competenze degli organi statutitensi che dovrebbero svolgere un controllo indipendente, le effettive garanzie di ricorso offerte agli interessati, anche in riferimento alle inibitorie, alla determinazione della legge applicabile e al risarcimento del danno, atteso anche il fatto che l'intervento della *Federal Trade Commission* (il principale organo cui verrebbero presentati i reclami degli interessati), risulta circoscritto negli ultimi due anni ad un numero assai ristretto di casi rispetto alle diverse centinaia di interpellati ricevuti.

Il Garante ha altresì rappresentato che un automatico inserimento nell'elenco delle società aderenti al sistema di autoregolamentazione, non assoggettato al controllo di determinati requisiti, potrebbe favorire l'attività di società di comodo, che potrebbero svanire nel nulla dopo aver trasferito i dati ad un'altra entità, sottraendosi di fatto a qualunque forma di responsabilità. Diverse altre osservazioni sono state formulate per quanto riguarda il livello di garanzie dei principi nonché la loro tutela giurisdizionale e amministrativa.

Sono altresì ancora da approfondire i rapporti tra la decisione della Commissione e i poteri delle autorità nazionali, giudiziarie e di garanzia. Ciò in quanto la base giuridica prospettata per la decisione (l'art. 26, par. 6 della direttiva) conferisce alla Commissione competenze di esecuzione relative alla valutazione di adeguatezza, ma lascia impregiudicati i poteri di tali autorità sui singoli casi.

Il *Safe Harbor* sembra peraltro destinato a coprire soltanto una parte dei flussi verso gli USA, lasciando non regolata un'alta percentuale di trasferimenti che, unitamente a quelli considerati nel negoziato, potrebbero essere con ogni probabilità regolati meglio. Ciò attraverso il ricorso a clausole contrattuali per vincolare sia chi esporta i dati, sia chi li utilizza nel Paese terzo, a condotte regolate più specificamente, anche sotto il profilo della giurisdizione applicabile e del risarcimento del danno, sulla falsariga della proficua esperienza maturata in diversi Paesi membri.

Alcuni schemi di clausole o contratti tipo in materia di protezione dei dati sono peraltro già stati valutati e perfezionati a cura del Consiglio d'Europa, dell'OCSE e dell'*International Chamber of Commerce*, e fanno quindi parte del materiale a disposizione della Commissione per l'elaborazione a livello comunitario. In tal senso, oltre all'attività propulsiva svolta in seno alla

Comunità europea, il Garante ha seguito con attenzione i lavori dell'*International Commerce Exchange* per la definizione di un codice di condotta sulla privacy, nonché di un modello contrattuale da utilizzare per il flusso transfrontaliero di dati, anche al fine di orientare la prassi degli operatori economici coinvolti tramite la formazione di regole condivise e, perciò, rispondenti alle indicate esigenze di effettività.

2.13 Videosorveglianza

L'Italia manca tuttora di una disciplina specifica in materia di video-sorveglianza che pure appare sempre più necessaria ed urgente. Altri Paesi quali Francia, Danimarca, Islanda, Norvegia (e, dal 1999, la Spagna) dispongono invece di un quadro normativo articolato. Nel 1998, il *Data-Protection Registrar* inglese ha predisposto al riguardo un codice di comportamento ("*Code of Practice*"). In Germania, nel marzo dell'anno in corso, la 59.^{ma} Conferenza delle Autorità di protezione dei dati a livello federale e regionale ha approvato una risoluzione che invita il legislatore a introdurre determinati principi di regolamentazione.

La direttiva comunitaria n. 95/46/CE e la Convenzione n. 108/1981 del Consiglio d'Europa vincolano i Paesi membri ad applicare la disciplina sul trattamento dei dati personali anche a dati cifrati o codificati, nonché ai suoni e alle immagini (quali quelle registrate nei controlli video o in altri sistemi di videosorveglianza), qualora permettano di identificare un soggetto anche in via indiretta.

La legge 31 dicembre 1996, n. 675 che - ha attuato la Convenzione n. 108 e ha in buona parte permesso di recepire la direttiva europea - considera anch'essa come "dato personale" qualunque informazione che permetta l'identificazione, anche in via indiretta, dei soggetti interessati, ivi compresi, appunto, i suoni e le immagini (art. 1, comma 1, lett. c), l. n. 675/1996).

Nella perdurante mancanza di una normativa specifica, il Garante ha perciò sollecitato, in sede di verifica dei vari sistemi realizzati o in progetto a cura di enti e di organismi che si sono rivolti all'Autorità, il rispetto di principi desumibili dalla legge n. 675, richiamando l'attenzione sulla necessità che ogni sistema di video-sorveglianza sia attivato e gestito solo in presenza di articolate garanzie che dovrebbero riguardare, in modo particolare, l'eventuale intenzione di conservare le immagini e i suoni in appositi archivi, l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'amministrazione preposta, nonché l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici.

Ad esempio, in merito al parere chiesto al Garante dalla Presidenza del Consiglio dei Ministri e dal Dipartimento della Funzione pubblica sullo schema di regolamento per l'autorizzazione all'installazione ed all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, il Garante (con provvedimento del 24 febbraio 1999, in Bollettino n. 7, pag. 25) ha constatato con soddisfazione la previsione di disposizioni riferite al trattamento dei dati personali.

In particolare, detto regolamento prevede che gli impianti rilevino immagini solo in caso di infrazione e, per il resto, effettuino il monitoraggio del traffico, attraverso dati anonimi. Sono altresì prevista l'utilizzazione dei dati per le sole finalità di applicazione del regolamento medesimo, salva la possibilità di uso dei dati per fini di giustizia e la disponibilità di dati anonimi per studi e statistiche; la conservazione delle immagini per il solo periodo necessario all'applicazione delle infrazioni e alla definizione dell'eventuale contenzioso; l'esclusione di interconnessioni con altri archivi o base dati; nonché il tracciamento delle consultazioni della banca dati che custodisce le immagini. Nell'ambito di una collaborazione istituzionale proficuamente instaurata, i suggerimen-

ti di modifica dello schema formulati dal Garante sono stati accolti pressoché interamente in sede di emanazione del d.P.R. 22 giugno 1999, n. 250.

In una successiva occasione il Garante ha invece esaminato l'ipotesi che il Comune di Torino ha formulato per installare nonché d'intesa con le forze di polizia, un sistema di video-sorveglianza sui mezzi di trasporto pubblico urbano dell'ATM (Azienda torinese mobilità), presso alcune fermate, nel quadro di un'azione mirante a contenere il fenomeno della criminalità e a diminuire la pericolosità di ambiti cittadini particolarmente insicuri.

Con provvedimento del 23 marzo 1999 (in Bollettino n. 8, p. 57), l'Autorità ha in primo luogo osservato come in tale progetto le finalità fossero da una parte ispirate alla prevenzione e alla repressione dei reati e, dall'altra, basate su una connessa tutela del patrimonio pubblico (mezzi di trasporto, impianti fissi ecc.), oltre che dettate da un intento di generale cura del benessere cittadino.

Alla luce di tali finalità, il Garante ha inteso verificare la posizione dei soggetti coinvolti nell'iniziativa, identificando il "titolare del trattamento" nel Comune di Torino, quale centro di imputazione e riferimento degli interessi coinvolti e ravvisando nell'Azienda il possibile ruolo del responsabile del trattamento. Il Garante ha poi indicato la necessità di regolare i seguenti profili prima dell'avvio del progetto:

- a) verificare la posizione dei soggetti coinvolti nell'iniziativa e procedere alla formale identificazione del titolare e del responsabile del trattamento;
- b) determinare con precisione la localizzazione delle telecamere e le modalità di ripresa in aderenza alle finalità che avevano suggerito l'installazione del sistema, tenendo conto dei principi fondamentali fissati dall'art. 9 della legge n. 675/1996, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti. Al riguardo, si è suggerito di predisporre modalità di ripresa che permettano, per quanto tecnicamente possibile, di evitare riprese particolareggiate tali da risultare eccessivamente intrusive della riservatezza delle persone o da permettere la rilevazione di particolari non rilevanti;
- c) evitare che le telecamere riprendano in modo stabile le postazioni di guida dei conducenti, anche in considerazione dei limiti posti all'installazione di impianti audiovisivi dall'art. 4 della legge 20 maggio 1970, n. 300 (cd. Statuto dei lavoratori);
- d) evidenziare che le immagini visionate per finalità di polizia giudiziaria possano essere utilizzate per controlli, anche indiretti, sull'attività lavorativa dei dipendenti ATM;
- e) delimitare puntualmente i soggetti legittimati a trattare i dati personali, individuando con precisione, così come richiesto dall'art. 19 della legge n. 675, gli incaricati del trattamento;
- f) prevedere tutte le misure di sicurezza idonee per evitare fenomeni di dispersione dei dati o di accessi non autorizzati, ecc.;
- g) garantire in modo costante l'impossibilità di accesso diretto alle immagini registrate, specie presso i terminali "locali" a bordo dei mezzi o presso le fermate; la regolare distruzione delle immagini non oggetto di segnalazione; il rigoroso controllo di sicurezza sui dati registrati che, a seguito di denuncia, vengono esaminati dall'autorità di polizia;
- h) consentire l'accesso alla cd. "stazione di lettura" mediante il sistema della "doppia chiave" congiunta (una in possesso del personale preposto ATM e una in possesso dell'autorità di polizia), essendo la visione "in chiaro" delle immagini registrate strettamente connessa alla commissione di atti criminosi ed alla previa denuncia degli stessi all'autorità di polizia;
- i) fornire agli interessati, da parte del titolare del trattamento, le informazioni previste dall'art. 10 della legge n. 675/1996, segnalando in maniera idonea agli utenti del servizio di trasporto l'esistenza del sistema di video-sorveglianza.

Inoltre, in risposta alle informazioni fornite dal Comune di Riomaggiore in ordine alla realizzazione di un sistema di video-sorveglianza nella zona B di Punta Montenegro della Riserva Marina delle Cinque Terre, d'intesa con la Capitaneria di Porto della Spezia, il Garante (con provvedimento del 21/10/1999, in Bollettino n. 10, pag. 80) ha sollecitato un'attenta riflessione volta ad appurare:

- j) l'esistenza di una fonte normativa che legittimi l'installazione di tali sistemi di video-sorveglianza e che ne indichi le relative finalità, e cioè se tale iniziativa risponda alle funzioni istituzionali demandate all'ente. A tal fine, è apparso altresì necessario che fosse precisato come si configurano dal punto di vista della legge n. 31 dicembre 1996, n. 675, le posizioni dei soggetti coinvolti nell'iniziativa (Capitaneria di Porto di La Spezia e Comune di Riomaggiore), anche alla luce degli scopi dagli stessi perseguiti;
- k) la precisa localizzazione delle telecamere e le modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limite della possibilità di avvicinamento dell'immagine), anche al fine di assicurare il rispetto dei principi fondamentali fissati dall'art. 9 della legge, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;
- l) l'individuazione di idonee ed appropriate misure per assicurare un utilizzo corretto dei dati da parte dei soggetti legittimati (art. 15 della l. n. 675/1996);
- m) le procedure e le modalità volte a fornire agli interessati le informazioni previste dall'art. 10 della legge.

In questo quadro, il Garante ha perciò manifestato perplessità per l'attivazione di un sistema di video-sorveglianza privo di un insieme articolato di garanzie, che dovevano 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.

Riguardo a quest'ultimo aspetto, l'Autorità ha fatto inoltre presente che la divulgazione di dati tra soggetti pubblici richiede l'esistenza di una puntuale norma di legge o di regolamento ed è possibile, in via del tutto residuale, anche quando non sia prevista da una norma, purché sia necessaria per lo svolgimento di alcune funzioni istituzionali e sia effettuata una comunicazione preventiva al Garante (il quale potrebbe vietarla in caso di violazione di legge: art. 27, comma 2).

In seguito, fornendo riscontro a una richiesta di parere in ordine alla delibera della Giunta comunale di Portici con la quale è stato approvato un regolamento per l'installazione e l'utilizzo di impianti di videosorveglianza del territorio, di telecontrollo ambientale e di pannelli a messaggi variabili, il Garante (con provvedimento del 17 febbraio 2000) ha ricordato che, per i soli aspetti riguardanti l'installazione e l'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici o nelle zone a traffico limitato, è stato introdotto, mediante apposito regolamento (d.P.R. 22 giugno 1999, n. 250), l'obbligo per i comuni di richiedere un'autorizzazione rilasciata dal Ministero dei lavori pubblici-Ispettorato generale per la circolazione e la sicurezza stradale. Il Garante ha altresì rilevato che il progetto tiene conto di alcune indicazioni formulate dall'Autorità in relazione ad analoghe iniziative di enti locali e di amministrazioni centrali. Il Garante ha ribadito, ad ogni modo che, tra le finalità elencate dal provvedimento della Giunta, possono essere perseguite solo quelle che rispondono alle funzioni istituzionali demandate all'ente, come già indicato nel caso del Comune di Riomaggiore. Analogamente ai casi già illustrati, il Garante ha reputato inoltre necessarie:

- a) una localizzazione più precisa delle telecamere e una limitazione delle modalità di ripresa delle immagini, con particolare riguardo al livello di dettaglio della ripresa dei tratti somatici delle persone presso gli impianti volti unicamente a prevenire le violazioni al codice di strada;

- b) l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'ente e la precisazione delle finalità per le quali potranno essere autorizzati eventuali accessi di persone diverse dai responsabili e dagli incaricati;
- c) una puntuale verifica, per quanto riguarda l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici;
- d) l'indicazione del soggetto o della struttura cui il cittadino può rivolgersi per esercitare i diritti di cui all'art. 13 della legge;
- e) le modalità dell'eventuale riutilizzazione dei supporti magnetici una volta cancellati;
- f) la precisazione che, ai fini dell'analisi dei flussi di traffico, il trattamento è effettuato con modalità volte a salvaguardare l'anonimato, ma solo successivamente alla fase della raccolta, giacché le immagini registrate possono contenere dati di carattere personale.

Analoghe indicazioni sulla necessità di apportare le opportune modificazioni sono state formulate dal Garante (con provvedimento del 7 marzo 2000) riguardo al progetto di installazione di un sistema di video-sorveglianza ipotizzato dal Comune di Mantova con finalità di rilevazioni a fini statistici e di studio degli accessi dei veicoli al centro storico e alle zone al traffico limitato, nonché per finalità di controllo a distanza con funzione di prevenzione e repressione di attività illecite.

Il Garante aveva potuto già evidenziare positivi elementi di collaborazione con il Ministero dell'interno, in merito all'attività del Comitato di sorveglianza del Programma operativo "Sicurezza per lo Sviluppo del Mezzogiorno d'Italia" con riguardo agli interventi di innalzamento dello standard di sicurezza lungo l'asse autostradale Salerno-Reggio Calabria, attraverso un sistema integrato di video-sorveglianza e di comunicazione satellitare. Va sottolineato in proposito che tale sistema prevede, tra l'altro, il controllo degli accessi autostradali e delle aree di servizio e di parcheggio tramite telecamere "intelligenti" per la lettura delle targhe delle autovetture in transito; dette telecamere avrebbero in dotazione un software che, programmato con liste di targhe "sensibili", effettuerebbe una comparazione in tempo reale con l'immagine ripresa, fornendo, in caso di rilevazione positiva, segnali di allerta al centro di controllo.

L'Autorità ha apprezzato l'attenzione dimostrata dal Ministero dell'interno nella predisposizione del progetto, ai fini dell'adozione di misure organizzative e di sicurezza volte a garantire il rispetto della normativa in materia di protezione dei dati personali. In particolare, su richiesta del Garante (con nota del 15 dicembre 1998), sono stati forniti elementi più dettagliati circa:

- a) le diverse modalità di gestione delle immagini riprese dalle videocamere utilizzate dal sistema di controllo, anche in riferimento alle aree di servizio lungo l'asse autostradale e al monitoraggio del traffico sospetto;
- b) le misure di sicurezza adottate anche in riferimento alla codifica dei segnali e delle immagini;
- c) i meccanismi per fornire un'adeguata informazione agli interessati sulla viabilità e nelle aree di servizio;
- d) la non previsione di rilevazioni di tipo acustico integrati al sistema di video-sorveglianza.

Il Garante, circa la conservazione delle informazioni e l'accesso alla consultazione, ha poi rilevato (con nota dell'8 giugno 1999) l'opportunità che:

- a) i dati relativi alle immagini o alle targhe automobilistiche non confluiscono in altri archivi o banche dati o, comunque, non siano intrecciati con altre informazioni diverse da quelle strettamente necessarie per l'espletamento dei controlli o delle indagini;
- b) si predisponga, ove non previsto, un sistema di tracciamento delle consultazioni degli archivi.

Principi analoghi potranno essere formulati dal Garante in riferimento ad altri interventi progettuali previsti nel Mezzogiorno presso altri percorsi autostradali e tratte viarie.

In sintesi, la differenza che il Garante ha riscontrato nello svolgimento della propria attività rispetto al precedente anno è stata la moltiplicazione dei progetti di installazione di sistemi vasti e articolati di video-sorveglianza dentro e fuori gli spazi urbani. I sistemi di monitoraggio visivo, dapprima circoscrivibili ad una piazza o a una strada, si estendono a percorsi tramviari cittadini, poi alla superficie urbana in porzione più o meno estesa, successivamente ad aree comunali con l'inclusione di spazi naturali e, infine, tendono a coprire settori sempre più estesi del territorio.

Allo scopo di avere un quadro dettagliato e capillare di questo fenomeno il Garante ha deciso - senza precedenti in Italia, ma con numerosi riscontri in altri Paesi industriali avanzati - di conferire un incarico di consulenza sulla diffusione e sulla consistenza delle diverse forme di video-sorveglianza utilizzate in luoghi pubblici, esercizi commerciali, supermercati, banche, ecc. La ricerca, necessariamente di tipo preliminare, è in via di espletamento in alcune città campione del Nord, del Centro e del Sud, sulla base di schede analitiche di rilevamento. La decisione è stata presa in attesa della complessiva regolamentazione della materia attraverso uno dei decreti legislativi che il Governo era stato delegato ad emanare (in base all'art. 1, comma 1, lettera i) l. n. 676/1996) e che, se verrà nuovamente conferita tale delega attualmente scaduta, dovrà fissare le norme per un giusto equilibrio tra il diritto alla riservatezza dei cittadini e le esigenze di pubblica sicurezza e della prevenzione dei reati.

Il Garante ha inoltre avviato una ricerca interna su vari aspetti specie giuridici, culturali e sociali del fenomeno della video-sorveglianza, in Italia e all'estero. La ricerca prevede la raccolta e la classificazione di articoli di stampa da quotidiani, periodici italiani e internazionali e riviste specializzate, nonché di saggi, monografie, repertori bibliografici e materiali riversati anche da siti Internet a partire dal 1 gennaio 1997.

2.14 La disciplina della sicurezza nel trattamento dei dati

L'attenzione della legge al tema della sicurezza non è episodica, essendo maturata in un contesto di iniziative nazionali ed internazionali che hanno inteso riempire un vuoto legislativo sulla materia evidenziato da tempo e in varie sedi.

A partire dalla fine degli anni ottanta, vari organismi e sedi internazionali quali l'OCSE, il G 7, il G 10, il GAFI, EUROPOL e il Consiglio d'Europa, ognuno per quanto di competenza ed in base alle tematiche in agenda, hanno richiamato l'attenzione sulla sicurezza informatica e telematica. Dal lungo e complesso dibattito internazionale sono derivate indicazioni utili, raccomandazioni, risoluzioni, direttive, convenzioni ed accordi.

Il riflesso di tale attività nell'ordinamento interno è stato, al contempo, intenso e significativo. Dalla legge n. 518/1992 sulla tutela giuridica dei programmi per elaboratore al successivo decreto n. 205 del 15 marzo 1996, nonché alla legge n. 547/1993 sui crimini informatici (che ha esteso, tra l'altro, l'operatività di determinate disposizioni incriminatrici ai soli sistemi informatici "protetti"). Sono intervenute inoltre alcune discipline particolari che, direttamente o indirettamente, riguardano il tema della sicurezza. Si allude, ad esempio, all'obbligo di misure di sicurezza nei centri edp tenuti al rispetto del segreto d'ufficio (d.P.C.M. del 15 febbraio 1989), al d.P.R. 5 luglio 1995, n. 417, riguardante le biblioteche pubbliche statali, così come alla legge n. 59/1997 sulla riforma della p.a. (art. 15, comma 2) e al d.lg. n. 115/1995 (che prevede precisi obblighi per produttori, distributori e detentori riguardo all'immissione di prodotti sicuri sul mercato).

Come è noto, anche la legge del 31 dicembre 1996, n. 675, attribuisce al tema della sicurezza

za dei dati grande importanza e rilievo, facendone scaturire obbligazioni di carattere "trasversale" riferibili ad ogni tipo di trattamento.

Tale esigenza ha trovato attuazione nella Sezione III del Capo III della legge n. 675/1996, significativamente intitolata *"Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento del danno"*.

L'articolo 15 della legge può essere considerato una norma "aperta", che si limita a fissare le finalità e gli "obiettivi di sicurezza" che devono essere perseguiti dal titolare, con modalità e strumenti destinati a essere dettagliati con diversi strumenti.

L'intervenuta emanazione del regolamento con il D.P.R. n. 318/1999, che va ad aggiungersi alle norme sopra richiamate, ha gettato quindi le basi per una disciplina "generale" della sicurezza, la cui importanza emerge anche dalla circostanza che le disposizioni previste al citato articolo 15 interessa anche a trattamenti pubblici in materia di polizia, giustizia, difesa e sicurezza dello Stato ai quali la legge n. 675, com'è noto, si applica solo in parte (v. art. 4 l. n. 675). Inoltre, nel corpo del testo del d. lg. n. 135/1999 recante *"Disposizioni integrative della legge 31 dicembre 1996 n. 675, sul trattamento dei dati sensibili da parte dei soggetti pubblici"*, segnatamente all'articolo 17, comma 4, è contenuto un esplicito richiamo al dettato dell'articolo 15, commi 2 e 3.

Ponendo attenzione al complessivo impianto normativo, emerge con evidenza la finalità di ridurre al minimo i predetti rischi mediante l'utilizzazione di sistemi di sicurezza costantemente adeguati nel tempo.

Ciò, per due diverse necessità: da un lato, l'articolo 18 della legge n. 675/1996, prevede che il titolare ed il responsabile (se designato) debbano risarcire gli eventuali danni ai sensi dell'articolo 2050 del codice civile. Dall'altro, la legge prevede l'individuazione di misure di sicurezza minime, la cui mancata adozione comporta l'irrogazione di una sanzione penale. L'art. 36 della legge stabilisce infatti che la responsabilità sussista qualora non siano rispettati, o lo siano stati solo parzialmente, gli standard "minimi" di sicurezza prescritti dall'apposito regolamento governativo.

L'art. 15 della legge n. 675/1996 disciplina due tipi differenti di misure: da un lato, il comma 1, che prescrive misure di sicurezza tali da ridurre al minimo il rischio, non individuate ma individuabili sulla base di soluzioni tecniche concretamente disponibili (la loro mancata predisposizione comporta responsabilità civile in caso di danno). Dall'altro, e al loro interno, le misure "minime" previste al comma 2, specificatamente individuate all'interno di un ulteriore atto (il regolamento), che contiene i vari precetti della norma contenuta nell'articolo 36, la cui violazione comporta anche una sanzione di carattere penale.

Pertanto, il regolamento non è destinato a contenere tutte le regole tecniche da adottare in ogni caso per la sicurezza dei dati personali, in riferimento alle diverse modalità di trattamento utilizzate, ma individua unicamente quei requisiti volti ad introdurre un livello *minimo* di protezione, il cui mancato rispetto comporta una maggiore esposizione a rischio del bene giuridico tutelato dalla norma.

La particolarità di tale strumento consiste poi in una impostazione di tipo flessibile, essendo destinato ad un aggiornamento avente cadenza almeno biennale, all'evidente fine di evitare una sua oggettiva "staticità" a fronte di un'evoluzione tecnologica sicuramente "dinamica". Il regolamento non intende quindi individuare le migliori misure evidenziate dalla scienza tecnica in un dato momento, mirando più semplicemente ad enucleare un minimo denominatore comune delle misure di sicurezza disponibili, tale da poter definire le stesse "minime".

In coerenza con la legge da cui promana, il regolamento previsto dalla legge n. 675 si rivolge a tutti i soggetti — pubblici e privati — che nell'ambito delle loro attività pongono in essere un trattamento di dati personali.

Con il regolamento si sono individuate categorie omogenee di modalità di trattamento di dati, al fine di correlare la soglia minima, da un lato, alla tipologia del dato e, dall'altro, allo strumento tecnico utilizzato per il trattamento, tenendo conto della distinzione già operata dalla legge tra dati "comuni" e "sensibili" (dovendosi considerare anche la loro diversa valenza nel quadro di una differente intensità del livello di garanzie per essi previsto).

Nel d.P.R. n. 318 una prima, grande distinzione ha avuto riguardo alle modalità delle operazioni svolte per effettuare il trattamento. Da una parte, quelle effettuate in sostanza con l'esclusivo ausilio di supporti cartacei; dall'altra, quelle poste in essere anche in parte mediante strumenti elettronici o comunque automatizzati.

L'ottica in cui sono state previste le misure di sicurezza è insita non solo nella protezione dei sistemi o delle trasmissioni in quanto tali, ma, più direttamente, nella protezione dei dati personali: il livello di sicurezza si modifica di conseguenza in relazione alla presenza o meno dei dati stessi. Così pure, nel caso siano contestualmente presenti dati "comuni" e "sensibili", è necessario osservare le misure previste per la categoria più elevata).

Va evidenziato, inoltre, come nel regolamento si sia preferito non individuare per ogni singola misura di sicurezza i soggetti tenuti ad adottarla. Tale individuazione dipenderà dalle attribuzioni del titolare del trattamento e dai ruoli ed incarichi conferiti in concreto all'interno della struttura.

Quanto alle definizioni, il regolamento, oltre ad utilizzare quelle già contenute dalla legge 675, prevede quelle di:

- "misure minime", intendendo per esse il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto, in relazione ai rischi a cui fa riferimento l'articolo 15, comma 1, della legge (misure, che possono ad esempio comportare, nei casi previsti nei successivi articoli: l'identificazione dell'utente, l'autorizzazione all'accesso alle funzioni, ai servizi, ai locali, ai dati, la registrazione degli ingressi e i limiti al riutilizzo di supporti per l'archiviazione elettronica o automatizzata o cartacea);
- "strumenti", intendendo per essi i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
- "amministratori di sistema", riferendosi ai soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne la utilizzazione.

Quanto agli effetti che il regolamento spiega sui trattamenti effettuati a fini esclusivamente personali, - eccettuati in generale dall'osservanza dei diversi obblighi normativi fissati dalla medesima legge (a condizione che i "dati non siano destinati ad una comunicazione sistematica o alla diffusione"), ma comunque sottoposti agli obblighi di sicurezza -, il regolamento ha previsto misure di sicurezza tali da tener conto in modo adeguato del possibile, minore rischio insito in tale attività.

Considerato che anche alcune osservazioni formulate nella fase di predisposizione del regolamento sia dal Consiglio di Stato, sia dal Garante andavano nella direzione di limitare, per quanto possibile, l'ambito di applicazione della norma penale in materia di sicurezza, con l'intuibile intento di evitare un'applicazione irragionevole e diffusa della sanzione, si è prevista la sua applicazione soltanto ai trattamenti dei dati di cui agli artt. 22 e 24 della legge organizzati in archivi ed effettuati mediante elaboratori stabilmente accessibili da altri elaboratori, escludendo in tal modo i computer "stand alone". Per quelli caratterizzati invece dalla predetta accessibilità, la misura minima di sicurezza è stata individuata nel solo obbligo, per il soggetto titolare, dell'utilizzo di una parola chiave che inibisca l'accesso al sistema o anche solamente ai dati.

L'ultima parte del regolamento è dedicata al trattamento di dati effettuato mediante strumenti diversi da quelli elettronici o comunque automatizzati (artt. 9 e 10). Si tratta di situazioni diffuse, in cui i dati sono tenuti in supporti cartacei. È il caso, ad esempio, di molti archivi (sia di privati che di pubbliche amministrazioni). Per questi ultimi, nell'individuare le misure minime di sicurezza, il d.P.R. fa riferimento a quelle comunemente già in essere.

A partire dal secondo semestre del 1999, il Garante, , ha già avuto modo di esprimere, nell'ambito di alcuni provvedimenti, la necessità di prevedere puntuali indicazioni in riferimento alle disposizioni contenute nell'art. 15 della legge.

Con un provvedimento del 29 febbraio 2000 si è richiamata l'attenzione degli operatori sulla scadenza del termine a partire dal quale dette misure diventeranno obbligatorie e cioè sei mesi dopo l'entrata in vigore del citato regolamento, così come previsto dalla legge n. 675/1996. In detto provvedimento è stato anche evidenziato come l'applicazione delle nuove norme sia tesa a favorire una più ampia diffusione della cultura della sicurezza, nel trattamento delle informazioni personali, già peraltro presente in alcuni settori specie nel privato.

Infine, circa i rapporti tra la "nuova" disciplina sulla sicurezza e gli adempimenti previsti dalla legge n. 675/1996, e segnatamente quello concernente l'obbligo di notificazione (v. articolo 7, l. cit.), il Garante ha stabilito che l'adozione delle "misure minime" non comporta l'obbligo di ripresentare la notificazione a suo tempo inviata al fine di segnalare l'avvenuto adeguamento alle disposizioni del D.P.R. n. 318/1999. A tale fine, è stato inserito nel modello di notificazione un apposito riquadro, che figura nel provvedimento riportato in allegato alla presente relazione.

3. Il Garante

3.1 I ricorsi ex art. 29: un bilancio d'insieme

Nella relazione dello scorso anno si era dato conto della procedura in base alla quale, pur in assenza del regolamento previsto dall'art. 33, comma 3, della legge n. 675, il Garante aveva comunque esaminato le questioni sollevate tramite i ricorsi presentati ai sensi dell'art. 29.

Il citato regolamento (d.P.R. 31 marzo 1998, n. 501) è stato poi pubblicato sulla Gazzetta Ufficiale il 1° febbraio 1999, entrando in vigore il successivo 16 febbraio.

Con la presente relazione è quindi possibile operare un primo, provvisorio bilancio sull'utilizzo di questo nuovo meccanismo di tutela e sulla congruità delle modalità procedurali che lo caratterizzano.

Va anzitutto osservato che il nuovo strumento di tutela, che si pone nel nostro ordinamento come strumento atipico e fortemente innovativo, si sta rapidamente affermando come valido meccanismo di garanzia, trovando applicazione nei settori più diversi.

Come è noto, la proposizione del ricorso al Garante ai sensi dell'art. 29, per la tutela dei diritti statuiti dall'art. 13 della legge n. 675, si pone in alternativa rispetto all'esercizio dei diritti stessi di fronte all'autorità giudiziaria ordinaria. Il procedimento dinanzi al Garante offre il vantaggio di una procedura caratterizzata da grande celerità che porta, entro 30 giorni dalla data di presentazione del ricorso, alla definizione dello stesso con un provvedimento espresso dell'Autorità (la mancata pronuncia sul ricorso entro il termine citato equivale altrimenti a rigetto: art. 29, comma 4). Il termine inizialmente previsto dal legislatore era di soli 20 giorni, che sono stati elevati poi a 30 in seguito a una modifica normativa introdotta dall'art. 13, comma 1, lettera a), del d.lg. 30 luglio 1999 n. 281. Il termine inizialmente previsto si era infatti dimostrato troppo breve per assicurare un regolare svolgimento dell'istruttoria e, soprattutto, per permettere al titolare di fornire i necessari elementi di valutazione (sia in situazioni di spontaneo adempimento, sia in caso di opposizione alle istanze dell'interessato).

Fra gli elementi che caratterizzano i ricorsi, va ricordata la possibilità per ogni interessato di presentare direttamente il ricorso stesso, senza l'obbligo di avvalersi dell'assistenza di un legale, nell'ambito di una procedura caratterizzata, oltre che da grande celerità, anche da spese di procedimento assai contenute (solo 50.000 lire di diritti di segreteria).

Nel 1999, primo anno di vigenza del d.P.R. n. 501, sono pervenuti 150 ricorsi (199 alla data del 13 aprile 2000) ed è quindi possibile individuare alcuni problemi di carattere generale emersi nella trattazione dei casi concreti.

Anzitutto, si deve segnalare come la novità del nuovo strumento abbia portato, specie nel primo periodo, ad un uso improprio dello stesso o, meglio, ad un utilizzo del ricorso ex art. 29 anche in riferimento ad ipotesi diverse da quelle per le quali tale strumento è apprestato. Va infatti ricordato che il procedimento previsto dall'art. 29 ha caratteri particolari, in quanto con il ricorso che lo introduce non si può lamentare ogni violazione di un diritto della personalità, ovvero ogni supposta violazione della legge n. 675/1996, come può avvenire invece mediante altri strumenti previsti dalla stessa legge, quali le segnalazioni ed i reclami di cui all'art. 31, comma 1, lettera d).

Il ricorso in senso proprio può infatti essere presentato solo per la tutela di una precisa richiesta (formulata in riferimento agli specifici diritti tutelati dall'art. 13, comma 1, della legge),

avanzata precedentemente al titolare o al responsabile del trattamento e da questi disattesa anche in parte. Non è cioè possibile presentare direttamente il ricorso al Garante, ed occorre anzi dapprima, avanzare le proprie richieste nei confronti dei titolari o dei responsabili del trattamento e, poi, attendere almeno 5 giorni dalla data della loro presentazione. Secondo l'art. 29, comma 2, la proposizione immediata del ricorso al Garante è infatti possibile solo nell'ipotesi in cui il decorso del tempo necessario per interpellare il titolare o il responsabile "esporrebbe taluno a pregiudizio imminente e irreparabile".

In numerosi casi si è dovuto così procedere a dichiarazioni di inammissibilità, in assenza, appunto, del previo esercizio dei diritti dell'art. 13 nei confronti del titolare, o in carenza di adeguate motivazioni che giustificassero l'immediata presentazione del ricorso al Garante.

In alcuni casi, poi (più frequenti, ovviamente nel primo periodo), prima di procedere all'avvio dell'istruttoria, il ricorrente è stato invitato a regolarizzare il ricorso medesimo (privò, ad esempio, della firma autenticata dell'interessato o della ricevuta del versamento dei diritti di segreteria), secondo quanto stabilito dall'Autorità stessa con propria delibera del 1° marzo 1999.

L'esperienza di questo primo anno ha evidenziato alcune classi di titolari del trattamento o settori di attività che sono stati oggetto della presentazione di molteplici ricorsi. Al di là delle vicende specifiche, questi "filoni" più ricorrenti hanno permesso di mettere a fuoco le più generali problematiche legate alla protezione dei dati personali in alcuni campi di rilevante interesse.

3.1.1
Principali
settori e
ambiti di
trattamento
dei dati

Il settore delle banche e delle compagnie di assicurazione è stato fortemente inciso dalla legge n. 675 che ha fornito agli utenti dei rispettivi servizi nuove opportunità di tutela. I ricorsi in tale ambito hanno riguardato, oltre all'esercizio del diritto di accesso, anche la richiesta di cancellazione di dati in ordine a presunte violazioni nel loro trattamento. Con riguardo al settore bancario, ciò è avvenuto specie in riferimento alla fase pre-contrattuale volta all'instaurazione di rapporti di finanziamento a favore dell'interessato. Per quanto concerne, invece, le imprese di assicurazione, le istanze sono state pressoché tutte rivolte ad avere accesso alle perizie medico legali curate dai medici fiduciari delle imprese stesse (sul punto si veda il capitolo 2.6).

Sempre con riferimento al settore di tali operatori economici, lo strumento del ricorso ex art. 29 ha trovato larga applicazione rispetto ai trattamenti di dati effettuati dalle c.d. centrali rischi private, largamente consultate da banche e società finanziarie, specie in rapporto a richieste di prestiti e finanziamenti. L'esame specifico delle singole vicende ha fatto emergere in diverse occasioni il diritto degli interessati ad ottenere la cancellazione di dati errati, la modificazione di informazioni inesatte o la cancellazione di dati relativi a trattamenti per i quali era già scaduto il termine legittimo di conservazione.

In riferimento a tutt'altro settore va invece rammentato che le pubbliche amministrazioni detengono e gestiscono una rilevante mole di dati personali, spesso assai delicati. Le possibilità offerte dall'art. 13 hanno aperto nuovi spazi di tutela per il cittadino sia nei confronti di ambiti caratterizzati da una tradizionale, limitata accessibilità (per es. le istituzioni militari con riferimento non ai particolari trattamenti di cui all'art. 4 della legge, ma a quelli riguardanti, più semplicemente, la gestione del personale dipendente). Sia, ad esempio, nei confronti delle strutture sanitarie pubbliche. In quest'ultimo settore sono emersi anche profili assai delicati che hanno riguardato la legittimità della comunicazione dei dati a soggetti esterni alla struttura sanitaria stessa, l'accessibilità di particolari dati medici da parte degli interessati (es. riscontri radiografici), la legittimità di trattamenti concernenti dati protetti da particolari garanzie di riservatezza (ad esempio, in materia di AIDS secondo il disposto della legge n. 135 del 1990).

Una numerosa serie di ricorsi è stata promossa, inoltre, da dipendenti pubblici e privati per

accedere ai dati personali contenuti nella documentazione relativa al rapporto di lavoro detenuta dal datore di lavoro. Ciò, sia per poter verificare l'esattezza e la completezza della documentazione conservata, sia, soprattutto, per poter accedere a particolari dati personali rappresentati da giudizi, note di qualifica o rapporti annuali particolarmente rilevanti al fine di ottenere avanzamenti di carriera o progressioni economiche.

In corso d'anno sono stati altresì proposti alcuni ricorsi nei confronti di titolari di trattamento o in riferimento a settori di attività che, ai sensi dell'art. 4 della legge, sono però esclusi dallo spettro applicativo dell'art. 13 e nei cui confronti non è quindi proponibile il ricorso ex art. 29.

Sono stati infatti presentati ricorsi nei confronti degli organismi di informazione e sicurezza, nonché nei confronti di trattamenti svolti da forze di polizia o da uffici giudiziari. In alcuni casi, sulla base delle informazioni acquisite in occasione della presentazione di tali ricorsi, il Garante, pur negando la possibilità di esercitare i diritti dell'art. 13, ha però autonomamente instaurato procedimenti volti ad accertare che i trattamenti in questione venissero svolti in coerenza con il disposto dell'art. 9 della legge (norma che trova applicazione anche nei confronti di tali particolari trattamenti).

Una serie significativa di ricorsi ha riguardato infine l'esercizio dei diritti dell'art. 13 in ambito giornalistico, sia della carta stampata, sia degli altri indirizzi di informazione. Si è trattato di casi spesso complessi ed articolati, non di rado intrecciati a più ampie ipotesi di violazione della normativa sulla protezione dei dati, oltre che di altre disposizioni normative. Le istanze hanno interessato ipotesi di accesso agli archivi giornalistici e di opposizione al trattamento di dati, nonché la richiesta di rettifica o di cancellazione degli stessi, anche in riferimento alla riproduzione di fotografie o alla messa in onda di riprese televisive.

3.1.2
Particolari
profili
applicativi e
considerazioni
finali

Nell'ambito dell'esame di diversi ricorsi, il Garante ha nuovamente puntualizzato alcuni concetti circa l'esatto significato dell'istituto dell'accesso di cui all'art. 13 della legge. Tale diritto si configura infatti come un diritto di accesso ai dati personali dell'interessato detenuti dal titolare del trattamento e non deve quindi essere confuso con il diverso diritto di accesso agli atti e documenti amministrativi di cui alla legge n. 241 del 1990.

Naturalmente i dati dell'interessato possono, e normalmente sono contenuti in atti o documenti. L'esatto adempimento del diritto dell'art. 13 spesso impone al titolare di estrapolare tali dati e di renderli disponibili al richiedente. Peraltro, in più occasioni il Garante ha precisato che l'esibizione o la consegna in copia della documentazione può costituire una modalità adeguata per corrispondere alle richieste dell'interessato. Ciò, qualora la consultazione dei documenti consenta ugualmente un'agevole comprensione dei dati richiesti, considerata anche la qualità e la quantità delle informazioni, e risulti invece particolarmente difficoltosa l'estrazione dei dati stessi dai documenti, nonché la loro trasposizione su apposito supporto cartaceo od informatico, secondo il disposto dell'art. 17, comma 6, del d.P.R. n. 501/1998.

Va inoltre messo in luce come spesso gli interessati ritengano erroneamente che, accanto al diritto di accesso, esista un diritto di cancellazione dei dati ugualmente esteso, di cui possano avvalersi. La legge distingue invece nettamente, nell'ambito del medesimo art. 13, le due ipotesi, configurando la possibilità di un diritto alla cancellazione nella sola ipotesi di trattamenti effettuati in violazione di legge.

La validità dello strumento del ricorso si è pienamente dimostrata nei numerosi casi nei quali si è pervenuto; ai sensi dell'art. 20 del d.P.R. n. 501, alla decisione di non luogo a provvedere sul ricorso medesimo. Sono infatti queste le situazioni nelle quali, dopo la proposizione del ricorso al Garante, il titolare del trattamento adempie spontaneamente alle richieste del ricorrente, soddi-

sfacendo quelle istanze che in un primo momento erano rimaste inevase. Resta peraltro da considerare, *de iure condendo*, la praticabilità di un qualche correttivo per rendere ancora più effettiva la tutela degli interessati, in modo da disincentivare la possibile prassi di chi, confidando nell'assenza di "sanzioni" in caso di ritardato riscontro alle richieste di cui all'art. 13 della legge (a parte la circoscritta misura delle spese e dei diritti connessi alla soccombenza nel procedimento di cui all'art. 29), possa tendere ad attivarsi nei confronti dell'interessato solo a seguito della formale presentazione di un ricorso.

Nei casi, invece, di accoglimento del ricorso, la decisione del Garante, riconoscendo la legittimità delle pretese dell'interessato, ha spesso fornito indicazioni e direttive volte a rendere pienamente conforme al dettato normativo il trattamento dei dati svolto dal titolare.

Uguualmente, i ricorsi sono stati strumento utile, al di là delle decisioni finali adottate, per enucleare situazioni di potenziale violazione della legge ed hanno permesso al Garante di attivare autonomamente procedimenti di segnalazione diretti a verificare la legittimità complessiva di molte operazioni di trattamento.

Va infine ricordato che, finora, solo tre decisioni del Garante in tema di ricorsi sono state oggetto di opposizione al tribunale ai sensi dell'art. 29, comma 6 della legge. Rispetto a tali vicende il Garante, dietro conforme parere dell'Avvocatura generale dello Stato, si è costituito in giudizio, attraverso le competenti avvocature distrettuali, al fine di sostenere le ragioni che avevano ispirato le decisioni adottate.

3.2 Rapporti con l'Ufficio del Garante

L'intensa attività di informazione che ha caratterizzato anche nel 1999 l'impegno del Garante è la riprova non solo della crescita del numero di interventi posti in atto e delle questioni affrontate dall'Autorità nei diversi settori della vita sociale, economica e culturale del nostro Paese, ma anche dello svilupparsi di una crescente sensibilità da parte di larga parte della società italiana sul tema della privacy. Il "valore privacy" sta progressivamente radicandosi nell'attitudine dei cittadini nei confronti delle informazioni che li riguardano, sia di tipo comune, sia a carattere sensibile, quando esse vengono raccolte, utilizzate e diffuse da parte di soggetti pubblici e privati. Sempre più persone si rivolgono al Garante per chiedere non solo la protezione dei loro dati, ma anche per poter esercitare il controllo su quelle informazioni e decidere in maniera responsabile e consapevole sul loro uso.

La novità sociale e culturale del concetto di privacy è testimoniata anche negli stessi linguaggi del settore pubblicitario, da sempre cartina di tornasole dei cambiamenti e delle tendenze dominanti. Quella della pubblicità è, d'altro canto, una comunicazione veloce e sintetica caratterizzata dall'immediata "cattura" di parole a forte connotazione informativa e di immediata riconoscibilità. Nel corso degli ultimi due anni è stato possibile riscontrare che termini come "privacy", "garante", "riservatezza" (quest'ultimo spesso in collegamento semantico con il termine "trasparenza") sono stati inseriti in varie pubblicità relative a diversi settori produttivi (borse, tendaggi, costruzioni ecc.), apparse su quotidiani e periodici.

D'altro canto, la fisionomia a "macchia indistinta" che, in molti casi, caratterizza ancora i concetti di protezione e riservatezza dei dati (di volta in volta strumentalizzati per nascondere disfunzioni e disservizi o per ottenere garanzie non previste, oppure utilizzati a fini di deresponsabilizzazione o invocati in maniera parossistica e gratuita) nel corso del 1999 ha reso necessari, da parte dell'Autorità, grandi sforzi di messa a fuoco, chiarificazione ed orientamento, in particolare sugli ambiti e sulle modalità di applicazione della normativa, nonché sul ruolo istituzionale svolto del Garante.

3.2.1
Relazioni
esterne e
rapporti
con i media

Consapevole di questo quadro di riferimento, il Garante ha cercato di mantenere in costante contatto l'istituzione con il cittadino e di promuovere quel "diritto alla privacy", da pochi anni introdotto nel nostro ordinamento e nel nostro orizzonte sociale, che si sta però vieppiù imponendo come uno dei diritti fondamentali nella Società dell'Informazione, dominata da una raccolta sempre più massiccia di dati. Va in questa direzione l'impegno svolto dall'Ufficio del Garante per fornire a cittadini, pubbliche amministrazioni ed enti privati un costante servizio di assistenza e supporto telefonico attraverso i suoi funzionari.

Nell'attività di relazione con il pubblico l'Autorità, nonostante i problemi ancora non risolti di completamento dell'organico, ha cercato di assicurare un flusso di informazione continuo verso i cittadini, gli organismi pubblici e le imprese, chiarendo dubbi interpretativi ed applicativi, dando indicazioni operative e ricevendo anche segnalazioni sui possibili casi di violazione del diritto alla privacy. Il numero di questi contatti si è mantenuto elevato anche nel 1999 (circa 12.000), a testimonianza di un interesse radicato nella società e di un'esigenza di rispetto che ha trovato finalmente un suo strumento di tutela.

Il servizio di relazioni con il pubblico, caratterizzato da modalità dirette ed informali, non solo ha consentito all'Autorità di mantenere uno stretto contatto con la società, ma anche di favorire un flusso di informazioni e problematiche provenienti dalla società civile, dal mondo del lavoro, della ricerca, della produzione e dell'amministrazione pubblica. Di conservare, in buona sostanza, la sua dimensione di istituzione "aperta", non burocratica, attenta ai processi in atto e alle nuove prospettive emergenti.

Intensa è stata anche la partecipazione da parte dei rappresentanti del Garante e dei funzionari dell'Ufficio a convegni, seminari ed incontri organizzati da università, associazioni di categoria o organismi privati, nei quali i diversi aspetti dell'attuazione della legge n. 675 del 1996 sono stati affrontati e discussi.

Anche nel corso del 1999, le tematiche legate alla privacy hanno ricevuto un'attenzione particolare e intensa da parte dei *media*. Programmi radiofonici e televisivi, quotidiani e periodici hanno dato ampio risalto e spazio alle iniziative del Garante, alle innovazioni legislative, come pure agli aspetti connessi all'applicazione e al rispetto della legge sulla protezione dei dati personali da parte degli stessi organi di informazione, della pubblica amministrazione e del settore privato. Le statistiche elaborate dall'Ufficio sulla presenza delle tematiche relative alla privacy sui mezzi di informazione danno un quadro confortante. Bastano alcune cifre: nel periodo che va dal marzo 1999 al marzo 2000, le pagine dedicate alla privacy dai maggiori quotidiani e periodici nazionali ed esteri sono state oltre 6.000, delle quali oltre 1.300 riguardanti specificamente l'attività del Garante. Le prime pagine sono state più di 200.

A differenza degli scorsi anni (-nei quali era dato riscontrare da parte dei *media* un'attitudine legata al sensazionalismo e alla "notiziabilità" della privacy, piuttosto che alle questioni sostanziali di tutela dei diritti coinvolte nelle decisioni del Garante-) la tematica della protezione dei dati ha acquisito caratteri più profondi ed è stata collegata alle dinamiche sociali, economiche e culturali del nostro Paese. Prova ne sia il rinnovato interesse dimostrato dagli organi di informazione alle problematiche legate alla tutela dei diritti dei minori e delle fasce deboli, alla sanità, al mondo del lavoro, alla raccolta dei dati da parte del settore pubblico e privato, all'espandersi dei sistemi di controllo e sorveglianza, ad Internet, all'uso delle nuove tecnologie, alla raccolta indiscriminata di informazioni sulle persone anche a scopo commerciale, alle nuove frontiere della privacy (a cominciare dalla tutela dei dati genetici), ai nuovi diritti di cittadinanza nella società elettronica dell'informazione.

Il ruolo svolto dal mondo dell'informazione riveste, del resto, un'importanza essenziale nella corretta diffusione e conoscenza non solo dell'attività del Garante, ma della stessa "intelligenza" delle tematiche legate alla privacy. La promozione della conoscenza di questa materia, oltre ad

essere un compito connesso direttamente all'adempimento di funzioni istituzionali attribuite al Garante dalla legge n. 675 del 1996, rappresenta anche l'obiettivo di una regolazione dei rapporti sociali.

Forse per nessuna delle altre autorità indipendenti come per quella sulla protezione dei dati personali, infatti, si è posta la necessità di svolgere un ruolo di comunicazione così peculiare, teso ad informare i cittadini dei nuovi diritti ad essi riconosciuti e delle modalità per il loro esercizio, ed insieme a promuovere un salto di qualità nella cultura complessiva della società. Obiettivo, questo, che il Garante ha cercato di raggiungere illustrando dettagliatamente i provvedimenti adottati, spiegando, attraverso casi concreti, i contenuti e le innovazioni introdotte dalla legge sulla protezione dei dati personali, nonché sottolineando la portata e le implicazioni di queste norme, aventi anche carattere organizzativo e strutturale, nei diversi ambiti istituzionali e produttivi.

I comunicati stampa emanati dal Garante sono stati in numero di 159 nel 1999, e di 24 nei primi mesi del 2000.

Nel corso del 1999, dunque, è stato profuso dall'Autorità un forte impegno nel campo della comunicazione per mettere maggiormente a fuoco la nozione di privacy, intesa nel suo significato di diritto dei cittadini a proteggere le proprie informazioni personali e di trasparenza nella loro gestione, nonché per illustrare le innovazioni che essa ha introdotto nel nostro ordinamento, nelle prassi consolidate di utilizzo dei dati e nei rapporti che intercorrono tra la società civile, da un lato, la pubblica amministrazione ed il settore privato, dall'altro.

Questo è stato possibile anche grazie alla predisposizione di nuovi strumenti di comunicazione attraverso i quali il Garante è stato in grado di offrire un quadro sempre più ampio, puntuale e articolato della sua attività e delle tematiche che coinvolgono direttamente la sfera privata dei cittadini.

La "Newsletter" del Garante per la protezione dei dati personali, realizzata a cura dell'ufficio stampa, viene inviata non solo alle redazioni giornalistiche, ma anche ad associazioni di categoria, a professionisti e pubbliche amministrazioni. Essa, è risultata uno strumento di comunicazione snello e a carattere continuativo, che ha consentito di informare organi di stampa e nuovi media in maniera più ampia, dettagliata e approfondita, utilizzando un linguaggio semplice ed immediato. La "Newsletter" è giunta ormai al suo secondo anno di pubblicazioni (nel 1999 sono usciti 36 numeri; 9 numeri, invece, nei primi mesi del 2000), e la sua periodicità settimanale -meno legata alla tempestività del comunicato stampa emesso su singole questioni e su problemi di urgente risoluzione- ha permesso di fornire in via continuativa un aggiornamento sull'attività del Garante, nonché di offrire uno strumento ulteriore di conoscenza e di approfondimento delle tematiche connesse alla riservatezza dei dati e alla tutela delle persone, nel quadro d'insieme delineato dalla Società dell'Informazione.

Nel corso del 1999 il Garante ha anche curato la realizzazione di un archivio informatico ipertestuale che contiene la documentazione integrale, relativa alla sua attività, alla normativa nazionale ed internazionale di riferimento e alle pubblicazioni fin qui realizzate.

L'archivio digitale, "Cittadini e Società dell'informazione", è stato distribuito su CD-Rom multiplatforma realizzato in formato Adobe PDF, scelto per la sua flessibilità nel gestire e riprodurre con precisione lunghi documenti di testo rispettandone i caratteri, l'impaginazione, le immagini e gli elementi grafici, in maniera del tutto indipendente dalle applicazioni software e dall'hardware con cui sono stati generati. I contenuti del CD-Rom sono accessibili con semplicità grazie al "lettore" Acrobat Reader il cui programma di installazione, disponibile per i più diffusi sistemi operativi, è accluso all'interno del CD e liberamente distribuibile.

L'accesso alle informazioni è facilitato da un'interfaccia sobria, studiata per consentire di "navigare" attraverso le varie sezioni dell'archivio grazie ai controlli dinamici inseriti nelle pagine

sotto forma di icone. I contenuti sono raggruppati in cinque sezioni principali (rispettivamente dedicate alla presentazione dei compiti e dell'organizzazione dell'Ufficio del Garante; raccolta integrale delle fonti normative relative all'attività dell'Autorità; relazioni presentate al Parlamento sull'attività svolta; pubblicazioni curate dal Garante), mentre un'ultima sezione, dedicata ai temi di maggiore interesse, raggruppa per settori e materie tutte le informazioni ed i provvedimenti, relativi ai campi di più frequente intervento da parte del Garante, tratte dalle fonti fin qui citate, semplificandone ulteriormente la ricerca. Un attento lavoro di catalogazione dei documenti consente infine, di effettuare ricerche "full text" grazie agli strumenti messi a disposizione da Acrobat.

Il CD, inviato gratuitamente a chi ne faccia richiesta, ha riscosso notevole successo, dimostrandosi uno strumento di consultazione richiesto ed utilizzato 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 sulla riservatezza dei dati.

Tra le attività di comunicazione va ricordata, inoltre, anche la pubblicazione, sinora a carattere bi/trimestrale, del bollettino "Cittadini e Società dell'Informazione" che ha raggiunto il numero 10 e raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa e altra documentazione sull'attività dell'Autorità. Nel Bollettino è stato predisposto un indice dei provvedimenti divisi per materia, in modo da agevolarne la consultazione e la ricerca. Utile si è rivelata inoltre la ripubblicazione dei testi normativi aggiornati e coordinati sulla base delle numerose novità intercorse in materia di riservatezza (si veda, ad esempio, il testo della legge n. 675 coordinato e aggiornato con i decreti legislativi di integrazione via via emanati ai sensi della legge delega n. 676 del 1996, pubblicato sul Bollettino n. 9).

Come si vedrà di seguito, l'apertura del sito Internet istituzionale www.garante.gov.it, unico sito del Garante, consente già oggi, pur in una configurazione ancora sperimentale, un contatto diretto con i cittadini ed offre un'ulteriore possibilità di diffusione e promozione. Il sito, infatti, è stato studiato per offrire un panorama completo sui provvedimenti e le pubblicazioni del Garante, nonché l'aggiornamento tempestivo sulle decisioni dell'Autorità, sulle modifiche normative, sulla giurisprudenza in materia di privacy, nonché sulle questioni all'ordine del giorno in tema di tutela dei diritti fondamentali.

Allo scopo di avvicinare i cittadini e gli operatori pubblici e privati alle tematiche di maggiore rilevanza messe in campo dalle norme sulla privacy, il Garante nel corso del 1999 è stato poi presente con un proprio stand al "Forum della Pubblica amministrazione" (Roma, 4-8 maggio 1999) e al "ComPa", Salone della comunicazione pubblica e dei servizi al cittadino (Bologna, 15-17 settembre 1999) dove ha partecipato a sessioni e convegni.

Nell'ambito delle due manifestazioni è stato fra l'altro proiettato un video, realizzato a cura dell'ufficio stampa, che contiene i contributi dei componenti del Garante sui temi della Società dell'Informazione, della pubblica amministrazione, del giornalismo e di Internet. Questo video, oltre a costituire un supporto informativo alla partecipazione del Garante al Forum della P.A. del 1999, manifestazione dove l'Autorità è stata presente con un proprio stand, è stato trasmesso in più di 100 emittenti televisive locali e 200 radiofoniche, oltre ad essere stato reso accessibile via Internet.

Muovendosi in questa direzione, il Garante, in collaborazione con la Presidenza del Consiglio dei ministri - Dipartimento dell'editoria, ha infine avviato un progetto per una campagna mirata di comunicazione istituzionale diretta alla promozione dei nuovi diritti riconosciuti alle persone dalla legge sulla protezione dei dati personali.

3.3 Contabilità, dotazione finanziaria, impegni di spesa e sedi dell'ufficio

Per il 1999 le risorse finanziarie a disposizione del Garante sono state pari a 22.345 milioni di lire, di cui 300 milioni previste per entrate derivanti dai diritti di segreteria per notificazioni, autorizzazioni e ricorsi, così come disciplinati dalla normativa.

Rispetto all'anno 1998, le risorse per trasferimenti provenienti dal bilancio dello Stato si sono infatti incrementate di 10 miliardi di lire, passando da 12.045 a 22.045 milioni. Ciò, in previsione dell'emanazione del decreto legislativo n. 51/1999, il quale, oltre ad aver conferito all'Autorità il potere di disciplinare con proprio regolamento l'organizzazione interna dell'Ufficio, ha previsto l'istituzione del ruolo organico del personale del Garante -fissato in cento unità- assegnandogli un trattamento economico provvisorio.

Il terzo anno di attività del Garante è stato caratterizzato, sotto il profilo finanziario, soprattutto, da due fondamentali impegni:

- a) la prosecuzione del processo organizzativo dell'Ufficio, anche alla luce del citato decreto n. 51/99;
- b) l'intensificazione delle iniziative per la stipula del contratto definitivo di locazione per la nuova sede stabile dell'Ufficio.

Nel corso del 1999, l'Autorità ha inoltre dedicato molte energie per assicurare una partecipazione attiva e costante dei propri funzionari alle riunioni ed agli incontri nelle diverse sedi dedicati alla protezione dei dati personali, a livello nazionale e comunitario.

Per adempiere ai crescenti impegni gravanti sull'Ufficio, durante il 1999 il Garante si è tra l'altro avvalso della collaborazione di tredici consulenti (le competenze di otto di essi sono state liquidate nell'esercizio del 1999). Scelti per le loro specifiche professionalità, essi hanno contribuito all'attività pubblicistica e di documentazione, ai servizi connessi alla rassegna stampa, allo studio, all'organizzazione sistematica ed alla massimizzazione delle decisioni del Garante e di altre pronunce giurisprudenziali in materia di dati personali, anche in vista dell'apertura del sito web.

I consulenti sono stati altresì utilizzati per la ricerca e l'organizzazione del materiale attinente all'attività comunitaria e internazionale, nelle more della costituzione di un servizio studi e documentazione sulle materie di interesse dell'Ufficio. La loro opera è stata inoltre utilizzata per l'organizzazione di taluni incontri di carattere comunitario ed internazionale che hanno consentito al Garante di conseguire importati risultati nella sempre intensa attività di cooperazione e scambio reciproco con gli altri soggetti impegnati nella tutela dei dati personali. A tale proposito, si devono in particolare ricordare la riunione dell'Autorità di controllo comune di Schengen, ospitata dal Garante a Firenze il 27 e 28 maggio 1999, nonché la XXII Conferenza internazionale delle Autorità garanti che sarà organizzata dal Garante a Venezia nei giorni 28-30 settembre 2000. I maggiori impegni a cui si è dovuto far fronte trovano riscontro, a livello di bilancio, nell'incremento della spesa erogata per oneri relativi al personale, cresciuta nel 1999, rispetto all'anno precedente, di oltre 260 milioni di lire, con un incremento di quasi il 16 per cento.

Per quanto attiene al secondo settore di impegno, si deve ricordare che l'8 novembre 1999 è stato sottoscritto il contratto definitivo di locazione relativo alla porzione di uno stabile sito in Roma, Piazza Monte Citorio nn. 115-121, che è già gradualmente occupato quale nuova sede stabile del Garante. Una parte dell'Ufficio si è già installata in tali ambienti, in attesa del completamento dei lavori di ristrutturazione e della consegna dei rimanenti locali, previsti a partire dal maggio del 2000 fino alla fine del corrente anno. In seguito a ciò, il Garante potrà finalmente avere una

3.3.1
La gestione
finanziaria
dell'esercizio
1999

sede idonea in grado di contenere tutti gli uffici necessari alla sistemazione operativa del personale attualmente dislocati in ben tre sedi, compreso quello previsto a completamento dell'organico dal d. lgs. n. 51/1999. Tale stabile offre anche spazi sufficienti per ospitare il progettato servizio studi e documentazione e la biblioteca e per organizzare seminari, convegni ed altri incontri di lavoro. Le risorse necessarie agli arredi e all'installazione degli impianti, prevedendo per questi ultimi l'impiego di idonee tecnologie, sono state reperite anche con somme accantonate negli anni precedenti. Nel complesso, le spese di funzionamento -sezione del bilancio nella quale rientrano anche quelle affrontate per la locazione e la sistemazione della sede di Piazza Monte Citorio- sono state liquidate e pagate nel 1999 per 2.392 milioni di lire, i tre quarti delle quali sono imputate agli esercizi pregressi.

Nel documento di programmazione finanziaria del 1999 era stato riservato un particolare rilievo ed impegno economico all'attività del Garante inerente a seminari di lavoro, incontri internazionali e convegni di studio. Nell'anno trascorso si è evidenziato su questo punto un aumento considerevole, documentato dall'incremento delle spese per le diverse missioni nazionali ed estere cui sono stati chiamati i componenti del Garante, il segretario generale e i funzionari dell'Ufficio. Tra le iniziative più significative conviene qui ricordare la partecipazione ad Helsinki e ad Hong Kong, nella primavera e nel mese di settembre del 1999, rispettivamente alla conferenza europea delle autorità di protezione dei dati e alla Conferenza internazionale sulla privacy.

Nel corso del 1999 si è dato inoltre inizio ad un programma di attività formative per il personale, con l'accantonamento di 144 milioni di lire finalizzati, soprattutto, in particolare, all'approfondimento della conoscenza di lingue straniere (delibera del 30 dicembre 1998). Queste sono risultate infatti di costante utilizzazione sia per l'ordinaria attività d'ufficio, sia nel corso delle frequenti missioni all'estero, sia in occasioni di incontri e seminari internazionali, promossi anche dal Garante, sia, infine, nello studio e nella predisposizione dei documenti che quotidianamente sono esaminati e predisposti dall'Ufficio.

In tale ambito, deve essere altresì ricordata l'attività diretta a favorire la conoscenza fra il pubblico della normativa sulla protezione dei dati personali e delle sue finalità, svolta nell'adempimento di uno specifico compito attribuito al Garante (art. 31, comma 1, lett. i). Si devono in proposito ricordare le già citate partecipazioni ad iniziative conoscitive con propri stand al Forum della Pubblica amministrazione di Roma del 4-8 maggio 1999 e al "ComPa", Salone della comunicazione pubblica e dei servizi al cittadino (Bologna, 15-17 settembre 1999). Per la partecipazione a queste due importanti manifestazioni, l'onere per il Garante è stato complessivamente non superiore ai 220 milioni, comprendendo in essi tutte le spese che vanno, da quelle sostenute per la locazione dell'area espositiva all'allestimento degli stand, a quelle concernenti il materiale espositivo e gli allacciamenti telematici.

Sul piano strettamente contabile in ambito amministrativo si è complessivamente registrato un impegno di risorse crescente. Ciò soprattutto perché, pur in assenza del regolamento di cui al d.lg. n. 51/1999, si sono dovute affrontare e risolvere le molteplici questioni legate alla piena funzionalità operativa del Garante. I pagamenti sono passati, in percentuale delle somme stanziare nel bilancio, dal 17,5 per cento del 1997, al 27 per cento del 1998, al 35 per cento del 1999. In quest'ultimo anno, le spese erogate hanno poi superato i sette miliardi di lire, di cui quasi tre miliardi per impegni degli anni trascorsi.

Come già effettuato per gli esercizi precedenti, si è provveduto a regolare le spese del Garante mediante prelevamenti dal fondo giacente in un conto di contabilità speciale presso la Banca d'Italia- Tesoreria provinciale dello Stato (sezione di Roma). Tuttavia, mentre nel periodo iniziale di attività dell'Ufficio la procedura relativa alla contabilità speciale ha consentito la gestione contabile senza particolari problemi, con l'entrata a regime di tutte o quasi le attività istituzionali (ricorsi, pareri, ispezioni, partecipazioni a commissioni comunitarie, registro dei trattamenti, ecc.),

la struttura si è vista via via caricata di ulteriori incombenze di natura logistico-operativa, quali, ad esempio, i bonifici urgenti dall'estero e per l'estero. Tutto ciò ha suggerito alcuni perfezionamenti che si avrà cura di apportare alla gestione della contabilità e delle spese che sarà ridisciplinata nel terzo dei regolamenti interni che il Garante si accinge ad adottare in attuazione del d.lg. n. 51/1999.

3.4 Registro generale dei trattamenti

Nel corso del 1999 il Garante ha proseguito e sviluppato le attività legate alla tenuta del registro generale dei trattamenti (art. 31, commi 1, lett. a) e 3, l. n. 675/1996). Come si era avuto modo di illustrare nella relazione per l'anno 1998, tale registro raccoglie le notificazioni che i titolari dei trattamenti dei dati devono inviare al Garante fuori dei casi di esonero (artt. 7 e 28).

Per adempiere all'obbligo di notificazione i titolari debbono avvalersi di un apposito modello cartaceo o di un programma su floppy disk, sulla base di quanto previsto dall'art. 12 del d.P.R. 501/1998, provvedendo altresì a versare i relativi diritti di segreteria, pari a 25.000 o 15.000 lire, a seconda del supporto utilizzato. Le notifiche sono inviate mediante raccomandata con avviso di ricevimento, oppure presentate direttamente all'Ufficio del Garante.

Il Garante ha profuso particolare impegno per assicurare che la distribuzione dei modelli e dei floppy disk agli utenti avvenisse gratuitamente ed in maniera capillare sul territorio. Essa viene svolta dalle agenzie di Poste italiane S.p.a. in base ad un'apposita convenzione rinnovabile anno per anno, nonché, in misura residuale, direttamente dall'Ufficio. La convenzione, già stipulata per gli anni passati, è stata rivista e aggiornata, adeguandola alle nuove esigenze anche in base all'esperienza maturata. Al fine di facilitare i cittadini, rendendo ancor meno oneroso tale adempimento, si è deciso di rendere possibile anche l'utilizzo della modulistica non direttamente distribuita dal Garante, purché conforme ai modelli approvati.

Le notificazioni complessivamente pervenute all'Ufficio dall'avvio delle procedure, fino al mese di febbraio del 2000, sono circa 270.000. La maggior parte di esse si riferiscono a nuovi trattamenti e costituiscono comunque la prima notificazione effettuata dal titolare, mentre in misura più contenuta giungono modifiche a precedenti notificazioni anche della cessazione di un trattamento. La registrazione di queste ultime è infatti necessaria anche al fine di tenere aggiornato il registro, nel quale sono riportate tutte le variazioni intervenute, salvaguardando così la serie storica degli avvenimenti.

Anche in relazione all'elevato numero di notificazioni risultate incomplete o irregolari (circa 42.000 pari all'11,4%), l'impegno dell'Ufficio non è limitato alla loro memorizzazione, ma si indirizza anche verso la loro possibile regolarizzazione. Procedura, questa, che si articola in maniera differente a seconda degli errori riscontrati, i più diffusi dei quali consistono nell'illeggibilità del dischetto, nella mancata firma da parte del titolare o responsabile, nella mancata compilazione di riquadri, nel fatto che il modello inviato non è conforme a quello prescritto o che i dischetti non sono accompagnati dalla stampa del relativo contenuto. A queste evenienze si devono aggiungere le numerose notificazioni che pervengono prive dell'attestato di pagamento dei diritti di segreteria e che conseguentemente devono essere anch'esse regolarizzate. In generale, si tratta di procedure non brevi, a volte complesse, il che differisce l'inserimento della notificazione nel registro essendo quest'ultima in relazione alla tempestività con cui il titolare provvede alla rettifica degli errori e alla spedizione la documentazione all'Ufficio.

In una prima fase, per lo svolgimento di alcuni degli adempimenti richiamati, ci si è avvalsi dei servizi di una società, che si è aggiudicata di servizio all'esito. Mediante detta società si è provveduto alla memorizzazione delle notificazioni pervenute e alla loro archiviazione.

L'Ufficio è stato particolarmente impegnato anche sul fronte dei numerosi quesiti, per lo più posti telefonicamente con una media di circa cinquanta telefonate giornaliere. Esse hanno costituito un onere non indifferente in considerazione della ridotta consistenza del personale che sarà nel prossimo futuro potenziato.

Come meglio illustrato al precedente punto 2.14, il d.P.R. n. 318/1999 ha individuato le diverse misure minime di sicurezza che i titolari dei trattamenti sono tenuti ad adottare per ridurre i rischi di distruzione, perdita, accesso non autorizzato, trattamento non conforme alle finalità della raccolta o comunque non consentito dei dati personali. Poiché nella notificazione deve essere fornita anche una descrizione generale di tali misure, gran parte dei soggetti che avevano effettuato già la notificazione avrebbero dovuto provvedere alla sua modifica in relazione a tale aspetto, inviando una nuova notificazione al Garante per la sola esigenza di dare comunicazione del doveroso adempimento ad un obbligo di legge. Per sgravare perciò i cittadini da tale onere, ed allo stesso tempo per evitare un nuovo ingente flusso di comunicazioni, il Garante, con proprio provvedimento, ha modificato i modelli per le notificazioni, prevedendo che quanti si adeguano alle disposizioni dal citato d.P.R. n. 318/1999 non debbano appunto, solo per tale ragione, effettuare una nuova notificazione. Per garantire il raggiungimento di tale obiettivo, l'Autorità si è impegnata a dare la massima diffusione di tale provvedimento sulla Gazzetta Ufficiale, sui mezzi di informazione, anche attraverso l'effettuazione di diversi comunicati stampa (v. il provvedimento riportato negli allegati).

Tutte le notificazioni pervenute, dopo una preliminare verifica di congruenza, sono confluite in un elaboratore, collegato in una *lan*, con un *software* che permette la gestione della banca dati. In questa fase sperimentale, il registro viene consultato esclusivamente tramite il personale del Garante. Questo, in base al livello di autorizzazione rilasciato, accede al sistema per effettuare verifiche, predisporre ispezioni e ricerche, nonché per altre finalità legate all'amministrazione del sistema.

In attuazione dell'art. 31 della legge n. 675/1996, il Garante ha adottato una deliberazione per la formale istituzione del registro, pubblicata anch'essa sulla Gazzetta Ufficiale. In tale provvedimento è stato anche regolamentato l'accesso in modo che la consultazione possa essere effettuata senza particolari formalità a oneri di spesa da chiunque vi abbia interesse (art. 13, comma 2, d.P.R. n. 501/1998).

La complessità delle procedure legate alle notificazioni fanno ritenere che il registro generale dei trattamenti possa trovare il definitivo assestamento entro il 2000 consentendo così, superata la fase di sperimentazione e completate le necessarie misure organizzative e di sicurezza, una consultazione più diffusa da parte del cittadino. Ciò in attuazione dell'art. 31, comma 3, della legge, che prevede il raggiungimento di opportune intese con le province e le altre pubbliche amministrazioni, al fine di assicurare la consultazione tramite strumenti informatici costituiti da almeno un terminale dislocato su base provinciale, preferibilmente nell'ambito dell'ufficio per le relazioni con il pubblico (art. 12 d.l.g. 3 febbraio 1993, n. 29 e successive modificazioni ed integrazioni).

Sul fronte delle modalità di compilazione delle notificazioni cartacee o informatiche, la produzione e la distribuzione del supporto informatico non ha ancora raggiunto risultati ottimali, come dimostra il fatto che le notificazioni presentate nella prima fase di applicazione della legge su modello cartaceo sono oltre l'80 per cento del totale.

Una volta completato il quadro normativo in materia di protezione dei dati, si potrà quindi completare la revisione del supporto informatico, aggiornandolo e semplificandone ancor più l'uso anche in relazione ai software più avanzati attualmente disponibili nel mercato. Probabilmente anche per il modello cartaceo sarà opportuno un perfezionamento, anche al fine di rendere possibile un'accelerazione dei tempi per la registrazione dei relativi dati.

Tali aspetti hanno indotto il Garante a prevedere, nel corso dell'anno 2000, una revisione di entrambi i supporti, introducendo elementi di semplificazione in vista di una loro ottimizzazione, pur nel rispetto della normativa europea. Ciò imporrà una valutazione rispetto ai moduli residui già in circolazione e relativamente alla loro distribuzione per via telematica (anche attraverso il sito web del Garante) o attraverso le convenzioni in essere.

3.5 Attività ispettive e applicazione di sanzioni amministrative

Al fine di illustrare l'attività svolta in tale ambito nel corso del 1999, è opportuno ricordare che per consentire al Garante di esercitare le funzioni di controllo e di vigilanza enumerate e descritte nell'articolo 31, la legge n. 675/1996 riconosce all'Autorità un complesso di poteri di accertamento anche di tipo "collaborativo".

3.5.1 Poteri di accertamento

I poteri di tipo "collaborativo" sono rappresentati, in particolare, dalla richiesta di informazioni e di esibizione di documenti (articolo 32, comma 1), nonché dagli accessi alle banche dati, dalle verifiche e dalle ispezioni effettuati con l'assenso scritto ed informato del titolare o del responsabile del trattamento (art. 15, comma 1, d.P.R. n. 501/1998).

Altri accertamenti previsti dall'articolo 32, comma 2, hanno invece una necessaria natura autoritativa e carattere di esecutività. Essi consistono, parimenti, in accessi alle banche dati con ispezioni, verifiche e altre rilevazioni utili al controllo della regolarità dei trattamenti di dati personali.

In via generale, l'accesso permette di entrare in determinati luoghi e uffici e di soffermarvisi anche senza o contro il consenso di chi ne ha la disponibilità, al fine di eseguirvi le operazioni consentite dalla legge. L'articolo 32 delimita il potere di accesso in primo luogo in riferimento alle banche dati ed ai luoghi ove si svolge il trattamento, permettendo però di disporre accessi, ispezioni e verifiche anche in altri luoghi "nei quali occorre effettuare rilevazioni comunque utili" al controllo del rispetto delle disposizioni in materia di trattamento dei dati personali.

Sono, invece, classificabili come *ispezioni* le attività amministrative di ricerca, analisi, osservazione, ricognizione, ecc. che, condotte nell'ambito delle prassi degli uffici pubblici, mirano ad accertare la liceità e la legittimità di una determinata situazione. Per l'Autorità, il contenuto autoritativo ed esecutivo dell'atto si sostanzia nel potere di pretendere dalla parte la visione, diretta consultazione ed eventuale disponibilità della cosa, nonché -in caso di rifiuto, ritardo o, comunque, mancato o inesatto adempimento- di procedere coattivamente alla sua acquisizione eventualmente necessaria.

I soggetti interessati agli accertamenti sono tenuti a norma di legge a farli eseguire (art. 32, comma 4, legge n. 675/1996) e devono anche prestare la collaborazione necessaria per eseguire l'accertamento (art. 15 comma 5, d.P.R. n. 501/1998). L'accertamento è poi eseguito anche in caso di rifiuto e le eventuali spese (ad esempio, per la remunerazione di un fabbro o di un tecnico informatico) sono poste a carico del titolare del trattamento (articolo 15, comma 5, cit.). Devono invece essere considerate a parte le ipotesi nelle quali si rinvercano, all'interno degli uffici, armadi, borse e cassaforti chiusi, pieghi sigillati, ripostigli non accessibili, ecc. In tali casi, per procedere coattivamente all'ispezione, debbono sussistere elementi dai quali desumere che, al loro interno, si trovino elementi utili per la verifica dell'osservanza delle disposizioni in materia di trattamento dei dati personali eventualmente reinvenibili nell'andamento generale.

Il potere di *verifica* consiste invece nell'esecuzione di tutte quelle operazioni che, specie a

seguito dell'acquisizione della disponibilità di una cosa, di un documento, di un registro, ecc. consentono di controllarne la rilevanza ai fini del controllo, l'autenticità, la validità, la regolarità, la conformità alle norme di legge, ecc. Anche la verifica, perciò, presuppone una qualche collaborazione del soggetto verso cui è diretta, oppure l'esercizio del potere di apprensione.

Negli accertamenti del Garante le verifiche vengono effettuate in modo particolare sulla base di un riscontro delle notizie che hanno dato origine all'accertamento sul trattamento, sugli archivi e sulle banche dati, siano esse esibite spontaneamente o acquisite attraverso l'esercizio del potere di ispezione. A tale scopo, è possibile effettuare rilievi, estrarre fotocopie, copiare files e procedere ad altre operazioni tecniche di varia natura.

Con riferimento alla possibile attivazione dalla procedura in esame, questa si sostanzia come ispezione disposta d'ufficio o avviate a seguito di segnalazione, reclamo o ricorso.

Le prime traggono origine da autonome iniziative dell'Autorità finalizzate alla tutela di interessi, di regola, non personalizzati (si vedano, in particolare, i compiti di vigilanza e controllo indicati alle lettere b), f) e p) dell'articolo 31). Sono le ipotesi, ad esempio, degli accertamenti eseguiti *motu proprio* a seguito di notizie apparse su organi di informazione, o di attività di cooperazione internazionale, ovvero, ancora, degli accertamenti avviati per conoscere lo stato di attuazione della normativa in determinati settori pubblici e privati.

Le ispezioni a seguito di segnalazioni, reclami o ricorsi presentati da soggetti esterni sono, invece, finalizzate alla tutela di diritti e interessi più facilmente soggettivizzabili, ai quali fanno maggiormente riferimento, in particolare, i compiti di cui alla lettera d) dell'articolo 31.

La scelta delle procedure da adottare nel caso concreto dipende strettamente dallo specifico fine istituzionale da raggiungere ed è comunque informata ai principi di *proporzionalità, adeguatezza, gradualità*. In linea di massima, i poteri ispettivi del comma 2 sono utilizzati, in qualunque fase del procedimento, quando si ritenga inutile o pregiudizievole (ad esempio, per il pericolo di distruzione degli elementi di prova) attivare taluno degli strumenti di tipo collaborativo. Le ipotesi più frequenti riguardano ad esempio i casi di inottemperanza alle richieste di informazioni e di esibizione di documenti, ovvero le ipotesi di risposte incomplete o ritenute non veritiere fornite all'Ufficio.

Gli accertamenti di tipo autoritativo sono subordinati alla preventiva concessione di un'autorizzazione da parte del presidente del tribunale competente per territorio. Si tratta, come osservato in dottrina, di un atto di partecipazione dell'autorità giudiziaria al procedimento amministrativo che investe la legittimità e non il merito del provvedimento, il quale rimane invece di competenza del Garante anche per quanto riguarda l'eventuale necessità di avvalersi della collaborazione di altri organi dello Stato (art. 32, comma 2, legge n. 675/1996).

3.5.2

Controllo dei
trattamenti e
accertamento
delle violazioni

Le attività ispettive del Garante rientrano nell'ambito di procedimenti amministrativi finalizzati al controllo della liceità e della correttezza dei trattamenti, ai quali si applicano le disposizioni della legge 7 agosto 1990, n. 241, con particolare riferimento alle norme del capo III, in tema di responsabile del procedimento, e del successivo capo IV, in tema di partecipazione al procedimento amministrativo.

L'avvio del controllo può essere preceduto da una fase preistruttoria nel corso della quale l'Ufficio esamina gli elementi disponibili e può acquisirne ulteriori, anche mediante richieste di informazioni o di esibizione di documenti. Nei casi in cui è necessario procedere nei modi di cui all'art. 32, comma 2, il collegio adotta apposita deliberazione sulla base di un'articolata proposta dell'Ufficio, il quale segue i rapporti con la presidenza del tribunale competente per l'autorizzazio-

ne eventualmente necessaria ed esegue il controllo. Si provvede anche alla designazione del personale che effettua il sopralluogo e del responsabile del procedimento amministrativo, nonché al formale avvio del procedimento amministrativo.

All'atto dell'intervento, viene consegnata alla parte una comunicazione anche ai sensi della legge n. 241/1990, mentre notizie del procedimento vengono inviate ai soggetti legittimati ad intervenire.

Può accadere peraltro che nel corso dell'intervento siano constatate le violazioni amministrative previste dall'articolo 39 della legge n. 675/1996 o alcuno degli illeciti penali previsti dai precedenti articoli 34-37.

Per le prime si procede in conformità alle disposizioni della legge 24 novembre 1981, n. 689. In particolare, la violazione viene rilevata in un apposito atto di contestazione al suo autore, nel termine di 90 giorni dall'accertamento (360 per i residenti all'estero). Successivamente, qualora non sia pervenuto il pagamento in misura ridotta, l'Ufficio procede all'inoltro del rapporto all'Autorità per l'emissione dell'ordinanza-ingiunzione. Nei casi di rilevazione di fatti costituenti invece reato, il responsabile degli accertamenti procede con i poteri di polizia giudiziaria, secondo le disposizioni del codice di procedura penale, assicurando le fonti di prova, identificando l'indagato e i testimoni e dando attuazione a quanto necessario affinché il reato non venga portato ad ulteriori conseguenze.

3.6 Codici di deontologia

Per evidenziare l'attività svolta dal Garante in questo ambito, conviene anzitutto ricordare che l'art. 31 della legge n. 675/1996 prevede, fra gli altri compiti ad esso attribuiti, quello di "promuovere, nell'ambito delle categorie interessate e 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". Tale articolo ha recepito pienamente l'art. 27, par. 1, della direttiva 95/46/CE, secondo il quale "gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della presente direttiva, adottate dagli Stati membri".

L'importanza attribuita ai codici di deontologia e di buona condotta sembra doversi ricondurre alla necessità di prevedere strumenti normativi fondati anche su una base autodisciplinare. Si è infatti ritenuto che la tutela dei dati personali potesse ricevere un forte impulso da un complesso di norme applicabili all'insieme dei titolari del trattamento, il cui contenuto fosse determinato dagli stessi operatori di un dato settore o da coloro che esercitano una determinata professione. I codici rappresentano, in qualche modo, una nuova area della strumentazione normativa ed un'innovazione significativa nel sistema delle fonti. La flessibilità che li caratterizza conferisce loro il grande vantaggio di poter essere facilmente modificati: ogni eventuale cambiamento o integrazione non richiede infatti un complesso procedimento normativo di riforma.

Il Gruppo di lavoro per la tutela delle persone fisiche con riguardo al trattamento dei dati personali, di cui all'art. 29 della direttiva, ha elaborato un documento (DG XV D/5020/97) concernente l'autodisciplina settoriale, con particolare riguardo all'incidenza di questa sul livello di tutela dei dati in un determinato Paese. In tale documento viene ribadito che, nella valutazione del contenuto dei codici, bisogna anzitutto accertare che siano compresi i necessari "principi sostanziali" in materia di tutela della riservatezza rispetto al trattamento dei dati personali: quello della qualità e

della proporzionalità dei dati, il principio della trasparenza, il principio della sicurezza, i diritti di accesso, rettifica e opposizione, nonché l'esigenza di una tutela rafforzata per i dati sensibili.

Oltre a quanto appena detto, il contenuto dei codici dovrebbe specificare e adattare, nel particolare settore della categoria interessata, la normativa contenuta nella legislazione generale, sforzandosi di mantenere la massima semplicità espositiva. In particolare, il codice dovrebbe occuparsi degli ambiti settoriali la cui specificità non può essere coperta dalla norma statuale.

Al momento della redazione dei codici, inoltre, si dovrebbe tenere conto dell'omogeneità e della compattezza del soggetto che si pone come rappresentativo degli interessi del settore nella stesura del codice. In tal senso, assume quindi particolare rilievo il problema della rappresentatività di coloro. Laddove esista un ordine o un collegio professionale, tali organismi dovrebbero svolgere un ruolo decisivo nell'adozione del codice, pur restando al Garante il potere di verificarne la conformità alle leggi e ai regolamenti e di contribuire a garantirne la diffusione e il rispetto. Quando, invece, non esistono ordini o collegi professionali, il codice deve essere elaborato pur sempre nell'ambito della categoria maggiormente rappresentativa del settore, ferma restando la possibilità della coesistenza di più codici nel caso in cui non sia possibile raggiungere una posizione unitaria dei diversi interlocutori.

Correlato a quest'ultimo aspetto è quello del generale livello di osservanza dei codici, a sua volta legato al potere dell'associazione od organizzazione di sanzionare gli aderenti che non li rispettano, tenendo anche presente che in alcuni casi, oltre alla rilevanza sul piano interno e quindi di tipo disciplinare, esiste anche una rilevanza esterna che attiene alla liceità del trattamento dei dati. Insieme al potere sanzionatorio, deve però configurarsi anche una forma di sostegno e di assistenza alle persone interessate dal trattamento dei dati da parte dell'organismo rappresentativo del settore, supportata dall'esistenza di mezzi di riparazione adeguati.

La legge n. 675/1996, e in particolare l'art. 31, comma 1, lett. h), pur non delineando organicamente l'iter del procedimento per l'adozione dei codici, prevede che il Garante debba promuoverne la sottoscrizione, nel rispetto del principio di rappresentatività delle categorie interessate, e che debba verificarne la conformità alle leggi e ai regolamenti nonché contribuire a garantirne il rispetto e la diffusione. Tale disposizione generale, di riferimento per tutti i tipi di codici, viene specificata più dettagliatamente per alcune materie in cui la disciplina per la protezione dei dati prevede l'obbligatorietà dei codici deontologici e di buona condotta. E', questo, per esempio, il caso del codice relativo ai dati personali utilizzati per i trattamenti ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato. L'art. 22, comma 4, infatti, prevede che il Garante prescriva le misure e gli accorgimenti a garanzia dell'interessato (che il titolare del trattamento è tenuto ad adottare) e promuova la sottoscrizione di un apposito codice di deontologia e di buona condotta secondo le modalità di cui all'art. 31, comma 1, lettera h).

Merita, invece, un discorso a parte il codice deontologico dei giornalisti, su cui ci si è già ampiamente soffermati nella *Relazione per l'anno 1998* (cfr. § 2.3.2, pag. 38 ss.). Esso è configurato in modo particolare dall'art. 25 della legge n. 675/1996 come modificata nel 1998, prevedendosi, fra l'altro, che debba essere adottato dal Consiglio nazionale dell'ordine dei giornalisti entro sei mesi dall'invito in tal senso formulato dal Garante. Durante la sua elaborazione, il Garante può anche indicare "misure ed accorgimenti a garanzia degli interessati, che il consiglio è tenuto a recepire". In caso di inerzia del Consiglio, il codice è invece adottato in via sostitutiva dal Garante, mentre nell'ipotesi di violazione delle prescrizioni contenute nel codice di deontologia, l'Autorità può vietare il trattamento ai sensi dell'articolo 31, comma 1, lettera l). Si è infine previsto che tale codice deve essere rispettato da chiunque tratti dati personali nei mezzi di informazione, stabilendosi altresì che il Garante ne curi la pubblicazione sulla Gazzetta Ufficiale (per il testo in vigore cfr. il provvedimento 29 luglio 1998, in Gazzetta Ufficiale n. 179 del 3 agosto 1998).

Di recente, infine, il d.lg. 11 maggio 1999, n. 135, quale modificato dal decreto legislativo 30 luglio 1999, n. 282, nonché il d.lg. 30 luglio 1999, n. 281 hanno previsto un ulteriore sviluppo dei codici: si tratta dei codici deontologici e di buona condotta relativi ai dati personali utilizzati per finalità storiche, statistiche, di ricerca scientifica, nonché di quelli utilizzati dagli operatori sanitari.

Una delle caratteristiche più rilevanti di questi ultimi codici attiene al fatto che, qualora si contravvenga alle loro disposizioni, il trattamento diviene illecito perché contrario alla legge n. 675/1996. Il rispetto delle disposizioni contenute nei codici, infatti, costituisce una condizione essenziale per la liceità e la correttezza del trattamento dei dati (art. 6, comma 2, d.lg. n. 281/1999). L'inottemperanza rileva poi sia sul piano disciplinare, sia ai fini della valutazione della colpa in caso di danno (art. 18 legge n. 675/1996). Le disposizioni deontologiche diventano quindi "obbligatorie", con una vera e propria funzione integrativa della legislazione.

Per quanto riguarda in particolare i trattamenti a scopi storici effettuati da archivisti e utenti, il codice di deontologia e di buona condotta deve individuare le regole di correttezza e di non discriminazione nei confronti degli utenti, anche rispetto alla comunicazione e alla diffusione dei dati, nonché le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti i dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando anche i casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati. Esso deve altresì individuare le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a scopi storici, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione (art. 7, comma 5, d.lg. n. 281/1999).

Con riguardo ai trattamenti per scopi statistici e di ricerca scientifica, il d.lg. n. 281/1999 specifica invece il contenuto dei relativi codici, soffermandosi in particolare sulla necessità di individuare i presupposti e i procedimenti diretti al fine di documentare e verificare che i trattamenti siano svolti per idonei ed effettivi scopi statistici e di ricerca scientifica.

Per quanto non previsto dalla legge, i codici devono indicare gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione ed alla diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza, nonché alle modalità per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato.

I codici devono altresì individuare l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare l'interessato, anche in base alle conoscenze acquisite grazie al progresso tecnico; le garanzie da osservare nei casi in cui può prescindere dal consenso dell'interessato; le modalità semplificate per la prestazione del consenso relativamente ai dati sensibili; le regole di correttezza da osservare nella raccolta dei dati; le istruzioni da impartire al personale incaricato; le misure da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'art. 15 della legge n. 675/1996, nonché, infine, l'impegno al rispetto di regole di condotta degli incaricati del trattamento che, in base alla legge, non siano tenuti al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.

I codici deontologici relativi al trattamento di dati personali idonei a rivelare lo stato di salute, effettuato da organismi sanitari ed esercenti le professioni sanitarie, sono previsti dall'art. 17 del d.lg. n. 135/1999, come modificato dall'art. 3 del d.lg. n. 282/1999. Per quanto non previsto dal decreto di cui all'art. 23, comma 1-bis, della legge n. 675/1996, i codici, adottati dalle federazioni nazionali degli ordini e dei collegi delle professioni sanitarie, devono prevedere l'impegno al rispetto di regole di condotta analoghe al segreto professionale da parte degli incaricati del trattamento che non sono tenuti in base alla legge al segreto professionale; devono inoltre prevedere modalità

per rendere noti all'interessato i dati personali idonei a rivelare lo stato di salute, nonché le modalità semplificate per l'informativa e per la prestazione del consenso; devono, infine, identificare i casi di urgenza nei quali l'informativa e il consenso possono intervenire successivamente alla richiesta della prestazione.

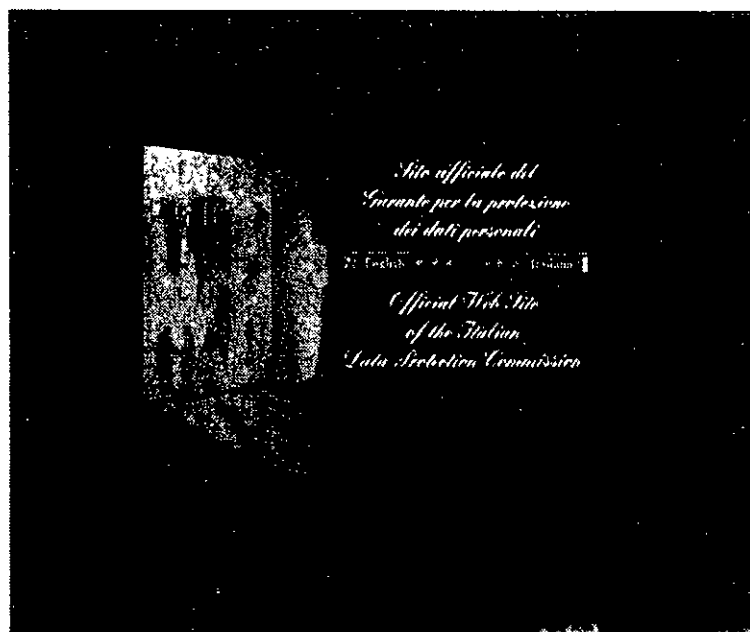
Il Garante, con un provvedimento del 10 febbraio 2000 pubblicato nella Gazzetta Ufficiale n. 46 del 25 febbraio 2000, ha dato avvio alla procedura per la sottoscrizione dei codici nei settori sopra evidenziati, aggiungendo anche il trattamento di dati personali effettuato da istituzioni bancarie e finanziarie in ragione dei diversi profili applicativi emersi e del loro rilievo rispetto alla generalità dei cittadini.

3.7 Informatizzazione e sito web

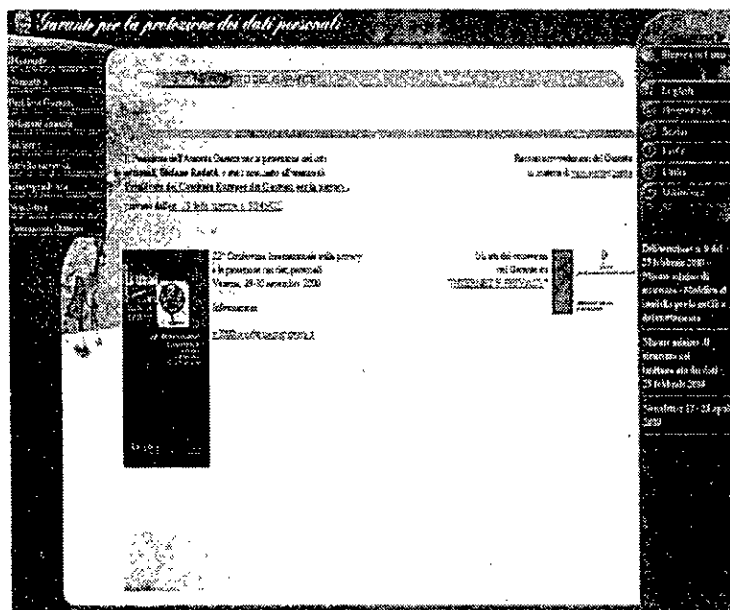
L'Ufficio del Garante, nell'intento di fornire al pubblico un efficiente servizio informativo, ha realizzato un sito Web che ha già attivato in via sperimentale.

L'iniziativa si ispira ad avanzate tecnologie informatiche e di informatica giuridica e mira ad instaurare un moderno e diretto contatto con gli utenti, nonché a coadiuvare questi ultimi e il personale dell'Ufficio nella ricerca e nella documentazione della copiosa documentazione disponibile.

Il sito appare in una veste grafica chiara e utile a rendere comprensibile l'organizzazione dei contenuti in sezioni dedicate. La pagina iniziale prevede la scelta della lingua (italiano ed inglese) attraverso la quale accedere in navigazione alle sezioni principali.



Successivamente al visitatore appare una pagina che verrà suddivisa in almeno quattro aree principali.



Nella parte sinistra figureranno le "sezioni" in cui verrà suddiviso il sito, a loro volta articolate in sottosezioni da curare in costante aggiornamento.

Nella parte destra superiore verranno inseriti collegamenti alle sezioni di utilità in particolare alle "F.A.Q." in continua implementazione, che prendendo le mosse dall'esperienza maturata dal servizio di assistenza telefonica quotidianamente operante in Ufficio, raccoglieranno le domande e le risposte più frequenti. La sezione sarà poi arricchita con collegamenti ipertestuali interni di rimando alla normativa ed ai provvedimenti citati. A completamento del sito, al fine di rendere l'Autorità parte di una rete globale, trova posto la sezione "Links" di collegamento agli altri siti web di altre autorità e di organismi internazionali e comunitari.

La parte inferiore è dedicata alla segnalazione delle notizie della "Ultima ora".

Nella parte centrale della pagina di navigazione appaiono i collegamenti a sezioni e argomenti di particolare rilevanza od attualità. La medesima area è utilizzata, nella navigazione successiva, per la visualizzazione dei contenuti.

Il sito, in via di completamento, proporrà le sottoelencate "sezioni":

<i>Il Garante</i>	Si indica la composizione dell'Autorità, una breve presentazione ed i suoi compiti istituzionali; il codice etico e gli atti costitutivi dell'Ufficio.		
<i>Normativa</i>	Rappresenta la raccolta dei principali testi normativi italiani relativi al trattamento dei dati. È prevista la realizzazione di un archivio storico che consentirà di conoscere le integrazioni normative dei testi con i relativi provvedimenti di modifica. Viene dato poi spazio all'attività legislativa comunitaria riportando alcuni atti e documenti relativi a:		
	<i>Unione europea</i>	<i>Consiglio d'Europa</i>	<i>OCSE</i>
	<i>Trattati e convenzioni</i>	<i>Europol</i>	<i>Schengen</i>
<i>Decisioni Garante</i>	Si riportano, nel testo integrale, i principali provvedimenti emanati dal Garante, suddivisi per anno o per materia, rendendo così agevole la ricerca anche in navigazione diretta. Le sottosezioni sono:		
	<i>Ricorsi</i>	<i>Segnalazioni e reclami</i>	<i>Pareri</i>
	<i>Autorizzazioni generali</i>	<i>Risposte e quesiti</i>	<i>Altri provvedimenti</i>

<i>Relazioni annuali</i>	La sezione ospita i testi delle relazioni presentate al Parlamento.
<i>Iniziative</i>	Sezione creata con l'intento di annunciare e diffondere le più importanti iniziative cui partecipa il Garante. In "Iniziative" è già attiva una sottosezione relativa a "Convegni e Seminari" che reca anche i lavori del Convegno "Internet e privacy: quali regole?".
<i>Attività Internazionale</i>	Verranno diffuse notizie ed informazioni in ordine ad alcune attività in corso a livello comunitario o sul piano internazionale.
<i>Giurisprudenza</i>	Dedicata alla raccolta della giurisprudenza civile, penale, amministrativa e comunitaria, relativa a questioni connesse con la tutela del trattamento dei dati personali.
<i>Newsletter</i>	È la rappresentazione telematica della rivista settimanale del Garante. La Newsletter illustra, con un taglio divulgativo, i provvedimenti dell'Autorità, dà informazioni sulla sua attività e sulle sue iniziative, ospita approfondimenti e contributi anche stranieri relativi alla protezione dei dati.
<i>Comunicati stampa</i>	Creata per raccogliere, suddivisi per anno, i comunicati diffusi dall'Autorità.
<i>Modulistica</i>	Sezione creata per venire incontro alle esigenze degli utenti di reperire la modulistica ufficiale, le notizie e le istruzioni in particolare per la compilazione del modello di notificazione. Ospiterà una sottosezione che permetterà il download del software predisposto dal Garante per la notifica in formato elettronico.

Tutta la documentazione presente nel sito verrà opportunamente correlata attraverso collegamenti che formano un rete di sinapsi ipertestuali per una agevole consultazione.

Dopo la prima sperimentazione del sito, i collegamenti saranno arricchiti con specifiche funzioni che consentiranno all'utente di navigare tra i provvedimenti, percorrendo l'evoluzione temporale del principio giuridico espresso, sia esso sostanziale o procedurale.

La reperibilità dei documenti è garantita da un'apposita interfaccia che permetterà di effettuare ricerche per:

- parole testuali, con l'ausilio di un *thesaurus*
- tipologia del provvedimento
- intervalli di data
- schema di classificazione - specificatamente realizzato - sulle tematiche della protezione dei dati personali.

A partire dal risultato della ricerca sarà possibile visualizzare in modo ordinato, i testi normativi che hanno dato origine ai provvedimenti, verificare se il principio di diritto espresso ha avuto evoluzioni od altre applicazioni in fattispecie simili, correlate attraverso lo schema di classificazione, raggiungere eventuali approfondimenti nelle "Newsletter", leggere il relativo comunicato stampa.

3.8 Attività di documentazione

Come già anticipato nella *Relazione per l'anno 1998* (pag. 117), la natura per molti aspetti interdisciplinare dell'attività del Garante rende necessario uno sviluppo qualitativo e quantitativo delle iniziative di documentazione del vasto materiale di diretto interesse dell'Autorità. Un apposito servizio studi e documentazione curerà pertanto questa significativa attività di supporto già avviata nell'Ufficio, e che già costituisce una significativa base di documentazione per i compiti attualmente svolti.

Il rafforzamento del servizio avrà la duplice finalità di fornire servizi interni di supporto al funzionamento dell'Autorità e di porsi come interfaccia con la più vasta platea di cittadini ed operatori interessati a conoscere e approfondire i temi collegati con la *privacy*.

Per quanto riguarda l'aspetto interno, si effettuerà un monitoraggio costante delle principali fonti di informazione alla ricerca di avvenimenti, osservazioni, proposte, segnalazioni e denunce relativi al tema della riservatezza e degli altri diritti fondamentali della persona, potenziando le analisi già in corso rispetto ai principali quotidiani nazionali ed esteri, a riviste tecniche e scientifiche, a siti Internet, agenzie di stampa e programmi radio-televisivi.

In riferimento alle reti telematiche, saranno attentamente consultati siti istituzionali italiani e stranieri, delle autorità garanti di altri Paesi, delle principali organizzazioni ed associazioni per la difesa di diritti e libertà civili, dei principali operatori in ambito informatico e telematico, nonché altri siti che comunque si interessano ai vari aspetti relativi alla *privacy*. Saranno seguiti anche i gruppi più rappresentativi di discussione e liste che trattano problemi tecnici collegati con lo sviluppo delle tecnologie.

Uno dei risultati di questa attività di monitoraggio sarà la redazione di rapporti monografici su argomenti esplicitamente richiesti all'interno dell'Ufficio, anche da funzionari ai fini dello svolgimento di attività istituzionali (formulazione di proposte o pareri, partecipazione a convegni o ad attività esterne), oppure finalizzati a richiamare l'attenzione dell'Ufficio stesso su tematiche emergenti, soprattutto come conseguenza dell'evoluzione tecnologica.

Per quanto riguarda la proiezione esterna di tale attività, essa potrà concretizzarsi anche nella fornitura di materiale documentale e di indicazioni bibliografiche soprattutto a ricercatori, studiosi, dottorandi e laureandi, interessati ad approfondire le tematiche rientranti nel variegato tema della protezione dei dati personali (aspetto, questo già avviato in risposta a qualificate richieste esterne di documentazione). La base documentale formata nei primi tre anni di attività dell'Ufficio, insieme ai documenti in materia di *privacy* in fase di organizzazione e classificazione, saranno infine resi di dominio pubblico anche attraverso il sito web del Garante.

L'intera attività, compresa quella descritta nel successivo paragrafo, sarà anche rivolta ad una costante informazione delle amministrazioni pubbliche, del settore privato e dell'opinione pubblica sui problemi legati agli sviluppi delle tecnologie dell'informazione e della comunicazione.

L'attività propria di un servizio studi e documentazione riceverà il necessario potenziamento con l'agibilità della nuova sede dell'Ufficio di Piazza Monte Citorio, nella quale locali adeguati verranno attrezzati per supportare una attrezzata biblioteca e una emeroteca (v. paragrafo 3.8.1), dotate di postazioni Internet, nonché di altri strumenti informatici e telematici necessari per l'attività di ricerca.

L'approccio multidisciplinare costituirà la base di un progetto che si vuole aperto e dialogante con le altre istituzioni e gli istituti di ricerca italiani e stranieri.

3.8.1
Servizio
studi e
documen-
tazione

Un comitato scientifico composto da eminenti personalità provenienti soprattutto dal mondo accademico, sulla scorta dell'esperienza di altre autorità, potrà offrire un valido contributo per individuare i temi ed i problemi con i quali l'Ufficio sarà chiamato a confrontarsi negli anni a venire, segnatamente in ragione del continuo evolversi degli scenari giuridici e culturali della Società dell'Informazione.

Il servizio si articolerà nelle aree delle risorse informative (anche in riferimento alla gestione della biblioteca e delle sue infrastrutture), della ricerca e della produzione editoriale.

La biblioteca raccoglierà testi ordinariamente utilizzati e specialistici; comprenderà una sala di lettura con postazioni multimediali aperta anche ad un pubblico selezionato di ricercatori interessati a svolgere ricerche sulla *privacy*. Sarà previsto l'accesso alle principali base dati pubbliche e private, italiane e straniere, così da consentire l'utilizzo di un insieme di servizi in rete ad alto valore aggiunto (il catalogo completo della biblioteca verrà reso disponibile sul sito web del Garante).

Nella cooperazione con l'esterno per il reperimento di testi e documenti, verrà prestata attenzione ai collegamenti esterni attraverso la creazione di contatti con altre biblioteche pubbliche e private, con istituzioni italiane e straniere e con autorità di garanzia di altri Paesi.

La ricerca organizzerà settori di produzione informativa interna:

- base dati delle rassegne stampa italiane e straniere, con l'analisi e la classificazione del materiale schedato e indicizzato nelle rassegne stampa diffuse quotidianamente sulla rete interna del Garante;
 - preparazione di raccolte mirate di articoli e di altro materiale documentale (selezioni tematiche e schede bibliografiche);
 - report periodici sugli aggiornamenti tecnologici nei settori di interesse del Garante;
 - raccolta del materiale normativo e bibliografico necessario per gli strumenti di aggiornamento quali il Notiziario mensile;
 - dossier di studio tematici e monografie relativi a materie o ambiti di interesse del Garante;
- § ricerche in campi nei quali è più carente l'elaborazione dottrinale e scientifica, anche in collaborazione con istituzioni di ricerca italiane e straniere.

L'area editoriale organizzerà la produzione informativa esterna. Verrà curato l'iter di pubblicazione degli atti di convegni e seminari del Garante e di eventuali altre iniziative, nonché quello di Quaderni periodici dell'Autorità aperti a collaboratori esterni. La loro finalità è quella di raccogliere contributi di provenienza diversa su singoli temi in modo da evidenziare il rapporto complesso e anche controverso tra le nuove strutture della società dell'informazione e la *privacy*.

3.9 Personale, regolamento e gestione risorse umane

3.9.1
Il d.lg.
n. 51/1999

Con il d.lg. 26 febbraio 1999, n. 51, sono state introdotte disposizioni integrative e correttive della legge n. 675/1996 che incidono significativamente sul funzionamento dell'Ufficio del Garante.

Il provvedimento, ampiamente illustrato con la precedente relazione annuale, nelle sue linee essenziali persegue l'obiettivo di dotare l'Ufficio dei mezzi e delle risorse umane indispensa-

bili per lo svolgimento dei propri compiti, attribuendo al Garante la connessa autonomia organizzativa.

In attuazione dei criteri direttivi previsti dalla legge 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"*), il decreto ha istituito il ruolo organico del Garante nel limite di cento unità, demandando ad uno o più regolamenti dell'Autorità la definizione dell'ordinamento delle carriere, delle modalità di inquadramento in ruolo del personale in servizio e del reclutamento del restante personale, nonché del trattamento giuridico ed economico.

Per quest'ultimo aspetto, il provvedimento attribuisce al personale dipendente del Garante un trattamento economico provvisorio pari all'80% di quello attribuito al personale dell'Autorità per le garanzie nelle comunicazioni, "nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti" (art. 33, comma 1-bis, l. n. 675/1996, introdotto dal d.lg. n. 51). Il decreto disciplina inoltre il periodo transitorio compreso tra la data di avvio dell'attività dell'Ufficio (8 maggio 1997) e quella di entrata in vigore del regolamento con il quale sono state previste le modalità di inquadramento in ruolo. Nel predetto periodo, al personale in servizio è attribuita una indennità di funzione nella misura del 50% della retribuzione in godimento, con esclusione dell'indennità integrativa speciale. Dal 1° gennaio 1998, e sino alla data di entrata in vigore del menzionato regolamento è stata altresì prevista la corresponsione al personale della differenza tra la retribuzione già in godimento, maggiorata dell'indennità di funzione, e il nuovo trattamento economico, quale sarà definito dal citato regolamento sul trattamento giuridico ed economico del personale.

Per la completa funzionalità dell'Ufficio, il provvedimento prevede poi l'applicabilità di istituti già presenti nell'ordinamento delle altre autorità indipendenti, sia pure in limiti numerici assai più contenuti: il collocamento fuori ruolo e i contratti a tempo determinato.

Il ricorso al primo istituto è ammesso per un numero non superiore a venti unità e per non oltre il 20% delle qualifiche dirigenziali. Inoltre, l'utilizzazione di personale a tale titolo comporta che un corrispondente numero di posti rimanga vacante nel ruolo organico. Per ciò che concerne invece i contratti a tempo determinato, si prevede che complessivamente non possano superare il limite di venti, ivi compresi anche i consulenti eventualmente assunti con tale forma contrattuale.

Nel complesso, quindi, il provvedimento appronta un insieme articolato di strumenti finalizzati al rafforzamento dell'Ufficio, che tiene conto delle esigenze di flessibilità e della necessità di giovare di professionalità e competenze provenienti dalle amministrazioni pubbliche come dall'impiego privato. Il provvedimento rimuove anche un ostacolo allo svolgimento dell'attività ispettiva, attribuendo la qualifica di agenti e ufficiali di polizia giudiziaria a non più di cinque unità di personale del Garante. Assume particolare rilievo, infine, la disposizione che, al pari di altre autorità indipendenti, prevede l'applicabilità all'Ufficio del Garante dei principi concernenti l'individuazione e le funzioni del responsabile del procedimento (legge n. 241/1990) e la separazione tra funzioni di governo e di gestione (d.lg. n. 29/1993).

Il d.lg. n. 51 ha delineato uno stabile assetto organizzativo e funzionale dell'Ufficio ed ha posto le premesse per una più incisiva azione istituzionale del Garante, sin qui limitata dall'insufficienza di mezzi e risorse. Tale decreto potrà dispiegare i suoi effetti positivi a partire dall'ormai imminente approvazione dei tre regolamenti con i quali saranno definiti l'organizzazione interna, il trattamento giuridico ed economico del personale e la gestione della contabilità e delle spese.

Nelle more dell'adozione di tali atti - quali costituiscono anche il presupposto per l'inqua-

3.9.2
La gestione
delle risorse
umane

drammento in ruolo del personale in servizio e per la copertura dei posti vacanti nel ruolo: l'Ufficio ha completato l'originario contingente di 45 unità, composto da dipendenti dello Stato o di altre amministrazioni ed enti pubblici in posizione di comando o fuori ruolo, rafforzando vari settori legati alle esigenze più immediate dell'Ufficio, i servizi strumentali e il settore informatico, impegnato nell'attuazione del sistema informativo dell'Ufficio e nell'allestimento del sito web. Sul profilo del collocamento fuori ruolo è stato richiesto anche un parere al Consiglio di Stato.

Un'apposita commissione preposta dal Garante con deliberazione del 25 febbraio 1999 ha contribuito ad individuare alcune figure e profili professionali. Essa ha infatti esaminato i numerosi *curricula* pervenuti sino al 30 aprile 1999 e, sulla base di specifici criteri di selezione e di diversi colloqui, ha potuto individuare alcune figure professionali e alcuni aspiranti ritenuti idonei nel breve periodo a soddisfare le più immediate esigenze di sviluppo organizzativo dell'Ufficio.

Nel corso del 1999 e nei primi mesi di quest'anno sono proseguiti i complessi approfondimenti legati all'elaborazione dei citati regolamenti interni, giunti ormai alla fase di approvazione definitiva sulla base di vari contributi per i quali l'Autorità si è avvalso anche delle proposte di esperti designati.

Parallelamente a tali attività, è stata data attuazione a due provvedimenti deliberati alla fine del 1998: l'uno concernente l'istituzione del fondo di incentivazione dell'Ufficio e, l'altro, la formazione professionale.

Il primo provvedimento, perfezionato in seguito al parere del Consiglio di Stato proposto dall'Ufficio, è stato attuato sul finire del 1999. Nel parere, il Consiglio di Stato, nel pronunciarsi sui criteri di determinazione del fondo di incentivazione, ha condiviso la tesi prospettata circa l'impossibilità di applicare meccanicamente all'Autorità la normativa contrattuale vigente nei comparti di provenienza del personale in servizio, ed ha convenuto sull'esigenza di applicare alcuni dei criteri desumibili da tale normativa, sia pure con le opportune integrazioni.

L'attuazione del fondo ha consentito di introdurre nel trattamento economico del personale un emolumento legato al risultato dell'attività lavorativa e al conseguimento di obiettivi previamente individuati.

La corresponsione degli incentivi è stata preceduta dalla valutazione, attribuita al segretario generale del Garante, con il concorso di un "nucleo di valutazione" formato da tre funzionari, sul grado di raggiungimento degli obiettivi e sullo stato di attuazione delle attività progettuali, individuate con una deliberazione adottata il 30 dicembre 1998.

La sperimentazione di forme di retribuzione di risultato ha creato le condizioni per una contestuale, ulteriore riduzione delle prestazioni di lavoro straordinario, le quali appaiono in linea con i limiti fissati da altre autorità indipendenti.

A sua volta, la riduzione dei trattamenti accessori legati alla durata della prestazione lavorativa a vantaggio di quelli finalizzati agli obiettivi ha consentito, a decorrere dall'esercizio finanziario 1998, un significativo trasferimento di risorse finanziarie da una voce all'altra.

Al di là di questi aspetti, la sperimentazione di un sistema premiante e la prima esperienza di un "nucleo di valutazione" hanno offerto validi spunti di riflessione e di approfondimento che si riveleranno proficui per la costruzione del sistema di valutazione dell'Ufficio, demandata al regolamento sul trattamento giuridico ed economico del personale.

Più in generale, la sperimentazione avviata è rivolta a creare una cultura del risultato; elemento, questo, cui dovrà sempre più ispirarsi l'attività dell'Ufficio.

Il secondo provvedimento, concernente la formazione professionale, rappresenta la traduzione pratica di una visione non tradizionale della formazione e dell'aggiornamento professionale cui il Garante annette grande importanza.

Con il predetto provvedimento sono stati infatti introdotti a livello sperimentale i "bonus formativi", i quali lasciano al personale ampia libertà di scelta sull'attività formativa da seguire, nell'ambito delle priorità definite dall'Ufficio e di un budget individuale previamente stabilito (per il 1999, ammontante a £. 3.000.000).

Per il 1999, l'Ufficio ha individuato come prioritarie la conoscenza e l'approfondimento delle lingue maggiormente utilizzate nell'ordinaria attività di ufficio e l'aggiornamento in materie di interesse per l'Autorità.

Accanto alle iniziative di formazione direttamente programmate dall'Ufficio sulla base delle proprie irrinunciabili esigenze funzionali e organizzative, è stato quindi sperimentato con successo un altro "canale formativo" che vede il personale come protagonista della propria formazione.

L'Autorità si avvale di un contingente di personale di 45 unità, poste in posizione di comando o fuori ruolo. Il personale con qualifica direttiva, ricompreso tra la VII e la IX qualifica funzionale, o dirigenziale rappresenta l'80% del totale (percentuale immutata rispetto al precedente anno).

3.9.3
Il personale

Nel corso dell'anno, l'Autorità si è avvalsa, altresì, dell'opera di 13 consulenti, uno dei quali ha iniziato a collaborare alla fine del 1999.

Il ricorso a tali consulenze si è reso necessario per far fronte ad esigenze contingenti (reperimento di una nuova sede; complessa ristrutturazione dei locali da adibire a sede dell'Ufficio) o per lo svolgimento di compiti di natura tecnica (quali la creazione dello schema di classificazione dei documenti e la razionale organizzazione dell'archivio dell'Ufficio). Alcuni rapporti di consulenza instaurati rispondono, invece, alla finalità di acquisire competenze e professionalità nel campo amministrativo e giuridico. Il Garante si è, inoltre, giovato della consulenza di qualificati esperti per la predisposizione dei regolamenti concernenti il trattamento giuridico ed economico del personale, l'organizzazione ed il funzionamento dell'Ufficio nonché la gestione delle spese.

Per le caratteristiche segnalate in precedenza, un certo numero di consulenze si esaurirà tra breve o si è già esaurito nel corso del 1999. Al 31 dicembre 1999, le consulenze in atto erano 10.

Tavola 1 - Contingente di personale attualmente in servizio e rapporti di consulenza

Qualifica	Comando	Fuori ruolo	Consulenti nel 1999
Dirigenti generali o equiparati		1	
Dirigenti o equiparati		7	
IX qualifica funzionale	1	4	
VIII qualifica funzionale		10	
VII qualifica funzionale	1	9	
VI qualifica funzionale	1	4	
V qualifica funzionale		5	
IV qualifica funzionale		1	
III qualifica funzionale		1	
Totale	3	42	13

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.

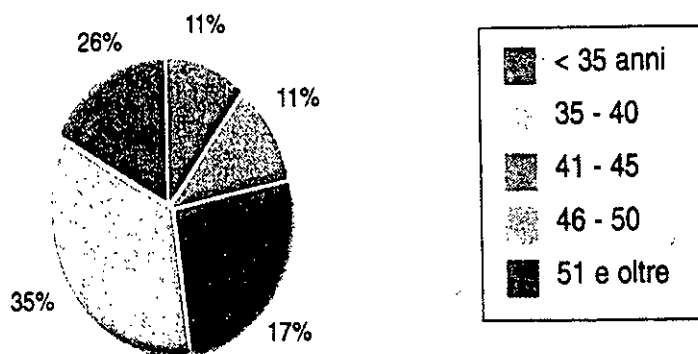
Quanto alla formazione, 31 unità su 45 sono in possesso della laurea, tredici di un diploma di scuola media superiore ed uno della licenza media.

Tavola 2 - Personale per tipo di formazione ed esperienza lavorativa precedente

Esperienze precedenti	Laurea	Diploma scuola	Licenza media	Totale
Pubblica amm.ne	29	13	1	42
Magistratura amministrativa ordinaria, contabile	2			3
Totale	31	13	1	45

Dall'analisi per classi di età, emerge che il sessanta per cento si colloca nelle fasce centrali di età (comprese tra 30 e 40 anni) e che un quarto del personale non supera i 35 anni, mentre solo 10 unità si collocano oltre i 45 anni di età. L'età media non supera i 40 anni.

Classi di età



3.10 Dati sulle principali attività del garante

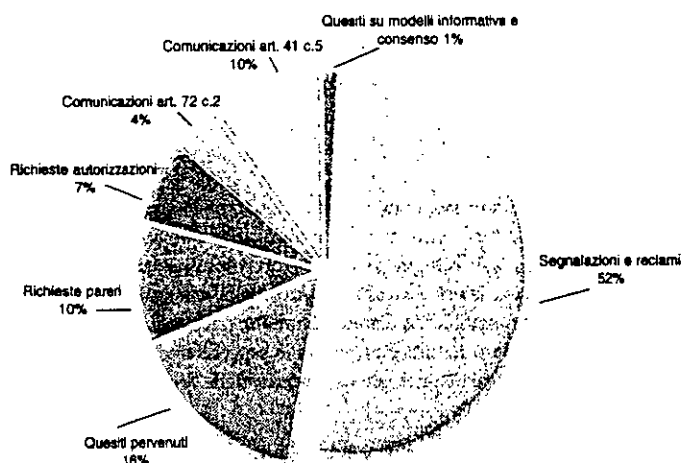
Richieste di informazione e quesiti telefonici	12.000
Segnalazioni e reclami pervenuti	1.946
Quesiti pervenuti	615
Richieste di parere pervenute	386
Richieste di autorizzazione pervenute	272

Notificazioni dei trattamenti previste dagli articoli 7, 16 e 28	270.000
Comunicazioni previste dall'art. 27, comma 2	157
Comunicazioni in tema di dati sensibili e giudiziari previste dall'art. 41, comma 5	366
Autorizzazioni al trattamento dei dati sensibili (art. 22) rilasciate per categorie di titolari e di trattamenti (art. 41, comma 7)	7
Autorizzazioni rilasciate a singoli destinatari	3
Risposte a richieste di autorizzazione (art. 22)	11
Risposte a segnalazioni	130
Risposte a quesiti	89
Risposte a richieste di parere	26
Pareri rilasciati in base all'art. 31, comma 2	27
Segnalazioni del Garante	66
Richieste di informazioni ai sensi dell'art. 32	24
Procedimenti contenziosi definiti sulla base di ricorsi (art. 29)	124
Risposte ad interrogazioni parlamentari	6
Modelli di informativa e consenso	52
Comunicati stampa e dichiarazioni alla stampa	159
Notiziari settimanali pubblicati dall'Ufficio Stampa (istituiti l' 8 marzo)	36

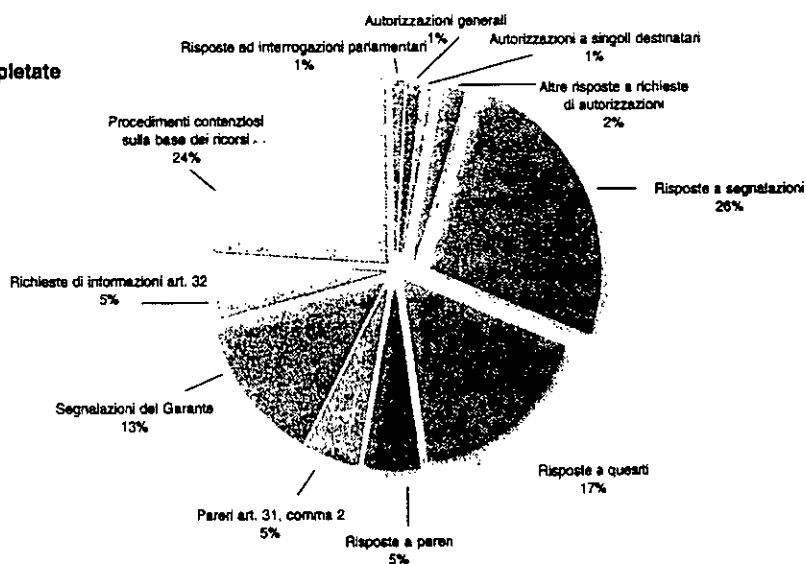
RICORSI

Pervenuti	150	di cui	decisi 124 in istruttoria 12 in fase di regolarizzazione 14
Tipo di decisione adottata: totale	124	di cui	non luogo a provvedere (composizionetra le parti durante il procedimento) 53 manifestamente infondato 6 infondato 4 inammissibile 42 accoglimento 19

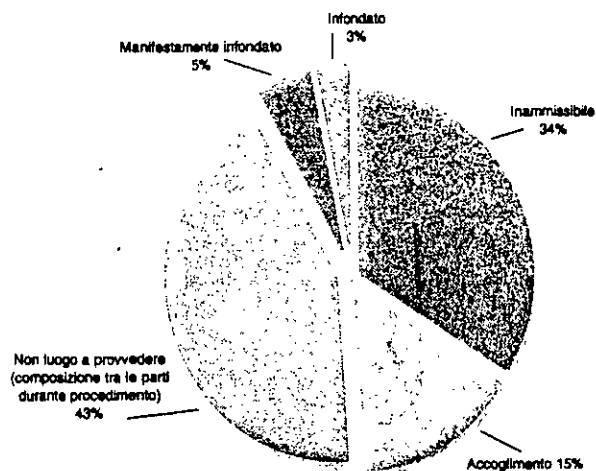
Atti e provvedimenti richiesti
(esclusa assistenza telefonica e notificazione)



Attività espletate



Statistica
dei ricorsi esaminati



3.11 Indagine conoscitiva sulle autorità indipendenti

Il 19 gennaio 1999 la Commissione affari costituzionali della Camera ha deliberato un'indagine conoscitiva sulle autorità indipendenti, volta ad acquisire elementi di conoscenza sul loro attuale *status* al fine di favorire, sulla base dei denominatori comuni eventualmente riscontrati, la predisposizione di una disciplina legislativa unitaria, pur nella salvaguardia della pluralità dei modelli e della specificità delle funzioni. L'indagine ha mirato, pertanto, ad una razionalizzazione delle autorità con riguardo alla loro natura giuridica, alle procedure di nomina dei componenti, all'inquadramento del loro potere regolamentare nel sistema delle fonti e al regime professionale del personale.

Dal marzo 1999 sino al gennaio scorso si è proceduto alle audizioni dei professori Sabino Cassese, Alberto Predieri e Antonio D'Atena, del prof. Enzo Cheli, presidente dell'Autorità per le garanzie nelle comunicazioni, del prof. Stefano Rodotà, presidente del Garante per la protezione dei dati personali, del prof. Giuseppe Tesouro, presidente dell'Autorità garante della concorrenza e del mercato, del prof. Paolo Tesouro e del Comitato dei consumatori *Altroconsumo*.

Nel suo intervento il Presidente del Garante, nel rimarcare che il ricorso all'istituzione di tali autorità si inserisce in una dinamica di redistribuzione di poteri all'interno del nostro sistema politico-istituzionale, ha sottolineato l'importanza di individuare le autorità che si potrebbero definire "necessarie" o alle quali siano attribuite funzioni di garanzia rivolte all'intera comunità.

Fra queste si colloca certamente il Garante per la protezione dei dati personali in quanto esso, da un lato, nasce quale adempimento di un obbligo comunitario - essendo la sua istituzione prevista dalla direttiva europea n. 95/46/CE - e, dall'altro, ha una vocazione istituzionale non settoriale, ma d'ordine generale, finalizzata alla tutela di diritti fondamentali della persona, come confermato dall'attribuzione delle controversie che riguardano l'applicazione della legge n. 675 all'autorità giudiziaria ordinaria.

Quanto poi, all'esigenza - fortemente avvertita - di individuare le corrette linee di raccordo ordinamentale di tali autorità con gli altri organi dello Stato, il Presidente ha sottolineato che le autorità indipendenti, per loro natura in posizione di indipendenza dall'esecutivo, sono tutt'altro che sciolte da forme di controllo, ove si considerino quella sui loro atti, demandata alle varie magistrature (ordinaria o amministrativa, Corte dei conti), quella dell'opinione pubblica e in particolare degli interessati alle attività delle autorità, e quella dello stesso Parlamento, attraverso un'attenta analisi delle relazioni annuali presentate e un più consistente ricorso ad udienze conoscitive.

La Commissione ha approvato un documento conclusivo nella seduta del 4 aprile 2000.

4. Quali prospettive per l'anno 2000

Il quadro sin qui delineato dello stato di attuazione della legge n. 675/1996 e dell'attività svolta dal Garante offre lo spunto per individuare alcune tematiche ed obiettivi sui quali l'Autorità potrà soffermarsi con particolare attenzione nel corrente anno.

Un primo contesto particolarmente significativo riguarda il completamento del quadro normativo italiano in materia di protezione dei dati. A parte singole iniziative normative all'esame delle Camere, l'auspicabile rinnovo della delega già contenuta nelle leggi-delega nn. 676/1996 e 344/1998 permetterebbe infatti al Governo di portare a termine l'armonizzazione della disciplina interna sul trattamento delle informazioni di carattere personale e di completare il recepimento della direttiva n. 95/46/CE.

In termini generali, i decreti delegati restano uno strumento utile per introdurre disposizioni integrative ed eventualmente correttive della legge n. 675/1996, la cui elaborazione risulta essere obiettivamente complessa anche perché destinata ad inserirsi nella disciplina settoriale in contesti assai diversificati tra loro.

Nonostante i nove decreti legislativi sin qui adottati, vi sono ancora diverse aree la cui normativa non è ancora completa e resta necessaria: basti pensare ai settori del direct marketing, del lavoro e della previdenza sociale, nonché del mondo assicurativo e bancario.

Particolarmente significativa appare poi l'integrazione normativa della legge n. 675/1996 in riferimento ai particolari settori pubblici ai quali la legge stessa è oggi applicabile solo in parte (in particolare, trattamenti di dati per ragioni di giustizia e di sicurezza pubblica), nonché in relazione al complesso fenomeno delle reti telematiche per le quali dovrà trovarsi un punto di equilibrio che permetta di combinare al meglio le varie fonti e strumenti disponibili (norme giuridiche, codici deontologici e di buona condotta, contratti, "tecnologie pulite"), tenendo conto anche del contesto mondiale.

L'Autorità resta fiduciosa della possibilità di vedere positivamente arricchita la disciplina di queste materie, grazie anche all'impulso che potranno continuare a dare le competenti commissioni parlamentari investite del parere sugli schemi di decreto. Resta quindi disponibile per offrire i propri contributi di esperienza e di studio anche comparato sulle singole materie affrontate.

Questa attività normativa dovrebbe auspicabilmente svilupparsi, almeno in larga parte, nella seconda metà del corrente anno, sebbene la scadenza del nuovo termine di delega sia prevista per il marzo del 2001.

Essenziale potrà rivelarsi poi la condivisibile previsione di un testo unico delle norme sulla protezione dei dati personali — di cui si parla nel disegno di legge all'esame del Senato —, che (grazie anche alle norme correttive e di coordinamento che potrebbero accompagnarlo, la cui laboriosa enucleazione potrebbe essere avviata di pari passo con l'attività normativa delegata) permetterà di offrire agli operatori uno strumento senz'altro più agevole di lavoro e di chiarimento sugli innumerevoli nodi in precedenza affrontati.

L'articolata attività normativa alla quale si è accennato potrà rivelarsi utile anche per un secondo obiettivo che si era riproposto lo stesso legislatore del 1996: quello di sviluppare e adattare nei singoli settori norme generali quali quelle contenute nella legge n. 675, redatte per essere applicabili ad innumerevoli contesti nei quali, però, la dialettica degli interessi contrapposti sia pubblici, sia privati determina a volte incertezze, dubbi applicativi più o meno fondati, inerzie e aspettative insoddisfatte.

In questa prospettiva, il Garante si riserva anche di segnalare alcuni interventi normativi che potrebbero rivelarsi più urgenti, quale quello in materia di video-sorveglianza, la quale, come si è già osservato, ha assunto ormai dimensioni particolarmente significative che appaiono rendere opportuna una riflessione più immediata del legislatore.

Il completamento dell'assetto normativo in materia di protezione dei dati non si svilupperà, peraltro, solo sul piano legislativo ed eventualmente regolamentare (si pensi, a tale proposito, all'ultima da parte delle pubbliche amministrazioni del procedimento di adozione delle fonti secondarie in materia di trattamento dei dati sensibili e di carattere giudiziario ai sensi del d.lg. n. 135/1999).

L'anno 2000 si presenta infatti come significativo anche per l'introduzione di ulteriori fonti di disciplina della materia, basate sui codici di deontologia e di buona condotta e su specifici provvedimenti autorizzatori.

Sotto il primo profilo, durante l'anno dovrebbe essere portato a definizione il procedimento per l'adozione e la pubblicazione dei codici già promossi dal Garante con la citata, recente deliberazione, e che riguardano, come si è detto, i settori della statistica, della ricerca scientifica e storica, la sanità, l'investigazione privata e il trattamento di dati per finalità di indagine difensiva o di difesa di un diritto in sede giudiziaria, le attività bancarie e finanziarie. Questa complessa attività, che vedrà direttamente impegnate le categorie interessate in cooperazione con l'Autorità, si articolerà subito dopo nell'impulso per l'adozione di altri codici in diversi codici, con particolare riguardo alle informazioni commerciali, alle reti telematiche, al direct marketing e all'attività assicurativa.

Anche questo secondo flusso di disposizioni potrà rivelarsi quindi utile — come è avvenuto già per l'attività giornalistica — per migliorare il livello di garanzie e il grado di effettività della disciplina sul trattamento dei dati.

Analogo contributo potrà derivare anche dall'apposita autorizzazione del Garante prevista riguardo al trattamento dei dati genetici, ovvero su un tema (attualmente regolato già da alcune prescrizioni contenute nell'autorizzazione generale n. 2/1999 sui dati idonei a rivelare lo stato di salute e la vita sessuale) sul quale la più recente cronaca anche a livello internazionale denota delicate implicazioni ed esigenze di bilanciamenti tra diritti, specie per evitare improprie utilizzazioni dei dati e per prevenire rischi di discriminazione degli interessati.

Un ultimo contesto che richiederà particolare attenzione nel corso del corrente anno riguarda il grado di effettiva applicazione della legge n. 675/1996 e la sfera dei controlli che il Garante ritiene doveroso intensificare dopo le integrazioni apportate in materia dal d.P.R. n. 501/1998 e dal d.lg. n. 51/1999, in particolare per quanto riguarda l'accertamento di violazioni costituenti reato.

Si avvia infatti a definitivo compimento la prima fase di applicazione della legge, la quale, oltre ad essere caratterizzata da varie norme di tipo transitorio, ha portato ad evidenza l'esigenza di un ragionevole e graduale approccio che non può ora spingersi, però, a differire oltre misura la piena esplicazione di norme e garanzie la cui inosservanza da parte di soggetti pubblici e privati si rivela del tutto ingiustificata.

Un'apposita deliberazione del Garante ha già individuato alcune priorità e criteri obiettivi di intervento per sviluppare in maniera equilibrata i controlli previsti, in riferimento a vari settori pubblici e privati nei quali suddividere le verifiche in loco (basate su controlli di tipo collaborativo oppure, ove necessario, su ispezioni autorizzate dal presidente del locale tribunale ordinario).

Infine, sul diverso piano dell'attività interna d'ufficio, l'Autorità tutta sarà attivamente impegnata in svariate attività che riguarderanno, in particolare, l'inquadramento in ruolo del personale in servizio, il reclutamento delle restanti unità, il completamento della sistemazione della nuova sede stabile dell'Autorità e la definizione di nuove e più agevoli procedure per riscontrare l'ingente numero di interPELLI del Garante.

5. Attività sul piano internazionale e comunitario

5.1 Profili generali

Il 1999 ha segnato un periodo molto importante nella vita del Garante anche sotto il profilo dell'impegno e delle realizzazioni nel settore delle attività svolte in ambito europeo ed internazionale.

L'Autorità ha infatti organizzato nel mese di aprile a Firenze la riunione annuale dell'Autorità comune di controllo di Schengen ed ha ottenuto l'approvazione, da parte della Commissione europea, di un progetto sulla "Lotta alla criminalità organizzata e protezione dei dati" proposto nell'ambito del Programma FALCONE. Il progetto, co-finanziato dalla stessa Commissione, si articola in due seminari, centrati il primo sull'attività di polizia e la protezione dei dati ed il secondo sull'attività giudiziaria in materia penale. I risultati dei seminari, il primo dei quali si è svolto il 27 e 28 marzo presso la sede di Europol a L'Aja, saranno presentati e discussi in una giornata conclusiva che si terrà a Roma.

Particolare attenzione è stata inoltre posta nell'impostazione e seguito del negoziato Europa-Usa per la definizione del livello di adeguatezza ai sensi dell'articolo 25 della direttiva 95/46/CE. Grande interesse e seguito ha avuto, nell'ambito della speciale audizione su protezione dei dati ed Unione europea, organizzata nei giorni 22 e 23 febbraio 2000 dal Parlamento europeo, Commissione delle libertà civili, giustizia e interno, l'intervento svolto dal prof. Rodotà proprio su questo tema.

E', inoltre, proseguita da parte del Garante l'opera di promozione della conoscenza della normativa italiana che ha attuato la direttiva 95/46/CE e la direttiva specifica sulla tutela della vita privata nel settore delle telecomunicazioni negli altri Paesi della Comunità.

Si ricorda anche la già segnalata adozione della direttiva volta ad armonizzare il quadro giuridico per l'utilizzo delle firme elettroniche e la posizione comune raggiunta dal Consiglio riguardo alla proposta di direttiva rivolta a definire alcuni aspetti giuridici del commercio elettronico: si tratta di due strumenti importanti per creare un insieme armonizzato di regole tra i Paesi della Comunità, anche riguardo a situazioni che si producono in Paesi terzi.

5.2 Direttiva n. 95/46/CE e Gruppo di lavoro ex art. 29

Gli aspetti relativi alla tutela dei dati personali sono affrontati, come già indicato nella precedente relazione, dal "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" (organismo a carattere consultivo ed indipendente composto da rappresentanti delle autorità di controllo nazionali, 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 sottoposti da quest'ultima).

Nel corso dell'anno il Gruppo, di cui il prof. Rodotà è divenuto di recente presidente, ha largamente concentrato i suoi interventi rispetto alla valutazione e delimitazione delle condizioni

necessarie per giungere ad una ipotesi di soluzione del negoziato aperto con gli Stati Uniti per definire le modalità attraverso le quali può essere consentito un trasferimento di dati personali verso o da quel Paese

Oltre a tale negoziato (di cui si è fatto cenno nel par. 2.12) per il quale è intervenuto ben cinque volte nel corso dell'anno con l'adozione di pareri e per definire i metodi di lavoro, il Gruppo ha espresso la sua opinione sul livello di protezione dei dati personali in Svizzera ed in Ungheria, (rispettivamente, con i pareri 5/99 doc. WP 22, approvato il 7 giugno 1999, e 6/99 doc. WP 24 approvato il 7 settembre 1999).

Il Gruppo è inoltre intervenuto, adottando specifiche raccomandazioni, su i seguenti profili:

- Trattamento invisibile ed automatico dei dati personali su Internet (Raccomandazione 1/99, doc. WP, 17 adottata il 23 febbraio 1999);
- Rispetto della vita privata nel contesto dell'intercettazione di telecomunicazioni (Raccomandazione 2/99, doc. WP 18, adottata il 3 maggio 1999);
- Conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari (Raccomandazione 3/99, doc. WP 25, adottata il 7 settembre 1999), nonché, in relazione ai lavori che si svolgono per pervenire alla definizione di una Carta europea dei diritti fondamentali, con la Raccomandazione n. 4/99 dedicata a:
- L'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali (doc WP 26, approvato il 7 settembre 1999).

I documenti elaborati dal Gruppo con riferimento al negoziato con gli Stati Uniti, tuttora in corso, sono i seguenti:

- Parere 1/99 sul livello di protezione dei dati personali negli Stati Uniti (doc. WP 15, adottato il 26 gennaio 1999);
- Parere 2/99 riguardante l'adeguatezza dei "principi internazionali per un approdo sicuro" stabiliti dal Ministero del commercio USA il 19 aprile 1999 (doc. WP 19, del 3 maggio 1999);
- Parere 4/99 riguardante le FAQ (domande poste frequentemente) che saranno pubblicate dal Ministero del commercio USA in relazione ai principi "Approdo sicuro" (Safe Harbor) proposti (doc. WP 21 del 7 giugno 1999);
- Documento di lavoro sullo stato attuale delle discussioni in corso tra la Commissione europea e il Governo degli Stati Uniti in merito ai principi internazionali dell'"Approdo sicuro" (Safe Harbor) (doc. WP 23 del 7 luglio 1999);
- Parere 7/99 riguardante il livello di tutela dei dati offerto dai principi dell'"Approdo sicuro" (Safe Harbor) pubblicati con le FAQ ed altri documenti in materia dal Ministero del commercio USA il 15 e 16 novembre 1999 (doc. WP 27 del 3 dicembre 1999).

Anche i lavori del Comitato dell'articolo 31 sono stati largamente influenzati dall'importanza del negoziato in corso, tanto che i componenti del Comitato e la Commissione hanno effettuato un viaggio ufficiale negli Stati Uniti cui ha preso parte il segretario generale del Garante.

In relazione al più generale tema dell'attuazione di principi della direttiva 95/46/CE, è da segnalare che il termine fissato dalla stessa per il recepimento è, com'è noto, scaduto il 24 ottobre 1998. Analogamente è scaduto il termine per il recepimento della direttiva 97/66/CE. Non tutti i Paesi hanno completato la trasposizione dei principi contenuti in una od entrambe le direttive, tanto che la Commissione ha deciso di aprire la procedura di infrazione per inadempimento nei confronti di Francia, Germania, Irlanda, Lussemburgo, Danimarca e Paesi Bassi, riguardo alla direttiva 95/46/CE.

5.3 Cenni comparativi sul recepimento delle direttive 95/46 CE e 97/66/CE

Nel corso del 1999, tre Stati membri dell'Unione hanno introdotto disposizioni di legge di recepimento della direttiva 95/46/CE: si tratta della Finlandia (legge sui dati personali n. 523/1999, entrata in vigore il 1 giugno 1999), dell'Austria (legge sulla protezione dei dati 2000, entrata in vigore il 1 gennaio 2000) e della Spagna (legge organica n. 15/99 sulla protezione dei dati, entrata in vigore il 14 gennaio 2000). Essi si aggiungono dunque alla Grecia, all'Italia, al Belgio, alla Svezia, al Regno Unito ed al Portogallo, che avevano recepito già la direttiva nei rispettivi ordinamenti (vedi Relazione annuale del Garante per il 1998; una tavola sinottica dello stato di recepimento della direttiva 95/46 e della 97/66, è disponibile in calce al presente capitolo).

Per quanto riguarda le disposizioni specifiche, occorre dire che nei tre Paesi era già in vigore una legge in materia di protezione dei dati; per il recepimento della direttiva si è però preferito emanare un testo del tutto nuovo anziché introdurre emendamenti alla legislazione precedente. La *Ley Organica* spagnola, ad esempio, era in vigore dal 1992 e il governo ha deciso, dopo un travagliato iter parlamentare, di riscriverne completamente il testo alla luce dei principi della direttiva 95/46/CE. Questi ultimi hanno dunque trovato pieno recepimento, anche se con alcune importanti differenze. In particolare, la legge spagnola — che si applica a tutti i trattamenti di dati personali, sia automatizzati, sia di tipo manuale — prevede un obbligo generale di notificazione dei trattamenti (v. art. 18 della direttiva) indipendentemente dalla natura dei dati oggetto di trattamento; non vi sono in pratica eccezioni all'obbligo di notificare il trattamento — neppure per quanto riguarda i trattamenti effettuati nell'ambito della professione giornalistica (sul contenuto specifico della notificazione la legge rimanda a disposizioni regolamentari ancora da emanare; la notificazione dovrà contenere almeno l'indicazione del responsabile, le finalità del trattamento, il luogo di conservazione, la tipologia dei dati personali, le misure di sicurezza, i trasferimenti previsti di dati a terzi). Per quanto riguarda il diritto di accesso, rettifica e cancellazione, la legge prevede che esso sia sempre esercitabile in forma gratuita (va detto che l'art. 15 della Ley prescrive che l'accesso non sia esercitabile a intervalli inferiori a 12 mesi — contro i 90 giorni nella legge italiana —, "salvo che l'interessato dimostri un interesse legittimo in materia"); nel caso di dati raccolti presso terzi, il titolare deve informare l'interessato dell'avvenuta registrazione dei suoi dati entro i tre mesi successivi. Va inoltre sottolineato l'obbligo di ottenere sempre il consenso per iscritto in rapporto al trattamento di dati di natura sensibile. Inoltre, la legge prevede in via generale il divieto di trasferire dati personali verso Paesi terzi che non garantiscono "un livello di protezione paragonabile a quello sancito dalla presente legge", salvo l'ottenimento di una previa "autorizzazione" da parte del direttore della Agencia de Protección de Datos; le eccezioni contemplate a tale disposizione sono sostanzialmente analoghe a quelle previste dalla legge italiana.

È interessante osservare che la legge spagnola prevede poi una serie di disposizioni in materia di trattamenti per scopi pubblicitari e di indagine commerciale, in base alle quali i cittadini possono chiedere di essere esclusi da un "registro pubblicitario" che abilita le varie ditte che operano nel settore pubblicitario e del marketing all'invio di materiale pubblicitario o promozionale; la richiesta di esclusione ha effetto immediato. L'articolo 32 della legge promuove, infine, la redazione di codici-modello di natura deontologica per quanto riguarda i trattamenti di dati personali nel settore privato; i codici dovranno essere depositati presso il Registro generale della protezione dei dati e potranno essere rifiutati se, a giudizio del direttore della APD, non risultano conformi alle disposizioni di legge e di regolamento in materia.

In Austria, la nuova legge sulla protezione dei dati è stata promulgata dal Parlamento il 17 agosto del 1999 ed è entrata in vigore, come già indicato, il 1 gennaio del 2000 (*Datenschutzgesetz* 2000). Si tratta di un testo che ha cercato di conciliare le disposizioni precedentemente in vigore (fissate nella Legge n. 565 del 1978) con i principi sanciti dalla direttiva 95/46/CE; la ricerca di tale

obiettivo ha comportato il "sacrificio" di alcuni principi, o ha condotto ad un'interpretazione restrittiva (anche in rapporto alla legislazione italiana).

In primo luogo va detto che l'articolo 4 della legge fornisce alcune definizioni che non corrispondono perfettamente a quelle della direttiva: si parla infatti non di "trattamento" di dati personali, ma di "impiego" di dati (con ciò intendendo "l'insieme delle operazioni logicamente interconnesse nella loro successione e preordinate al raggiungimento di un risultato specifico (...) effettuate in tutto o in parte con l'ausilio di mezzi automatizzati"). In pratica la legge austriaca (leggendo tale articolo insieme all'articolo 2, comma 1: "L'attività legislativa in materia di tutela dei dati personali nei flussi di dati automatizzati è di competenza dello Stato federale") riserva ai Länder (i singoli Stati che compongono la federazione austriaca) l'emanazione di norme specifiche in materia di trattamento di dati personali con l'ausilio di strumenti non automatizzati, salvo per le materie in cui la competenza è assegnata per legge allo Stato federale (v. art. 2, comma 2 della Legge). Viene inoltre introdotta la distinzione fra "dati personali" e "dati solo indirettamente personali" — questi ultimi corrispondendo ai dati per i quali il titolare ("committente del trattamento", secondo la definizione di legge) o il destinatario "non sono in grado di determinare l'identità dell'interessato attraverso strumenti giuridicamente leciti".

Per quanto riguarda i diritti fondamentali degli interessati (accesso, informazione, rettifica, opposizione), va sottolineato che la legge impone al titolare l'obbligo di comunicare all'interessato soltanto le finalità dell'impiego dei dati e le generalità del titolare — senza imporre anche l'obbligo di informativa sugli eventuali destinatari della comunicazione dei dati o sull'esistenza di un diritto di accesso ai dati. Queste informazioni sono ottenibili dall'interessato soltanto previa presentazione di una richiesta per iscritto (o anche verbalmente, se il titolare è d'accordo) (art. 26), e dietro versamento di una somma pari a 260 scellini (a meno che si tratti della prima richiesta presentata nel corso dell'anno o la richiesta riguardi i dati "attualmente" oggetto di trattamento), salva l'esistenza di "interessi pubblici prevalenti" (difesa nazionale, interessi di politica estera, economici o finanziari della Repubblica austriaca, prevenzione o repressione di reati, attività dell'esercito federale austriaco); il titolare ha otto settimane di tempo per fornire i dati richiesti. Da notare che i diritti degli interessati non sono esercitabili in rapporto ai dati che la legge definisce "solo indirettamente personali" (art. 27).

Mentre le disposizioni in materia di notificazione dei trattamenti sono analoghe a quelle previste dalla direttiva (e dalla legge italiana), e contemplano una serie di eccezioni fra cui, in particolare, i trattamenti per scopi di natura pubblicistica (v. infra), vi sono alcune specificità per quanto concerne i rimedi giuridici di cui gli interessati dispongono. La legge austriaca prevede la possibilità per "chiunque" (art. 30) di segnalare alla Commissione per la protezione dei dati presunte violazioni dei propri diritti o degli obblighi che la legge impone ai titolari; tuttavia, la Commissione è competente a conoscere soltanto i ricorsi presentati contro titolari del settore pubblico per presunte violazioni del diritto degli interessati alla riservatezza, alla correzione o alla cancellazione dei dati (art. 31). Per quanto riguarda le presunte violazioni commesse da titolari del settore privato, i diritti degli interessati devono essere fatti valere per via giudiziaria; la Commissione eventualmente può costituirsi in giudizio con l'interessato, su sua esplicita richiesta (art. 32). Inoltre, è previsto un risarcimento del danno da parte del titolare soltanto in caso di comportamento negligente da parte di quest'ultimo.

Va infine rilevato che la legge austriaca prevede alcune eccezioni per le attività di natura pubblicistica (che non sono soggette all'obbligo di notificazione, né di informativa) (art. 48), e che per quanto concerne le "decisioni individuali automatizzate" l'opposizione dell'interessato a tale tipo di trattamenti non può essere fatta valere se la decisione "derivante in via esclusiva da trattamenti automatizzati è prevista espressamente per legge" — anche se l'interessato ha comunque il diritto di conoscere la "logica alla base della decisione automatizzata, in una forma comunemente comprensibile" (art. 49).

Anche il testo di legge licenziato dal Parlamento finlandese nel marzo del 1999 (legge sulla

protezione dei dati n. 523/1999) ha sostituito la legge precedentemente in vigore (n. 471/1987) modificandone l'impianto. La nuova legge ha recepito nella sostanza i principi fondamentali della direttiva, ad iniziare dalle definizioni (art. 3) che sono modellate su quelle della direttiva (anche se manca la definizione di "responsabile" del trattamento, cui si fa riferimento in via indiretta nella definizione di "terzi": "(soggetti) diversi dall'interessato, il titolare, il responsabile del trattamento di dati personali o chiunque tratti dati personali per conto del titolare o del responsabile") e dai principi relativi alla qualità dei dati (art. 9).

Anche l'informativa agli interessati (art. 24) è modellata sulla direttiva, nel senso che il legislatore ha compiuto la scelta di non andare oltre le prescrizioni dell'art. 11 della norma comunitaria (informazioni relative all'identità del titolare, alle finalità del trattamento, ai destinatari dei dati e all'esistenza di un diritto di accesso). Non vengono indicate le modalità con cui l'informativa deve raggiungere l'interessato (essendo previsto soltanto che "il titolare deve fare in modo che l'interessato possa disporre di informazioni..."). Nell'esercizio del diritto di accesso (artt. 26-28) è previsto l'obbligo per l'interessato di presentare una richiesta per iscritto ovvero di recarsi di persona nel luogo ove il titolare effettua il trattamento; il titolare ha tre mesi di tempo per rispondere, sempre per iscritto, ovvero per fornire copia dei dati. In caso di mancata risposta, l'interessato può sottoporre il caso all'attenzione del Data Protection Ombudsman (l'autorità garante della protezione dei dati). In base alla normativa precedente, l'interessato poteva esercitare il diritto di accesso agli archivi contenenti dati che lo riguardavano non più di una volta all'anno; nella legge attuale, l'esercizio del diritto di accesso non è soggetto invece a vincoli del genere, tranne il pagamento di una somma "ragionevole" se è trascorso meno di un anno dall'ultimo accesso effettuato.

È interessante osservare che la notificazione dei trattamenti (artt. 36-37) si fonda su una "descrizione" dell'archivio di dati (non del trattamento) (art. 10) che il titolare è tenuto a compilare e a tenere sempre a disposizione di chiunque voglia prenderne visione. La notificazione deve essere presentata al Data Protection Ombudsman almeno 30 giorni prima di dare corso alla raccolta o alla registrazione dei dati personali. Anche la legge finlandese prevede esenzioni dall'obbligo di notificazione, in particolare per quanto riguarda l'attività giornalistica (esplicitamente menzionata nell'art. 15).

Per quanto concerne i poteri del Data Protection Ombudsman, va detto che, oltre alla possibilità di emanare direttive e raccomandazioni (anche in materia di codici deontologici), le sue competenze si limitano all'esame delle segnalazioni degli interessati per il mancato esercizio dei diritti di accesso e rettifica (art. 40), mentre per ogni altra violazione della normativa in materia la competenza è dell'autorità giudiziaria ordinaria ovvero del Data Inspection Board (Commissione per la protezione dei dati) - un ente di nomina governativa già previsto dalla legge precedentemente in vigore. In particolare, il pubblico ministero deve sentire l'Ombudsman prima di formulare un'imputazione per violazione delle norme di protezione dati (art. 41). La legge (art. 44) prevede inoltre che, su richiesta dell'Ombudsman, il Data Protection Board possa emettere ordinanze finalizzate a vietare o bloccare trattamenti illegittimi di dati personali, ovvero ad imporre rimedi giuridici per condotte illecite. Va rilevato che la legge prevede la responsabilità per danni morali e materiali da parte del titolare (art. 47) indipendentemente dalle modalità dell'atto.

Un ulteriore elemento di interesse è l'attenzione dedicata ai trattamenti di dati per fini di marketing diretto (art. 19) o di valutazione della solvibilità (art. 20). In particolare, il trattamento di dati personali per fini di marketing diretto necessita del consenso dell'interessato e presuppone l'inserimento delle sole generalità della persona (compresa età e sesso) e di "un dato distintivo"; nel caso degli archivi contenenti valutazioni della solvibilità il consenso non occorre, ma l'inserimento deve basarsi su una sentenza definitiva (anche in contumacia) di fallimento o su una dichiarazione di protesto, ovvero su una clausola presente in accordi di leasing stipulati fra l'interessato e il titolare. La legge prescrive la cancellazione (art. 21) dei dati contenuti in questi ultimi archivi dopo quattro anni in caso di mancato pagamento, dopo cinque per quanto riguarda i casi di fallimento, e dopo non oltre due anni nei casi restanti.

Per quanto riguarda la direttiva "figlia", ossia la n. 97/66, lo stato della sua trasposizione nel diritto nazionale degli Stati membri dell'UE è piuttosto complesso. Mentre alcuni Stati non hanno sinora adottato le misure legislative necessarie (si tratta, più precisamente, di Grecia, Irlanda e Lussemburgo), ve ne sono altri nei quali si può parlare (anche in base alla documentazione in possesso della Commissione europea - Direzione generale XIII - Società dell'informazione) di "parziale trasposizione" - con ciò intendendo il fatto che alcuni importanti principi della direttiva non sono stati recepiti o lo sono stati in modo solo parziale. Rientrano in questo gruppo:

- il Belgio, dove la direttiva ha trovato parziale trasposizione nella legge sulla protezione dei dati del 1999 e in un decreto reale (del 22 giugno 1998) che fissa gli importi per il servizio di telefonia vocale e la procedura relativa alla concessione delle autorizzazioni individuali. Sono in via di preparazione norme di legge in materia di fatturazione dettagliata e informazioni sul volume del traffico e la fatturazione;
- la Danimarca, dove la direttiva è stata trasposta in misura parziale attraverso un decreto che riguarda i fornitori di reti e servizi di telecomunicazioni e le basi di dati dei servizi di informazioni su abbonati. L'articolo 12 della direttiva (chiamate indesiderate) richiede un emendamento della legge sul marketing ai fini della trasposizione;
- la Francia, dove due leggi in materia di telecomunicazioni (Loi 96-659 e Loi 90-1170) e un decreto (Décret 96-1175 del 29 dicembre 1990) danno parziale attuazione alle disposizioni della direttiva. Mancano però norme che disciplinino l'obbligo di informare gli abbonati in materia di rischi per la sicurezza delle reti, la cancellazione dei dati, le limitazioni relative alla fatturazione dettagliata, l'identificazione della linea chiamante e le chiamate indesiderate;
- i Paesi Bassi, dove esiste una legge sulle telecomunicazioni ed un regolamento sull'identificazione numerica (del 1998); si prevede di introdurre legislazione secondaria per quanto riguarda fatturazione e chiamate indesiderate;
- il Regno Unito, dove esiste un regolamento in materia di telecomunicazioni (Data Protection and Privacy, Direct Marketing) del 1998 che recepisce in misura molto parziale le disposizioni della direttiva. È prevista l'emanazione di normativa secondaria (ma anche primaria) per dare piena attuazione alle disposizioni comunitarie.

Nei restanti Paesi dell'UE la direttiva 97/66 è stata "sostanzialmente" trasposta - il che significa che tutti i principi fondamentali trovano attuazione ed è dunque possibile la realizzazione delle finalità che la direttiva si prefigge. Va detto, comunque, che nei singoli Paesi varia la natura degli atti con cui si è recepito il dettato comunitario, nel senso che spesso occorre fare riferimento ad un complesso insieme di norme primarie, norme secondarie e regolamentari che si applicano specificamente a settori determinati; ad esempio, in Finlandia, oltre alla legge sulla tutela della privacy e la sicurezza dei dati nelle telecomunicazioni, n. 565/1999, esiste un regolamento sulla sicurezza informatica delle telecomunicazioni ed un regolamento sulla tutela fisica dei locali e delle reti di operatori di telecomunicazioni. In Portogallo la trasposizione della direttiva è invece demandata alla Legge 69/98 che regola il trattamento di dati personali e la tutela della riservatezza nel settore delle telecomunicazioni, sostanzialmente analoga nell'impianto al decreto legislativo n. 171/98 che ha recepito la direttiva per l'Italia.

5.4 Altri gruppi di lavoro in materia di protezione dei dati

Sempre collegato al quadro comunitario che ruota attorno alle direttive 95/46/CE e 97/66/CE, va indicato come particolarmente importante per il Garante, che prende parte attiva ai lavori, il Gruppo protezione dei dati.

Nel corso dell'anno è proseguita da parte del Gruppo l'attività di coordinamento per defi-

nire la posizione dei Paesi comunitari rispetto ai documenti e testi normativi in discussione, in particolare presso il Consiglio d'Europa, in materia di protezione dei dati personali e, grazie al positivo esito delle riunioni, è stato possibile completare l'iter relativo alla definizione dei modi per consentire l'adesione delle Comunità europee alla Convenzione n. 108 del Consiglio d'Europa.

È stato inoltre completato l'esame del Protocollo aggiuntivo alla Convenzione n. 108 con il quale si intendono apportare alla stessa importanti modificazioni per allinearla meglio alla direttiva 95/46/CE. Il Protocollo introduce infatti specifiche disposizioni intese a pervenire alla creazione di autorità di controllo nazionali ed a disciplinare compiutamente la trasmissione di dati da e verso Paesi terzi.

Il Gruppo sta ora concentrando la sua attenzione sulla proposta di regolamento del Parlamento e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni e degli organi della Comunità europea. La proposta, che è stata presentata dalla Commissione al Gruppo protezione dei dati nella riunione dell'8 settembre 1999 (doc. COM (1999) 337 def. del 14 luglio) è intesa a dare attuazione al dettato dell'art. 286 del Trattato di Amsterdam, in base al quale:

- a decorrere dal 1° gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, si applicano alle istituzioni e agli organismi istituiti dal Trattato o sulla base del medesimo;
- anteriormente alla data di cui al paragrafo 1 il Consiglio, deliberando secondo la procedura di cui all'articolo 251, istituisce un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni.

Il provvedimento mira pertanto ad introdurre all'interno delle istituzioni e degli organismi comunitari un livello di tutela dei dati personali corrispondente a quello assicurato in ciascuno degli Stati membri con la trasposizione delle direttive comunitarie 95/46/CE e 97/66/CE.

Le direttive citate si indirizzano ai soli Stati membri. Tuttavia, già prima del ricordato articolo 286 e precisamente al momento dell'adozione della direttiva 95/46/CE nel 1995, la Commissione ed il Consiglio si impegnarono con un dichiarazione pubblica ad applicarne i principi, impegno divenuto oggi vincolante.

I principi di protezione dei dati contenuti nella proposta di regolamento sono quindi basati sulle disposizioni comunitarie esistenti e li integrano dettando specifiche disposizioni laddove la direttiva quadro 95/46/CE lascia margini attuativi agli Stati.

La proposta è articolata in sei capi e si compone di 49 articoli:

Capo I - Disposizioni generali (artt. 1-3 riguardanti l'oggetto, le definizioni, il campo di applicazione).

Capo II - Condizioni generali di liceità delle operazioni di trattamento dei dati personali (artt. 4-28 contenenti diverse sezioni riguardanti i principi di qualità dei dati, di legittimazione al trattamento -inclusi i principi relativi al trasferimento dei dati ed il trattamento dei dati sensibili- la definizione dei diritti degli interessati all'informativa sui trattamenti che li riguardano e le modalità di esercizio del diritto di accesso, la riservatezza e sicurezza del trattamento. Si prevede inoltre l'istituzione della figura del responsabile della protezione dati all'interno di ogni istituzione ed organismo comunitario ed i casi in cui è necessario il preventivo avviso del Garante europeo rispetto a trattamenti di dati personali che possono comportare dei rischi).

Capo III - Mezzi di ricorso e sanzioni (artt. 29 e 30).

Capo IV - Protezione dei dati personali e tutela della riservatezza nell'ambito delle reti interne di

telecomunicazione (artt. 31-37 largamente incentrati sull'adattamento ai principi della direttiva 97/66/CE relativa alla tutela della vita privata nel settore delle telecomunicazioni).

Capo V - Autorità di vigilanza: il Garante europeo della tutela dei dati (artt. 38-47 che definiscono i requisiti di indipendenza, le modalità di nomina e revoca, i poteri e la struttura di cui si avvale il Garante).

Capo VI - Disposizioni finali (artt. 48 e 49).

Risulta quindi giustificata l'attenzione con la quale si procede alla definizione della figura, dei compiti e della struttura della futura autorità di vigilanza, il c.d. "Garante europeo". Quest'ultimo sarà infatti costituito come un organo indipendente e sarà responsabile della vigilanza e del controllo sulla corretta applicazione delle norme in materia di protezione dei dati da parte delle istituzioni e degli organismi comunitari. Avrà pertanto competenze e poteri simili a quelli garantiti alle autorità nazionali di protezione dei dati: in particolare potrà essere adito dai cittadini che si ritengono lesi da comportamenti o atti delle istituzioni tenute all'applicazione del regolamento.

La discussione del regolamento procede con un ritmo abbastanza intenso e ciò ha consentito di concludere la prima lettura del provvedimento all'inizio di gennaio e di iniziare quindi la seconda lettura che dovrebbe concludersi entro il mese di aprile. I lavori si basano sul testo iniziale anche se largamente modificato a seguito della discussione avutasi. La Commissione presenterà una proposta modificata non appena il Parlamento europeo avrà espresso il suo parere sul testo. Da parte di tutte le delegazioni è stato espresso l'auspicio di una rapida adozione del regolamento.

5.5 Cooperazione europea nel settore giustizia e affari interni

L'entrata in vigore il 1 maggio 1999 del Trattato di Amsterdam ha determinato, da un lato la progressiva comunitarizzazione di materie come l'immigrazione e l'asilo, che sono disciplinate nei modi e nelle forme previsti dal titolo IV del Trattato e che comprendono modelli di "cooperazione rafforzata" già definiti tra Paesi dell'Unione, come la cooperazione in ambito Schengen.

Il Trattato di Amsterdam prevede infatti l'incorporazione dell'acquis di Schengen nelle attività del Consiglio, secondo modalità fissate in un apposito protocollo. A queste attività, almeno tendenzialmente e fatta salva la competenza dell'Autorità comune di controllo Schengen in relazione alla vigilanza sulla parte centrale del Sistema d'Informazione Schengen, dovrà applicarsi, in quanto svolte da istituzioni e/o organismi comunitari, il regolamento attuativo dell'articolo 286 cui si è fatto cenno. Conseguentemente la vigilanza ed il controllo sulla corretta attuazione dei principi in materia di protezione dei dati sarà attribuita all'istituendo Garante europeo.

La restante parte del titolo VI del Trattato di Maastricht, dedicato alla cooperazione in materia di affari interni e giustizia, forma ora il titolo VI del Trattato di Amsterdam ed è centrato sulla creazione di uno spazio di sicurezza, libertà e giustizia, obiettivo da raggiungere mediante strumenti che affinino la cooperazione di polizia e giudiziaria in materia penale tra gli Stati (non va dimenticata la particolare posizione di Danimarca, Irlanda e Regno Unito).

Lo svilupparsi della cooperazione nel settore, ripresa ora nel testo stesso del Trattato, conferma senz'altro la riflessione del Garante circa la necessità di razionalizzare il quadro esistente ed evitare che si pervenga ad altri accordi che prevedano la creazione di strumenti basati su scambi informatizzati di dati personali in assenza di un riferimento normativo unitario. Infatti la tendenza a prevedere, nelle elaborazioni dei gruppi che lavorano sui diversi aspetti della cooperazione nelle materie previste dal titolo VI, specifiche disposizioni in materia di protezione dei dati personali, non

serve a creare un insieme armonizzato di regole applicabili in via generale a quei trattamenti, ma invece, a differenziare i diritti e le tutele.

Come già evidenziato nella precedente relazione, queste preoccupazioni sono state accolte e, su proposta italiana, il Consiglio dei ministri europei della giustizia e affari interni ha deciso di far effettuare una ricognizione puntuale dei diversi strumenti esistenti ed 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, nonché di razionalizzare la complessa tematica pervenendo ad un grado più elevato di armonizzazione ed evitando duplicazioni di personale e mezzi.

Per sviluppare eventuali ipotesi, anche normative, di soluzione, è stato costituito presso il Consiglio un apposito gruppo di lavoro, di cui il Garante fa parte.

I lavori del Gruppo, iniziati nel febbraio del 1999, si sono finora articolati seguendo, su impulso di diverse delegazioni, un approccio pragmatico. Partendo dalle perplessità di alcuni Paesi rispetto all'idea che si potesse giungere alla definizione di principi comuni in materia di tutela dei dati volti ad incidere sull'effettività dell'azione di polizia e di magistratura nel contrasto della criminalità organizzata in ambito sovranazionale, si è proposto di partire da un altro angolo visuale ovvero dalle questioni più facilmente risolvibili. Si è così discusso di un problema di funzionalità delle autorità, cioè della costituzione di un segretariato comune, per fornire supporto alle autorità di controllo già previste ed istituite dalle convenzioni Schengen, Europol e Sistema informativo doganale, della sua composizione e della sua autonoma collocazione per farne un ufficio dotato di effettiva indipendenza; si è discusso inoltre dell'unificazione della composizione delle suddette autorità.

Minore attenzione è stata invece posta, almeno sinora, riguardo al tema della definizione dei principi, sebbene con la presidenza di turno portoghese si è tentato di riprendere il discorso in base alla logica iniziale. La presidenza ha infatti presentato di recente un documento recante "principi generali concernenti la protezione dei dati nel terzo pilastro", che costituisce il frutto della riflessione sui principi già consolidati in materia di protezione dei dati derivanti dalla Convenzione n. 108 del Consiglio d'Europa e dalla direttiva 95/46/CE, e di quelli, che, già dettati per l'attività in senso generale "di polizia" dalla Racc. 87(15) del Consiglio d'Europa e dalla Convenzione Europol, potrebbero, in tutto od in parte, essere riconosciuti applicabili alle attività del terzo pilastro.

Il ritorno al senso della proposta iniziale e l'approfondimento degli spunti dalla stessa suggeriti rappresenta una prospettiva di spiccato interesse, pur nel mutato scenario istituzionale. Del resto la profonda convinzione che l'introduzione di norme specifiche in materia di protezione dei dati non solo non costituisce un vulnus dell'attività di inquirenti e forze di polizia nella prevenzione e repressione dei reati, ma che, anzi, ne consente una maggiore incisività e trasparenza, ha determinato il Garante a presentare, come già accennato, nell'ambito del "programma Falcone", un progetto denominato "Lotta alla criminalità organizzata e protezione dei dati", volto, attraverso seminari specificamente dedicati all'approfondimento concreto e lo studio dei casi, proprio alla verifica dell'impatto che la legislazione in materia di protezione dei dati ha avuto ed ha sull'attività ricordata.

5.6 Schengen

Nel 1999, come riassunto in altra parte della presente relazione, è proseguita l'opera di controllo svolta dal Garante sul funzionamento dell'archivio della sezione nazionale del Sistema d'Informazione di Schengen.

A seguito dell'entrata in vigore del Trattato di Amsterdam, l'attività di cooperazione svolta

in ambito Schengen è stata ricollocata nel Consiglio. In base allo specifico Protocollo annesso al Trattato, infatti, sono state definite le modalità per l'incorporazione del c.d. "acquis" e la ripartizione delle attività nei diversi titoli del Trattato. Le riunioni si svolgono quindi presso il Consiglio, che è competente anche per gli aspetti finanziari e logistici. Questa nuova collocazione ha avuto immediati ed importanti riflessi anche sul funzionamento dell'Autorità comune di controllo. Con una decisione del 12 maggio 1999 il Consiglio ha adottato specifiche disposizioni, in particolare riguardo alla tenuta delle riunioni ed al finanziamento dell'attività dell'Autorità di controllo comune.

Delicati problemi si pongono con particolare riguardo alla indipendenza dell'Autorità ed alla mancanza di un suo proprio segretariato, problemi cui forse potrà essere data positiva soluzione con l'auspicata istituzione del segretariato comune delle Autorità comuni di controllo già ricordato.

Il Garante partecipa all'Autorità comune di controllo, istituita ai sensi dell'art. 115 della Convenzione di applicazione dell'Accordo di Schengen, contribuendo alla definizione ed adozione di specifiche raccomandazioni e pareri. L'intensa e faticosa opera prestata si riflette nella nomina a vice-presidente dell'ACC del segretario generale dott. Buttarelli, avvenuta nel novembre scorso.

Si allega alla presente relazione il Rapporto dell'ACC relativo al periodo marzo 1998-marzo 1999, che è stato ufficialmente presentato a Firenze il 27 e 28 maggio scorsi. Si differisce invece la pubblicazione di quello relativo al periodo marzo 1999-marzo 2000 la cui predisposizione è ancora in corso.

Come già accennato, a seguito della deliberazione dell'ACC di invito per tutti i Paesi partecipanti al sistema Schengen ad attuare una campagna informativa per il pubblico da svolgere mediante la distribuzione di opuscoli e depliant plurilingue recanti le modalità per esercitare il diritto di accesso ai dati detenuti nel Sistema informativo Schengen da parte dei soggetti interessati, il Garante, ha curato la stampa del materiale necessario, e con la collaborazione delle amministrazioni competenti, Ministero degli Affari Esteri e dell'Interno, ha disposto la distribuzione presso le ambasciate ed i varchi di frontiera. Poiché tra le informazioni fornite negli opuscoli illustrativi distribuiti vi era anche l'indirizzo del Garante come autorità di tutela cui fare riferimento in caso di chiarimenti, doglianze, errori, può senz'altro ascriversi anche ai risultati della campagna l'incremento delle richieste riscontrate nella seconda metà dell'anno.

5.7 Europol

La legge 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 ed a tal fine il Garante avrà accesso ai dati ed agli archivi. Sulla base dei principi dettati nelle leggi 675 e 676 del 1996, il Garante dovrà inoltre controllare le attività svolte dall'unità nazionale e dagli ufficiali di collegamento per la parte concernente le tutele 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 legge n. 675.

Dall'entrata in vigore della Convenzione, avvenuta il 1° ottobre 1998, sono state presentate ad Europol due richieste che non hanno dato luogo a ricorso.

Nel corso dell'anno ha continuato i suoi lavori l'Autorità comune di controllo, prevista dall'art. 24 della Convenzione. Questa Autorità, composta da due rappresentanti per Paese delle autorità nazionali di controllo, esercita incisivi controlli sulla gestione degli archivi Europol, che dal luglio 1999 comprendono gli archivi di analisi. L'Autorità valuta, in relazione ai compiti affidati dalla Convenzione gli ordini di apertura dei file di analisi.

L'Autorità ha definito in un regolamento interno, che è stato approvato nel mese di maggio e pubblicato sulla Gazzetta ufficiale delle Comunità europee, le necessarie misure procedurali, anche riguardo al comitato ricorsi, ed ha definito i suoi compiti.

È da ricordare inoltre l'ampio dibattito parlamentare in relazione alla ratifica del Protocollo relativo ai privilegi ed immunità di Europol, volto ad approfondire un tema analizzato anche dal Garante, relativo alle garanzie riconosciute ad Europol ed ai suoi agenti e rappresentanti. Il Protocollo conferisce infatti ad Europol (art. 2, comma 1) l'immunità giurisdizionale per la responsabilità di cui all'art. 38, paragrafo 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 possibile attenuazione delle garanzie contenute nella Convenzione. Il Parlamento, al momento del voto finale, ha pertanto raccomandato di limitare le immunità ed i privilegi all'essenziale, e cioè alle attività svolte in relazione al mandato iniziale di Europol quale risulta dalla Convenzione e di studiare eventuali interventi di chiarificazione anche attraverso la revisione della Convenzione stessa.

5.8 Sistema informativo doganale

Con la legge 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 ad 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 -SID) che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La Convenzione istituisce una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

La Convenzione non è ancora entrata in vigore, né è stata ancora istituita l'autorità comune di controllo.

5.9 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 od in via di elaborazione nel settore della cooperazione affari interni e giustizia proposta dall'Italia, anche se con l'entrata in vigore del Trattato di Amsterdam l'autorità incaricata della vigilanza e controllo in materia di protezione dei dati dovrebbe essere il c.d. Garante europeo previsto del regolamento attuativo dell'articolo 286 del Trattato.

5.10 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 plenaria annuale, ha trattato i seguenti temi:

- esame ed approvazione del testo di un protocollo aggiuntivo alla Convenzione, destinato ad introdurre l'obbligo dell'istituzione di autorità nazionali di controllo ed a disciplinare i flussi transfrontalieri di dati;
- modifica delle procedure da seguire per l'adozione di provvedimenti del Consiglio d'Europa, esaminata dal Comitato dei Ministri nel mese di aprile 1999;
- progetto di raccomandazione per estendere, su base volontaria, l'applicazione dei principi della convenzione anche ai dati cartacei;
- questionario sui dati sensibili volto ad accertare l'uniformità delle definizioni adottate dai diversi Paesi e la possibilità di inserirvi altre categorie di dati.

È stata inoltre approvata dal Comitato dei Ministri la modifica alla Convenzione predisposta dal Comitato e discussa nelle riunioni di coordinamento comunitario, volta a permettere l'adesione delle Comunità europee alla Convenzione. La modifica entrerà in vigore quando avrà raggiunto il numero di ratifiche richiesto. La decisione adottata è nel senso di emendare il testo seguendo la procedura ordinaria prevista dall'art. 21, in quanto questa risulta più flessibile e rapida.

Le modifiche conseguentemente apportate consistono nell'inserimento del riferimento alle Comunità europee accanto a quello agli Stati ed 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 clausola dell'opting out, liberi questi ultimi (Regno Unito, Irlanda e Danimarca) di accettare caso per caso il coordinamento comunitario.

Sono state adattate di conseguenza le disposizioni del regolamento interno per tutelare gli Stati parte non membri dell'Unione qualora, vertendosi in materie attribuite alle competenze comunitarie, gli Stati dell'U.E. votino attraverso la Commissione europea.

Sono inoltre proseguiti i lavori per la definizione del progetto di protocollo addizionale alla Convenzione, facoltativo per i Paesi che intendano accedere alla Convenzione, per gli aspetti relativi alle autorità di controllo ed ai flussi transfrontalieri. Come già ricordato, anche questo tema ha formato oggetto di previa concertazione comunitaria in seno al gruppo protezione dati dell'U.E.

È stata inoltre adottata la Raccomandazione 99 (5), predisposta dal Gruppo di progetto sulla protezione dei dati-CJ-PD e concernente "linee-guida per la protezione della privacy in INTERNET".

Il CJ-PD, sotto-comitato istituito nell'ambito della cooperazione giudiziaria, che tratta dell'elaborazione di proposte e progetti di raccomandazioni rivolti ad integrare e specificare le disposizioni della Convenzione n. 108 con riguardo a settori determinati, nella sua riunione di ottobre

1999 ha completato l'esame della proposta di Raccomandazione sul trattamento dei dati personali raccolti e trattati a fini assicurativi e ne ha definitivamente messo a punto il testo, anche sulla scorta della posizione comunitaria ufficializzata in una nota della Commissione europea.

Altri argomenti all'esame del Gruppo sono stati il progetto di Raccomandazione n. 1402/1999 del Parlamento europeo concernente il "Controllo dei servizi di sicurezza negli Stati membri del Consiglio d'Europa" e l'elezione del nuovo presidente.

Gran parte del lavoro preparatorio delle riunioni del CJ-PD viene svolto dal bureau, composto dal Presidente e dai vice presidenti, che restano in carica per un biennio e possono essere rinnovati.

Il comitato ha inoltre istituito un Gruppo di lavoro, denominato Gruppo di lavoro nuove tecnologie, che in particolare affronta i temi della videosorveglianza e della criminalità nel cyber spazio. Il gruppo si riunisce in genere, a seconda delle compatibilità di bilancio, una o due volte l'anno, in autunno e/o in primavera.

Nel corso dell'ultima riunione si è svolta una discussione sui primi problemi riscontrati nell'applicazione delle linee guida per l'uso di Internet ed è stato esaminato il progetto di Raccomandazione sulla videosorveglianza.

5.11 O.C.S.E.

Il Garante partecipa anche ai lavori di alcuni gruppi in sede O.C.S.E. nei gruppi e comitati che hanno tra le loro attribuzioni la materia della protezione dei dati.

In particolare, le attività di interesse dell'Autorità sono demandate al Comitato per la politica dell'informazione (ICCP) istituito all'interno della Direzione scienza, tecnologia e industria dell'OCSE.

Il Comitato si riunisce due volte l'anno ed organizza seminari su temi specifici.

Il suo mandato, scaduto il 20 febbraio 1999, è stato prorogato fino al 1° marzo 2004 ed è stato ampliato, alla luce delle conclusioni della Conferenza ministeriale di Ottawa, per comprendere agli aspetti legati al "commercio elettronico, alla sicurezza dell'informazione, alla protezione della privacy e all'infrastruttura della società dell'informazione".

Il Comitato ICCP è articolato in quattro gruppi di lavoro:

- Gruppo di lavoro per la politica dei servizi di informazione e di telecomunicazione;
- Gruppo di lavoro sull'economia delle infrastrutture;
- " " sugli indicatori della società di informazione;
- " " sulla sicurezza dell'informazione e sulla privacy.

Il gruppo si riunisce di regola due volte l'anno, a maggio ed a ottobre e segue le tematiche connesse alla tutela della riservatezza, con specifico riferimento al mondo delle telecomunicazioni.

Ha elaborato in particolare le linee-guida per la politica in materia di crittografia, approvate dal Consiglio OCSE nel 1997 ed ha organizzato nel 1998 una Conferenza sulla privacy nelle comunicazioni on-line.

Le elaborazioni del gruppo WPISP sono sottoposte al Comitato ICCP per l'approvazione.

Il Garante, su richiesta di quel Ministero, ha partecipato alle riunioni di coordinamento interministeriali organizzate presso il Ministero degli affari esteri allo scopo di definire temi e

modalità e la composizione della delegazione italiana per la partecipazione al Forum organizzato dalla Direzione della scienza-tecnologia generale per approfondire i temi trattati nel corso della Conferenza di Ottawa sul commercio elettronico, che si è svolto il 12 e 13 ottobre 1999.

L'OCSE ha adottato infine il 9 dicembre alcune linee-guida sulla protezione del consumatore on-line, che contengono specifici principi in materia di rispetto della privacy.

5.12 Collaborazione con altre autorità di garanzia

Oltre agli obblighi di collaborazione con le altre autorità di controllo nascenti dalla Convenzione n. 108/1981 e da altri atti internazionali e comunitari, come ad esempio l'Accordo di Schengen e la convenzione Europol, il Garante ha continuato a mantenere nel corso dell'anno stretti contatti con tali istituzioni per favorire lo scambio di esperienze ed opinioni, anche al fine di raggiungere, ove possibile, interpretazioni convergenti o 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 ed hanno consentito un puntuale aggiornamento.

Sono state, in particolare seguite le Conferenze internazionali ed europee delle autorità garanti, che sono organizzate anche nel 1999 con criteri di periodicità, nella primavera e in autunno come in altri anni.

Nel corso del 1999 la conferenza europea si è tenuta a Helsinki dal 14 al 16 aprile 1999 e quella mondiale ad Hong Kong il 13- 15 settembre 1999.

Da segnalare la particolare attenzione rivolta dalle autorità europee agli strumenti elaborati od 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.

L'incontro periodico dell'Autorità comune di controllo Schengen si è svolto a Firenze il 27 e 28 maggio 1999.

6. ALLEGATI

Quadro sinottico dello stato di recepimento delle direttive comunitarie in materia di protezione dei dati personali

Direttiva 95/46/CE (Situazione al gennaio 2000)

Paesi nei quali la direttiva è stata recepita con legge

Austria - Legge n. 165/99 del 17 agosto 1999

Belgio - Legge 3 febbraio 1999 sulla protezione dei dati personali

Finlandia - Legge 10 febbraio 1999

Grecia - Legge n. 2472 del 10 aprile 1997

Italia - Legge n. 675/1996 del 31 dicembre 1996

Portogallo - Legge n. 67/98 del 26 ottobre 1998

Regno Unito - Legge 16 luglio 1998 (Data Protection Act)

Spagna - Legge organica n. 15/99 (entrata in vigore il 14 gennaio 2000)

Svezia - Legge 204/98 del 29 aprile 1998 e regolamento attuativo 1191/98 del 03 settembre 1998

Paesi nei quali disegni di legge di recepimento sono all'esame del Parlamento

Danimarca - Progetto di legge L-44 (presentato al Parlamento per tre volte senza giungere alla discussione del testo);

Lussemburgo - Il Governo avrebbe dovuto presentare un disegno di legge nel mese di marzo 1999

Paesi Bassi - Il progetto di legge è stato discusso e approvato dalla Camera Alta e dalla Camera Bassa; si attende l'emanazione definitiva attraverso il decreto della Regina.

Paesi nei quali non è stato ancora presentato in sede parlamentare un disegno di legge per il recepimento

Francia - Il Governo deve presentare un disegno di legge in materia

Germania - L'esame in Parlamento del nuovo disegno di legge governativo (*Novellierung des Bundesdatenschutzgesetzes* - ripresentato dall'attuale Governo) deve ancora iniziare.

Irlanda - Il Governo ha elaborato un disegno di legge in materia che però non è stato ancora presentato al Parlamento.

Direttiva 97/66/CE (Situazione al gennaio 2000)

Paesi nei quali la direttiva è stata recepita "in misura sostanziale"

Austria - Legge sulle telecomunicazioni (*Telekommunikationsgesetz*) del 19 agosto 1997

Finlandia - Legge sulla tutela della privacy e della sicurezza dei dati nelle telecomunicazioni (n. 565/1999); Regolamento sulla sicurezza informatica degli operatori di telecomunicazioni, del 1999; Regolamento sulla protezione fisica degli ambienti e delle reti degli operatori di telecomunicazioni, del 1999

Germania - Legge sulle telecomunicazioni (*Telekommunikationsgesetz*) del 25 luglio 1996 e Regolamento sulla protezione dei dati (*Telekommunikationsdienstunternehmen* -

Datenschutzverordnung) del 12 luglio 1996

Italia — Decreto legislativo n. 171 del 13 maggio 1998

Portogallo — Legge n. 69/98, relativa al trattamento dei dati personali e alla tutela della riservatezza nel settore delle telecomunicazioni

Spagna — Decreto reale n. 1736/98 (di attuazione del titolo III della legge generale sulle telecomunicazioni)

Svezia — Legge sulle telecomunicazioni; Regolamento sui servizi telefonici.

Paesi nei quali la direttiva è stata recepita "in misura parziale"

Belgio — Legge sulle telecomunicazioni del 21 marzo 1991; decreto reale del 22 giugno 1998 (servizi telefonici) — Mancano: fatturazione dettagliata; dati sul traffico; chiamate indesiderate

Danimarca — Decreto sulla fornitura di reti e servizi di telecomunicazioni; Decreto sulle basi di dati dei servizi di ricerca abbonati — Mancano: chiamate indesiderate

Francia — Legge sulle telecomunicazioni (96-659; 90-1170) — Mancano: informativa abbonati su rischi sicurezza; fatturazione dettagliata; chiamate indesiderate

Paesi Bassi — Legge sulle telecomunicazioni; Regolamento sull'identificazione numerica del 1998 — Mancano: fatturazione; chiamate indesiderate

Regno Unito — Regolamento sulle telecomunicazioni (protezione dati e privacy; marketing diretto) del 1998 — Mancano: fatturazione dettagliata; chiamate indesiderate; identificazione linea chiamante

Paesi nei quali la direttiva non è stata sinora trasposta

Grecia

Irlanda

Lussemburgo

6.1 DISPOSIZIONI NORMATIVE

6.1.1 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

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-bis¹. 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;

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;

¹ Commi aggiunti dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

c-bis)² per scopi storici, di ricerca scientifica e di statistica in conformità alle leggi, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

5-ter³. 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;

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;

q-bis)³ è compreso nel programma statistico nazionale o in atti di programmazione statistica previsti dalla legge ed è effettuato in conformità alle leggi, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

² Lettera inserita dall'art. 2, comma 1, lett. a), d.l.g. 30 luglio 1999, n. 281.

³ Lettera inserita dall'art. 2, comma 1, lett. b), d.l.g. 30 luglio 1999, n. 281.

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.

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.

1-bis⁴ Il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi.

¹ Comma aggiunto dall'art. 3, d.lg. 30 luglio 1999, n. 281.

Art. 10.

(Informazioni rese al momento della raccolta)

1.⁵ 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. 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 regola-

⁵ Comma così modificato dall'art. 1, d.lg. 9 maggio 1997, n. 123.

mento 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 ed è effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31;

e) 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 comunicazione 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'interes-

* Lettera così sostituita dall'art. 4, comma 1, d.l.g. 30 luglio 1999, n. 281.

† Lettera così modificata dall'art. 12, comma 1, d.l.g. 13 maggio 1998, n. 171.

sato, 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;

c-bis) conservati o ceduti ad altro titolare, per scopi storici, di ricerca scientifica e di statistica, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.*

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.

* Lettera inserita dall'art. 5, d.lg. 30 luglio 1999, n. 281.

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)^{*} 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;
- 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 18 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)¹⁰ *qualora siano necessarie per finalità di ricerca scientifica o di statistica e siano effettuate nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31;*

^{*} Lettera così modificata dall'art. 12, comma 2, d.lg. 13 maggio 1998, n. 171.

¹⁰ Lettera così sostituita dall'art. 4, comma 2, d.lg. 30 luglio 1999, n. 281.

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)¹¹

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.

1-bis.¹² Il comma 1 non si applica ai dati relativi agli aderenti alle confessioni religiose i cui rapporti con lo Stato siano regolati da accordi o intese ai sensi degli articoli 7 e 8 della Costituzione, nonché relativi ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, che siano trattati dai relativi organi o enti civilmente riconosciuti, sempreché i dati non siano comunicati o diffusi fuori delle medesime confessioni.

Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati.

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.

3.¹³ 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. In mancanza di espressa disposizione di legge, e fuori dai casi previsti dai decreti legislativi di modificazione ed integrazione della presente legge, emanati in attuazione della legge 31 dicembre 1996, n. 676, i soggetti pubblici possono richiedere al Garante, nelle more della specificazione legislativa, l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono rilevanti finalità di interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi del comma 2, il trattamento dei dati indicati al comma 1.

3-bis.¹⁴ Nei casi in cui è specificata, a norma del comma 3, la finalità di rilevante interesse pubblico, ma non sono specificati i tipi di dati e le operazioni eseguibili, i soggetti pubblici, in applicazione di quanto previsto dalla presente legge e dai decreti legislativi di attuazione della legge 31 dicembre 1996, n. 676, in materia di dati sensibili, identificano e rendono pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando tale identificazione periodicamente.

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,

¹¹ Per quanto concerne il presente articolo, si richiama l'attenzione sul disposto dell'Articolo 17 ("Tutela della salute") del d.lg. 11 maggio 1999, n. 135, recante "Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici".

¹² Comma inserito dall'art. 5, comma 1, d.lg. 11 maggio 1999, n. 135.

¹³ Comma così sostituito dall'art. 5, comma 2, d.lg. 11 maggio 1999, n. 135.

¹⁴ Comma inserito dall'art. 5, comma 3, d.lg. 11 maggio 1999, n. 135.

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)¹⁵

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.

1-bis.¹⁶ Con decreto del Ministro della sanità adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentiti la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano e il Garante, sono individuate modalità semplificate per le informative di cui all'articolo 10 e per la prestazione del consenso nei confronti di organismi sanitari pubblici, di organismi sanitari e di esercenti le professioni sanitarie convenzionati o accreditati dal Servizio sanitario nazionale, nonché per il trattamento dei dati da parte dei medesimi soggetti, sulla base dei seguenti criteri:

a) previsione di informative effettuate da un unico soggetto, in particolare da parte del medico di medicina generale scelto dall'interessato, per conto di più titolari di trattamento;

b) validità, nei confronti di più titolari di trattamento, del consenso prestato ai sensi dell'articolo 11, comma 3, per conto di più titolari di trattamento, anche con riguardo alla richiesta di prestazioni specialistiche, alla prescrizione di farmaci, alla raccolta di dati da parte del medico di medicina generale detenuti da altri titolari, e alla pluralità di prestazioni mediche effettuate da un medesimo titolare di trattamento;

c) identificazione dei casi di urgenza nei quali, anche per effetto delle situazioni indicate nel comma 1-ter, l'informativa e il consenso possono intervenire successivamente alla richiesta della prestazione;

d) previsione di modalità di applicazione del comma 2 del presente articolo ai professionisti sanitari, diversi dai medici, che intrattengono rapporti diretti con i pazienti;

e) previsione di misure volte ad assicurare che nell'organizzazione dei servizi e delle prestazioni sia garantito il rispetto dei diritti di cui all'articolo 1.

1-ter.¹⁷ Il decreto di cui al comma 1 disciplina anche quanto previsto dall'articolo 22, comma 3-bis, della legge.

1-quater.¹⁸ In caso di incapacità di agire, ovvero di impossibilità fisica o di incapacità di intendere o di volere, il consenso al trattamento dei dati idonei a rivelare lo stato di salute è validamente manifestato nei confronti di esercenti le professioni sanitarie e di organismi sanitari, rispettivamente, da chi esercita legalmente la potestà ovvero da un familiare, da un prossimo congiunto, da un convivente, o, in loro assenza, dal responsabile della struttura presso cui dimori.

2.¹⁹ I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui al comma 1-ter solo per il tramite di un medico designato dall'interessato o dal titolare.

¹⁵ Si richiama l'attenzione sul disposto dell'art. 17 ("Tutela della salute") del d.lg. 11 maggio 1999, n. 135, recante "Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici".

¹⁶ Commi inseriti dall'art. 2, comma 1, d.lg. 30 luglio 1999, n. 282.

¹⁷ Comma così modificato dall'art. 2, comma 2, d.lg. 30 luglio 1999, n. 282.

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)

1.¹⁸ 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.

2.¹⁹ 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).

4.²⁰ 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.²¹ 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 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.

¹⁸ Comma così sostituito dall'art. 12, comma 3, d.lg. 13 maggio 1998, n. 171.

¹⁹ Comma così modificato dall'art. 12, comma 4, d.lg. 13 maggio 1998, n. 171.

²⁰ Comma così modificato dall'art. 2, comma 1, d.lg. 9 maggio 1997, n. 123.

²¹ Comma aggiunto dall'art. 2, comma 2, d.lg. 9 maggio 1997, n. 123.

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;

g-bis)²² il trattamento sia finalizzato unicamente a scopi di ricerca scientifica o di statistica e sia effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

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 *trenta*²³ giorni dalla data di presentazione, equivale a rigetto.

²² Lettera inserita dall'art. 4, comma 3, d.lg. 30 luglio 1999, n. 281.

²³ Parola così sostituita dall'art. 13, comma 1, lett. a), d.lg. 30 luglio 1999, n. 281.

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.

6-bis²⁴. Il decorso dei termini previsti dai commi 4, 5 e 6 è sospeso di diritto dal 18 al 30 agosto di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Ove il decorso abbia inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussista il pregiudizio di cui al comma 2 e non preclude l'adozione dei provvedimenti di cui al comma 5.

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 PERSONALI²⁵

Art. 30.

(Istituzione del Garante)

1.²⁶ 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 retribu-

²⁴ Comma inserito dall'art. 13, comma 1, lett. b), d.lg. 30 luglio 1999, n. 281.

²⁵ Denominazione così modificata dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123.

²⁶ Comma così modificato dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123.

zione 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;
 - 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, ²⁷ 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

²⁷ Parole inserite dall'art. 1, comma 1, d.lg. 26 febbraio 1999, n. 51.

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. ⁽²⁸⁾ ⁽²⁹⁾ 1-bis. ⁽³⁰⁾ 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-ter.³⁰ 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 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.³¹ 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.³¹ 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.³¹ 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.

28 Parole aggiunte dall'art. 3, comma 2, d.lg. 9 maggio 1997, n. 123.

29 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."

30 Commi aggiunti dall'art. 1, comma 2, d.lg. 26 febbraio 1999, n. 51.

31 Commi aggiunti dall'art. 2, comma 1, d.lg. 26 febbraio 1999, n. 51.

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.

3.³² 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'articolo 13, nonché della notificazione di cui all'articolo 7, 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.³³

3-bis.³⁴ 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.

4.³⁵ 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.³⁶ 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.

³² Comma così modificato dall'art. 2, comma 2, d.lg. 26 febbraio 1999, n. 51.

³³ 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."

³⁴ Comma inserito dall'art. 2, comma 3, d.lg. 26 febbraio 1999, n. 51.

³⁵ Comma così modificato dall'art. 2, comma 4, d.lg. 26 febbraio 1999, n. 51.

³⁶ Comma aggiunto dall'art. 2, comma 5, d.lg. 26 febbraio 1999, n. 51.

CAPO VIII
SANZIONI

Art. 34.

(Omessa o infedele notificazione)

1. Chiunque, essendovi tenuto, 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.

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 paga-

mento 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.

3.⁷ 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. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 33, comma 2, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 31, comma 1, lettera i) e 32.

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. ⁸ 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.

5.⁹ 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.

7.¹⁰ 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'ar-

⁷ Comma così modificato dall'art. 14, d.lg. 30 luglio 1999, n. 281.

⁸ Comma così sostituito dall'art. 2, d.lg. 28 luglio 1997, n. 255.

⁹ Comma da ultimo così modificato dall'art. 1, comma 1, d.lg. 6 novembre 1998, n. 389.

¹⁰ Comma così sostituito dall'art. 4, comma 1, d.lg. 9 maggio 1997, n. 123.

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.⁴¹ 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. ⁴²Il controllo sul Centro elaborazione dati è esercitato dal *Garante per la protezione dei dati personali*, nei modi previsti dalla legge e dai regolamenti.

2. ⁴²I 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. ⁴²Esperiti 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 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

⁴¹ Comma aggiunto dall'art. 4, comma 2, d.lg. 9 maggio 1997, n. 123.

⁴² Comma così modificato dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

tenendo conto dei limiti di incremento previsti per la categoria IV per il triennio 1996-1998.”.

4.^a 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.

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.

6.1.2 **Decreto Legislativo 11 maggio 1999, n. 135**
 (con aggiornamenti)

Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Visto l'articolo 14 della legge 23 agosto 1988, n. 400;

Vista la legge 31 dicembre 1996, n. 675, e successive modifiche ed integrazioni;

Vista la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e le raccomandazioni del Consiglio d'Europa ivi citate;

Vista la legge 6 ottobre 1998, n. 344;

Visto il decreto legislativo 6 novembre 1998, n. 389;

Sentito il Garante per la protezione dei dati personali;

Sentita l'Autorità per l'informatica nella pubblica amministrazione;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 21 aprile 1999;

Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 7 maggio 1999;

Sulla proposta del Presidente del Consiglio dei Ministri, di concerto con i Ministri per la funzione pubblica, per la solidarietà sociale, di grazia e giustizia, dell'interno, degli affari esteri, delle finanze, del tesoro, del bilancio e della programmazione economica, per i beni e le attività culturali, della sanità, della pubblica istruzione e dell'università e della ricerca scientifica e tecnologica;

EMANA

il seguente decreto legislativo:

CAPO I

PRINCIPI GENERALI IN MATERIA DI TRATTAMENTO
DI DATI PARTICOLARI DA PARTE DI SOGGETTI PUBBLICI

Art. 1.

(Ambito di applicazione e definizioni)

1. Il presente decreto:

a) definisce i principi generali in base ai quali i soggetti pubblici sono autorizzati a trattare dati sensibili o attinenti a particolari provvedimenti giudiziari ai sensi degli articoli 22, comma 3, e 24 della legge 31 dicembre 1996, n. 675, nel rispetto delle altre disposizioni previste dalla medesima legge;

b) individua, inoltre, alcune rilevanti finalità di interesse pubblico, per il cui perseguimento è consentito detto trattamento, nonché le operazioni eseguibili e i tipi di dati che possono essere trattati.

2. Il presente decreto non si applica:

- a) ai trattamenti di cui all'articolo 4 della legge 31 dicembre 1996, n. 675, e all'articolo 1, comma 1, lettera i), della legge 31 dicembre 1996, n. 676;
- b) agli enti pubblici economici, ai quali restano applicabili le disposizioni previste per i soggetti privati, ai sensi della legge 31 dicembre 1996, n. 675;
- c) ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale, in conformità ai rispettivi ordinamenti.

3. Ai fini del presente decreto:

- a) si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata «legge»;
- b) per «dati» si intendono i dati sensibili o attinenti a provvedimenti giudiziari indicati negli articoli 22, comma 1, e 24 della legge.

4. Salvo quanto previsto dal comma 2, i principi di cui al presente Capo si applicano in ogni caso di trattamento dei dati comunque effettuato da soggetti pubblici.

5. Resta fermo quanto previsto dall'articolo 1, lettera b), n. 1), della legge 31 dicembre 1996, n. 676, e dall'articolo 1, comma 2, della legge 8 aprile 1998, n. 94, per la compiuta disciplina della riservatezza dei dati personali in ambito sanitario.

Art. 2.

(Modalità del trattamento e informativa agli interessati)

1. I soggetti pubblici effettuano il trattamento dei dati con modalità atte ad assicurare il rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato; adottano, inoltre, le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'articolo 13 della legge.

2. Nell'informare gli interessati ai sensi dell'articolo 10 della legge, i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento.

Art. 3.

(Dati trattati)

1. I soggetti pubblici sono autorizzati a trattare i soli dati essenziali per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2. I dati sono raccolti, di regola, presso l'interessato.

3. Ai sensi dell'articolo 9, comma 1, lettera c), d) ed e), della legge, i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati siano strettamente pertinenti e non eccedenti rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

4. I dati contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi che, considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di necessità.

5. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo. Al trattamento di tali dati si procede con le modalità di cui al comma 4 anche quando detti dati non sono contenuti in elenchi, registri o banche dati o non sono tenuti con l'ausilio di mezzi elettronici o comunque automatizzati.

6. I dati non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato.

Art. 4.

(Operazioni eseguibili)

1. Rispetto ai dati la cui disponibilità è essenziale ai sensi dell'articolo 3, comma 1, i soggetti pubblici sono autorizzati a svolgere unicamente le operazioni di trattamento strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi esercitati anche su richiesta di altri soggetti.

2. Le operazioni di raffronto tra dati, nonché i trattamenti di dati ai sensi dell'articolo 17 della legge, sono effettuati solo con l'indicazione scritta dei motivi.

3. In ogni caso, la diffusione dei dati, nonché le operazioni e i trattamenti di cui al comma 2, se effettuati utilizzando banche dati di diversi titolari, sono ammessi solo se previsti da espressa disposizione di legge.

4. Resta fermo il divieto di diffusione dei dati idonei a rivelare lo stato di salute sancito dall'articolo 23, comma 4, della legge.

Art. 5.

(Modificazioni alla legge 31 dicembre 1996, n. 675)

1. Dopo il comma 1 dell'articolo 22 della legge è inserito il seguente:

«1-bis. Il comma 1 non si applica ai dati relativi agli aderenti alle confessioni religiose i cui rapporti con lo Stato siano regolati da accordi o intese ai sensi degli articoli 7 e 8 della Costituzione, nonché relativi ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, che siano trattati dai relativi organi o enti civilmente riconosciuti, sempreché i dati non siano comunicati o diffusi fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati».

2. Il comma 3 dell'articolo 22 della legge è sostituito dal seguente:

«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 tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite. In mancanza di espressa disposizione di legge, e fuori dai casi previsti dai decreti legislativi di modificazione ed integrazione della presente legge, emanati in attuazione della legge 31 dicembre 1996, n. 676, i soggetti pubblici possono richiedere al Garante, nelle more della specificazione legislativa, l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono rilevanti finalità di interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi del comma 2, il trattamento dei dati indicati al comma 1.

3. Dopo il comma 3 dell'articolo 22 della legge è inserito il seguente:

«3-bis. Nei casi in cui è specificata, a norma del comma 3, la finalità di rilevante interesse pubblico, ma non sono specificati i tipi di dati e le operazioni eseguibili, i soggetti pubblici, in applicazione di quanto previsto dalla presente legge e dai decreti legislativi di attuazione della legge 31 dicembre 1996, n. 676, in materia di dati sensibili, identificano e rendono pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando tale identificazione periodicamente».

4. I soggetti pubblici avviano l'adeguamento dei propri ordinamenti a quanto previsto dai commi 3 e 3-bis dell'articolo 22 della legge, introdotto dal comma 3 del presente articolo entro il 31 dicembre 1999. Per le richieste presentate al Garante, a norma del comma 3 dell'articolo 22 della legge, come modificato dal presente decreto, entro il 31 dicembre 1999, il termine per la decisione del Garante medesimo è di novanta giorni, durante i quali il trattamento dei dati già in corso può essere proseguito sino alla decisione.

5. I provvedimenti di cui all'articolo 22, comma 3-bis, della legge, introdotto dal comma 3 del pre-

sente articolo, costituiscono attuazione dei principi di cui agli articoli da 1 a 4 del presente decreto.

«5-bis. In relazione alle finalità individuate nel Capo II, i soggetti pubblici identificano e rendono pubblici con le modalità di cui ai commi 4 e 5 e nel rispetto delle disposizioni di cui al Capo I del presente decreto, anche i tipi di dati e di operazioni oggetto del trattamento di cui all'articolo 24 della legge».

CAPO II INDIVIDUAZIONE DI ALCUNE RILEVANTI FINALITÀ DI INTERESSE PUBBLICO

Art. 6.

(Stato civile, anagrafi e liste elettorali)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati concernenti la tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, nonché delle liste elettorali.

Art. 7.

(Cittadinanza, immigrazione e condizione dello straniero)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività dirette all'applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e di profugo e sullo stato di rifugiato.

2. Le disposizioni del presente Capo non riguardano i trattamenti di dati effettuati in esecuzione della convenzione di cui alla legge 23 marzo 1998, n. 93, o dell'accordo di cui all'articolo 4, comma 1, lettera a), della legge, ovvero previsti dalla lettera e) del medesimo articolo.

3. Per le finalità di cui al comma 1 è, in particolare, ammesso il trattamento dei dati strettamente necessari:

a) al rilascio di visti, permessi, attestazioni, autorizzazioni e documenti anche sanitari, nonché alla tenuta di registri;

b) al riconoscimento del diritto di asilo o dello stato di rifugiato, o all'applicazione della protezione temporanea e di altri istituti o misure di carattere umanitario, ovvero all'attuazione degli obblighi di legge in materia di politiche migratorie;

c) agli obblighi dei datori di lavoro e dei lavoratori, ai ricongiungimenti, all'applicazione delle norme vigenti in materia di istruzione e di alloggio, alla partecipazione alla vita pubblica e all'integrazione sociale.

Art. 8.

(Esercizio dei diritti politici e pubblicità dell'attività di determinati organi)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività dirette all'applicazione della disciplina in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché all'esercizio del mandato degli organi rappresentativi.

2. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività dirette all'applicazione della disciplina in materia di documentazione dell'attività istituzionale di organi pubblici.

3. I trattamenti dei dati per le finalità di cui ai commi 1 e 2 sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti:

- a) lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità;
- b) le richieste di referendum, le relative consultazioni e la verifica della relativa regolarità;
- c) l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi;
- d) l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni d'inchiesta, il rapporto con gruppi politici;
- e) la designazione e la nomina di rappresentanti in commissioni, enti e uffici.

4. Ai fini del presente articolo, è consentita la diffusione dei dati per le finalità di cui al comma 1, in particolare con riguardo alle sottoscrizioni di liste, alle presentazioni delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti.

5. Ai fini del presente articolo, in particolare, sono consentiti:

- a) il trattamento di dati contenuti in verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
- b) il trattamento dei dati strettamente necessario allo svolgimento della funzione di controllo, di indirizzo politico e di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo.

6. I dati trattati per le finalità di cui ai commi 1 e 2 possono essere comunicati e diffusi nelle forme previste dai rispettivi ordinamenti anche per via telematica. Non è comunque consentita la divulgazione dei dati che non risultino strettamente necessari ad assicurare il rispetto del principio di pubblicità dell'attività istituzionale, fermo restando quanto previsto dall'articolo 23, comma 4, della legge per i dati idonei a rivelare lo stato di salute.

Art. 9.

(Rapporti di lavoro)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività dirette all'instaurazione ed alla gestione di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli svolti al fine di:

- a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;
- b) garantire le pari opportunità;
- c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;
- d) adempiere obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corrispondenza di premi e benefici assistenziali;
- e) adempiere specifici obblighi o compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;
- f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche per via telematica, agli istituti di patronato ed assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato in relazione a tipi di dati individuati specificamente;
- g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile

ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;

h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;

i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;

j) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;

k) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;

l) svolgere l'attività di indagine e ispezione presso soggetti pubblici;

m) valutare la qualità dei servizi resi e dei risultati conseguiti.

3. I dati raccolti mediante impianti audiovisivi o altre apparecchiature, anche informatiche o telematiche, richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, possono essere utilizzati unicamente per tali finalità, individuate secondo le procedure di cui all'articolo 4 della legge 20 maggio 1970, n. 300, e all'articolo 24 della legge 29 marzo 1983, n. 93. Gli interessati sono edotti delle modalità di tale trattamento, anche attraverso l'informativa di cui all'articolo 10 della legge.

4. La diffusione dei dati di cui alle lettere da k) a m) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

Art. 10.

(Materia tributaria e doganale)

1. Ai sensi dell'articolo 1 si considerano di rilevante interesse pubblico le attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonché in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane.

2. Ai sensi dell'articolo 1 del presente decreto, si considerano, inoltre, di rilevante interesse pubblico le attività dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi ed all'adozione dei provvedimenti previsti da leggi, regolamenti o normativa comunitaria, nonché al controllo ed all'esecuzione forzata dell'esatto adempimento di tali obblighi, all'effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari.

Art. 11.

(Attività di controllo e ispettive)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le finalità di verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti.

2. Nell'esercizio di tali funzioni, i soggetti di cui al comma 1 possono effettuare trattamenti dei dati legittimamente trattati presso i soggetti controllati.

3. Ai sensi dell'articolo 1 si considerano altresì di rilevante interesse pubblico le attività di accertamento, nei limiti delle proprie finalità istituzionali, con riferimento a dati relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'articolo 8, comma 5.

Art. 12.

(Istruzione)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività di istruzione e di formazione, in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata.

Art. 13.

(Benefici economici e abilitazioni)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività dirette all'applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.

2. Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli necessari relativi a:

- a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia;
- b) all'elargizioni di contributi previsti dalla normativa in materia di usura e antiracket;
- c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti;
- d) al riconoscimento di benefici connessi all'invalidità civile;
- e) alla concessione di contributi in materia di formazione professionale;
- f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;
- g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da regolamento o dalla normativa comunitaria.

4. Il trattamento può comprendere la diffusione nei soli casi in cui ciò sia indispensabile per la trasparenza delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguente alle attività medesime.

Art. 14.

(Onorificenze, ricompense e riconoscimenti)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le attività dirette all'applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilità e di professionalità per le nomine, per quanto di propria competenza, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché di rilascio e revoca di titoli autorizzatori o abilitativi, di concessione di patroncini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali.

Art. 15.

(Volontariato e obiezione di coscienza)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati volti all'applicazione della disciplina in materia di rapporti tra i soggetti pubblici e le organizzazioni di volontariato, in particolare per quanto riguarda l'elargizione di contributi finalizzati al loro sostegno, la tenuta dei registri generali delle medesime organizzazioni e la cooperazione internazionale.

2. Si considerano parimenti di rilevante interesse pubblico le attività dirette all'applicazione della legge 8 luglio 1998, n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza.

Art. 16.

(Attività sanzionatorie e di predisposizione di elementi di tutela in sede amministrativa o giurisdizionale)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati:

- a) volti all'applicazione delle norme in materia di sanzioni amministrative e ricorsi;
- b) necessari per far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da

parte di un terzo, o per ciò che attiene alla riparazione di un errore giudiziario o di un'ingiusta restrizione della libertà personale;

c) effettuati in conformità alle leggi e ai regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi.

2. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se il diritto da far valere o difendere, di cui alla lettera b) del comma 1, è di rango almeno pari a quello dell'interessato.

Art. 17.

(Tutela della salute)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico le seguenti attività rientranti nei compiti del servizio sanitario nazionale e degli altri organismi sanitari pubblici, nel rispetto dell'articolo 23, comma 1, della legge:

a) la prevenzione, la diagnosi, la cura e la riabilitazione dei soggetti assistiti dal servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché l'assistenza sanitaria erogata al personale navigante ed aeroportuale;

b) la programmazione, la gestione, il controllo e la valutazione dell'assistenza sanitaria;

c) la vigilanza sulle sperimentazioni, la farmacovigilanza, l'autorizzazione all'immissione in commercio ed all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

d) le attività certificatorie;

e) il monitoraggio epidemiologico, ivi compresi la sorveglianza della emergenza o riemergenza delle malattie, e degli eventi avversi nelle vaccinazioni, i registri di patologia e la gestione della profilassi internazionale;

f) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;

g) i trapianti d'organo e le trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;

h) l'instaurazione, la gestione, la pianificazione ed il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.

2. L'identificazione dell'interessato è riservata ai soggetti che perseguono direttamente le finalità di cui al comma 1. L'accesso alle diverse tipologie di dati è consentito ai soli incaricati del trattamento, preposti caso per caso, alle specifiche fasi delle attività di cui al comma 1, secondo il principio della pertinenza dei dati di volta in volta trattati.

3. Per quanto non previsto dal decreto di cui all'articolo 23, comma 1-bis della legge, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale da parte di organismi sanitari e di esercenti le professioni sanitarie è fatto oggetto di appositi codici di deontologia e buona condotta adottati ai sensi dell'articolo 31, comma 1, lettera h), della legge dalle federazioni nazionali degli ordini e dei collegi delle professioni sanitarie, la cui accettazione è condizione essenziale per il trattamento dei dati da parte degli incaricati del trattamento. Il codice prevede anche:

a) l'impegno al rispetto di regole di condotta analoghe al segreto professionale da parte degli incaricati del trattamento che non sono tenuti in base alla legge al segreto professionale;

b) le modalità di applicazione dell'articolo 23, comma 2, della legge ai professionisti sanitari, diversi dai medici, che intrattengono rapporti diretti con i pazienti;

c) modalità semplificate per l'informativa agli interessati e per la prestazione del loro consenso;

c-bis) identificazione dei casi di urgenza nei quali l'informativa e il consenso possono intervenire successivamente alla richiesta della prestazione.

4. Con i decreti di cui all'articolo 15, commi 2 e 3, della legge, sono individuate le misure minime per garantire la sicurezza dei trattamenti effettuati con tecniche di cifratura o mediante codici identificativi, anche al fine di assicurare il trattamento disgiunto dei dati di cui al comma 3 dagli altri dati personali che permettono di identificare direttamente gli interessati.

5. Il trattamento dei dati genetici è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante, sentito il Ministro della sanità, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità. I trattamenti autorizzati dal Garante possono essere proseguiti fino al rilascio dell'autorizzazione prevista dal presente comma, che in sede di prima applicazione della presente disposizione è rilasciata entro dodici mesi dalla data della relativa entrata in vigore.

Art. 18.

(Interruzione volontaria della gravidanza)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati volti all'applicazione della disciplina in materia di tutela sociale della maternità e sull'interruzione volontaria della gravidanza, con particolare riferimento ai trattamenti svolti per:

- a) la gestione dei consultori familiari;
- b) l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza.

Art. 19.

(Tossicodipendenze)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati volti all'applicazione della disciplina in materia di stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare quelli svolti al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti e gli interventi preventivi, curativi e riabilitativi previsti dalle leggi e di applicare le misure amministrative previste.

Art. 20.

(Portatori di handicap)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati volti all'applicazione della disciplina in materia di assistenza, integrazione sociale e diritti delle persone handicappate.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, anche quelli svolti al fine di:

- a) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni;
- b) assicurare adeguata informazione alla famiglia della persona handicappata;
- c) curare l'integrazione sociale, l'educazione e l'istruzione del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge;
- d) realizzare comunità-alloggio e centri socio riabilitativi;
- e) curare la tenuta degli albi regionali degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.

Art. 21.

(Rapporti con enti di culto)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati strettamente necessari allo svolgimento dei rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose.

Art. 22.

(Statistica)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti svolti dai soggetti pubblici che fanno parte del sistema statistico nazionale ai sensi del decreto legislativo 6 settembre 1989, n. 322.

Art. 23.

(Ricerca storica e archivi)

1. Ai sensi dell'articolo 1, si considerano di rilevante interesse pubblico i trattamenti di dati a fini storici, di studio, di ricerca e di documentazione, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti conservati negli archivi di Stato e negli archivi storici degli enti pubblici, secondo quanto disposto dal decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, e successive modificazioni e integrazioni.

Art. 24.

(Entrata in vigore)

1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

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.

6.1.3 Decreto Legislativo 30 luglio 1999, n. 281

Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Visto l'articolo 14 della legge 23 agosto 1988, n. 400;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni;

Vista la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e le raccomandazioni del Consiglio d'Europa ivi citate;

Visto il decreto legislativo 11 maggio 1999, n. 135;

Vista la legge 6 ottobre 1998, n. 344;

Visto il decreto legislativo 5 giugno 1998, n. 204;

Visto il decreto legislativo 6 settembre 1989, n. 322;

Sentito il Garante per la protezione dei dati personali;

Vista la deliberazione preliminare del Consiglio dei Ministri adottata nella riunione del 2 luglio 1999;

Acquisito il parere delle competenti commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 29 luglio 1999;

Sulla proposta del Presidente del Consiglio dei Ministri, di concerto con i Ministri per i beni e le attività culturali, dell'università e della ricerca scientifica e tecnologica, di grazia e giustizia e dell'interno;

EMANA

il seguente decreto legislativo:

CAPO I**DISPOSIZIONI COMUNI****Art. 1.**

(Ambito di applicazione e definizioni)

1. Il presente decreto disciplina le modalità di trattamento dei dati personali utilizzati per scopi storici, di ricerca scientifica e di statistica, e individua alcune garanzie per il rispetto dei diritti e delle libertà fondamentali degli interessati, tenendo conto dei principi contenuti nelle raccomandazioni del Consiglio d'Europa n. R (83)10, adottata il 23 settembre 1983, e n. R (97) 18 adottata il 30 settembre 1997.

2. Ai fini del presente decreto e delle disposizioni da esso modificate, si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata "legge", e si intendono per:

a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "scopi di ricerca scientifica", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;

c) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici.

3. Ai trattamenti di cui al presente decreto restano applicabili le disposizioni del decreto 11 maggio 1999, n. 135, relativamente ai soggetti in detto decreto indicati.

Art. 2.

(Notificazione)

1. All'articolo 7 della legge sono apportate le seguenti modifiche:

a) nel comma 5-bis, dopo la lettera c), è inserita la seguente lettera:

"c-bis) per scopi storici, di ricerca scientifica e di statistica in conformità alle leggi, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31";

b) nel comma 5-ter, dopo la lettera q), è inserita la seguente lettera:

"q-bis) è compreso nel programma statistico nazionale o in atti di programmazione statistica previsti dalla legge ed è effettuato in conformità alle leggi, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31".

Art. 3.

(Compatibilità tra gli scopi e durata del trattamento)

1. All'articolo 9 della legge, dopo il comma 1 è aggiunto il seguente comma:

"1-bis. Il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi."

Art. 4.

(Presupposti del trattamento e casi di esclusione del consenso)

1. La lettera d) dell'articolo 12, comma 1, della legge, è sostituita dalla seguente:

"d) è finalizzato unicamente a scopi di ricerca scientifica o di statistica ed è effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31".

2. La lettera a) dell'articolo 21, comma 4, della legge, è sostituita dalla seguente:

"a) qualora siano necessarie per finalità di ricerca scientifica o di statistica e siano effettuate nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31".

3. Nell'articolo 28, comma 4, della legge, dopo la lettera g) è inserita la seguente lettera:

"g-bis) il trattamento sia finalizzato unicamente a scopi di ricerca scientifica o di statistica e sia effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31".

Art. 5.

(Cessazione del trattamento e conservazione dei dati)

Nel comma 2 dell'articolo 16 della legge 31 dicembre 1996, n. 675, è inserita, in fine, la seguente lettera:

"c-bis) conservati o ceduti ad altro titolare, per scopi storici, di ricerca scientifica e di statistica, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31".

Art. 6.

(Codici di deontologia e di buona condotta)

1. Ai sensi dell'articolo 31, comma 1, lettera h), della legge, entro sei mesi dalla data di entrata in vigore del presente decreto, il Garante promuove la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per gli scopi indicati nell'articolo 1 del presente decreto, tenendo conto della specificità dei trattamenti nei diversi ambiti. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante.

2. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità del trattamento dei dati.

CAPO II

TRATTAMENTI PER SCOPI STORICI

Art. 7.

(Modalità di trattamento e codici di deontologia e di buona condotta)

1. I dati personali raccolti per scopi storici non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 9 della legge.

2. I documenti trattati per scopi storici possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento dei predetti scopi. I dati personali possono essere diffusi solo se pertinenti utilizzati per il perseguimento dei medesimi scopi.

3. I dati personali possono essere comunque diffusi qualora siano relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico.

4. Le disposizioni dell'articolo 4 si applicano anche agli archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 36 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409.

5. Il codice di deontologia e di buona condotta per i trattamenti a scopi storici effettuati da archivisti e utenti individua, in particolare:

a) le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni della legge applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero;

b) le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati;

c) le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a scopi storici, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 8.

(Consultabilità di documenti)

1. Nell'articolo 2 del decreto del Presidente della Repubblica 30 dicembre 1975, n. 854, recante "Attribuzioni del Ministero dell'interno in materia di documenti archivistici non ammessi alla libera consultabilità", è inserito, in ultimo, il seguente comma:

"Con decreto del Ministro dell'interno è istituita la commissione per le questioni inerenti alla consultabilità degli atti d'archivio riservati. La commissione fornisce la consulenza al Ministro nel-

l'analisi comparativa degli interessi alla accessibilità degli atti e la tutela della riservatezza individuale. Nella composizione della commissione è assicurata la partecipazione di un rappresentante del Ministero per i beni e le attività culturali".

2. All'articolo 21 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, recante "Norme relative all'ordinamento ed al personale degli Archivi di Stato", sono apportate le seguenti modifiche:

a) nel primo comma, le parole da: ", e di quelli riservati relativi a situazioni puramente private" fino alla fine del comma sono sostituite dalle seguenti: "e di quelli contenenti i dati di cui agli articoli 22 e 24 della legge 31 dicembre 1996, n. 675, che diventano liberamente consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute o la vita sessuale o rapporti riservati di tipo familiare. Anteriormente al decorso dei termini di cui al presente comma, i documenti restano accessibili ai sensi della disciplina sull'accesso ai documenti amministrativi; sull'istanza di accesso provvede l'amministrazione che deteneva il documento prima del versamento o del deposito";

b) il secondo comma è sostituito dal seguente: "Il Ministro dell'interno, previo parere del direttore dell'Archivio di Stato competente e udita la commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati istituita presso il Ministero dell'interno, può permettere, se necessario per scopi storici, la consultazione di documenti di carattere riservato anche prima della scadenza dei termini indicati nel comma precedente. In tal caso l'autorizzazione è rilasciata, a parità di condizioni, ad ogni altro richiedente."

c) nel terzo comma, sono aggiunte in fine le parole: "nonché dell'articolo 21-bis".

Art. 9.

*(Comunicazione e diffusione di dati
consultabili presso l'Archivio centrale dello Stato e gli Archivi di Stato)*

1. Dopo l'articolo 21 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, recante "Norme relative all'ordinamento ed al personale degli Archivi di Stato", è inserito il seguente:

Art. 21-bis

(Trattamento di dati personali per scopi storici)

1. I documenti per i quali è autorizzata la consultazione ai sensi dell'articolo 21, secondo comma, conservano il loro carattere riservato e non possono essere diffusi.

2. I documenti detenuti presso l'Archivio centrale dello Stato e gli Archivi di Stato sono conservati e consultabili anche in caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 13 della legge 31 dicembre 1996, n. 675, qualora ciò risulti necessario per scopi storici. Ai documenti è allegata la documentazione relativa all'esercizio dei diritti. Su richiesta di chiunque vi abbia interesse ai sensi del medesimo articolo 13, può essere comunque disposto il blocco dei dati personali, qualora il loro trattamento comporti un concreto pericolo di lesione della dignità, della riservatezza o dell'identità personale degli interessati e i dati non siano di rilevante interesse pubblico".

3. Nell'articolo 22 del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, recante "Norme relative all'ordinamento ed al personale degli Archivi di Stato", sono apportate le seguenti modifiche:

a) nella rubrica, le parole: "nell'articolo precedente" sono sostituite dalle seguenti: "negli articoli 21 e 21-bis";

b) nel primo comma, le parole: "dell'articolo precedente" sono sostituite dalle seguenti: "degli articoli 21 e 21-bis";

c) nel primo comma, è inserita in fine la seguente lettera:

"b-bis) agli archivi privati utilizzati per scopi storici, secondo le modalità individuate, nel rispetto della normativa in materia di protezione dei dati personali, dal codice di deontologia e di buona condotta sottoscritto ai sensi dell'articolo 31, comma 1, lettera h), della legge 31 dicembre 1996, n. 675".

CAPO III
TRATTAMENTI PER SCOPI STATISTICI E DI RICERCA SCIENTIFICA

Art. 10.

(Modalità di trattamento e codici di deontologia)

1. Le disposizioni del presente capo si applicano ai trattamenti di dati per scopi statistici e, in quanto applicabili, di ricerca scientifica.

2. Gli scopi statistici e di ricerca scientifica devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui all'articolo 10 della legge anche in relazione a quanto previsto dal comma 6, lettera b) e dall'articolo 6-bis del decreto legislativo 6 settembre 1989, n. 322, introdotto dall'articolo 11 del presente decreto.

3. I dati personali trattati per scopi statistici e di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura.

4. Fermo restando quanto previsto dall'articolo 22, commi 3 e 3-bis, della legge e fuori dei casi di particolari indagini statistiche o di ricerca scientifica previste per legge, il consenso per il trattamento dei dati di cui al medesimo articolo 22 può essere prestato con modalità semplificate individuate dal codice deontologico e l'autorizzazione del Garante può essere rilasciata anche ai sensi dell'articolo 41, comma 7, della legge.

5. Agli effetti dell'applicazione del presente Capo, per "dati identificativi" si intendono i dati personali che permettono l'identificazione diretta dell'interessato. Per quanto riguarda l'identificabilità dell'interessato si osserva quanto previsto ai sensi del comma 6, lettera c).

6. Con uno o più codici di deontologia e di buona condotta per il trattamento a scopi statistici e di ricerca scientifica in ambito pubblico e privato sono individuati, tenendo conto, per i soggetti già compresi nell'ambito del Sistema statistico nazionale, di quanto già previsto dal decreto legislativo 6 settembre 1989, n. 322, in particolare:

a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal decreto legislativo 6 settembre 1989, n. 322, siano svolti per idonei ed effettivi scopi statistici e di ricerca scientifica;

b) per quanto non previsto dalla legge e dal presente decreto, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalità per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle raccomandazioni di cui all'articolo 1;

c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare l'interessato, anche in base alle conoscenze acquisite in base al progresso tecnico;

d) le garanzie da osservare ai fini dell'applicazione delle disposizioni di cui agli articoli 12, comma 1, lettera d) e 21, comma 4, lettera a), della legge che permettono di prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle raccomandazioni di cui all'articolo 1;

e) modalità semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati di cui all'articolo 22, comma 1, della legge;

f) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire al personale incaricato;

g) le misure da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'articolo 15 della legge, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche non incaricate del trattamento e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per scopi statistici e di ricerca scientifica da effettuarsi con enti ed uffici situati all'estero anche sulla base delle garanzie previste dall'ar-

ticolo 28, comma 4, lettera g), della legge;

h) l'impegno al rispetto di regole di condotta degli incaricati del trattamento che non sono tenuti in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.

Art. 11.

(Disposizioni sul Sistema statistico nazionale)

1. Dopo l'articolo 6 del decreto legislativo 6 settembre 1989, n. 322, recante "Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400", è inserito il seguente:

Art. 6-bis

(Trattamenti di dati personali)

1. I soggetti che fanno parte o partecipano al Sistema statistico nazionale possono raccogliere ed ulteriormente trattare i dati personali necessari per perseguire gli scopi statistici previsti dal presente decreto, dalla legge o dalla normativa comunitaria, qualora il trattamento di dati anonimi non permetta di raggiungere i medesimi scopi.

2. Nel programma statistico nazionale sono illustrate le finalità perseguite e le garanzie previste dal presente decreto e dalla legge 31 dicembre 1996, n. 675. Il programma indica anche i dati di cui agli articoli 22 e 24 della medesima legge, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento. Il programma è adottato sentito il Garante per la protezione dei dati personali.

3. Quando sono raccolti per altri scopi, i dati personali possono essere ulteriormente trattati per scopi statistici, se ciò è previsto dal presente decreto, dalla legge, dalla normativa comunitaria o da un regolamento.

4. I dati personali raccolti specificamente per uno scopo statistico possono essere trattati dai soggetti di cui al comma 1 per altri scopi statistici di interesse pubblico previsti ai sensi del comma 3, quando questi ultimi sono chiaramente determinati e di limitata durata. Tale eventualità, al pari di quella prevista dal medesimo comma 3, è chiaramente rappresentata agli interessati al momento della raccolta o, quando ciò non è possibile, è resa preventivamente nota al pubblico e al Garante nei modi e nei termini previsti dal codice di deontologia e di buona condotta.

5. I dati personali sono resi anonimi dopo la raccolta o quando la loro disponibilità non sia più necessaria per i propri trattamenti statistici.

6. I dati identificativi, qualora possano essere conservati, sono custoditi separatamente da ogni altro dato personale salvo che ciò, in base ad un atto motivato per iscritto, risulti impossibile in ragione delle particolari caratteristiche del trattamento o comporti un impiego di mezzi manifestamente sproporzionato. I dati personali trattati per scopi statistici sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

7. I dati identificativi, qualora possano essere conservati, sono abbinabili ad altri dati, sempre che l'abbinamento sia temporaneo ed essenziale per i propri trattamenti statistici.

8. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 13 della legge 31 dicembre 1996, n. 675, l'aggiornamento, la rettificazione o l'integrazione dei dati sono annotate senza modificare questi ultimi qualora il risultato di tali operazioni non produca effetti significativi sull'analisi statistica o sui risultati statistici".

Art. 12.

(Modifiche a disposizioni vigenti)

1. Il comma 2 dell'articolo 7 del decreto legislativo 6 settembre 1989, n. 322, recante "Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400", è sostituito dal seguente:

“2. Non rientrano nell’obbligo di cui al comma 1 i dati personali di cui agli articoli 22 e 24 della legge 31 dicembre 1996, n. 675”.

2. Nell’articolo 9, comma 1, del decreto legislativo 6 settembre 1989, n. 322, le parole: “, in modo che non se ne possa trarre alcun riferimento individuale” sono sostituite dalle parole: “, in modo che non se ne possa trarre alcun riferimento relativamente a persone identificabili”.

3. Il comma 2 dell’articolo 9 del decreto legislativo 6 settembre 1989, n. 322, è sostituito dal seguente:

“2. I dati di cui al comma 1 non possono essere comunicati o diffusi se non in forma aggregata e secondo modalità che rendano non identificabili gli interessati ad alcun soggetto esterno, pubblico o privato, né ad alcun ufficio della pubblica amministrazione. In ogni caso, i dati non possono essere utilizzati al fine di identificare nuovamente gli interessati”.

4. Nel comma 4 dell’articolo 9, del decreto legislativo 6 settembre 1989, n. 322, le parole: “presenti nei pubblici registri” sono sostituite dalle seguenti: “provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque”.

5. Nell’articolo 12, comma 1, lettera a), del decreto legislativo 6 settembre 1989, n. 322, le parole: “e sull’osservanza delle norme” sono sostituite dalle seguenti: “e contribuisce alla corretta applicazione delle norme” e alla fine del periodo sono aggiunte le seguenti: “segnalando anche al Garante per la protezione dei dati personali i casi di inosservanza delle medesime norme o assicurando altra collaborazione nei casi in cui la natura tecnica dei problemi lo richieda”.

6. Nell’articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322, sono inserite in fine le seguenti parole: “ed è sentita ai fini della sottoscrizione dei codici di deontologia e di buona condotta relativi al trattamento dei dati personali nell’ambito del Sistema statistico nazionale”.

CAPO IV NORME MODIFICATIVE E INTEGRATIVE DELLA LEGGE N. 675/1996 E DISPOSIZIONI FINALI E TRANSITORIE

Art. 13.

(Ricorsi)

1. All’articolo 29 della legge 31 dicembre 1996, n. 675, sono apportate le seguenti modifiche:

a) nel comma 4, la parola: “venti” è sostituita dalla parola “trenta”;

b) dopo il comma 6 è aggiunto, in fine, il seguente comma:

“6-bis. Il decorso dei termini previsti dai commi 4, 5 e 6 è sospeso di diritto dal 1 al 30 agosto di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Ove il decorso abbia inizio durante tale periodo, l’inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussista il pregiudizio di cui al comma 2 e non preclude l’adozione dei provvedimenti di cui al comma 5”.

Art. 14.

(Sanzioni amministrative)

1. Nel comma 3 dell’articolo 39 della legge 31 dicembre 1996, n. 675, è aggiunto, in fine, il seguente periodo: “I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all’articolo 33, comma 2, e sono utilizzati unicamente per l’esercizio dei compiti di cui agli articoli 31, comma 1, lettera i) e 32”.

Art. 15.

(Dati relativi ai provvedimenti di cui all’articolo 686 del codice di procedura penale)

1. All'articolo 5 del decreto legislativo 11 maggio 1999, n. 135, è aggiunto il seguente comma:

"5-bis. In relazione alle finalità individuate nel capo II, i soggetti pubblici identificano e rendono pubblici, con le modalità di cui ai commi 4 e 5 e nel rispetto delle disposizioni del capo I del presente decreto, anche i tipi di dati e di operazioni oggetto del trattamento di cui all'articolo 24 della legge".

Art. 16.

(Dati genetici)

1. Nell'articolo 17, comma 5, del decreto legislativo 11 maggio 1999, n. 135, tra le parole: "dei dati genetici" e le parole: "è consentito" sono inserite le seguenti: "da chiunque effettuato", ed è aggiunto, in fine, il seguente periodo: "I trattamenti autorizzati dal Garante possono essere proseguiti fino al rilascio dell'autorizzazione prevista dal presente comma, che in sede di prima applicazione della presente disposizione è rilasciata entro dodici mesi dalla data della relativa entrata in vigore".

Art. 17.

(Divulgazione di dati a cura di scuole e istituti scolastici)

1. Nella parte II, titolo VII del decreto legislativo 16 aprile 1994, n. 297, è inserito il seguente capo:

"CAPO VIII

Art. 330-bis.

(Comunicazioni relative agli studenti)

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o attinenti a provvedimenti giudiziari indicati negli articoli 22 e 24 della legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 10 della citata legge n. 675 del 1996. I dati possono essere successivamente trattati esclusivamente per le predette finalità. Restano ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati".

2. I dati di cui all'articolo 330-bis del decreto legislativo 16 aprile 1994, n. 297, introdotto dal comma 1, raccolti prima dell'entrata in vigore della medesima disposizione e riguardanti studenti già diplomati, per i quali non è prontamente acquisibile la richiesta, possono essere comunicati o diffusi decorsi trenta giorni dalla notizia che le scuole e gli istituti scolastici, ovvero il Ministero della pubblica istruzione, rendono nota mediante annunci al pubblico. Gli interessati possono opporsi alla divulgazione, in tutto o in parte, dei dati che li riguardano.

Art. 18.

Entrata in vigore

1. Le disposizioni del presente decreto entrano in vigore il 1° ottobre 1999. Le disposizioni di cui al capo IV entrano in vigore il giorno successivo a quello della pubblicazione del presente decreto nella Gazzetta Ufficiale della Repubblica italiana.

2. Le disposizioni di cui all'articolo 4 si applicano nei singoli settori della ricerca scientifica e della statistica a decorrere dalla data in cui nei medesimi settori divengono efficaci i codici di cui all'articolo 6.

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.

6.1.4 Decreto Legislativo 30 luglio 1999, n. 282

Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni;

Vista la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e le raccomandazioni del Consiglio d'Europa ivi citate;

Visto il decreto legislativo 11 maggio 1999, n. 135;

Vista la legge 6 ottobre 1998, n. 344;

Visto il decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94;

Sentito il Garante per la protezione dei dati personali;

Visto l'articolo 14 della legge 23 agosto 1988, n. 400;

Vista la deliberazione preliminare del Consiglio dei Ministri, adottata nella riunione del 2 luglio 1999;

Acquisito il parere delle competenti commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 29 luglio 1999;

Sulla proposta del Presidente del Consiglio dei Ministri e del Ministro della sanità, di concerto con il Ministro di grazia e giustizia;

EMANA

il seguente decreto legislativo:

Art. 1.

(Ambito di applicazione e definizioni)

1. Il presente decreto disciplina il trattamento dei dati idonei a rivelare lo stato di salute da parte di organismi sanitari pubblici, nonché di organismi sanitari e di esercenti le professioni sanitarie in regime di convenzione o di accreditamento con il Servizio sanitario nazionale.

2. Il medesimo decreto disciplina anche, limitatamente a quanto specificamente previsto, i trattamenti di dati idonei a rivelare lo stato di salute in ambito sanitario da parte di soggetti diversi da quelli indicati nel comma 1.

3. Ai fini del presente decreto si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata "legge".

Art. 2.

(Informativa e consenso)

1. Dopo il comma 1 dell'articolo 23 della legge sono inseriti i seguenti:

"1-bis. Con decreto del Ministro della sanità adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentiti la Conferenza permanente per i rapporti tra lo Stato, le regioni

e le province autonome di Trento e Bolzano e il Garante, sono individuate modalità semplificate per le informative di cui all'articolo 10 e per la prestazione del consenso nei confronti di organismi sanitari pubblici, di organismi sanitari e di esercenti le professioni sanitarie convenzionati o accreditati dal Servizio sanitario nazionale, nonché per il trattamento dei dati da parte dei medesimi soggetti, sulla base dei seguenti criteri:

a) previsione di informative effettuate da un unico soggetto, in particolare da parte del medico di medicina generale scelto dall'interessato, per conto di più titolari di trattamento;

b) validità, nei confronti di più titolari di trattamento, del consenso prestato ai sensi dell'articolo 11, comma 3, per conto di più titolari di trattamento, anche con riguardo alla richiesta di prestazioni specialistiche, alla prescrizione di farmaci, alla raccolta di dati da parte del medico di medicina generale detenuti da altri titolari, e alla pluralità di prestazioni mediche effettuate da un medesimo titolare di trattamento;

c) identificazione di casi di urgenza nei quali, anche per effetto delle situazioni indicate nel comma 1-ter, l'informativa e il consenso possono intervenire successivamente alla richiesta della prestazione;

d) previsione di modalità di applicazione del comma 2 del presente articolo ai professionisti sanitari, diversi dai medici, che intrattengono rapporti diretti con i pazienti;

e) previsione di misure volte ad assicurare che nell'organizzazione dei servizi e delle prestazioni sia garantito il rispetto dei diritti di cui all'articolo 1.

1-ter. Il decreto di cui al comma 1 disciplina anche quanto previsto dall'articolo 22, comma 3-bis, della legge.

1-quater. In caso di incapacità di agire, ovvero di impossibilità fisica o di incapacità di intendere o di volere, il consenso al trattamento dei dati idonei a rivelare lo stato di salute è validamente manifestato nei confronti di esercenti le professioni sanitarie e di organismi sanitari, rispettivamente, da chi esercita legalmente la potestà ovvero da un familiare, da un prossimo congiunto, da un convivente, o, in loro assenza, dal responsabile della struttura presso cui dimori.

2. Nel comma 2 dell'articolo 23 della legge, dopo le parole: "all'interessato" sono inserite le seguenti: "o ai soggetti di cui al comma 1-ter".

Art. 3.

(Modifiche al decreto legislativo 11 maggio 1999, n. 135)

1. All'articolo 17, comma 3, del decreto legislativo 11 maggio 1999, n. 135, sono apportate le seguenti modifiche:

a) all'inizio del comma sono inserite le seguenti parole: "Per quanto non previsto dal decreto di cui all'articolo 23, comma 1-bis, della legge,";

b) nella lettera c), tra la parola: "interessati" e la parola: "per" è inserita la congiunzione: "e";

c) dopo la lettera c) è inserita la seguente:

"c-bis. identificazione di casi di urgenza nei quali l'informativa e il consenso possono intervenire successivamente alla richiesta della prestazione".

Art. 4.

(Prescrizioni mediche)

1. Fermi restando i casi in cui norme speciali prevedono che le ricette siano rilasciate in forma anonima o con particolari annotazioni, con decreto del Ministro della sanità da adottarsi entro sei mesi dalla data di entrata in vigore del presente decreto, sentito il Garante, sono individuati i medicinali diversi da quelli di cui al comma 2 per la cui prescrizione non è richiesta l'indicazione delle generalità dell'interessato.

2. Le ricette relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale sono redatte su apposito modello, approvato con il decreto di cui al comma 1. Detto modello, la cui utilizzazione è obbligatoria decorsi diciotto mesi dalla data di entrata in vigore del decreto di cui al comma 1, è conformato in modo da permettere di risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della correttezza della prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca, nel rispetto delle norme deontologiche applicabili.

3. I modelli di cui al comma 2 sono utilizzati entro diciotto mesi dalla data di entrata in vigore del decreto di cui al comma 1.

4. Nei casi in cui è fatto obbligo di accertare l'identità dell'interessato ai sensi del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, le ricette sono conservate separatamente da ogni altro documento che non ne richieda l'utilizzo.

5. Le ricette disciplinate dall'articolo 5 del decreto legislativo 30 dicembre 1992, n. 539, e successive modificazioni, sono conservate dal farmacista per il periodo prescritto, e successivamente distrutte, con modalità atte ad escludere l'accesso di terzi ai dati contenuti nelle stesse.

Art. 5.

(Ricerca medica ed epidemiologica)

1. Per il trattamento dei dati idonei a rivelare lo stato di salute finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, il consenso dell'interessato non è necessario qualora la ricerca sia prevista da un'espressa previsione di legge o rientri nel programma di ricerca biomedica o sanitaria di cui all'articolo 12-bis del 30 dicembre 1992, n. 502, e successive modificazioni ed integrazioni.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 13 della legge nei riguardi dei trattamenti di cui al comma 1, l'aggiornamento, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, qualora il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca.

3. Resta fermo quanto previsto per la ricerca scientifica dai decreti legislativi emanati in attuazione della legge 31 dicembre 1996, n. 676.

Art. 6.

(Carte sanitarie elettroniche)

1. Le carte sanitarie elettroniche di cui all'articolo 59, comma 50, lettera i), della legge 27 dicembre 1997, n. 449 e dall'articolo 2 del decreto-legge 28 dicembre 1998, n. 450, convertito, con modificazioni, dalla legge 26 febbraio 1999, n. 39, sono fornite a tutti i soggetti residenti nelle aree territoriali delle aziende sanitarie locali nelle quali si svolge la sperimentazione, previa informativa ai sensi dell'articolo 10 della legge.

2. Gli interessati possono opporsi all'inserimento nelle carte di cui al comma 1 dei dati idonei a rivelare lo stato di salute che li riguardano e che eccedano i dati relativi alla gestione amministrativa e alle situazioni di interventi di urgenza, quali definite a livello internazionale.

3. Il decreto del Ministro della sanità di cui all'articolo 2, comma 1, del decreto-legge 28 dicembre 1998, n. 450, convertito, con modificazioni, dalla legge 26 febbraio 1999, n. 39, determina anche, tra le altre garanzie previste dall'articolo 6, comma 4, del decreto legislativo 29 aprile 1998, n. 124, le categorie di incaricati delle aziende sanitarie locali e di operatori sanitari che possono accedere

alle diverse categorie di dati inseriti nelle carte, nonché le categorie professionali tenute ad inserire i dati e il periodo massimo entro i quali i dati devono essere aggiornati.

Art. 7.

(Entrata in vigore)

1. Le disposizioni del presente decreto entrano in vigore il 1° ottobre 1999.

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.

6.1.5 Decreto del Presidente della Repubblica 28 luglio 1999, n. 318

Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87, comma quinto, della Costituzione;

Visto l'articolo 15 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 dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675, occorre individuare, in via preventiva, le misure minime di sicurezza per i dati personali oggetto di trattamento, al fine di assicurare il funzionamento delle misure sanzionatorie penali previste dall'articolo 36 della medesima legge;

Visto l'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400;

Sentiti l'Autorità per l'informatica nella pubblica amministrazione e il 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 26 aprile 1999;

Ritenuto di dover comunque garantire la possibilità, in caso di più incaricati del trattamento, di limitare l'accesso a determinati dati personali attraverso la previsione di una specifica parola chiave per tali dati, senza operare, quindi, alcuna equiparazione tra tale ipotesi e quella relativa alla previsione di un'unica parola chiave per l'accesso al sistema;

Viste le deliberazioni del Consiglio dei Ministri, adottate nelle riunioni del 16 luglio e del 23 luglio 1999;

Sulla proposta del Ministro di grazia e giustizia;

EMANA

il seguente regolamento:

**CAPO I
PRINCIPI GENERALI****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 intendono per:

a) «misure minime»: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge;

b) «strumenti»: i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;

c) «amministratori di sistema»: i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

CAPO II
TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI
O COMUNQUE AUTOMATIZZATI.

Sezione I

TRATTAMENTO DEI DATI PERSONALI EFFETTUATO MEDIANTE ELABORATORI
NON ACCESSIBILI DA ALTRI ELABORATORI O TERMINALI

Art. 2.

(Individuazione degli incaricati)

1. Salvo quanto previsto dall'articolo 8, se il trattamento dei dati personali è effettuato per fini diversi da quelli di cui all'articolo 3 della legge mediante elaboratori non accessibili da altri elaboratori o terminali, devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure:

a) prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b);

b) individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.

Sezione II

TRATTAMENTO DEI DATI PERSONALI EFFETTUATO
MEDIANTE ELABORATORI ACCESSIBILI IN RETE

Art. 3.

(Classificazione)

1. Ai fini della presente sezione gli elaboratori accessibili in rete impiegati nel trattamento dei dati personali sono distinti in:

- a) elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico;
- b) elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Art. 4.

(Codici identificativi e protezione degli elaboratori)

1. Nel caso di trattamenti effettuati con gli elaboratori di cui all'articolo 3, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure:

a) a ciascun utente o in caricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;

b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;

c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.

2. Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui è consentita la diffusione.

Art. 5.

(Accesso ai dati particolari)

1. Per il trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato ai sensi dell'articolo 3, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento è effettuato ai sensi dell'articolo 3, comma 1, lettera b), sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico.

2. L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

3. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.

4. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.

5. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.

6. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

7. Le disposizioni di cui ai commi da 1 a 6 non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Art. 6.

(Documento programmatico sulla sicurezza)

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma 1, lettera b), deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;

b) i criteri e le procedure per assicurare l'integrità dei dati;

c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;

d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

2. L'efficacia delle misure di sicurezza adottate ai sensi del comma 1 deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Art. 7.

(Reimpiego dei supporti di memorizzazione)

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato con gli strumenti di cui all'articolo 3, i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Sezione III

TRATTAMENTO DEI DATI PERSONALI EFFETTUATO PER FINI ESCLUSIVAMENTE PERSONALI

Art. 8.

(Parola chiave)

1. Ai sensi dell'articolo 3 della legge, il trattamento per fini esclusivamente personali dei dati di cui agli articoli 22 e 24 della legge, effettuato con elaboratori stabilmente accessibili da altri elaboratori, è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati.

CAPO III

TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI
DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI.

Art. 9.

(Trattamento di dati personali)

1. Nel caso di trattamento di dati personali per fini diversi da quelli dell'articolo 3 della legge, effettuato, con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità:

a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;

b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.

2. Nel caso di trattamento di dati di cui agli articoli 22 e 24 della legge, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità:

a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;

b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Art. 10.

(Conservazione della documentazione relativa al trattamento)

1. I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge devono essere conservati e custoditi con le modalità di cui all'articolo 9.

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.

6.1.6 Autorizzazioni generali per il trattamento di dati sensibili

(Pubblicate sulla gazzetta ufficiale n. 232, serie generale del 2 ottobre 1999)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

6.1.6.1 Autorizzazione n. 1/1999 al trattamento dei dati sensibili nei rapporti di lavoro

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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'art. 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;

Visto l'art. 22, comma 3 e comma 3-bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, 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;

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, legge n. 675/1996, come sostituito dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 30 settembre 1998 relativa al trattamento dei dati "sensibili" nei rapporti di lavoro, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 1° ottobre 1998 e avente efficacia fino al 30 settembre 1999;

Visti i risultati positivi conseguiti con le autorizzazioni generali numeri 1/1997 e 1/1998, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli adempimenti che la legge 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, alla luce dell'esperienza maturata;

Vista la legge 5 febbraio 1999, n. 25, che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria 95/46/CE;

Ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'ufficio di questa autorità emanato con decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Ritenuta la necessità che anche le nuove autorizzazioni prendano 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire 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 adottate in materia dal Consiglio d'Europa;

Considerato che un elevato 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 legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Stefano Rodotà;

AUTORIZZA

il trattamento dei dati sensibili di cui all'art. 22, comma 1, della legge n. 675/1996, finalizzato alla gestione dei rapporti di lavoro, alle condizioni di seguito indicate.

1) Ambito di applicazione

La presente autorizzazione è rilasciata 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 legge 24 giugno 1997, n. 196, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lettere b) e c);

b) ad organismi paritetici e ad altri organismi che gestiscono osservatori in materia di lavoro, previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi anche aziendali.

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 mandatari;

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, dalla normativa comunitaria da regolamenti o da contratti collettivi anche aziendali, 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 anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempreché, 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 l'esercizio del diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;

f) 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;

g) per garantire le pari opportunità.

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 (sempreché 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 articoli 9, 15 e 17 della legge n. 675/1996 e dal decreto del Presidente della Repubblica n. 318/1999, 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 articoli 10 e 22 della legge n. 675/1996.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lettera e) della legge 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 legge 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 legge 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 legge 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 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.1.6.2 Autorizzazione n. 2/1999 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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'art. 22, comma 1, della legge n. 675/1996, il quale individua come "sensibili", tra l'altro, i dati personali idonei a rivelare lo stato di salute o la vita sessuale;

Visto l'art. 23 della legge n. 675/1996, come modificato dall'art. 2 del decreto legislativo 30 luglio 1999, n. 282;

Visto l'art. 22, comma 3 e comma 3-bis, della legge n. 675/1996, rispettivamente modificato ed introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, n. 135;

Visto l'art. 17 del decreto legislativo 11 maggio 1999, n. 135, e successive modificazioni ed integrazioni;

Visto l'art. 23, comma 1-bis, della legge n. 675/1996 che prevede "modalità semplificate per le informative di cui all'art. 10 della medesima legge e per la prestazione del consenso nei confronti di organismi sanitari pubblici, di organismi sanitari e di esercenti le professioni sanitarie convenzionati o accreditati dal Servizio sanitario nazionale, nonché per il trattamento dei dati da parte dei medesimi soggetti"; considerato che analoghe modalità semplificate sono previste dall'art. 17, comma 3, del decreto legislativo n. 135/1999;

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 (art. 41, comma 7, della legge n. 675/1996, modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 30 settembre 1998 relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 1° ottobre 1998 e avente efficacia fino al 30 settembre 1999;

Visti i risultati positivi conseguiti con le autorizzazioni generali numeri 2/1997 e 2/1998, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli adempimenti che la legge 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, alla luce dell'esperienza maturata;

Considerato che il trattamento dei dati genetici da chiunque effettuato previa autorizzazione del Garante può essere proseguito sino al rilascio dell'autorizzazione prevista dall'art. 17, comma 5, del decreto legislativo n. 135/1999, e successive modificazioni ed integrazioni, che sarà emanata entro dodici mesi dalla data di entrata in vigore del medesimo decreto n. 135/1999;

Vista la legge 5 febbraio 1999, n. 25, che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria n. 95/46/CE;

Ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie a tempo determinato, in conformità anche a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'ufficio di questa autorità emanato con il decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Ritenuta 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 legge 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 di garantire 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 adottate in materia di dati sanitari dal Consiglio d'Europa ed in particolare dalla raccomandazione N.R (97) 5 in base alla 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;

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'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Ugo De Siervo;

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 il consenso non sia prestato o non possa essere prestato per effettiva irreperibilità;

1) il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;

2) manchi il consenso (art. 23, comma 1, ultimo periodo, legge n. 675/1996), in quanto non sia prestato o non possa essere prestato per effettiva irreperibilità;

3) il trattamento non sia previsto da una disposizione di legge che specifichi, ai sensi dell'art. 22, comma 3, della legge n. 675/1996, come modificato dall'art. 5 del decreto legislativo n. 135/1999, i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Il consenso, ove previsto, è acquisito in conformità anche a quanto previsto dall'art. 23, commi 1-bis e 1-quater, della legge n. 675/1996 e dall'art. 17, comma 3, del decreto legislativo n. 135/1999, e successive modificazioni ed integrazioni.

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 esi-

gere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, dalla normativa comunitaria o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni, di diagnosi e cura, ivi compresi i trapianti di organi e tessuti, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di profilassi delle malattie infettive e diffuse, 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, nel rispetto di quanto previsto dall'art. 17, comma 3, del decreto legislativo n. 135/1999.

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 relazioni 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'art. 23, comma 1, ultimo periodo, della legge n. 675/1996 e dall'art. 5, comma 1, del decreto legislativo 30 luglio 1999, n. 282), 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. Resta fermo quanto previsto dai decreti legislativi 30 luglio 1999, numeri 281 e 282 in materia di ricerca scientifica e di ricerca medica ed epidemiologica;

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, salvo quanto previsto dall'art. 22, comma 1-bis, della legge n. 675/1996;

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;

g) alle persone fisiche e giuridiche e ad altri organismi, limitatamente ai dati dei beneficiari e dei donatori e alle operazioni indispensabili all'effettuazione di trapianti di organi e tessuti, nonché di donazioni di sangue.

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'art. 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 anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempreché 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 nascituri, 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 ai sensi degli articoli 22 e 23 della legge 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 legge 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 in cui sarà efficace l'apposita autorizzazione per il trattamento dei dati genetici prevista dall'art. 17, comma 5, del decreto n. 135/1999, e successive modificazioni ed integrazioni, 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 articoli 9, 15 e 17 della legge n. 675/1996 e dal decreto del Presidente della Repubblica n. 318/1999, 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 sopra elencati.

Restano inoltre fermi gli obblighi di acquisire il consenso dell'interessato e di informarlo in conformità a quanto previsto dagli articoli 10, 22 e 23 della legge n. 675/1996. Per le informazioni relative ai nascituri, il consenso è prestato dalla gestante.

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 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 deve essere verificata periodicamente la stretta pertinenza e la non eccedenza dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati.

5) Comunicazione e diffusione dei dati

Ai sensi dell'art. 23, comma 4, della legge 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'art. 5, comma 2, della legge 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'art. 11 della legge 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'art. 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 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 3 ottobre 1998 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 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.1.6.3 Autorizzazione n. 3/1999 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale;

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'art. 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;

Visto l'art. 22, comma 3 e comma 3-bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, 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;

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 (art. 41, comma 7, della legge n. 675/1996, modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante rilasciata il 30 settembre 1998 relativa al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 1° ottobre 1998 e avente efficacia fino al 30 settembre 1999;

Visti i risultati positivi conseguiti con le autorizzazioni generali numeri 3/1997 e 3/1998, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli adempimenti che la legge 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, alla luce dell'esperienza maturata;

Vista la legge 5 febbraio 1999, n. 25, che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria 95/46/CE;

Ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'ufficio di questa autorità emanato con decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Ritenuta, tuttavia, la necessità che anche 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 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire 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 adottate in materia dal 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 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;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Ugo De Siervo;

AUTORIZZA

il trattamento dei dati sensibili di cui all'art. 22, comma 1, della legge n. 675/1996 da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, alle condizioni di seguito indicate:

1) Ambito di applicazione e finalità del trattamento

La presente autorizzazione è rilasciata senza richiesta:

a) alle associazioni anche non riconosciute, ivi comprese le confessioni religiose e le comunità religiose, salvo quanto previsto dall'art. 22, comma 1-bis, come introdotto dall'art. 5, comma 1 del decreto legislativo n. 135/1999, 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'art. 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 anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempreché 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.

La presente autorizzazione è rilasciata inoltre per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di regi-

stri 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. 2/1999.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'art. 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, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi.

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 articoli 9, 15, 17 e 28 della legge n. 675/1996 e dal decreto del Presidente della Repubblica n. 318/1999, 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, lettera e), della legge n. 675/1996, 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, dalla normativa comunitaria o di regolamento 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 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.1.6.4 Autorizzazione n. 4/1999 al trattamento dei dati sensibili da parte dei liberi professionisti

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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'art. 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;

Visto l'art. 22, comma 3 e comma 3-bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, 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;

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, della legge n. 675/1996, come sostituito dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 30 settembre 1998 relativa al trattamento dei dati "sensibili" nei rapporti di lavoro, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 1° ottobre 1998 e avente efficacia fino al 30 settembre 1999;

Visti i risultati positivi conseguiti con le autorizzazioni generali numeri 4/1997 e 4/1998, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli adempimenti che la legge 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, alla luce dell'esperienza maturata;

Vista la legge 5 febbraio 1999, n. 25, che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria 95/46/CE;

Ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'ufficio di questa Autorità emanato con decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Ritenuta la necessità che anche le nuove autorizzazioni prendano 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire 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 adottate in materia dal 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 gene-

rale ai sensi dell'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Giuseppe Santaniello;

AUTORIZZA

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 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'art. 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'art. 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'art. 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. 2/1999;

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. 1/1999;

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. 2/1999.

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 fisco-

le 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 anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi;

c) ai fini dello svolgimento da parte del difensore nel procedimento penale delle investigazioni di cui all'art. 38 delle norme di attuazione del codice di procedura penale, anche a mezzo di sostituti e di consulenti tecnici;

d) per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

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 e dal decreto del Presidente della Repubblica n. 318/1999, 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'art. 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'art. 9, comma 1, lettera e), della legge n. 675/1996, i dati sensibili possono essere conservati, per il periodo di tempo previsto da leggi, dalla normativa comunitaria o da regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine deve essere verificata 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 (art. 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 dalla normativa comunitaria o da regolamenti 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 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.1.6.5 Autorizzazione n. 5/1999 al trattamento dei dati sensibili da parte di diverse categorie di titolari

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Buttarelli, segretario generale;

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'art. 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;

Visto l'art. 22, comma 3 e comma 3-bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, 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;

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 (art. 41, comma 7, della legge n. 675/1996, modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 30 settembre 1998 relativa al trattamento dei dati sensibili da parte di diverse categorie di titolari, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 1° ottobre 1998 e avente efficacia fino al 30 settembre 1999;

Visti i risultati positivi conseguiti con le autorizzazioni generali numeri 5/1997 e 5/1998, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli adempimenti che la legge 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, alla luce dell'esperienza maturata;

Vista la legge 5 febbraio 1999, n. 25, che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria 95/46/CE;

Ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'ufficio di questa Autorità emanato con decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Ritenuta la necessità che anche le nuove autorizzazioni prendano 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire 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 adottate in materia dal 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 inter-

mediazione 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'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore l'ing. Claudio Manganelli;

AUTORIZZA

il trattamento dei dati sensibili di cui all'art. 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, DEL SETTORE TURISTICO, 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

La presente 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, dalla normativa comunitaria, dai regolamenti, 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 contabi-

li, 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'art. 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 (art. 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, sempreché 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. 1/1999, rilasciata il 29 settembre 1999, 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. 4/1999, rilasciata il 29 settembre 1999, 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**

La presente 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

La presente 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 trattamento

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 (art. 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. 2/1999, rilasciata il 29 settembre 1999.

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 e dal decreto del Presidente della Repubblica n. 318/1999, 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'art. 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 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.1.6.6 Autorizzazione n. 6/1999 al trattamento di alcuni dati sensibili da parte degli investigatori privati

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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'art. 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 (art. 22, comma 1, legge n. 675/1996);

Considerato che una speciale disposizione (art. 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 30 settembre 1998 relativa al trattamento di alcuni dati sensibili da parte degli investigatori privati, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 1° ottobre 1998 e avente efficacia fino al 30 settembre 1999;

Visti i risultati positivi conseguiti con le autorizzazioni generali numeri 6/1997 e 6/1998, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli adempimenti che la legge 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, alla luce dell'esperienza maturata;

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. 2/1999, rilasciata il 29 settembre 1999), 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. 2/1999 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. 2/1999 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 (art. 22, comma 4, legge n. 675/1996);

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;
Visti gli atti d'ufficio;
Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;
Relatore l'ing. Claudio Manganelli;

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

La presente 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 (art. 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 un diritto della personalità o 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. 1/1999, rilasciata il 29 settembre 1999);

b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione generale n. 2/1999, rilasciata il 29 settembre 1999);

c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione generale n. 3/1999, rilasciata il 29 settembre 1999);

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. 4/1999, rilasciata il 29 settembre 1999);

e) relativamente ai dati di carattere giudiziario (autorizzazione generale n. 7/1999, rilasciata il 29 settembre 1999).

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 entro cui questa deve essere conclusa.

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'art. 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 nell'autorizzazione generale n. 2/1999, 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'art. 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 (art. 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 (anteporre "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'art. 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 e dal decreto del Presidente della Repubblica n. 318/1999 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, sempreché i dati non siano destinati ad una comunicazione sistematica o alla diffusione (art. 3 della legge n. 675/1996).

8) Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.1.6.7 Autorizzazione n. 7/1999 al trattamento di dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici

PROVVEDIMENTO 29 settembre 1999

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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'art. 24, comma 1, della medesima legge, che ammette il trattamento di dati personali idonei a rivelare i provvedimenti giudiziari indicati nell'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, da parte di soggetti pubblici e privati e di enti pubblici economici, "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";

Constatata la necessità di evitare che diversi soggetti privati ed enti pubblici economici debbano interrompere alcuni trattamenti di dati che risultano giustificati da una finalità di rilevante interesse pubblico in ragione della loro natura e degli scopi ai quali essi sono strumentali;

Considerato che diversi trattamenti dei predetti dati da parte di soggetti pubblici sono disciplinati nel decreto legislativo 11 maggio 1999, n. 135;

Considerato che i trattamenti dei medesimi dati giudiziari da parte dei soggetti pubblici, per finalità non previste nel capo II del decreto legislativo 11 maggio 1999, n. 135, devono essere autorizzati dal Garante ai sensi dell'art. 24 della legge 31 dicembre 1996, n. 675;

Ritenuta la necessità di autorizzare i soggetti pubblici al trattamento dei dati di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, e ciò al fine di consentire l'accertamento dell'assenza di alcune situazioni che la normativa in materia di appalti pubblici considera quali cause di esclusione dalla partecipazione a gare d'appalto, in modo che, per esigenze di buon andamento e imparzialità dell'azione amministrativa, i soggetti operanti in materia presentino i requisiti previsti di professionalità e correttezza;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (art. 41, comma 7, della legge n. 675/1996, come modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Visti i risultati positivi conseguiti con l'autorizzazione al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e soggetti pubblici rilasciata il 10 maggio 1999, come integrata con provvedimenti del 3 giugno 1999 e del 9 settembre 1999, che è risultata uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto opportuno rilasciare una nuova autorizzazione generale in ordine ai dati di carattere giudiziario citati in premessa, al fine di semplificare gli adempimenti previsti dalla legge n. 675/1996, di armonizzare le prescrizioni da impartire ad una ampia categoria di titolari del trattamento e di favorire altresì la funzionalità dell'ufficio del Garante, alla luce dell'esperienza maturata;

Vista la legge 5 febbraio 1999, n. 25, che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria n. 95/46/CE del 24 ottobre 1995;

Considerato che l'art. 8, paragrafo 5, di tale direttiva prevede specifiche garanzie per i dati sopraindicati e per altre categorie di dati a carattere giudiziario, in quanto ammette il trattamento dei dati relativi alla più ampia categoria delle "infrazioni, ... condanne penali o ... misure di sicurezza" "... solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che possono essere fissate dallo Stato

membro in base ad una disposizione nazionale che preveda garanzie appropriate e specifiche", sempreché un "registro completo" delle condanne penali sia tenuto "solo sotto il controllo dell'autorità pubblica";

Ritenuto che in vista della completa attuazione legislativa di tale disciplina comunitaria è opportuno che la presente autorizzazione generale non rechi disposizioni particolarmente dettagliate, in modo da evitare che l'attività dei titolari dei trattamenti sia soggetta a modifiche sostanziali nel corso di un breve periodo di tempo, ferme restando alcune garanzie per gli interessati;

Ritenuta la necessità di favorire la prosecuzione dell'attività di documentazione, studio e ricerca in campo giuridico, in particolare per quanto riguarda la diffusione di dati relativi a precedenti giurisprudenziali, in ragione sia dell'affinità che tali attività presentano con quelle di manifestazione del pensiero già disciplinate dagli articoli 12, 20 e 25 della legge n. 675/1996, sia della possibile adozione di norme volte a favorire lo sviluppo dell'informatica giuridica;

Ritenuto, tuttavia, opportuno che la presente autorizzazione prenda comunque in considerazione le finalità dei trattamenti, le categorie di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati, 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 (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;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996, e adottato con decreto del Presidente della Repubblica 28 luglio 1999, n. 318;

Visto l'art. 14 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Giuseppe Santaniello;

AUTORIZZA

i trattamenti di dati personali idonei a rivelare i provvedimenti di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, per le rilevanti finalità di interesse pubblico di seguito specificate ai sensi dell'art. 24 della legge n. 675/1996 e secondo le seguenti prescrizioni:

CAPO I

RAPPORTI DI LAVORO

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta di parte, a persone fisiche e giuridiche, enti, associazioni ed organismi che:

a) sono parte di un rapporto di lavoro;

b) utilizzano prestazioni lavorative anche atipiche, parziali o temporanee ai sensi della legge 24 giugno 1997, n. 196 (in materia di prestazioni di lavoro temporaneo);

c) conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatarî.

Il trattamento deve essere strettamente necessario per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario.

L'autorizzazione è altresì rilasciata a soggetti che in relazione ad un'attività di composizione di controversie esercitata in conformità alla legge svolgono un trattamento strettamente necessario al medesimo fine.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti a soggetti che hanno assunto o intendono assumere la qualità di:

- a) lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione lavoro, ovvero di associati anche in compartecipazione o di titolari di borse di lavoro e di rapporti analoghi;
- b) amministratori o membri di organi esecutivi o di controllo;
- c) consulenti e liberi professionisti, agenti, rappresentanti e mandatari.

CAPO II

ORGANISMI DI TIPO ASSOCIATIVO E FONDAZIONI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata anche senza richiesta:

a) ad associazioni anche non riconosciute, ivi compresi partiti e movimenti politici, associazioni ed organizzazioni sindacali, patronati, associazioni a scopo assistenziale o di volontariato, a fondazioni, comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché a cooperative sociali e società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381, e 15 aprile 1986, n. 3818;

b) ad enti ed associazioni anche non riconosciute che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi.

Il trattamento deve essere strettamente necessario per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti:

- a) ad associati, soci e aderenti, nonché, nei casi in cui l'utilizzazione dei dati sia prevista dall'atto costitutivo o dallo statuto, a soggetti che presentano richiesta di ammissione o di adesione;
- b) a beneficiari, assistiti e fruitori delle attività o dei servizi prestati dall'associazione, dall'ente o dal diverso organismo.

CAPO III

LIBERI PROFESSIONISTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata anche senza richiesta ai:

- a) liberi professionisti, anche associati, 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'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza;

b) soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578, e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato;

c) sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti ai clienti.

I dati relativi ai terzi possono essere trattati solo ove ciò sia strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

CAPO IV

IMPRESE BANCARIE ED ASSICURATIVE ED ALTRI TRATTAMENTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta:

a) ad imprese autorizzate o che intendono essere autorizzate all'esercizio dell'attività bancaria e creditizia, assicurativa o dei fondi pensione, anche se in stato di liquidazione coatta amministrativa, ai fini:

1) dell'accertamento, nei casi previsti dalle leggi e dai regolamenti, del requisito di onorabilità nei confronti di soci e titolari di cariche direttive o elettive;

2) dell'accertamento, nei soli casi espressamente previsti dalla legge, di requisiti soggettivi e di presupposti interdittivi in particolare ai sensi del regio decreto 21 dicembre 1933, n. 1736, sull'assegno bancario;

3) dell'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana;

4) dell'accertamento di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, in relazione ad illeciti direttamente connessi con la medesima attività. Per questi ultimi casi, limitatamente ai trattamenti di dati registrati in una specifica banca di dati ai sensi dell'art. 1, comma 2, lettera a), della legge n. 675/1996, il titolare deve inviare al Garante una dettagliata relazione sulle modalità del trattamento;

b) a soggetti titolari di un trattamento di dati svolto nell'ambito di un'attività di richiesta, acquisizione e consegna di atti e documenti presso i competenti uffici pubblici, effettuata su incarico degli interessati;

c) alle società di intermediazione mobiliare, alle società di investimento a capitale variabile, e alle società di gestione del risparmio e dei fondi pensione, ai fini dell'accertamento dei requisiti di onorabilità in applicazione dei decreti legislativi 24 febbraio 1998, n. 58, e 21 aprile 1993, n. 124, dei decreti ministeriali 11 novembre 1998, n. 468, e 14 gennaio 1997, n. 211, e di eventuali altre norme di legge o di regolamento.

2) Ulteriori trattamenti

L'autorizzazione è rilasciata altresì:

a) a chiunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempreché il diritto da far valere o difendere 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 suo perseguimento;

b) a chiunque, per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

c) a persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n.

773, e successive modificazioni e integrazioni). Il trattamento deve essere necessario:

1) 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;

2) 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);

d) a chiunque, per adempiere ad obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale, contenute anche nella legge 19 marzo 1990, n. 55, e successive modificazioni ed integrazioni, o per poter produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto;

e) ai soggetti pubblici, ai fini dell'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, come previsto dalla normativa in materia di appalti pubblici e, in particolare, dall'art. 11 del decreto legislativo 24 luglio 1992, n. 358, come da ultimo modificato dall'art. 9 del decreto legislativo 20 ottobre 1998, n. 402"

CAPO V

DOCUMENTAZIONE GIURIDICA

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati per finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali.

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 trattati

Possono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2) Modalità di trattamento

Il trattamento dei dati deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate agli obblighi, ai compiti o alle finalità precedentemente indicati.

Fuori dei casi previsti dai capi IV, punto 2 e V, o nei quali la notizia è acquisita da fonti accessibili a chiunque, i dati devono essere forniti dagli interessati, nel rispetto della disciplina prevista dall'art. 689 del codice di procedura penale in tema di richiesta di certificati, salvo quanto previsto dall'art. 688 del medesimo codice per ciò che riguarda l'acquisizione di certificati del casellario giudiziale da parte di amministrazioni pubbliche e di enti incaricati di pubblici servizi.

3) Conservazione dei dati

Con riferimento all'obbligo previsto dall'art. 9, comma 1, lettera e), della legge n. 675/1996, i

dati possono essere conservati per il periodo di tempo previsto da leggi o regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per le finalità perseguite.

Ai sensi dell'art. 9, comma 1, lettere c), d) ed e), della legge, i soggetti autorizzati verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi. Al fine di assicurare che i dati siano strettamente pertinenti e non eccedenti rispetto alle finalità medesime, i soggetti autorizzati valutano specificamente il rapporto tra i dati e i singoli obblighi, compiti e prestazioni. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente gli obblighi, i compiti e le prestazioni.

4) Comunicazione e diffusione

I dati possono essere comunicati e, ove previsto dalla legge, diffusi, a soggetti pubblici o privati, nei limiti strettamente necessari per le finalità perseguite e nel rispetto, in ogni caso, del segreto professionale e delle altre prescrizioni sopraindicate.

5) 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 al Garante, 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 si riserva l'adozione di ogni altro provvedimento per i trattamenti non considerati nella presente autorizzazione.

Per quanto riguarda invece i trattamenti disciplinati nel presente provvedimento, il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle relative prescrizioni, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

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 disposizioni contenute nell'art. 8 della legge 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.

6) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 1999, fino al 30 settembre 2000.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, addì 29 settembre 1999

IL Presidente
RODOTÀ

6.2 PROVVEDIMENTI DEL GARANTE

6.2.1. PROVVEDIMENTO 30 dicembre 1999-13 gennaio 2000 - n. 1/P/2000 (in G.U. 2 febbraio 2000, n. 26, p. 31)

Individuazione di attività che perseguono rilevanti finalità di interesse pubblico per le quali è autorizzato il trattamento dei dati sensibili da parte dei soggetti pubblici.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nelle sedute del 30 dicembre 1999 e del 13 gennaio 2000, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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 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;

Visto, in particolare, l'articolo 22, comma 3, della medesima legge, come modificato dall'articolo 5 del decreto legislativo 11 maggio 1999, n. 135, che ammette il trattamento dei dati "sensibili" da parte dei soggetti pubblici, esclusi gli enti pubblici economici, solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite;

Considerato che per i trattamenti non autorizzati da una espressa disposizione di legge avente tali caratteristiche, i soggetti pubblici possono chiedere al Garante per la protezione dei dati personali di individuare, tra le attività ad essi demandate dalla legge, quelle che perseguono rilevanti finalità di interesse pubblico e per le quali il trattamento dei dati "sensibili" è conseguentemente autorizzato nelle more di una specificazione legislativa;

Considerato che diverse amministrazioni pubbliche tra cui, in particolare, enti locali, aziende sanitarie locali e uffici periferici dell'amministrazione statale, hanno chiesto al Garante di individuare alcune attività, tra quelle ad esse attribuite dalla legge, che perseguono rilevanti finalità di interesse pubblico;

Considerato che il termine per la decisione del Garante, limitatamente alle richieste presentate entro il 31 dicembre 1999, è di novanta giorni durante i quali il trattamento dei dati può essere proseguito sino alla decisione (articolo 5, comma 4, d.l.g. n. 135/1999);

Considerato che il capo I del decreto legislativo n. 135/1999 individua alcuni principi generali in materia di trattamento di dati sensibili e di carattere giudiziario da parte dei soggetti pubblici;

Visto l'articolo 22, comma 3-bis, della legge n. 675/1996, introdotto dall'articolo 5, comma 3, del d.l.g. n. 135/1999, secondo cui, nei casi in cui la rilevante finalità di interesse pubblico è specificata per legge o con provvedimento del Garante, ma non sono specificati i tipi di dati e le operazioni eseguibili, i soggetti pubblici dovranno identificare e rendere pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando tale identificazione periodicamente;

Considerato che il citato articolo 22, comma 3, della legge può essere applicato dal Garante anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti cui si riferiscono le richieste presentate (cfr. articoli 22, comma 3, ultimo periodo e 41, comma 7, della legge n. 675/1996, come modificato dall'articolo 4, comma 1, del d.l.g. 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante n. 7/1999 del 29 settembre 1999, relativa al trattamento di dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici;

Visti gli atti d'ufficio e le richieste di soggetti pubblici sinora pervenute;

Considerato che alcune richieste non devono essere prese in considerazione in quanto si riferiscono, in tutto o in parte, a rilevanti finalità di interesse pubblico menzionate nel capo II del citato decreto legislativo n. 135/1999, per le quali il trattamento dei dati "sensibili" e di carattere giudiziario è già consentito (articolo 5, comma 5-bis, d.lg. n. 135/1999);

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'articolo 7, comma 2, lett. a) del D.P.R. 31 marzo 1998, n. 501;

Relatore il prof. Ugo De Siervo;

TUTTO CIÒ PREMESSO IL GARANTE:

1) nelle more di una specificazione legislativa e ai sensi dell'articolo 22, comma 3, della legge n. 675/1996, individua, tra le attività che le leggi demandano a soggetti pubblici, le seguenti attività che perseguono rilevanti finalità di interesse pubblico:

- a) *attività socio-assistenziali*, con particolare riferimento a
 - interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
 - interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
 - assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;
 - indagini psico-sociali relative all'adozione di provvedimenti di adozione anche internazionale;
 - compiti di vigilanza per affidamenti temporanei;
 - iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;
 - interventi in tema di barriere architettoniche;
- b) *attività relative alla gestione di asili nido*;
- c) *attività concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico*;
- d) *attività ricreative o di promozione della cultura e dello sport*, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;
- e) *attività finalizzate all'assegnazione di alloggi di edilizia residenziale pubblica*;
- f) *attività relative alla leva militare*;
- g) *attività di polizia amministrativa locale*, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente;
- h) *attività degli uffici per le relazioni con il pubblico*;
- i) *attività in materia di protezione civile*;
- j) *attività di supporto al collocamento e all'avviamento al lavoro*, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;
- k) *attività dei difensori civici regionali e locali*, con particolare riferimento alla trattazione di petizioni e segnalazioni;

2) dichiara conseguentemente autorizzato il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, da parte dei soggetti pubblici, anche diversi da quelli che hanno presentato richiesta, cui le leggi demandano le attività indicate nel precedente punto 1), nel rispet-

to dei principi generali di cui agli articoli 2, 3 e 4 del decreto legislativo 11 maggio 1999, n. 135, e in relazione ai tipi di dati e di operazioni che saranno identificati e resi pubblici dalle amministrazioni ai sensi del comma 3-bis del medesimo articolo 22, secondo i rispettivi ordinamenti;

3) dichiara non luogo a provvedere sulle richieste riconducibili a finalità menzionate nel capo II del decreto legislativo 11 maggio 1999, n. 135.

Roma, 30 dicembre 1999-13 gennaio 2000

6.2.2 PROVVEDIMENTO 10 febbraio 2000 (in G.U. 25 febbraio 2000, n. 46, p. 35)

Codici di deontologia e di buona condotta relativi ai dati personali utilizzati per finalità storiche, statistiche, di ricerca scientifica, di investigazioni difensive, e ai dati personali utilizzati da operatori sanitari e da istituzioni bancarie e finanziarie.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta del 10 febbraio 2000, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganello, componenti, e del dott. Giovanni Buttarelli, segretario generale;

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'art. 31, comma 1, lett. h), della citata legge n. 675/1996, il quale attribuisce al Garante il compito di 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;

Considerato che la legge n. 675/1996 prevede che il Garante promuova un codice di deontologia in materia di attività giornalistica (adottato il 29 luglio 1998 e pubblicato sulla G.U. n. 179 del 3 agosto 1998), nonché un codice di deontologia e di buona condotta in materia di investigazioni difensive e di dati utilizzati per far valere o difendere un diritto in sede giudiziaria (art. 22, comma 4, legge n. 675/1996);

Considerato che il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare l'art. 6, comma 1, prevede che entro sei mesi dalla data del 1° ottobre 1999, il Garante promuova la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per le finalità sopra indicate, tenendo conto della specificità dei trattamenti nei diversi ambiti;

Visti gli artt. 7, comma 5, e 10, comma 6, del medesimo decreto legislativo;

Considerato che l'art. 17, comma 3, del decreto legislativo 11 maggio 1999, n. 135, quale modificato dall'art. 3 del decreto legislativo 30 luglio 1999, n. 282, prevede che per quanto non previsto dal decreto di cui all'articolo 23, comma 1-bis, della legge n. 675/1996, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale da parte di organismi sanitari e di esercenti le professioni sanitarie è fatto oggetto di appositi codici di deontologia e di buona condotta adottati ai sensi dell'articolo 31, comma 1, lettera h), della medesima legge;

Considerata la necessità di adempiere alle predette disposizioni di legge e di promuovere altresì un ulteriore codice relativo alle attività bancarie e finanziarie in ragione dei diversi profili applicativi emersi e del loro rilievo rispetto alla generalità dei cittadini;

Considerata la necessità di osservare il principio di rappresentatività nell'ambito delle categorie coinvolte e di acquisire maggiori elementi di valutazione dai diversi soggetti potenzialmente interessati alla sottoscrizione di codici di deontologia e di buona condotta per determinati settori;

Ritenuta l'opportunità di conferire la massima pubblicità all'iniziativa del Garante e al procedimento per la sottoscrizione dei predetti codici di deontologia e di buona condotta anche attraverso la pubblicazione del presente provvedimento sulla *Gazzetta Ufficiale*;

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva, adottate dagli Stati membri;

Considerata la necessità che i codici su base nazionale siano adottati tenendo conto degli even-

tuali progetti di codici di condotta comunitari;

Riservata l'iniziativa di promuovere ulteriori codici di deontologia e di buona condotta in altri settori di rilevante interesse generale;

Visti gli atti d'ufficio e le richieste di soggetti pubblici e privati sinora pervenute;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a) del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Ugo De Siervo;

TUTTO CIÒ PREMESSO IL GARANTE:

1) promuove la sottoscrizione di uno o più codici di deontologia e di buona condotta nei settori di seguito indicati:

- a) trattamenti di dati personali per scopi storici effettuati da archivisti e utenti;
- b) trattamenti di dati personali per scopi statistici e di ricerca scientifica;
- c) trattamenti di dati personali ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato;
- d) trattamenti di dati personali effettuati da istituzioni bancarie e finanziarie;
- e) trattamenti di dati personali effettuati da organismi sanitari ed esercenti le professioni sanitarie;

2) invita tutti i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività di cui all'art. 31, comma 1, lett. h), della legge n. 675/1996, a darne comunicazione a questa Autorità entro il 31.03.2000 al seguente indirizzo: Garante per la protezione dei dati personali, Largo del Teatro Valle, 6 - 00186 Roma / fax 06.6818649 / e-mail: codici@garanteprivacy.it;

3) riserva ad altri provvedimenti la verifica della conformità alle leggi e ai regolamenti dei progetti di codici, l'esame di eventuali osservazioni, nonché le iniziative necessarie ai sensi del citato art. 31, comma 1, lett. h) per garantirne la diffusione e il rispetto.

Roma, 10 febbraio 2000

6.2.3. DELIBERAZIONE 29 febbraio 2000 n. 8 (in G.U. 18 marzo 2000, n. 65, p. 17)

Applicazione delle misure minime di sicurezza di cui al decreto del Presidente della Repubblica n. 318/1999. Modifica da apportare al modello per la notificazione del trattamento dei dati personali.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, Presidente, del prof. Giuseppe Santaniello, vice-presidente, del prof. Ugo De Siervo, dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale:

PREMESSO CHE:

- l'art. 7 della legge 31 dicembre 1996, n. 675, prevede per i titolari che intendano procedere ad un trattamento di dati l'obbligo di darne notificazione al Garante e, in caso di successive modifiche apportate per i profili indicati nel medesimo articolo, di comunicarle attraverso una successiva notificazione;
- l'art. 12, commi 1 e 3, del d.P.R. 31 marzo 1998, n. 501, stabilisce che le notificazioni sono effettuate utilizzando modelli conformi allo schema predisposto dal Garante;
- detti modelli sono stati predisposti e resi disponibili al pubblico, in particolare attraverso convenzioni con Poste italiane S.p.A. ed altri soggetti ed organismi interessati;
- l'art. 15, commi 2 e 3, della l. 675/1996 stabilisce che con regolamento devono essere individuate le misure minime di sicurezza relative ai dati personali oggetto di trattamento;
- il regolamento è stato emanato con d.P.R. n. 318 del 28 luglio 1999;
- ai sensi dell'art. 41, comma 3, della legge n. 675/1996 il termine per l'adozione delle misure minime di sicurezza previste da tale d.P.R. è fissato al 29 marzo 2000;

CONSIDERATO CHE:

- il modello di notificazione sarà aggiornato e perfezionato nel suo complesso entro la fine del corrente anno, in base all'esperienza acquisita e tenendo conto delle novità intercorse;
- l'applicazione del d.P.R. n. 318/1999 potrebbe indurre numerosi titolari dei trattamenti a modificare la precedente notificazione ai sensi dell'art. 7, commi 2 e 4 della citata legge, relativamente al riquadro d) del modello adottato dal Garante ai sensi del richiamato art. 12 del d.P.R. 31 marzo 1998, n. 501;
- si potrebbe così determinare l'afflusso al Garante di un enorme numero di notificazioni non necessarie in quanto non è indispensabile annotare nel registro generale dei trattamenti, in questa fase transitoria, modifiche di notificazioni già effettuate derivanti dall'adempimento di un obbligo di legge;

VISTE le osservazioni in atti formulate dall'Ufficio ai sensi dell'art. 7, comma 2, lett. a), del d.P.R. n. 501/1998, con nota a firma del segretario generale;

RELATORE il prof. Ugo De Siervo;

DELIBERA:

a) di inserire nel riquadro d) (*"descrizione generale delle misure adottate per la sicurezza dei dati"*) dei modelli di notificazione al Garante del trattamento dei dati personali l'avvertenza che figura in allegato alla presente deliberazione;

b) di dare atto che i soggetti che hanno notificato i trattamenti dei dati personali prima del 29 marzo 2000 non devono presentare una nuova notificazione di modifica in relazione al medesimo riquadro d) qualora abbiano adottato le misure previste dal d.P.R. n. 318 del 28 luglio 1999;

c) di consentire ai titolari dei trattamenti, in riferimento a nuove notificazioni, di continuare ad utilizzare i modelli precedentemente approvati dal Garante.

Roma, lì 29 febbraio 2000

ALLEGATO

Nel riquadro d) (*descrizione generale delle misure adottate per la sicurezza dei dati*) è inserita la seguente avvertenza:

I soggetti che hanno notificato il trattamento dei dati personali prima del 29 marzo 2000 non devono effettuare una nuova notificazione per modificare il presente riquadro, qualora abbiano adottato le misure minime previste dal d.P.R. n. 318 del 28 luglio 1999 (*"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15, comma 2, della legge 31 dicembre 1996, n. 675"*).

6.3 GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

6.3.1. Raccomandazione 4/99 sulla Carta europea dei diritti fondamentali

5143/99/IT/def.
WP 26

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 4/99 concernente l'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali

Adottata il 7 settembre 1999

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 1995,¹

visto l'articolo 29 e l'articolo 30, paragrafo 3 della direttiva,
visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO LA SEGUENTE RACCOMANDAZIONE:

Il Consiglio europeo, riunito a Colonia il 4 giugno 1999, ha deciso l'elaborazione di una Carta dei diritti fondamentali dell'Unione europea. Nella sua decisione, il Consiglio afferma: "Allo stato attuale dello sviluppo dell'Unione è necessario elaborare una Carta di tali diritti al fine di sancirne in modo visibile l'importanza capitale e la portata per i cittadini dell'Unione."

Il Gruppo, composto da rappresentanti delle autorità responsabili della protezione dei dati personali negli Stati membri dell'Unione europea, appoggia pienamente l'iniziativa del Consiglio europeo mirante ad elaborare una Carta dei diritti fondamentali dell'Unione europea. Esso rileva che alcuni paesi europei hanno incluso nella loro costituzione un diritto fondamentale alla protezione dei dati personali. In alcuni altri paesi la giurisprudenza riconosce a tale diritto il carattere di diritto fondamentale.

Nella loro prassi, la Commissione europea e la Corte europea dei diritti dell'uomo hanno definito e concretizzato un diritto fondamentale sulla base delle implicazioni che vari diritti dell'uomo hanno in materia di protezione dei dati personali.

Infine, il nuovo articolo 286 del trattato che istituisce la Comunità europea dispone che, a decorrere dal 1° gennaio 1999, gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali si applicano alle istituzioni e agli organismi europei.

Includere la protezione dei dati personali nel quadro dei diritti fondamentali europei significherebbe rendere tale protezione giuridicamente vincolante in tutta l'Unione e tener conto della crescente importanza della protezione dei dati nella società dell'informazione.

¹ GU L 281 del 23.11.1995, p. 31; il testo della direttiva è disponibile al seguente indirizzo:
<http://europa.eu.int/comm/dg15/de/media/dataprot/index.htm>

Il Gruppo raccomanda pertanto alla Commissione europea, al Parlamento Europeo e al Consiglio dell'Unione europea di includere il diritto fondamentale alla protezione dei dati personali nella Carta dei diritti fondamentali. Il Gruppo è disposto a collaborare all'elaborazione della Carta.

Fatto a Bruxelles, il 7 settembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

6.3.2. Negoziato Europa-Usa sul trasferimento dati

Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti

5092/98/IT/finale
WP 15

Gruppo di per la tutela delle persone
con riguardo al trattamento dei dati personali

Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti

Adottato il 26 gennaio 1999

Il Gruppo di lavoro è a conoscenza delle discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti al fine di garantire il duplice obiettivo di un livello elevato di tutela dei dati personali e la libera circolazione di tali dati attraverso l'Atlantico. Il Gruppo di lavoro ritiene che queste discussioni siano importanti e spera che esse potranno conseguire risultati positivi in tempi brevi. Alla luce di tali discussioni, il 4 novembre 1998 l'Ambasciatore Aaron ha inviato una lettera con allegati, contenente una serie di proposte da discutere negli Stati Uniti tra rappresentanti di società USA e il Ministero federale del Commercio. A questo proposito, il Gruppo di lavoro invita le parti e i governi degli Stati membri dell'UE rappresentati nel Comitato istituito dall'articolo 31 della Direttiva 95/46/EC² a tener conto dei punti che seguono:

Le norme sulla tutela dei dati non sono fatte solo per proteggere gli utenti delle nuove tecnologie (in particolare, informatica e Internet) al fine di garantirne la fiducia e aiutare così lo sviluppo di tali tecnologie e lo scambio internazionale di dati. Esse esprimono anche l'adesione ad alcuni principi e diritti fondamentali basati su una cultura comune di rispetto della sfera privata e di altri valori intrinseci all'essere umano e condivisi tanto dagli Stati membri dell'UE che dagli Stati Uniti.

1. Negli USA, la tutela della sfera privata e dei dati si affida a un complesso tessuto di norme settoriali, a livello federale e statale, e di autoregolamentazione dell'industria. In tempi recenti, c'è stato uno sforzo per migliorare credibilità e applicabilità degli strumenti autoregolamentari dell'industria, soprattutto in relazione ad Internet e al commercio elettronico. Il Gruppo di lavoro ritiene però che non si possa contare su questo mosaico di leggi settoriali, il cui ambito di applicazione è limitato, e di autoregolamentazione volontaria per tutelare adeguatamente tutti i casi di dati personali trasferiti dall'UE.
2. Data la complessità del sistema USA di tutela della sfera privata e dei dati, la definizione di un "punto di riferimento" convenuto della tutela in forma di "principi per un approdo sicuro", offerto a tutti gli operatori economici USA, è un buon approccio che, in casi specifici, potrebbe essere completato da soluzioni contrattuali. Tuttavia, per garantire la libera circolazione dei dati verso gli Stati Uniti in base a tali principi, sono necessari miglioramenti ulteriori. Inoltre, potrebbe rivelarsi necessario trovare metodi che chiariscano quali società

² Direttiva 95/46/EC 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, GU L 281, del 23.11.1995, p. 31.

Disponibile presso: <http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

saranno coperte dai "principi per un approdo sicuro".

3. Si noti che la decisione di aderire a tali principi riguarda solo le singole società, e, in mancanza di una legislazione globale, resta quindi il problema delle società che non vogliono applicarli.
4. In generale, va chiarito lo statuto di tali principi. Se, in prima istanza, l'adesione ai principi può essere volontaria, una volta che una società aderisce, reclamando perciò i vantaggi di un "approdo sicuro", il rispetto dei principi deve essere obbligatorio.
5. La credibilità del sistema è seriamente compromessa dalla mancanza di controlli di conformità indipendenti e dall'affidarsi alla sola autocertificazione della società. La verifica indipendente va fatta in modo serio ma al tempo stesso praticabile anche per le piccole imprese. I modelli attualmente sviluppati negli USA dal *Better Business Bureau OnLine and Trust-E* stanno andando nella giusta direzione.
6. Deve essere possibile che i reclami di singoli, i cui dati sono stati trasferiti dall'UE, siano trattati in un modo pratico ed efficace e che in ultima istanza siano giudicati da un'entità indipendente. In proposito è importante individuare uno o più enti pubblici od organizzazioni indipendenti negli USA disposti a fungere da punto di contatto per le autorità di tutela dei dati dell'UE e a indagare sui reclami. Occorre anche accertarsi che esistano accordi pratici per tutti i corrispondenti settori USA. Enti normativi già esistenti (*Federal Trade Commission; Office of the Comptroller of the Currency*) possono assumere tale ruolo nei settori di loro competenza.
7. Sui contenuti, i principi del tipo "approdo sicuro" devono comprendere, per essere accettabili, almeno tutti i principi precisati nelle direttive OCSE del 1980 sulla tutela della sfera privata, sottoscritti anche dagli Stati Uniti e recentemente riaffermati alla Conferenza OCSE di Ottawa sul commercio elettronico. Tali principi sono anche applicati dalla Direttiva 95/46/EC e dalla legislazione nazionale degli Stati membri dell'UE. In proposito, l'elenco di principi sopra ricordato, pubblicato il 4.11.1998 dal Ministero del commercio USA suscita le seguenti preoccupazioni:
 - a) il diritto di accesso delle persone è limitato a quanto è "ragionevole". Le direttive OCSE sulla tutela della sfera privata non limitano il diritto in quanto tale, affermano solo che esso va esercitato "in modo ragionevole";
 - b) manca il requisito dell'indicazione di uno scopo, presente nelle direttive OCSE, solo in parte sostituito da una possibilità di "scelta" che permette di usare per uno scopo dati raccolti per un altro, a meno che le persone non possano decidere di negarla;
 - c) i dati "proprietary" e quelli elaborati manualmente sono esclusi dall'ambito di applicazione dei principi USA; il principio della "scelta" non garantisce alcuna tutela ai dati raccolti da terzi e quello di "accesso" esclude le informazioni provenienti da pubblici registri;
 - d) secondo il terzo paragrafo dell'introduzione, "l'adesione ai principi è soggetta" a numerose eccezioni e limiti come la "gestione di rischio" e la "sicurezza delle informazioni". Per il Gruppo di lavoro si tratta di nozioni troppo vaghe e incerte: esso raccomanda che siano chiarite o cancellate.

Fatto a Bruxelles, il 26 gennaio 1999

Per il Gruppo
Il Vicepresidente
Stefano RODOTÀ

Parere 2/99 riguardante l'adeguatezza dei "principi internazionali per un approdo sicuro" stabiliti dal Ministero del commercio USA il 19 aprile 1999

5047/99/EN/final
WP 19

Gruppo per la tutela delle persone fisiche
con riguardo al trattamento dei dati personali

Parere 2/99 riguardante l'adeguatezza dei "principi internazionali per un approdo sicuro" stabiliti dal Ministero del commercio USA il 19 aprile 1999

Adottato il 3 maggio 1999

Le discussioni fra la Commissione delle Comunità europee e il Governo degli Stati Uniti sono proseguite dopo che il Gruppo di lavoro ha pubblicato, nel gennaio 1999³, il suo parere sul livello di protezione dei dati negli Stati Uniti. Recentemente, la Commissione ha presentato al Gruppo di lavoro una versione riveduta dei principi del Ministero federale del commercio per avere un suo parere sul livello di tutela dei dati che essi offrono.

La Commissione ha anche comunicato al Gruppo di lavoro che prevede l'adozione di una decisione, basata sull'articolo 25.6 della direttiva⁴, concernente questi principi, se risultano assicurare un livello adeguato di protezione per il trasferimento di dati da società europee a società statunitensi aderenti ai principi per un "approdo sicuro".

L'attuale versione dei principi non può comunque essere considerata definitiva poiché contiene varie note che indicano i campi in cui non è ancora stato raggiunto un accordo soddisfacente con gli Stati Uniti. Il Gruppo di lavoro considera quindi questo parere provvisorio e parziale. Esso è provvisorio perché i documenti non sono ancora definitivi e lo status delle FAQ (frequently asked questions - domande poste frequentemente) stabilito dal Ministero federale del commercio non è ancora stato indicato chiaramente al Gruppo di lavoro (il loro contenuto non viene quindi preso in considerazione nel presente parere). Inoltre, si tratta di un parere parziale perché il Gruppo di lavoro non dispone ancora di tutti i documenti necessari per un esame globale della situazione negli Stati Uniti, e in particolare di un quadro delle modalità d'applicazione dei principi e di un'analisi della tutela offerta dalle leggi settoriali statunitensi.

Il Gruppo di lavoro ribadisce la sua opinione che il complesso tessuto di leggi settoriali con un limitato ambito d'applicazione e di norme di autoregolamentazione attualmente esistente negli Stati Uniti non è sufficiente a fornire in tutti i casi una tutela adeguata dei dati personali trasferiti dall'Unione europea. Ritiene perciò utile l'approccio "approdo sicuro" ed incoraggia la Commissione a continuare il suo lavoro volto alla ricerca di una serie di principi che saranno adottati dal Ministero federale del commercio in modo da fornire un punto di riferimento alle società statunitensi che desiderano assicurarsi di soddisfare i requisiti di tutela adeguata stabiliti dalla direttiva.

³ Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le attuali discussioni fra la Commissione europea e il Governo degli Stati Uniti, adottato dal Gruppo di lavoro il 26 gennaio 1999.

⁴ Un progetto di decisione della Commissione è stato consegnato al Gruppo di lavoro il 30 marzo 1999.

Il Gruppo di lavoro ritiene utile esaminare le implicazioni pratiche di quest'accordo per il lavoro delle autorità di controllo nazionali.

Implicazioni pratiche dell'"approdo sicuro" per il lavoro delle autorità di controllo nazionali

Il Gruppo di lavoro ritiene molto importante che le società con sede negli Stati Uniti aderenti ai principi per un "approdo sicuro" siano individuate in modo inequivocabile e quindi considera molto opportuna la raccomandazione del Ministero federale del commercio alle società americane di notificare al Ministero la loro intenzione di aderire al programma. Il Gruppo di lavoro ritiene che tale notifica debba essere per quanto possibile completa, essere resa pubblica ed indicare in particolare una persona di contatto nella società in grado di trattare le richieste dei singoli individui e l'organo di controllo responsabile dell'applicazione dei principi.

Per poter partecipare al programma "approdo sicuro", le organizzazioni statunitensi possono partecipare a un programma sulla tutela della vita privata sviluppato dal settore privato... o farlo in base alle leggi statunitensi che proteggono efficacemente la vita privata nella misura in cui le sue attività siano disciplinate da tali leggi. Il Gruppo di lavoro chiede ulteriori chiarimenti su questi programmi e sui loro criteri operativi. Per quanto riguarda le leggi settoriali statunitensi, il Gruppo di lavoro chiede chiarimenti sul loro esatto contenuto riguardo alla tutela della vita privata.

Il Gruppo di lavoro sottolinea anche che i principi per un "approdo sicuro" si riferiscono solo alla legittimità degli aspetti internazionali del trasferimento dei dati derivanti dagli articoli 25 e 26 della direttiva. Gli esportatori di dati con sede in Europa (affiliati o meno a una società con sede negli Stati Uniti aderente all'"approdo sicuro") sono soggetti all'applicazione delle altre disposizioni della direttiva, per esempio quelle relative alla notifica del trattamento dei dati alle autorità di controllo nazionali.

Il compito delle autorità di controllo sarebbe inoltre facilitato da una descrizione precisa dei poteri delle autorità di regolamentazione. Il Gruppo di lavoro è stato informato che le autorità statunitensi stanno preparando questo documento.

Considerando il ruolo delle autorità di controllo nazionali nel rilascio delle autorizzazioni di trasferimenti internazionali basati su contratti, il Gruppo di lavoro chiede chiarimenti sul significato dell'ultima frase del paragrafo 4 dell'introduzione, che dice *"Le organizzazioni possono applicare le salvaguardie ritenute necessarie dall'UE anche per i trasferimenti di dati personali dall'UE agli USA incorporando i principi per un 'approdo sicuro' pertinenti negli accordi conclusi con parti che trasferiscono dati personali dall'UE"*.

Infine, per quanto riguarda la possibilità per le organizzazioni aderenti ai principi del Ministero federale del commercio di affidarsi alle autorità di controllo nazionali per l'applicazione dei principi, il Gruppo di lavoro sottolinea che le autorità di controllo nazionali non hanno giurisdizione nei paesi terzi e di conseguenza non dispongono dei poteri necessari per controllare efficacemente l'applicazione dei principi da parte delle organizzazioni statunitensi.

- Per quanto riguarda il contenuto dei principi stessi, il Gruppo di lavoro riconosce che rispetto alla versione del 4 novembre, sebbene i principi siano stati indeboliti sotto alcuni aspetti, sono stati compiuti progressi in vari campi, in particolare:
- La definizione dei dati personali si riferisce ora a una persona fisica identificata o identificabile;
- Le eccezioni ai principi appaiono più coerenti e riflettono in parte quelle previste nella direttiva. È il caso, in particolare, della soppressione di espressioni come "gestione del rischio", "sicurezza delle informazioni" e "dati proprietari".
- Nell'"avviso" la persona fisica va informata su un cambiamento di finalità;
- I dati "sensibili" sono ora descritti con precisione nell'articolo 2 "Scelta";
- Nei trasferimenti successivi si differenzia ora tra trasferimenti tra organizzazioni aderenti ai principi e trasferimenti verso Paesi terzi non partecipanti al programma per un "approdo sicuro".

Il Gruppo di lavoro ritiene che non si possa derogare alla norma stabilita dagli orientamenti dell'OCSE del 1980 dato che costituisce un requisito minimo per l'accettazione di un livello adeguato di tutela in qualsiasi Paese terzo. In base al lavoro svolto in precedenza dal Gruppo di lavoro sulla questione del trasferimento dei dati verso Paesi terzi⁵, i principi per un "approdo sicuro" del Ministero federale del commercio del 19 aprile pongono i problemi seguenti:

- Nell'introduzione c'è un riferimento alle eccezioni previste dalla legislazione degli Stati membri. Il Gruppo di lavoro non lo considera opportuno perché potrebbe dar luogo all'interpretazione delle misure d'applicazione nazionali da parte di organizzazioni aderenti a un programma di autoregolamentazione di un Paese terzo. Il Gruppo di lavoro ritiene inoltre che limitare l'applicazione dei principi per un "approdo sicuro" alla misura necessaria per soddisfare le disposizioni regolamentari statunitensi sia un'esenzione troppo ampia, i cui limiti non sono prevedibili.

- Riguardo ai dati trattati manualmente, il Gruppo di lavoro giudica che dovrebbe esserci uguaglianza di trattamento per i dati elaborati elettronicamente e quelli elaborati a mano conservati negli archivi. Esso approva quindi le riserve formulate dalla Commissione nelle note, ma ritiene anche che le organizzazioni aderenti ai principi per un "approdo sicuro" che applicano tali principi ai dati elaborati manualmente debbano poter beneficiare, se lo desiderano, dei vantaggi dell'"approdo sicuro" per i dati raccolti in Europa.

Principi 1 e 2: Avviso e scelta

Considerando che la tutela offerta dai principi per un "approdo sicuro" si basa sul concetto di "avviso e scelta", è molto importante che questi principi offrano una protezione della vita privata completa sia per quanto riguarda l'utilizzazione che la divulgazione dei dati.

Per quanto riguarda il principio di "avviso", affinché sia coerente con il principio di "sicurezza dei dati", si ricorda che la persona va informata che saranno raccolti dati solo nei limiti necessari per soddisfare le finalità della raccolta stessa.

Va inoltre reinserita l'espressione "quale tipo di informazioni" perché è importante che la persona sappia che tipo di informazioni personali si raccolgono su di lei.

È necessario anche indicare esplicitamente che la persona va avvisata del trattamento effettuato da un'organizzazione statunitense se i dati non sono stati forniti direttamente bensì da terzi. Ciò è importante nell'ambito dell'opportunità di "scelta".

Il Gruppo di lavoro chiede chiarimenti riguardo all'esatto significato dell'espressione "non appena possibile", dato che ritiene che la persona vada informata al momento della raccolta e non a discrezione dei singoli controllori.

Per quanto riguarda il principio di "scelta", come indicato nel parere precedente, manca il principio di specificazione della finalità degli orientamenti dell'OCSE, sostituito solo parzialmente dal principio di "scelta", che permette in effetti che dati raccolti per una data finalità siano utilizzati per un'altra.

Le persone hanno inoltre la possibilità di opporsi solo se la nuova finalità è considerata incompatibile con quella indicata nell'"avviso". Secondo il parere del Gruppo di lavoro, la persona dovrebbe almeno avere la possibilità di opporsi in tutti i casi in cui i suoi dati vengono utilizzati per finalità non pertinenti e per una commercializzazione diretta. Il livello di consenso è più alto, ad esempio, quando i dati sono raccolti nell'ambito di un rapporto contrattuale e sono soggetti ai termini impliciti o espliciti di un contratto.

Ciò è particolarmente importante perché inevitabilmente in un sistema di autoregolamentazione non esiste una valutazione indipendente di cosa sia una finalità incompatibile o dei criteri per stabilire l'incompatibilità della finalità con quanto stabilito nell'"avviso".

Il Gruppo di lavoro è anche del parere che qualsiasi consenso sia richiesto, esso debba esse-

⁵ Trasferimento di dati verso Paesi terzi: applicazione degli articoli 25 e 26 della direttiva sulla tutela dei dati, approvata dal Gruppo di lavoro il 24 luglio 1998.

re concesso liberamente, in maniera specifica e informata, e che la mancanza di una risposta non possa essere interpretata come un tacito consenso.

Infine, per quanto riguarda l'ultima frase del principio di "scelta", il Gruppo di lavoro chiede chiarimenti sull'esatto significato del termine "o" nell'espressione "scelta (di opporsi) affermativa o esplicita", nel senso di "scelta affermativa, cioè esplicita".

Principio 3: Trasferimenti successivi

Sebbene non sia presente negli orientamenti dell'OCSE, questo principio è necessario per garantire che i dati non vengano trasferiti da una società statunitense che rispetta i principi per un "approdo sicuro" ad un altro controllore situato negli Stati Uniti o altrove che non garantisce una tutela adeguata. In base all'attuale progetto non è chiaro quale sia la regola da applicare. L'individuo dovrebbe essere in grado di opporsi al trasferimento a una terza parte. Per questo motivo, egli deve almeno essere informato sul trasferimento dei dati e sull'adesione o meno della terza parte ai principi per un "approdo sicuro", o su quale altra tutela adeguata venga fornita. Il Gruppo di lavoro sostiene quindi la richiesta della Commissione, espressa nella nota 5, che un avviso e una scelta espliciti vadano offerti quando i dati personali sono trasferiti a una terza parte non aderente ai principi per un "approdo sicuro".

Principio 6: Accesso

Si sottolinea che non esiste un accordo sul testo del principio 6. Secondo il parere del Gruppo di lavoro, il principio 6 dovrebbe affermare chiaramente che in generale l'accesso va concesso sebbene esistano alcune restrizioni, descritte chiaramente nel testo. Nell'articolo 13 la direttiva menziona una serie di deroghe. Un esempio potrebbero essere i "segreti commerciali", sebbene i partecipanti ritengano che a livello degli Stati membri questo problema non potrebbe mai portare al rifiuto di ogni informazione alla persona interessata. Nei suoi contatti con il Ministero federale del commercio, a questo proposito la Commissione dovrebbe essere guidata dagli orientamenti dell'OCSE. Il Gruppo di lavoro propone il seguente testo come base di lavoro:

"Le persone interessate devono avere accesso alle informazioni che le riguardano raccolte da un'organizzazione ed avere il diritto di rettificare ed emendare i dati inesatti, fuorché nel caso in cui quest'accesso danneggi l'organizzazione rivelando segreti commerciali o non rispettando i diritti di proprietà intellettuale o se gli oneri e i costi o le altre conseguenze che il reperimento delle informazioni comporta per l'organizzazione risultano chiaramente sproporzionati rispetto ai rischi specifici derivanti dalla mancata rivelazione per la tutela della riservatezza dell'individuo."

Il principio dovrebbe inoltre specificare chiaramente il diritto della persona interessata alla cancellazione dei dati se il relativo trattamento è illegale.

Per i motivi indicati nell'introduzione, il Gruppo di lavoro non ha esaminato il testo delle domande poste frequentemente (FAQ) sull' "accesso".

Principio 7: Applicazione

Dal testo del principio stesso e da quello della "nota" non è sufficientemente chiaro lo standard richiesto alle società. Secondo il parere del Gruppo di lavoro, le norme di tutela dei dati contribuiscono alla protezione degli individui solo se sono applicate in pratica. In un programma completamente volontario come questo, l'osservanza delle norme deve essere garantita almeno da un meccanismo d'indagine indipendente per reclami e sanzioni, che devono avere carattere deterrente ed offrire, se opportuno, un risarcimento alle persone. Il testo presente del principio 7 dice che il risarcimento sarà fornito solo se "la legge applicabile e le iniziative del settore privato lo richiedono". Il Gruppo di lavoro approva fortemente anche la richiesta della Commissione che le società debbano soddisfare tutte le condizioni descritte nel principio 7 prima di poter essere giudicate in regola con i principi per un "approdo sicuro".

Il principio 7 non stabilisce inoltre le norme da seguire per verificare la conformità e non indica le autorità responsabili dell'applicazione dei principi. Analogamente, dovrebbe essere indicato il tipo di sanzioni previste, chi le impone e in base a quali procedure.

Come indicato nell'introduzione, per quanto riguarda la cooperazione fra le autorità di con-

trollo nazionali e le organizzazioni con sede negli Stati Uniti che desiderano partecipare all' "approdo sicuro", il Gruppo di lavoro non ritiene possibile che l'applicazione dei principi sia affidata alle autorità di controllo nazionali. Tuttavia, se negli Stati Uniti l'applicazione è garantita da organi di controllo indipendenti, potrebbe essere prevista una cooperazione *ad hoc* fra questi organi e le autorità di controllo nazionali.

Conclusioni

Sulla base di quanto precede, il Gruppo di lavoro invita la Commissione a continuare gli sforzi di dialogo con il Ministero federale del commercio per rafforzare la tutela offerta nei "principi internazionali per un approdo sicuro".

In particolare, il Gruppo di lavoro invita la Commissione a prendere in considerazione gli interrogativi sollevati e ad informarlo sugli ulteriori contatti con il Ministero del commercio USA.

Fatto a Bruxelles, il 3 maggio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

Parere 4/99 riguardante le FAQ (domande poste frequentemente) che saranno pubblicate dal Ministero del Commercio USA in relazione ai principi "Approdo sicuro" (Safe Harbor) proposti

5066/99/IT/def.
WP 21

Gruppo di lavoro sulla tutela delle persone fisiche
con riguardo al trattamento dei dati personali

Parere 4/99 riguardante le FAQ (domande poste frequentemente) che saranno pubblicate dal Ministero del Commercio USA in relazione ai principi "Approdo sicuro" (Safe Harbor) proposti

Adottato il 7 giugno 1999

Nel parere 2/99¹ adottato il 3 maggio 1999, riguardante i principi internazionali "Safe Harbor" (qui di seguito denominati "i principi"), il Gruppo di lavoro non aveva preso in considerazione le domande poste frequentemente (qui di seguito "le FAQ") pubblicate dal Ministero del Commercio USA il 30 aprile 1999. Prima di esprimere un parere sul contenuto delle FAQ, il Gruppo di lavoro ha chiesto che sia chiarito il loro status.

Il 2 giugno 1999 la DG XV ha trasmesso al Gruppo di lavoro la lettera inviata ai membri del Comitato istituito dall'articolo 31 della direttiva 95/46/CE e tutti i documenti allegati, in particolare una versione riveduta e riservata dei principi "Safe Harbor" e un elenco delle FAQ, sei delle quali sono allegate all'elenco³.

Dopo aver esaminato la lettera di cui sopra, il Gruppo di lavoro ritiene che la parte americana abbia intenzione di pubblicare le FAQ come guida autorevole ai principi e che ciò debba riflettersi nella versione definitiva della decisione relativa all'articolo 25(6).

Il Gruppo di lavoro riconosce che questa soluzione sarebbe auspicabile per due ragioni: da un lato permetterebbe di chiarire e, in alcuni casi, di completare i principi per quanto riguarda talune categorie di operazioni di trattamento, il che sarebbe di aiuto nella valutazione dei principi stessi; dall'altro, la guida autorevole aiuterebbe gli organi di reclamo ad interpretare ed applicare i principi ai casi concreti. Tuttavia, questo richiede che, prima di prendere una decisione sull'adeguatezza dei principi, tutte le FAQ siano prese nella dovuta considerazione. Il Gruppo di lavoro ritiene che tale attenta valutazione sia richiesta dall'articolo 25(2) della direttiva, secondo il quale "l'adeguatezza del livello di protezione è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati".

Il Gruppo di lavoro osserva che è stato redatto un elenco di FAQ comprendente quindici domande, cinque in più rispetto alle nove FAQ diffuse in aprile e maggio. Esso rileva inoltre che, rispetto alla versione precedente, sono state apportate varie modifiche alle FAQ allegate alla lettera della DG XV.

¹ Parere 2/99 sull'adeguatezza dei principi internazionali "Safe Harbor" stabiliti dal Ministero del Commercio USA il 19 aprile 1999, adottato il 3 maggio 1999, disponibile in: <http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

² Stabilita dall'articolo 29 della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, GU L 281, 23 novembre 1995, p. 31. Disponibile in: v. nota 1.

³ Cfr. allegato 1: Elenco delle FAQ. Cfr. allegato 2: FAQ, n. 1 - 6, versione 1° giugno 1999.

⁴ Il testo relativo a queste 6 nuove FAQ non era disponibile il 3 giugno.

Il Gruppo di lavoro ritiene che un termine ragionevole sia indispensabile per procedere a una valutazione attenta delle FAQ, come richiesto dall'articolo 25 della direttiva. Il termine dovrebbe permettere in particolare le opportune consultazioni interne a livello nazionale secondo la procedura stabilita all'articolo 31 della direttiva. Il presente parere intende fornire solo un quadro preliminare sul possibile status delle FAQ e sulle FAQ distribuite il 2 giugno 1999, senza che ciò influisca sui commenti che il Gruppo di lavoro intende presentare sulla nuova versione dei principi e sulle FAQ ancora da distribuire, né sulla valutazione globale dell'approccio "Safe Harbor", dato che sarà necessario considerare altri elementi del dossier (p. es.: il progetto di scambio di lettere).

I. Status delle FAQ

In base a quanto precede, il Gruppo di lavoro è dell'opinione che:

1. le FAQ elencate nell'allegato dovrebbero avere, quando saranno pubblicate dal Ministero del Commercio USA, uno status vincolante a condizione che siano coerenti con i principi "Safe Harbor" e vengano considerate insieme ad essi;
2. è necessaria un'attenta valutazione di tutte le FAQ, entro un termine ragionevole per le consultazioni interne, prima di stabilire se i principi "Safe Harbor" forniscono un livello adeguato di protezione;
3. la decisione eventualmente presa in relazione ai principi dovrebbe contenere un riferimento alle FAQ;
4. l'elenco definitivo delle FAQ dovrà essere completo e nessuna modifica dovrà essere apportata unilateralmente. Esse dovranno comunque essere considerate alla luce dell'esperienza in sede di esame dell'attuazione dell'accordo "Safe Harbor" e potranno eventualmente essere adattate e/o integrate.

II. Elenco delle FAQ

Il Gruppo di lavoro accoglie con favore il principio di un ampliamento dell'elenco delle FAQ e ritiene che, data la mancanza di chiarezza di alcuni principi, le FAQ dovrebbero fornire una guida autorevole, chiara ed inequivocabile ai controllori di dati, nonché le necessarie garanzie alle persone fisiche interessate. Il Gruppo di lavoro desidera esaminare al più presto i rimanenti testi di progetti di FAQ ed attribuisce particolare importanza a:

1. "indagini indipendenti sui reclami" (FAQ n. 11). Dato che non sono stati apportati miglioramenti al principio dell'"applicazione" e in mancanza di garanzie equivalenti, il Gruppo di lavoro conferma che la credibilità del "Safe Harbor" nel suo insieme dipende soprattutto da una risposta soddisfacente a quest'elemento del principio di applicazione;
2. "possibilità di opporsi" (FAQ n. 13). Secondo il principio di "scelta", la possibilità di opporsi è data solo se "l'utilizzazione e la divulgazione sono incompatibili con la finalità per la quale l'informazione personale è stata raccolta originariamente o con qualsiasi altra finalità o divulgazione indicata in un avviso alla persona". Nel suo parere 2/99, il Gruppo di lavoro ha già presentato e motivato le sue obiezioni a questa ristretta nozione di "scelta" e ha suggerito alcuni miglioramenti. Il modo migliore per raggiungere quest'obiettivo rimane un miglioramento del principio, tenendo presente i suggerimenti fatti precedentemente nel parere 2/99, il che significa introdurre almeno una possibilità incondizionata di opporsi alla commercializzazione diretta.

III. Dati sensibili (FAQ n. 1)

Il Gruppo di lavoro ribadisce la sua opinione, espressa nel parere 2/99, che i principi "Safe Harbor" riguardano solo la legittimità degli aspetti internazionali dei trasferimenti di dati (articoli 25 e 26 della direttiva). Esso ricorda che i controllori di dati con sede nell'UE (affiliati o meno a organizzazioni americane aderenti al "Safe Harbor") sono soggetti alle disposizioni nazionali di applicazione delle altre norme della direttiva, vale a dire quelle relative alla legittimità del trattamento (articoli 6 e 7) e agli ulteriori requisiti riguardanti i dati sensibili (articolo 8). Lo stesso vale se orga-

nizzazioni americane raccolgono dati personali direttamente nell'UE. Il Gruppo di lavoro sottolinea che, per evitare equivoci, le FAQ dovrebbero comprendere i punti suddetti.

In particolare va ricordato che gli Stati membri possono stabilire che il consenso della persona interessata non sia sufficiente per derogare al divieto di trattare dati sensibili (art. 8, paragrafo 2a della direttiva) e che può essere richiesta una notifica preventiva alle autorità di controllo.

IV. Eccezioni riguardanti il trattamento dei dati personali a scopi giornalistici (FAQ n. 2)

Il Gruppo di lavoro considera molto importante la libertà di stampa e ritiene che la direttiva dimostri il giusto equilibrio lasciando agli Stati membri la possibilità di prevedere esenzioni e deroghe (articolo 9). Tuttavia, tali deroghe riguardano solo i capitoli III, IV e VI e non si applicano alle altre disposizioni della direttiva, come la sicurezza dei trattamenti (articolo 17). Il Gruppo di lavoro sottolinea che, a suo parere, la FAQ riguarda il trattamento esclusivamente per scopi giornalistici coperti dal primo emendamento e che il principio di sicurezza, lungi dall'essere in conflitto con la libertà di stampa, intende favorire anche i giornalisti (in particolare, proteggere le loro fonti e il loro lavoro nei casi di accesso o divulgazione non autorizzati, di perdita o alterazione accidentale o illegale, specialmente se il trattamento comporta la trasmissione di dati attraverso una rete). Il Gruppo di lavoro ritiene perciò che non ci sia motivo di derogare al principio di sicurezza definito nel "Safe Harbor".

V. Responsabilità secondaria (FAQ n. 3)

Secondo il Gruppo di lavoro questo testo non presenta difficoltà, a condizione che venga interpretato in senso stretto ed applicato solo alla situazione descritta nella domanda.

VI. Cacciatori di teste ecc. (FAQ n. 4)

Nel suo parere 2/99, il Gruppo di lavoro aveva già riaffermato l'irrinunciabilità dello standard stabilito dagli orientamenti dell'OCSE del 1980, che costituisce un requisito minimo per l'accettazione di un livello adeguato di protezione.

Il Gruppo di lavoro nota che la FAQ introduce eccezioni non menzionate nei principi stessi. Sarebbe necessario spiegare quali operazioni di trattamento sono coperte da ciascuna delle eccezioni menzionate e perché sono di carattere limitato. Inoltre, andrebbe chiarito per quali principi (avviso, scelta) il requisito di interesse legittimo dell'organizzazione e di interesse pubblico prevede esenzioni. Infine, la legittimità dell'attività di un cacciatore di teste o di un "investment banker" sembra dipendere da altri fattori non menzionati.

VII. Il ruolo delle autorità di protezione dei dati (FAQ n. 5)

Il Gruppo di lavoro apprezza il chiarimento introdotto da questa FAQ e ritiene auspicabile una più ampia considerazione positiva della questione, specialmente per quanto riguarda il ruolo che le autorità nazionali di protezione dei dati potrebbero svolgere nella gestione dei reclami. Varie questioni richiedono tuttavia un esame più dettagliato, in particolare:

- come sarà esercitata l'opzione, che cosa determinerà l'identità dell'«autorità pertinente di protezione dei dati» e se sarà ancora necessario l'accordo dell'autorità interessata;
- per alcune autorità, la compatibilità di questo ruolo con i loro poteri ed obblighi statutari, stabilita e limitata dalle leggi nazionali;
- l'impatto sulle risorse.

Se quest'esame conferma che le autorità possono svolgere un ruolo costruttivo, il Gruppo di lavoro ritiene necessari:

- una definizione più precisa possibile dei casi in cui la loro partecipazione diretta può essere una soluzione appropriata e praticabile;
- una chiara comprensione dell'adozione di seguito richiesta nei casi in cui un'organizzazione

ne americana non rispetta il suo impegno di cooperare con l'autorità di protezione dei dati.

Il Gruppo di lavoro sottolinea in ogni caso l'importanza di assicurare che i tre elementi del principio 7 (risoluzione delle controversie e dei ricorsi, verifica e sanzioni) siano garantiti per tutti i partecipanti al "Safe Harbor", indipendentemente dal meccanismo prescelto, e che le procedure siano accessibili e facili da seguire per le persone interessate.

VIII. Autocertificazione (FAQ n. 6)

Il Gruppo di lavoro ribadisce la sua preoccupazione che l'autocertificazione possa portare ad abusi. Esso ritiene che, in caso di falsa dichiarazione nell'ambito dei criteri di qualifica (p. es. se un'organizzazione non soddisfa i requisiti del principio 7), il responsabile debba essere cancellato dall'elenco. Lo stesso vale per le organizzazioni con sede negli Stati Uniti aderenti agli accordi "Safe Harbor" che si sono impegnate a cooperare con un'autorità europea di protezione dei dati e non rispettano pienamente tale impegno.

Fatto a Bruxelles, il 7 giugno 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

ALLEGATO 1: ELENCO DELLE FAQ, VERSIONE 1° GIUGNO 1999
ELENCO DELLE FAQ NEL QUADRO DEI PRINCIPI "SAFE HARBOR"

- 1) DATI SENSIBILI
- 2) ECCEZIONI RIGUARDANTI IL TRATTAMENTO DEI DATI PERSONALI A SCOPI GIORNALISTICI
- 3) RESPONSABILITÀ SECONDARIA
- 4) CACCIATORI DI TESTE
- 5) IL RUOLO DELLE AUTORITÀ DI PROTEZIONE DEI DATI
- 6) AUTOCERTIFICAZIONE
- 7) VERIFICA
- 8) ACCESSO
- 9) DATI SULLE RISORSE UMANE
- 10) CONTRATTI DELL'ARTICOLO 17
- 11) INDAGINE INDIPENDENTE SUI RECLAMI
- 12) GESTIONE DEI RISCHI
- 13) POSSIBILITÀ DI OPPORSI
- 14) PRENOTAZIONE VOLI AEREI
- 15) FARMACEUTICA

ALLEGATO 2: TESTO DELLE FAQ N. 1 - 6, VERSIONE 1° GIUGNO 1999

Domande poste frequentemente (FAQ)

FAQ N. 1 - Dati sensibili - 31 maggio 1999

Q: Un'organizzazione deve sempre offrire un'esplicita possibilità di opporsi per quanto riguarda i dati sensibili?

A: No, tale possibilità non è richiesta se il trattamento è: (1) nell'interesse vitale della persona interessata o di un'altra persona; (2) necessario per presentare azioni o ricorsi giudiziari; (3) richiesto per fornire cure o diagnosi mediche; (4) effettuato nel corso di attività legittime da parte di una fondazione, associazione o altro ente senza scopo di lucro con un obiettivo politico, filosofico, religioso o sindacale e a condizione che il trattamento riguardi solo i membri dell'ente o le persone che hanno regolare contatto con tale ente in connessione con le sue finalità e che i dati siano rivelati ad una terza parte senza il consenso delle persone interessate; (5) necessario per adempiere gli obblighi di un'organizzazione nel campo della legislazione del lavoro; (6) connesso a dati che sono resi manifestamente pubblici dalla persona interessata o sono necessari per azioni o ricorsi giudiziari.

FAQ n. 2 - Eccezioni riguardanti il trattamento di dati personali a scopi giornalistici - 31 maggio 1999

Q: Dato che la costituzione americana tutela la libertà di stampa e la direttiva prevede un'esecuzione per il materiale giornalistico, i principi "Safe Harbor" si applicano alle informazioni raccolte, detenute o diffuse per scopi giornalistici?

A: Nel caso in cui i diritti di libertà di stampa tutelati dal primo emendamento della costituzione americana siano in contrasto con gli interessi di tutela della privacy, il primo emendamento deve assicurare l'equilibrio di questi interessi per quanto riguarda le attività dei cittadini o delle organizzazioni americane. Le informazioni raccolte per la pubblicazione, la trasmissione o altre forme di comunicazione pubblica di materiale giornalistico, utilizzate o meno, nonché le informa-

zioni ricavate da materiale già pubblicato diffuso da archivi di media, non sono soggette ai principi "Safe Harbor".

FAQ n. 3 - Responsabilità secondaria - 31 maggio 1999

Q: I fornitori di servizi Internet, le società di telecomunicazioni o le altre organizzazioni sono soggette ai principi "Safe Harbor" se, per conto di un'altra organizzazione, provvedono soltanto a trasmettere, instradare, smistare od occultare informazioni che possono violarne i termini?

A: No. Come nel caso della direttiva stessa, il "Safe Harbor" non crea una responsabilità secondaria. Se un'organizzazione agisce da tramite per i dati e non stabilisce le finalità e i mezzi di trattamento dei dati personali, non sarà responsabile.

FAQ N. 4 - Cacciatori di teste, banche d'investimento e revisione dei conti - 30 aprile 1999

Q: Alcune attività economiche richiedono necessariamente il trattamento di dati personali senza che la persona interessata ne sia a conoscenza, ad esempio le attività di cacciatori di teste, delle banche d'investimento e dei revisori dei conti. I principi "Safe Harbor" lo permettono?

A: Sì. Come nel caso della direttiva stessa, il "Safe Harbor" non introduce l'obbligo incondizionato di ottenere il consenso delle persone interessate, per informarle sul trattamento dei loro dati o dare loro accesso ai propri dati. Le eccezioni sono permesse, ad esempio, per esigenze di interesse pubblico o se il trattamento è necessario per interessi legittimi perseguiti dalle organizzazioni o da terzi a cui i dati sono rivelati, tranne nel caso in cui i diritti di privacy dell'individuo prevalgono su tali interessi. Le attività dei cacciatori di teste, delle banche di investimento e dei revisori dei conti sono interessi legittimi.

FAQ n. 5 - Il ruolo delle autorità di protezione dei dati³

Q: Come saranno presi e realizzati gli impegni delle società intenzionate a cooperare con le autorità europee di protezione dei dati?

A: Nel quadro del "Safe Harbor", le organizzazioni americane che ricevono dati dall'UE devono impegnarsi ad utilizzare meccanismi efficaci per assicurare il rispetto dei principi "Safe Harbor". In particolare, devono fornire (1) mezzi di ricorso per le persone a cui si riferiscono i dati, (2) procedure di seguito per verificare se le attestazioni e le dichiarazioni relative alla tutela della sfera privata sono veritiere e (3) l'obbligo di risolvere i problemi che nascono dal mancato rispetto dei principi e dalle sue conseguenze per tali organizzazioni. Il principio di applicazione permette alle organizzazioni di impegnarsi a cooperare con le autorità di protezione dei dati (DPA - Data Protection Authorities) dell'Unione europea come mezzo per soddisfare il principio di applicazione nel quadro del "Safe Harbor". Le organizzazioni che scelgono questa possibilità dovranno seguire la procedura di notifica e le altre condizioni indicate qui di seguito.

PROCEDURA DI NOTIFICA

Un'organizzazione può impegnarsi a cooperare con le DPA dichiarando nella sua notifica "Safe Harbor" al Ministero del Commercio che l'organizzazione:

(1) sceglie di soddisfare i punti (a) e (c) del principio di applicazione "Safe Harbor" impegnandosi a cooperare con le DPA competenti;

(2) coopererà con la DPA competente nell'esame e nella risoluzione dei ricorsi presentati nel quadro del "Safe Harbor";

(3) conformemente alle decisioni di cui all'articolo 25, paragrafo 6, e al progetto di documento sulle procedure UE, rispetterà qualsiasi decisione delle DPA, se queste stabiliscono che l'organizzazione deve adottare ulteriori misure per rispettare i principi "Safe Harbor", comprese le misure di risarcimento o di compensazione a favore delle persone interessate dal mancato rispetto dei principi e dalle sue conseguenze per l'organizzazione.

³ Testo distribuito ai partecipanti durante l'ultima riunione del Comitato dell'articolo 31, il 21 maggio. Diventerà una FAQ se le autorità nazionali di protezione dei dati accettano di svolgere questo ruolo.

FUNZIONAMENTO

Nelle situazioni "Safe Harbor" in cui le organizzazioni americane hanno scelto di cooperare con le autorità di protezione dei dati, i consumatori, i lavoratori o altri interessati europei, dopo aver presentato un reclamo all'organizzazione americana, possono sottoporre il caso, se non è stata raggiunta una soluzione, alla DPA competente. Questa si rivolge a sua volta all'organizzazione importatrice americana per ogni questione relativa al reclamo. Nel caso in cui i reclami o altre questioni specifiche portino la DPA a compiere ulteriori indagini, l'organizzazione americana è tenuta a cooperare con la DPA, nel quadro della notifica "Safe Harbor" al Ministero del Commercio.

Questo significa, ad esempio, che l'organizzazione americana deve rispondere a domande della DPA e mettersi a sua disposizione, fornire informazioni o dati raccolti su richiesta della DPA, informare sulle misure di sicurezza o fornire alla DPA un accesso fisico o remoto a banche di dati e altre strutture di dati. L'organizzazione americana fornisce le informazioni richieste alle DPA in Europa. Le DPA non devono recarsi negli USA per esaminare i reclami.

Se le parti stesse accettano di risolvere il reclamo, cancellando una persona da un elenco postale o correggendo o eliminando determinati dati, l'organizzazione americana, in conformità al suo impegno di cooperazione, è tenuta ad applicare tale accordo per quanto riguarda i dati pertinenti conservati negli USA. Se le parti non riescono a giungere ad un accordo sul rispetto dei principi "Safe Harbor" o sulle misure di risarcimento o di compensazione che devono essere prese dalle società americane, la decisione spetta alla DPA. L'organizzazione americana è tenuta, in base al suo impegno pubblico, ad attenersi ai risultati di queste procedure, con riserva delle procedure di revisione stabilite nel progetto di documento sulle procedure dell'UE.

Questi risultati sono essenzialmente gli stessi che si otterrebbero se un'organizzazione americana non rispettasse le decisioni di un organo di autodisciplina. La differenza è che l'indagine e la determinazione del rispetto dei principi e delle sanzioni sono effettuate in prima istanza dalla DPA senza prima utilizzare i meccanismi di ricorso offerti da un organo di autodisciplina negli USA.

Ciò non dovrebbe essere eccessivamente gravoso per le DPA. In assenza di quest'opzione di applicazione nel quadro del "Safe Harbor", le DPA sarebbero obbligate in ogni caso a indagare e a prendere decisioni sui ricorsi relativi a trasferimenti di dati negli USA, ma tale applicazione avverrebbe in una fase successiva della procedura di ricorso stabilita nel progetto di documento sulle procedure dell'UE.

MOTIVAZIONE

La scelta di impegnarsi a cooperare con le DPA è, per vari motivi, un'importante alternativa di applicazione per le organizzazioni americane. In primo luogo, ricorrere al settore privato per trovare una soluzione negli Stati Uniti non è un modo ideale per risolvere questioni di protezione dei dati che sorgono da rapporti di lavoro in Europa. La cooperazione con le DPA sarebbe un'alternativa molto migliore per questo tipo di ricorsi. In secondo luogo, quest'opzione di applicazione potrebbe permettere alle organizzazioni americane di conformarsi al "Safe Harbor" più velocemente che affidandosi a meccanismi di autodisciplina sviluppati negli USA. È improbabile che i meccanismi di autodisciplina siano disponibili per tutte le categorie di trasferimento di dati verso gli Stati Uniti non appena il "Safe Harbor" sarà in vigore. Alcuni programmi del settore privato sono in via di elaborazione, ma lo sviluppo completo e l'attuazione di questi e di altri programmi si protrarranno indubbiamente fino alla chiusura delle discussioni sul "Safe Harbor". L'impegno a cooperare con la DPA può contribuire a colmare questa lacuna. Quest'opzione permetterebbe infine a più organizzazioni americane di partecipare al "Safe Harbor". Alcune organizzazioni americane possono avere difficoltà, data la relativa singolarità della loro attività o per altre ragioni, a trovare organismi di autodisciplina in grado di rispondere ai loro bisogni specifici. Inoltre, può non esserci un ente regolatore o statuario americano autorizzato a trattare tali reclami. L'impegno a cooperare con le DPA permetterebbe comunque a queste organizzazioni di conformarsi al "Safe Harbor".

FAQ n. 6 - Autocertificazione - 31 maggio 1999*

Q: Come può un'organizzazione autocertificare che aderisce ai principi "Safe Harbor"?

A: Per autocertificare l'adesione al "Safe Harbor", le organizzazioni devono fornire al Ministero del Commercio o a una persona da esso designata una lettera firmata da un loro funzionario, contenente almeno le seguenti informazioni:

- nome dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax;
- descrizione delle principali attività dell'organizzazione;
- descrizione delle disposizioni adottate dall'organizzazione in materia di tutela della privacy, precisando dove il pubblico può prenderne conoscenza;
- la data della loro effettiva applicazione;
- la persona con cui prendere contatto per il trattamento dei reclami, delle richieste di accesso e di qualsiasi altra questione relativa al "Safe Harbor";
- gli organi statutari specifici competenti a esaminare i reclami contro l'organizzazione riguardanti possibili pratiche sleali o ingannevoli;
- il nome dei programmi relativi alla privacy a cui partecipa l'organizzazione;
- il metodo di verifica (p. es. all'interno della società, effettuata da terzi)*;
- il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti.

Il Ministero (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che si autocertificano per il "Safe Harbor". Quest'elenco e le lettere di autocertificazione presentate dalle organizzazioni saranno resi pubblici. Tutte le organizzazioni che si autocertificano per il "Safe Harbor" devono specificare nelle loro dichiarazioni pubbliche sulla politica in materia di privacy che esse aderiscono ai principi "Safe Harbor". Qualsiasi falsa dichiarazione resa al Ministero o in pubblico sull'adesione dell'organizzazione ai principi "Safe Harbor" è perseguibile dalla Commissione federale per il commercio o da un altro organo statutario competente.

Fatto a Bruxelles, il 7 giugno 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

* Dato che la FAQ sull'autocertificazione descrive le informazioni che le società devono fornire al Ministero del Commercio per essere iscritte nel registro "Safe Harbor", questo testo non dovrebbe più essere una FAQ, ma essere allegato ai principi "Safe Harbor" stessi. La parte americana è disposta ad accettare questo, se otterrà soddisfazione sullo status delle FAQ.

* Vedere FAQ sulla verifica

Documento di lavoro sullo stato attuale delle discussioni in corso tra la Commissione europea e il governo degli Stati Uniti in merito ai principi internazionali dell'“approdo sicuro” (“Safe harbor”)

5075/99/IT/def.
WP 23

Gruppo di lavoro sulla tutela delle persone fisiche
con riguardo al trattamento dei dati personali

Documento di lavoro sullo stato attuale delle discussioni in corso tra la Commissione europea e il governo degli Stati Uniti in merito ai principi internazionali dell'“approdo sicuro” (“Safe harbor”)

Adottato il 7 luglio 1999

Il presente documento non costituisce un parere del gruppo di lavoro Istituito in virtù dell'articolo 29 della direttiva 95/46/CE in merito alle disposizioni dell'“approdo sicuro”, ma semplicemente un messaggio indirizzato al comitato Istituito in virtù dell'articolo 31 della direttiva, che si riunirà il 14 luglio, per renderlo partecipe di alcune delle opinioni emerse in seno al gruppo di lavoro nella sua riunione del 7 luglio.

Richiamandosi al contenuto dei pareri 1/99, 2/99 e 4/99 (acclusi al presente documento, per semplicità, rispettivamente come Allegati 1, 2 e 3), il gruppo di lavoro fa presente quanto segue.

Il gruppo di lavoro è pienamente consapevole dell'importanza del dibattito in corso tra UE e USA in materia di tutela dei dati e delle ripercussioni che la posizione che verrà adottata avrà per la maggior parte degli altri paesi terzi. È cosciente anche dei vincoli di tempo che tali discussioni presentano e delle difficoltà determinate dalla disparità degli approcci in campo politico, economico e culturale.

Finora il gruppo di lavoro ha scrupolosamente esaminato le successive versioni dei principi dell'“approdo sicuro” nonché delle domande più correnti (Frequently Asked Questions - FAQ), apparse successivamente e non ancora tutte formulate in via definitiva, tra cui alcune delle più importanti. Essendo stato informato dalla Commissione che le FAQ costituiranno parte integrante delle disposizioni dell'“approdo sicuro” e assumeranno lo stesso valore vincolante dei principi, il gruppo di lavoro ritiene che per l'avvenire il suo approccio debba includere entrambi i testi e che sia pertanto suo compito emettere un parere riguardante tanto i principi quanto le FAQ. Ne consegue che finché il gruppo di lavoro non disporrà di tutte le FAQ annunciate dalla controparte americana, nonché dei relativi testi giuridici, esso non sarà in grado di formulare un parere completo e definitivo in merito alle disposizioni dell'“approdo sicuro”.

Con riferimento alle discussioni della riunione del 7 luglio, il gruppo di lavoro desidera attirare l'attenzione del comitato sui seguenti punti:

(base giuridica) - Nell'interesse reciproco di entrambe le parti è auspicabile che l'articolo 25 della direttiva costituisca un solido fondamento giuridico;

(campo di applicazione delle disposizioni dell'“approdo sicuro”) - Va specificato:

se taluni settori siano esclusi dal campo di applicazione del meccanismo dell'“approdo sicuro” in forza di disposizioni specifiche (ad esempio, il settore pubblico) o a causa della mancanza di un ente pubblico di controllo preposto a trattare la materia in questione come richiesto dall'articolo 1.b. del progetto di decisione della Commissione (ad esempio: dati sui lavoratori dipendenti o connessi ad attività non aventi scopo di lucro);

se le organizzazioni, nella notifica di adesione ai principi dell'“approdo sicuro”, avranno la possibilità di escludere taluni settori della propria attività (ad esempio, servizi in linea) e come ciò

potrà essere reso pubblico e comunicato alle autorità nazionali di controllo.

Il gruppo di lavoro nota che il livello di protezione attualmente accordato ai dati sui lavoratori dipendenti non è soddisfacente. Due soluzioni sembrano possibili: rafforzare in generale il livello di protezione garantito dai principi oppure escludere tali dati dal campo di applicazione delle disposizioni onde assicurare loro una maggiore protezione, in considerazione anche della mancanza di un ente pubblico indipendente, come richiesto dall'articolo 1.b. del progetto di decisione, in grado di trattare tale tipo di dati.

Il gruppo di lavoro riafferma la propria preoccupazione per il fatto che le autorità statunitensi potrebbero derogare ai principi attraverso una regolamentazione, senza attribuire sufficiente peso agli interessi della tutela della sfera privata.

Condizioni di attuazione e applicazione

Quale sarà l'impatto sul ruolo delle autorità nazionali di controllo della scelta di un'impresa americana di far trattare i reclami da un ente specifico?

A livello europeo, in sede di trattamento dei reclami, quali saranno i poteri rispettivamente delle autorità nazionali di controllo e dell'Unione europea?

Nel caso di procedure simultanee o successive da parte americana e europea che portino a posizioni contraddittorie in merito a un reclamo, come verranno risolte tali disparità?

Il gruppo di lavoro osserva inoltre che il ruolo che le autorità nazionali di controllo dovrebbero svolgere secondo le autorità americane con riferimento alle imprese che scelgono di cooperare con loro può sollevare problemi di natura costituzionale, finanziaria o di personale per alcune autorità nazionali.

Il gruppo di lavoro ritiene auspicabile inoltre garantire l'indipendenza della procedura di verifica citata al principio 7, lettera (b), ossia che essa sia condotta da un terzo; in caso contrario, ritiene auspicabile che una relazione sulla verifica sia messa a disposizione, se necessario, delle autorità nazionali di controllo.

Contenuto dei principi

Pur riconoscendo che taluni miglioramenti sono stati apportati rispetto al testo del 19 aprile 1999, il gruppo di lavoro nota che i principi, nella loro versione del 1° giugno, non soddisfano ancora i requisiti di un'adeguata tutela. Oltre che sui problemi sollevati nei precedenti pareri, in attesa del suo nuovo e più ampio parere, il gruppo di lavoro ritiene fondamentale attirare in particolare l'attenzione del comitato sui seguenti elementi:

Principio 1 "Notifica" e 2 "Scelta"

Il campo di applicazione è diverso nel caso del principio della notifica e del principio della scelta.

Rispetto alla versione del 4 novembre 1998, la combinazione di entrambi i principi determina ora la possibilità per le imprese americane di utilizzare i dati per uno scopo diverso da quello per il quale sono stati originariamente rilevati, senza essere obbligate a proporre una scelta agli interessati. Quantunque la direttiva consenta l'ulteriore elaborazione dei dati purché non vi sia incompatibilità tra l'impiego e lo scopo del rilevamento, il gruppo di lavoro considera che i principi dell'"approdo sicuro" non legittimino i criteri di trattamento e ritiene pertanto auspicabile un rafforzamento del principio della scelta.

Principio 6 "Accesso"

Le eccezioni contenute nelle FAQ sono troppo ampie.

Vanno presi in considerazione i dati pubblici.

I dati trattati in violazione dei principi dovrebbero essere corretti o cancellati.

Fatto a Bruxelles, il 7 luglio 1999

Per il Gruppo di Lavoro
Il Vicepresidente
Stefano RODOTÀ

Parere 7/99 riguardante il livello di tutela dei dati offerto dai principi dell'“approdo sicuro” (Safe Harbor) pubblicati con le FAQ (domande poste frequentemente) ed altri documenti in materia dal Ministero del commercio USA il 15 e 16 novembre 1999

5146/99/IT/def.
WP 27

Gruppo di lavoro sulla tutela delle persone fisiche
con riguardo al trattamento dei dati personali

Parere 7/99 riguardante il livello di tutela dei dati offerto dai principi dell'“approdo sicuro” (Safe Harbor) pubblicati con le FAQ (domande poste frequentemente) ed altri documenti in materia dal Ministero del commercio USA il 15 e 16 novembre 1999

Adottato il 3 dicembre 1999

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito con la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995^a,

Visti gli articoli 29 e 30, paragrafo b, della suddetta direttiva,

Visto il suo regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL SEGUENTE PARERE 7/99:

Introduzione

Il gruppo di lavoro riafferma la sua politica generale sulla metodologia per la valutazione dell'adeguatezza della tutela dei dati nei paesi terzi, esposta nel suo documento di lavoro del 24 luglio 1998 (WP 12: “Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati”^b).

Il gruppo di lavoro ha seguito con attenzione i colloqui della Commissione con il Ministero del commercio degli Stati Uniti, ne riconosce l'importanza e valuta positivamente l'impostazione di “Safe Harbor”; il gruppo di lavoro desidera contribuire al buon esito di tali colloqui e ritiene che un risultato positivo dipenda dalla conformità ad un certo numero di requisiti di base.

In questo contesto, il gruppo di lavoro ricorda che le versioni precedenti dei principi dell'“approdo sicuro” (Safe Harbor) e delle domande poste frequentemente (FAQ) sono state il tema dei seguenti documenti programmatici:

- Parere 1/99 del 26 gennaio 1999 (WP 15);
- Parere 2/99 del 19 aprile 1999 (WP 19);
- Parere 4/99 del 7 giugno 1999 (WP 21) e documento di lavoro del 7 settembre 1999 riguar-

^a GU n. L 281 del 23 novembre 1995, p. 31, disponibile all'indirizzo:
<http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

^b WP 12 (5025/98): documento di lavoro sul trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati, adottato il 24 luglio 1998, disponibile in 11 lingue all'indirizzo indicato alla nota 1.

dante una parte delle FAQ (non reso pubblico);
- Documento di lavoro del 7 luglio 1999 (WP 23).

Questo parere si riferisce all'ultima versione dei principi dell'"approdo sicuro", delle FAQ e dei relativi documenti, pubblicati il 15 e 16 novembre 1999⁴. Il gruppo di lavoro si rammarica che il tempo per una presa di posizione su una questione così importante sia stato così breve, rileva che nessuno dei documenti è considerato "definitivo" e riserva pertanto la sua posizione per quanto riguarda ogni ulteriore modifica dei testi.

Il gruppo di lavoro constata che sono stati realizzati progressi, ma deplora che la maggior parte delle osservazioni formulate nei suoi documenti programmatici precedenti non abbia trovato eco nella versione più aggiornata dei documenti statunitensi. Il gruppo di lavoro ribadisce pertanto le sue preoccupazioni.

Ai fini di una possibile constatazione di adeguatezza, e considerando l'effetto particolare che tale constatazione positiva avrebbe come punto del riferimento per altri paesi terzi, il gruppo di lavoro ritiene che l'"approdo sicuro" debba offrire sicurezza giuridica non solo alle organizzazioni degli Stati Uniti ma anche alle parti interessate dall'UE (responsabili del controllo che desiderano trasferire dati agli Stati Uniti, persone oggetto di un trasferimento di dati, autorità di protezione dei dati). Fin dal parere 1/99 il gruppo di lavoro ha costantemente ribadito il punto di vista che, in termini di contenuto, i principi dell'"approdo sicuro" devono comprendere, per essere accettabili, "almeno tutti i principi precisati nelle direttive OCSE sulla tutela della sfera privata", adottati anche dagli Stati Uniti e recentemente riaffermati alla Conferenza OCSE di Ottawa dell'ottobre 1998.

Campo di applicazione e struttura

Il gruppo di lavoro ritiene che i principi dell'"approdo sicuro" siano tali da poter guidare l'elaborazione dei dati trasferiti agli Stati Uniti da un responsabile del controllo dell'Unione Europea. Per quanto riguarda la raccolta di dati personali da singoli nell'UE, il gruppo di lavoro ricorda che si applicano, in linea di principio, le disposizioni nazionali di applicazione della direttiva. Il gruppo di lavoro ricorda che ogni constatazione di adeguatezza ai sensi dell'articolo 25, paragrafo 6 della direttiva può soltanto fare riferimento alla tutela degli individui per quanto riguarda l'elaborazione dei dati nel paese terzo in questione e non può influire sul diritto nazionale applicabile ai sensi dell'articolo 4 (c) della direttiva stessa.

Per quanto riguarda l'"approdo sicuro", il gruppo di lavoro raccomanda che il suo campo d'applicazione sia definito chiaramente e senza ambiguità, sia per quanto riguarda i beneficiari che per quanto riguarda le categorie di trasferimenti dei dati.

In base al quarto paragrafo dei Principi, i vantaggi dell'"approdo sicuro" si applicano dalla data in cui le organizzazioni che desiderano qualificarsi per l'"approdo sicuro" forniscono un'autocertificazione al Ministero del commercio o alle istanze da esso designate notificando la propria adesione a tali principi. In base alla FAQ 6, tali lettere di autocertificazione vanno fornite a distanza di almeno un anno l'una dall'altra; il Ministero (o la persona da esso designata) "conserverà un elenco di tutte le organizzazioni che inoltrano queste lettere, assicurando così la disponibilità dei benefici «Safe Harbor», ed aggiornerà tale elenco in base alle lettere annuali" e alle notifiche di non-conformità. In base alla FAQ 11, i casi di non conformità di organizzazioni aderenti all'"approdo sicuro" saranno inseriti nell'elenco. A tale riguardo, il gruppo di lavoro rileva che:

1. Nessun controllo preliminare viene effettuato dal Ministero del Commercio per accertare se un'organizzazione soddisfi effettivamente i criteri di qualificazione (conformità ai principi della politica in materia di riservatezza, giurisdizione di un ente tipo FTC in caso di pratiche ingannevoli);

⁴ Progetto di principi internazionali di approdo sicuro - 15 novembre 1999; domande poste frequentemente (bozza) - 15 novembre 1999 (FAQ da 1 a 15), Compendio della decisione di cui all'articolo 25.6; lettera di David Aaron a John Mogg che trasmette i principi dell'"approdo sicuro", le FAQ, etc., 16 novembre 1999; lettera di John Mogg a David Aaron relativa alla decisione di cui all'articolo 25.6., 16 novembre 1999. Disponibili all'indirizzo: <http://www.ita.doc.gov/td/ecom/menu.htm>

2. La richiesta di un'autocertificazione annuale è intesa a migliorare l'affidabilità dell'elenco; tuttavia, poiché il rinnovo dell'autocertificazione non è obbligatorio, un'organizzazione potrebbe aderire ai principi per un anno e successivamente ritirarsi dall'"approdo sicuro"; inoltre, è possibile che le organizzazioni non conformi che non vengono identificate come tali scompaiano dall'elenco soltanto dopo un periodo relativamente lungo, nel corso del quale i dati personali continuerebbero a essere trasferiti;

3. Le fusioni e gli assorbimenti tra imprese sono sempre più frequenti, in particolare per le imprese che operano on-line. Un'organizzazione che aderisce ai principi potrebbe essere ripresa da un'organizzazione che non può o non vuole qualificarsi per l'"approdo sicuro", o fondersi con essa.

Nella sua forma attuale, "approdo sicuro" è un metodo volontario offerto alle organizzazioni statunitensi sulla base dell'autocertificazione (FAQ 6) e della valutazione autonoma (FAQ 7), sostenuto dalle disposizioni di legge nel caso di falsa dichiarazione o di pratiche ingannevoli. Ciò significa che, salvo in caso di reclamo, qualsiasi organizzazione americana che rivendichi i vantaggi dell'"approdo sicuro" sarebbe autorizzata a ricevere i dati personali dall'UE. Considerando quanto esposto sopra, il gruppo di lavoro invita la Commissione a prendere in considerazione mezzi per assicurare la tutela continuata dei dati personali che possono essere trasferiti a:

- organizzazioni che non avrebbero mai dovuto figurare sull'elenco perché non soddisfacevano i criteri di qualificazione;
- organizzazioni che, pur figurando nell'elenco, non sono conformi ai principi;
- organizzazioni che, dopo aver figurato nell'elenco per un anno, non dovrebbero più figurare nell'elenco dell'anno successivo, perché non rinnovano l'autocertificazione o perché non si qualificano più per l'"approdo sicuro";
- organizzazioni figuranti nell'elenco che vengono rilevate da una società che non si qualifica per l'"approdo sicuro" (perché non può o non vuole aderire ai principi).

Fra i mezzi possibili per assicurare la protezione continuata, il gruppo di lavoro invita la Commissione a considerare la soppressione o la rimozione dei dati trasferiti ad un'organizzazione che rientra in una delle categorie di cui sopra. Il gruppo di lavoro auspica inoltre il chiarimento della possibile applicabilità continuata delle disposizioni sulle pratiche ingannevoli del Federal Trade Commission Act.

Per ragioni di certezza del diritto, il gruppo di lavoro ribadisce che l'elenco dei beneficiari deve essere completamente affidabile, aggiornato e facilmente accessibile al pubblico.

Nel suo documento di lavoro del 7 luglio 1999 il gruppo di lavoro aveva già richiesto un chiarimento su due punti specifici, ossia:

- a) i settori che sarebbero esclusi dal campo d'applicazione dell'"approdo sicuro" perché non rientrano nella giurisdizione di un organismo pubblico del tipo FTC (ad esempio: i dati sui dipendenti, il settore senza scopo di lucro);
- b) le attività che l'organizzazione che si qualifica per l'"approdo sicuro" può scegliere di escludere per scelta imprenditoriale.

Per quanto riguarda il punto a), il gruppo di lavoro attribuisce la massima importanza alle lettere del presidente della FTC del 23 settembre 1998 e dell'1 novembre 1999; da tali lettere emerge chiaramente che la giurisdizione della FTC si estende alle azioni o prassi sleali o ingannevoli solo se "nel commercio o tali da avere ripercussioni su di esso". Ciò sembra escludere la maggior parte dei dati elaborati rilevati nell'ambito di un rapporto di lavoro (FAQ 9) e i dati elaborati senza scopo commerciale (per esempio, organizzazioni senza scopo di lucro, settore della ricerca). Il gruppo di lavoro raccomanda pertanto che queste categorie di trasferimenti di dati siano espressamente escluse dall'"approdo sicuro".

Per quanto riguarda il punto b), il gruppo di lavoro nota che la FAQ 6 invita le organizzazioni a descrivere le "attività dell'organizzazione coperte dai suoi impegni Safe Harbor". Ciò implica che la stessa organizzazione potrebbe aderire all'"approdo sicuro" e restarne nel contempo al di

fuori. Il gruppo di lavoro ritiene che una situazione del genere crei un'incertezza giuridica (in particolare per quanto riguarda lo scambio di informazioni all'interno di un'organizzazione) e richieda il chiarimento della nozione di "attività".

Eccezioni ed esenzioni

Il gruppo di lavoro ribadisce la sua preoccupazione che l'adesione ai principi possa essere limitata da un'eventuale "legge, regolamento governativo o giurisprudenza" (paragrafo 5 lettera b) dei principi) senza ulteriore qualifica. Questo sembra applicarsi alle leggi di Stato come pure alle leggi federali, al presente o in futuro. Per garantire la certezza del diritto e la non discriminazione rispetto ad altre constatazioni di adeguatezza, il gruppo di lavoro raccomanda che siano fissati criteri più precisi per tali eccezioni e limitazioni, illustrati da esempi concreti, e che il loro effetto sia adeguatamente preso in considerazione. Per quanto riguarda l'esigenza di criteri più precisi, il gruppo di lavoro raccomanda di effettuare una chiara distinzione tra le opzioni e gli obblighi: l'adesione ai principi dovrebbe essere limitata soltanto nella misura in cui ciò è necessario per adempiere agli obblighi di legge o normativi (che comunque prevarrebbero sui principi) ma non a seguito di opzioni concesse dalla legislazione degli Stati Uniti, poiché questo causerebbe un serio indebolimento dei principi.

Per ragioni di trasparenza e di certezza del diritto, il gruppo di lavoro ritiene essenziale che la Commissione sia informata di ogni statuto o decreto legge che possa influire sull'adesione ai principi.

Per quanto riguarda il paragrafo 5, lettera c), il gruppo di lavoro raccomanda che ci si limiti alle eccezioni permesse dalla direttiva, che copre tutte le eccezioni ammesse dalla legge degli Stati membri. Il gruppo di lavoro ritiene che nessuna eccezione possa essere invocata al di fuori del suo contesto specifico, e che ogni eccezione può essere fatta valere soltanto per conseguire un fine specifico.

Il gruppo di lavoro esprime preoccupazione per il fatto che, oltre alle eccezioni già esposte, le FAQ contemplano un lungo elenco di ulteriori eccezioni, che portano in alcuni casi all'esenzione di intere categorie di dati: questo è vero, in particolare, per la vasta categoria dei "dati disponibili pubblicamente", che possono essere in effetti "disponibili pubblicamente" indipendentemente da qualsiasi considerazione di legittimità di elaborazione o di precisione dei dati. Il gruppo di lavoro sottolinea che tale esenzione non è contemplata dagli orientamenti OCSE e ritiene che accettarla significherebbe creare una comoda scappatoia alla tutela dei dati.

Notifica

Il gruppo di lavoro ribadisce la posizione, reiterata in tutti i suoi pareri precedenti, secondo la quale l'"approdo sicuro" (e di fatto ogni constatazione di adeguatezza) può soltanto interessare il trattamento dei dati trasferiti da un dispositivo di controllo dei dati dell'UE ad un paese terzo: i dispositivi di controllo dei dati dell'UE sono soggetti alle disposizioni nazionali che applicano la direttiva; lo stesso dicasi per i casi in cui i dati personali sono raccolti direttamente da singoli nell'UE da un'organizzazione statunitense che utilizza strutture situate sul territorio di uno Stato membro (articolo 4 della direttiva).

Tutto questo è ora riconosciuto dagli Stati Uniti al punto D1 delle FAQ n.14 sui prodotti farmaceutici e medicinali, ed nelle FAQ 9 sui dati riguardanti le risorse umane. Tuttavia, il principio della notifica afferma che:

"L'avviso dev'essere formulato (...) quando gli individui vengono invitati per la prima volta a fornire informazioni personali alle organizzazioni, oppure non appena possibile".

La frase sopra citata sembra implicare che la raccolta dei dati da singoli nell'UE da parte di organizzazioni statunitensi sarebbe regolata dai principi dell'"approdo sicuro", e non dalle disposizioni nazionali di applicazione della direttiva. Le sue conseguenze andrebbero quindi al di là del principio di notifica.

Il gruppo di lavoro ritiene che ciò non sia conforme all'articolo 4 della direttiva e raccomanda che la frase succitata sia omessa e sostituita dalla chiara indicazione che:

- qualora un'organizzazione USA intenda rilevare dati personali direttamente dai singoli cittadini nell'UE, essa deve conformarsi alle disposizioni nazionali in materia ai sensi della direttiva (ad esempio: articoli 6, 7, 10, 14 e, se del caso, articolo 8);
- qualora i dati personali vengano trasferiti all'organizzazione USA da un responsabile del controllo dei dati riconosciuto nell'UE, l'organizzazione dovrà richiedere a quest'ultimo di indicare a quale scopo i dati erano stati originariamente raccolti (questo è essenziale per determinare se un cambiamento di finalità si è verificato dopo il trasferimento, rendendo operativi i principi di avviso e di scelta; inoltre, la precisazione contribuirebbe alla ripartizione del rischio e della responsabilità).

Il gruppo di lavoro suggerisce che i punti di cui sopra siano oggetto di un nuovo documento FAQ volto a chiarire il principio di notifica.

Il gruppo di lavoro inoltre raccomanda di modificare il principio di notifica in modo da garantire che sia data notifica nel caso in cui i dati siano usati da un'organizzazione diversa.

Per quanto riguarda le FAQ 4, il gruppo di lavoro nota che nulla giustifica l'elaborazione di dati personali senza il consenso o la conoscenza degli interessati. Inoltre, lo stesso documento fa riferimento ad "altre circostanze in cui l'applicazione dei suddetti principi pregiudicherebbe gli interessi legittimi dell'organizzazione stessa" che il gruppo di lavoro considera una scappatoia troppo evidente.

Il gruppo di lavoro fa notare che il documento FAQ 14 sui prodotti farmaceutici e medicinali è recente e che il testo nella sua forma attuale pone diversi interrogativi, in particolare l'utilizzazione di dati per scopi incompatibili con quelli relativi alla ricerca scientifica.

Scelta

Il gruppo di lavoro ribadisce il parere espresso nel suo documento di lavoro del 7 luglio 1999: poiché i principi non includono alcun criterio di "legittimazione del trattamento", è auspicabile un rafforzamento del principio di scelta. Nella sua attuale versione, la combinazione dei principi di notifica e di scelta risulta nella possibilità di utilizzare i dati per scopi diversi da quelli notificati senza dovere offrire la possibilità di scegliere (a meno che lo scopo sia incompatibile o si tratti di informazioni a carattere delicato); questo contravviene agli orientamenti dell'OCSE ("Principio della limitazione dell'utilizzazione")⁹. Il gruppo di lavoro sostiene il principio che la possibilità di scegliere debba essere offerta quando i dati sono utilizzati per uno scopo compatibile ma diverso.

Il gruppo di lavoro condivide la posizione della Commissione espressa nella nota a piè di pagina al paragrafo relativo al principio di scelta, raccomanda che la definizione di dati delicati sia conforme all'articolo 8 della direttiva e ritiene che la scelta possa soltanto essere una base per l'elaborazione legittima solo se è basata su un'informazione adeguata.

Trasferimento successivo

Il gruppo di lavoro constata con preoccupazione l'aggiunta a questo principio dell'ultima frase, che solleva completamente le organizzazioni dalle loro responsabilità nel caso in cui le informazioni siano trasferite a terzi. Il singolo può non disporre di alcun ricorso legale eccetto contro l'organizzazione che ha operato il trasferimento e che può avere effettivamente agito avventatamente nel trasferire le informazioni. Il gruppo di lavoro raccomanda che la limitazione della responsabilità sia riconsiderata per mantenere la responsabilità dell'organizzazione che opera il trasferimento nei casi di negligenza e di comportamento incauto ed affinché l'organizzazione che opera il trasferimento sia tenuta ad assistere il singolo in caso di ricorso.

⁹ "I dati personali non dovrebbero essere rivelati, resi disponibili o altrimenti utilizzati a scopi diversi da quelli precisati ai sensi del paragrafo 9 (Specificazione degli scopi) tranne che:

a) con il consenso dell'interessato
b) in forza di legge."

Sicurezza

Il gruppo di lavoro raccomanda che il testo della FAQ n. 10 sia modificato togliendo l'affermazione che all'interno del contratto non sono necessarie disposizioni riguardanti la sicurezza, poiché la legge di diversi Stati membri richiede tali disposizioni anche nei contratti per l'elaborazione dei dati presso lo Stato membro stesso.

Integrità dei dati

Il gruppo di lavoro ricorda che al paragrafo 8 degli orientamenti OCSE "i dati devono essere attinenti all'uso cui sono destinati e, nella misura in cui è necessario per l'uso suddetto, devono essere attendibili, completi ed aggiornati". Il principio dell'"approdo sicuro" dovrebbe riflettere questa posizione.

Accesso

Il gruppo di lavoro ricorda che il principio dell'accesso è di fondamentale importanza per ogni efficace regime di protezione dei dati, in quanto è il punto dal quale si dipartono tutti i diritti delle persone interessate. Il gruppo di lavoro insiste sul fatto che le eccezioni a questo principio fondamentale sono permesse soltanto in circostanze eccezionali e ribadisce la preoccupazione espressa in tutte le prese di posizione precedenti per quanto riguarda la portata e il carattere vago delle eccezioni e delle condizioni che gli Stati Uniti prevedono in relazione all'esercizio di questo diritto fondamentale.

Il gruppo di lavoro ribadisce il punto di vista che le considerazioni di costo sono necessarie per determinare le condizioni alle quali il diritto può essere esercitato, ma non possono essere una condizione al diritto stesso.

A differenza degli orientamenti³⁹ dell'OCSE, i principi dell'"approdo sicuro" non riconoscono il diritto individuale di ricevere le informazioni "in forma facilmente comprensibile". Inoltre, il principio dell'accesso limita il diritto di cancellare i dati ai casi in cui questi sono inesatti (il che è ovvio); nel suo parere 2/99 il gruppo di lavoro ha già espresso l'opinione che, per avere un senso, il diritto della persona interessata alla cancellazione dei dati deve applicarsi a tutti i casi in cui il relativo trattamento è illegale; ciò dovrebbe essere specificato nel principio e non nel testo delle FAQ.

La FAQ 8 elenca numerose eccezioni al principio di accesso; il gruppo di lavoro accoglie favorevolmente il fatto che alcune di queste eccezioni, rispetto al testo precedente, sono state limitate o chiarite. Tuttavia, il quadro globale dà ancora l'impressione che l'enunciato di questa FAQ indebolisca il principio anziché fornire indicazioni sulla sua applicazione. In particolare, il gruppo di lavoro ripete le sue obiezioni in merito ai punti D2 (nozione poco chiara), e D7. Per quanto riguarda il punto D5, il gruppo di lavoro ribadisce il suo punto di vista che i casi in cui l'accesso deve essere negato sono troppo ampi e vaghi e che la formulazione implica che tali considerazioni automaticamente scavalcano il diritto di accesso. Il gruppo di lavoro esprime preoccupazione per il fatto che ciò potrebbe provocare un serio indebolimento del livello globale di protezione dei dati.

Per quanto riguarda il punto D6, il gruppo di lavoro ritiene inadeguata la formulazione del secondo paragrafo e raccomanda o la sua soppressione o una formulazione più restrittiva, in modo da limitarlo all'esclusione degli abusi del diritto d'accesso.

Il gruppo di lavoro ribadisce altresì la sua opposizione al punto D8, per le ragioni già esposte nel documento di lavoro del 7 settembre 1999; inoltre, il fatto che le informazioni siano pubblicamente disponibili non priva gli interessati del loro diritto di accesso.

Applicazione

Il gruppo di lavoro accoglie favorevolmente le informazioni dettagliate fornite dagli Stati Uniti nelle ultime settimane di colloqui (in particolare: lettera della FTC, raffronto dei meccanismi del settore privato americano per il componimento delle controversie in materia di privacy, la FAQ 11, il memorandum sul Fair Credit Reporting Act). Tali informazioni sono preziose ed hanno per-

³⁹ "Principio della partecipazione individuale", punto a) iv.

messo al gruppo di lavoro di disporre di un quadro più chiaro delle strutture di applicazione che possono essere messe a disposizione degli interessati. Avendo esaminato i documenti succitati, il gruppo di lavoro esprime il timore che:

1. I meccanismi del settore privato esistenti si occupino esclusivamente delle attività on-line: BBB On-line; Web Trust; TRUSTe; (sottolineatura aggiunta)¹¹ ;
2. Lo stesso si constata nella lettera del Presidente FTC dell'1 novembre 1999 (paragrafo 2: "online privacy", "Internet environment"; paragrafo 3: online marketplace, survey of web sites; paragrafo 4: "online privacy policies" e così via; sottolineatura aggiunta)¹² .
3. Ai sensi del paragrafo 4 dei principi, possono godere dei vantaggi dell'"approdo sicuro" le organizzazioni soggette a "norme statutarie, di regolamentazione, amministrative o d'altro tipo (o a norme stabilite da borse valori nazionali, associazioni registrate di agenti di borsa, agenzie di compensazione registrate, ovvero enti normativi in materia di titoli municipali) che tutelino efficacemente la riservatezza dei dati personali". Tuttavia, nessun'informazione è stata fornita sugli enti pubblici che assicurerebbero l'applicazione di una così vasta gamma di regolamentazioni.

In queste circostanze, il gruppo di lavoro esprime il parere che il campo d'applicazione di ogni constatazione di adeguatezza debba essere espressamente limitato ai settori per i quali informazioni sufficienti ed inequivocabili sono state raccolte e per i quali è stata accertata l'esistenza di meccanismi di applicazione. In effetti, l'estensione del campo d'applicazione di una constatazione di adeguatezza oltre questo limite esporrebbe la decisione alla contestazione e questo non è auspicabile per nessuna delle parti interessate.

Per quanto riguarda il principio di applicazione, il gruppo di lavoro ritiene che, per avere un significato, il principio debba comprendere il risarcimento di ogni danno subito dall'individuo in seguito alla violazione dei principi: questo è un parere generale del gruppo di lavoro e si applica ad ogni paese terzo (documento di lavoro sul trasferimento dei dati personali verso paesi terzi: WP 12 del 24 luglio 1998, pagina 14: "riparazione adeguata". Nei casi in cui la riparazione dei danni non è contemplata nella normativa americana esistente, l'organizzazione privata dovrebbe poter offrire questa possibilità come condizione per qualificarsi per l'"approdo sicuro".

Per quanto riguarda le FAQ 11 (Risoluzione delle controversie e applicazione), il gruppo di lavoro rileva che questo testo esamina una serie di aspetti relativi all'applicazione l'importanza dei quali è tale che dovrebbero essere inclusi nel principio di applicazione stesso. Per il collegamento tra i diversi livelli d'applicazione è particolarmente importante che gli organismi preposti alla composizione delle controversie adottino la prassi di riferire i casi irrisolti alla FTC. I requisiti di trasparenza e rapidità del meccanismo di composizione delle controversie dovrebbero inoltre essere integrati nel principio.

In base alle FAQ 11, gli organismi preposti alla composizione delle controversie possono richiedere requisiti di ammissibilità per l'accettazione dei reclami. Il gruppo di lavoro ritiene che requisiti di questo tipo debbano essere espliciti, oggettivi e ragionevoli. Inoltre, il rifiuto di dare seguito ai reclami dovrebbe essere debitamente motivato.

In generale, il gruppo di lavoro nota che le disposizioni di applicazione negli Stati Uniti presentano un quadro piuttosto confuso nel quale non è possibile identificare con facilità quali siano i diritti del cittadino in caso di violazione dei principi. Le FAQ 11 offrono semplicemente una serie di raccomandazioni che possono condurre ad un'esecuzione frammentata ed irregolare.

FAQ 5 - Ruolo delle autorità di protezione dei dati

Il gruppo di lavoro ha discusso il testo della FAQ 5 proposto dagli USA e conclude che il

¹¹ Come già detto, le attività on line possono essere soggette alla legislazione UE nei casi in cui esse riguardano la raccolta di dati personali direttamente da singoli nell'UE (cfr. I capitoli Campo di applicazione e struttura e Notifica).

¹² V. Nota 6.

ruolo delle autorità di protezione dei dati previsto in questo testo non è legalmente o praticamente realizzabile. In particolare, il gruppo di lavoro nota che la legislazione nazionale non conferisce alle autorità nazionali la competenza di trattare i reclami concernenti le violazioni delle norme di protezione dei dati al di fuori della loro giurisdizione.

Il gruppo di lavoro prende atto d'altra parte della disponibilità delle autorità nazionali ad offrire la loro cooperazione sotto forma di informazioni e di consulenza, se questo può essere utile nel contesto dell'"approdo sicuro". Il gruppo di lavoro constata che la cooperazione è stata promossa dagli Stati Uniti per un periodo limitato successivo al lancio dell'"approdo sicuro".

In questo contesto, il gruppo di lavoro invita la Commissione a considerare se l'offerta di fornire informazioni e consulenza, combinata con l'impegno unilaterale da parte dell'organizzazione americana interessata di adeguarsi al parere delle autorità nazionali - un impegno che, se non rispettato, avrebbe come conseguenza un'azione per frode da parte della FTC - potrebbe contribuire al rispetto dei requisiti di cui alla parte (a) del principio di applicazione dell'"approdo sicuro". In caso affermativo, il gruppo di lavoro fa notare che le autorità nazionali potrebbero essere disposte a cooperare in questo modo per un periodo iniziale di 3 anni. Il gruppo di lavoro rileva inoltre che le autorità nazionali potranno voler rivedere l'accordo entro la fine di quel periodo se il numero di organizzazioni americane che si valgono di questa possibilità fosse tale da poter affermare che, in luogo di essere un accordo provvisorio per colmare una lacuna limitata, esso viene a sostituirsi negli Stati Uniti agli accordi di applicazione veri e propri.¹³

Il gruppo di lavoro invita inoltre la Commissione a studiare in che modo potrebbe essere utile un meccanismo a livello europeo, che potrebbe *inter alia* fornire una tribuna per contribuire ad assicurare un'impostazione coordinata ed armonizzata.

Proposta di decisione della Commissione del 24 novembre 1999

Il gruppo di lavoro desidera attirare l'attenzione della Commissione su quanto segue:

1. La proposta non fa alcun riferimento al lavoro effettuato dal gruppo di lavoro per stabilire i criteri di valutazione dell'adeguatezza nei paesi terzi (WP 12). Il gruppo di lavoro ritiene che la valutazione dell'adeguatezza debba essere effettuata sulla base di tali criteri per garantire un'impostazione equilibrata ed imparziale a tutti i paesi terzi, indipendentemente dal modo scelto - norme di legge o autodisciplina - per garantire la protezione dei dati. Dovrebbe inoltre essere fatto riferimento specifico ai pareri già espressi dal gruppo di lavoro sull'"approdo sicuro", indicando dove sono stati pubblicati.
2. Sulla sostanza della decisione, il gruppo di lavoro osserva che i criteri per l'adesione all'"approdo sicuro" non sono gli stessi nei testi americani e nella proposta di decisione. Ai sensi dei paragrafi introduttivi 3 e 4 dei principi degli Stati Uniti, le organizzazioni possono qualificarsi per l'"approdo sicuro" in uno dei seguenti modi:
 - a) *aderendo a un programma di autodisciplina in materia di riservatezza che ottemperi ai principi,*
 - b) *sviluppando proprie politiche in materia di riservatezza, purché conformi ai principi,*
 - c) *essendo soggette a normative statutarie, di regolamentazione, amministrative o altre che tutelino efficacemente la riservatezza"*

Secondo l'articolo 1 della proposta di decisione della Commissione, si considera che aderiscono all'"approdo sicuro", le organizzazioni che:

"dichiarano pubblicamente di conformarsi ai principi e sono soggette ai poteri statutari di un ente pubblico indipendente autorizzato ad esaminare qualsiasi reclamo e ad ottenere provvedimenti inibitori contro prassi sleali o ingannevoli."

I principi devono conformarsi alla decisione.

3. Il gruppo di lavoro osserva inoltre che il considerando 8 afferma che la legge contempla diverse eccezioni alla giurisdizione della Federal Trade Commission, senza peraltro indica-

¹³ Alcune delegazioni riservano la propria posizione su questo paragrafo.

re in modo specifico i settori esclusi o se tutti i settori esclusi sono soggetti alla giurisdizione di un altro organismo pubblico. Analogamente, si dovrebbe fare riferimento alle disposizioni che conferiscono ai pochi enti pubblici citati il potere di agire contro le pratiche ingannevoli o le dichiarazioni false.

Poiché l'essere soggette alla giurisdizione di un organismo pubblico abilitato ad agire contro le pratiche sleali o ingannevoli è una *conditio sine qua non* per le organizzazioni che desiderano aderire all'"approdo sicuro", il gruppo di lavoro ritiene fondamentale chiedere che vengano forniti chiarimenti su questo punto e che il campo d'applicazione dell'"approdo sicuro" sia limitato ai settori soggetti alla giurisdizione di un organismo pubblico di questo tipo.

4. La proposta di decisione della Commissione non fa menzione del modo in cui le organizzazioni possono perdere i vantaggi dell'"approdo sicuro" - o, per dirlo in parole più semplici, quali siano le procedure per l'esclusione dall'elenco del Ministero del commercio.

Il solo impegno che figura nei testi statunitensi è quello di inserire nell'elenco "*qualsiasi notifica ricevuta da organismi di risoluzione delle controversie, di autoregolamentazione e/o governativi riguardante casi in cui organizzazioni che aderiscono all'"approdo sicuro" continuano a non conformarsi ai suoi principi o eventuali decisioni dei suddetti organismi. Ciò avverrà però solo dopo aver fornito all'organizzazione in questione la possibilità di replicare entro trenta giorni.*" (FAQ 11)

In base alla proposta di decisione, un'indicazione negativa può solo dare origine alla sospensione del trasferimento dei dati, ai sensi dell'articolo 2.2.(a). Nella situazione attuale, l'eventuale sospensione ai sensi dell'articolo 2.2.(a) non comparirebbe nell'elenco, in quanto questo non fa menzione di constatazioni negative effettuate nell'Unione europea.

Inoltre, il gruppo di lavoro è dell'avviso che le condizioni previste dall'articolo 2.2⁴ per la sospensione del trasferimento dei dati rischia di dimostrarsi di difficile applicazione pratica, cosa inaccettabile nel caso in cui ci sia violazione dei diritti individuali. Nel testo dell'articolo 2.2, pertanto, le parole "danno irreparabile" andrebbero sostituite con "danno grave e imminente".

5. Il gruppo di lavoro rileva che l'articolo 1, paragrafo 3, riporta un testo proposto dagli Stati Uniti che recita: "*Si presume che il rispetto delle leggi statunitensi Fair Credit Reporting Act o Financial Modernization Act garantisca un livello adeguato di protezione per quanto riguarda le attività di un'organizzazione che rientrano nel campo d'applicazione di tali leggi.*" Per quanto riguarda queste leggi degli Stati Uniti, il gruppo di lavoro attira l'attenzione della Commissione sul fatto che un'analisi della FCRA era all'ordine del giorno della 17^a riunione del 7 giugno, ma né la legge né la valutazione di adeguatezza erano state discusse per mancanza di tempo e, per quanto riguarda la legge Financial Modernization Act, il gruppo di lavoro ha soltanto di recente preso visione del testo.

Alla luce di quanto sopra, il gruppo di lavoro può esprimere un parere sul livello di adeguatezza di queste due leggi soltanto dopo una discussione approfondita. Qualora dall'esame delle due leggi non emergesse alcuna constatazione di adeguatezza, ogni riferimento ad esse dovrà essere tolto dalla decisione.

⁴ Articolo 2.2: "Le autorità competenti degli Stati membri possono altresì avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che rispetta i principi nei casi in cui:

a) gli organismi pubblici statunitensi di cui all'articolo 1, paragrafo 1, lettera b), o un meccanismo indipendente di ricorso degli Stati Uniti nell'ambito di quanto esposto alla lettera a) del "principio di applicazione" abbiano rilevato violazioni dei principi, oppure

b) vi siano sufficienti motivi per ritenere che il meccanismo di attuazione negli Stati Uniti non stia adottando o non adotterà misure adeguate e tempestive volte a risolvere il caso in questione, che sia sostanzialmente probabile che una violazione dei principi sia stata commessa e le autorità competenti dello Stato membro abbiano fatto il possibile per informare l'organizzazione dandole l'opportunità di reagire e che la continuazione del trasferimento dei dati potrebbe provocare danni irreparabili agli interessati.

I flussi di dati devono riprendere non appena sia garantito il rispetto dei principi."

6. Il gruppo di lavoro è inoltre dell'avviso che l'articolo 2.1 debba essere modificato come segue:

"L'articolo 1 non pregiudica il potere delle autorità competenti degli Stati membri di intervenire per garantire la conformità con le disposizioni nazionali approvate conformemente a disposizioni diverse da quelle previste agli articoli 25 e 26 della direttiva"

Scambio di lettere

(non datate ma pubblicate sul sito web il 15 novembre)

Il gruppo di lavoro desidera attirare l'attenzione della Commissione sui seguenti punti:

- Il cosiddetto *"periodo di grazia"*, ovvero *data di entrata in vigore*: sia nel progetto di lettera degli Stati Uniti che nel progetto di risposta della Commissione si fa cenno al fatto che la Commissione e gli Stati membri faranno uso della flessibilità offerta dall'articolo 26 per evitare di interrompere i flussi di dati verso le organizzazioni statunitensi per un determinato periodo successivo alla decisione di cui all'articolo 25.6 dell'"approdo sicuro". In tal modo le organizzazioni statunitensi avranno l'opportunità di decidere se partecipare o meno all'"approdo sicuro" e, se necessario, di adeguare le loro prassi nell'ambito dell'informazione.

Considerando che, ai sensi della direttiva, la Commissione può agire in materia di trasferimenti a paesi terzi soltanto quando: a) un paese terzo non garantisce un livello di protezione adeguato e la Commissione avvia negoziati per porre rimedio alla situazione (articolo 25, paragrafi 4, 5 e 6) oppure b) qualora la Commissione decida che alcune clausole contrattuali tipo offrono le garanzie sufficienti (articolo 26.4), il gruppo di lavoro si domanda su quale base la Commissione intende utilizzare la flessibilità consentita dall'articolo 26 della direttiva per dare alle organizzazioni statunitensi tempo sufficiente per decidere se aderire o meno all'"approdo sicuro".

- *Uso dei contratti - articolo 26 della decisione*: Nel progetto di lettera dell'UE si afferma che *"la Commissione e gli Stati membri sono del parere che i principi (dell'"approdo sicuro" US) possono essere utilizzati in tali accordi come disposizioni fondamentali in materia di tutela dei dati. La Commissione ha avviato colloqui con gli Stati membri in seno al comitato di cui all'articolo 31 riguardo a tali disposizioni, in vista dell'adozione di una decisione in virtù dell'articolo 26.4 per autorizzare clausole tipo..."*

Considerando che il gruppo di lavoro è sempre stato del parere che l'analisi dell'adeguatezza delle soluzioni contrattuali richiede la considerazione di un'insieme di questioni più complesse di quelle prese in considerazione nell'ambito di soluzioni quadro, un impegno del genere appare prematuro. Va da sé che i principi dell'"approdo sicuro" devono essere migliorati e risultare adeguati prima che si possano prendere in considerazione come parte del contenuto di clausole tipo.

Conclusioni

Il gruppo di lavoro conclude, alla luce delle osservazioni e raccomandazioni fin qui esposte, che gli accordi per l'"approdo sicuro" come risultano nelle versioni attuali dei diversi documenti restano insoddisfacenti. Il gruppo di lavoro invita la Commissione a sollecitare la controparte statunitense ad apportare una serie di miglioramenti sostanziali, volti in particolare a:

- chiarire il campo d'applicazione dell'"approdo sicuro" e soprattutto ad eliminare ogni possibile malinteso sulla facoltà delle organizzazioni Statunitensi di scegliere di seguire i principi dell'"approdo sicuro" nei casi per i quali si applica la direttiva;
- stabilire disposizioni più affidabili che consentano di identificare con certezza gli aderenti all'"approdo sicuro" e che evitino il rischio che i vantaggi dell'"approdo sicuro" continuino ad essere accordati anche dopo che l'adesione all'approdo sicuro, per una ragione o un'altra, è stata ritirata;
- stabilire in modo inequivocabile che la giurisdizione di un organismo pubblico adeguatamente autorizzato è valida per tutti i partecipanti all'"approdo sicuro";
- far sì che gli organismi del settore privato preposti alla composizione delle controversie siano tenuti a riferire i casi di reclami non risolti ad un organismo pubblico del tipo di cui sopra;

- rendere le eccezioni e le esenzioni ammesse meno generiche e meno vaghe, in modo che le eccezioni siano effettivamente tali, ossia si applichino solo quando necessario e nella misura del necessario e non siano un invito generalizzato a scavalcare i principi; questo punto è particolarmente importante per quanto riguarda il diritto di accesso;
- rinforzare il principio della scelta, che è la chiave di volta dell'impostazione degli Stati Uniti.

Questi punti sono stati sviluppati in modo particolareggiato nelle sezioni precedenti di questo parere; il gruppo di lavoro auspica che si tenga conto delle considerazioni esposte.

Il gruppo di lavoro invita inoltre la Commissione a rivedere l'articolo 2 del progetto di decisione affinché sia chiaro che la decisione non pregiudica il potere delle autorità nazionali competenti per quanto riguarda le leggi nazionali per l'applicazione di disposizioni della direttiva diverse dagli articoli 25 e 26 e affinché sia possibile intervenire, ai sensi dell'articolo 2, paragrafo 2, nei casi in cui il trasferimento dei dati potrebbe provocare "danni irreparabili" agli interessati.

Il gruppo di lavoro sottolinea infine l'importanza di continuare e addirittura accelerare i lavori sulle clausole contrattuali tipo, in vista di una decisione o delle decisioni ai sensi dell'articolo 26 paragrafo 4, che è una parte importante del lavoro per semplificare e rendere più trasparenti le misure di sicurezza richieste per i trasferimenti ai settori nei quali una protezione adeguata non è altrimenti garantita.

Fatto a Bruxelles, il 3 dicembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

6.3.3. Internet**Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware**5093/98/IT/def.
WP 17

Gruppo di lavoro per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet
effettuato da software e hardware

Adottato dal gruppo di lavoro il 23 febbraio 1999

**IL GRUPPO DI LAVORO 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,

Visti gli articoli 29 e 30, paragrafo 3 della direttiva,

Viste le sue regole di procedura e in particolare gli articoli 12 e 14,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

1. Il gruppo di lavoro incoraggia l'industria del software e dell'hardware a lavorare su prodotti Internet rispettosi della privacy, fornendo i necessari strumenti per conformarsi alla normativa europea sulla protezione dei dati.

Una condizione per rendere legittimo il trattamento lecito dei dati personali è che il soggetto dei dati sia informato e sia messo al corrente del trattamento in questione. Il gruppo di lavoro è quindi particolarmente interessato a tutti i tipi di operazioni di trattamento attualmente effettuate da software ed hardware su Internet senza che la persona interessata ne sia a conoscenza e che quindi sono per lei "invisibili".

Esempi tipici di questo trattamento invisibile sono il "chattering" a livello HTTP¹⁵, "hyperlink" automatici a terzi, il contenuto attivo (come Java, ActiveX o altre tecniche di scrittura basate sull'utente) e il meccanismo dei "cookies", così come attualmente applicato nei comuni browser.

2. I prodotti Internet di software ed hardware dovrebbero mettere a disposizione degli utenti Internet informazioni sui dati che si intendono raccogliere, memorizzare o trasmettere e lo scopo per cui ciò viene fatto.

I prodotti Internet di software ed hardware dovrebbero anche permettere all'utente dei dati di avere facilmente accesso, in qualsiasi momento, ai dati raccolti che lo riguardano.

Ciò significa ad esempio:

¹⁵ Ciò significa che nella richiesta http sono trasmesse informazioni che oltrepassano quelle necessarie per contattare il server.

- nel caso di un browser software, che, al momento di stabilire un collegamento con un web server (spedendo una richiesta o ricevendo una pagina web), l'utente debba essere informato di quale informazione s'intende trasferire e a quale fine;
 - nel caso di hyperlink spediti da un sito web ad un utente mediante qualsiasi mezzo, che il browser dell'utente dovrebbe indicarli tutti all'utente;
 - nel caso di cookies, che l'utente dovrà essere informato quando un cookie dovrebbe essere ricevuto, memorizzato o spedito dal software Internet. Il messaggio dovrebbe specificare, in un linguaggio generalmente comprensibile, quali informazioni s'intendono memorizzare nel cookie, ed a quale fine, nonché il periodo di validità del cookie stesso.
3. La configurazione dei prodotti hardware e software non dovrebbero, per default, consentire la raccolta, la memorizzazione o la trasmissione d'informazioni persistenti sul cliente¹⁶. Ad esempio:
- il browser software dovrebbe, per default, essere configurato in modo tale da trattare solamente la quantità minima di informazioni necessarie per stabilire un collegamento Internet. I cookies, per default, non dovrebbero essere né spediti, né memorizzati.
 - durante la sua installazione, una funzione browser destinata a memorizzare e a trasmettere i dati sull'identità dell'utente o sul suo comportamento riguardo le comunicazioni (profilo) non dovrebbe essere completata automaticamente con dati preventivamente memorizzati sull'attrezzatura dell'utente.
4. I prodotti Internet di hardware e software dovrebbero permettere al soggetto dei dati di decidere liberamente sul trattamento dei propri dati personali, mettendo a disposizione strumenti di facile utilizzazione per filtrare (cioè respingere o modificare) la ricezione, la memorizzazione o la trasmissione di informazioni persistenti sul cliente seguendo alcuni criteri (compresi i profili, il campo o l'identità del server Internet, il tipo e la durata delle informazioni raccolte, memorizzate o spedite e così via). L'utente dovrebbe poter disporre di chiare istruzioni sull'impiego del software e dell'hardware per l'applicazione di queste opzioni e strumenti. Ad esempio:
- ciò significa che il browser software dovrebbe fornire opzioni in modo che l'utente possa configurare il browser, specificando quali informazioni quest'ultimo potrà o meno raccogliere e trasmettere;
 - ciò significa per i cookies che l'utente potrà sempre scegliere se accettare o respingere la trasmissione o la memorizzazione di un cookie nel suo insieme. L'utente potrà anche scegliere di decidere quali elementi dell'informazione andranno conservati o eliminati da un cookie, a seconda, ad esempio, del periodo di validità dello stesso o della spedizione e ricezione di siti web.
5. I prodotti Internet di software ed hardware dovrebbero permettere all'utente di eliminare le informazioni persistenti sul cliente in modo semplice e senza partecipazione del mittente. Dovranno essere fornite all'utente chiare informazioni sulle modalità d'esecuzione. Se le informazioni non possono essere tolte dovrà esistere un modo affidabile per prevenirne il trasferimento e la lettura.
- I cookies e le altre informazioni persistenti sul cliente vanno memorizzati in un modo standardizzato e devono essere facilmente e selettivamente cancellabili sul computer del cliente.

Contesto generale

Attualmente è quasi impossibile utilizzare Internet senza essere confrontati a elementi che invadono la privacy e a operazioni di trattamento dei dati personali effettuate in un modo che resta

¹⁶ Informazioni persistenti sul cliente è un termine tecnico (non giuridico) con il quale s'intendono le informazioni comunicate al cliente (il PC dell'utente) e che rimangono più a lungo di una sessione sul computer. Una sessione inizia quando il cliente chiede una pagina di un particolare sito web e finisce quando decide di chiudere il programma browsing o il computer, oppure quando chiede una pagina di un altro sito web. I cookies sono informazioni persistenti tipiche del cliente, lo stesso dicasi per le preferenze riguardanti la privacy.

invisibile al soggetto dei dati. In altre parole, l'utente Internet non sa che i suoi dati personali sono stati raccolti, successivamente elaborati, e che potrebbero essere utilizzati a fini a lui sconosciuti. Il soggetto dei dati non sa nulla del trattamento e non ha la libertà di prendere decisioni al riguardo.

Un esempio di questo tipo di tecnica è costituito dal cosiddetto cookie, che può essere definito come una registrazione informatica d'informazioni trasmessa da un web server ad un computer dell'utente per la futura identificazione di tale computer al momento di future visite allo stesso sito web.

I browser sono programmi di software progettati, tra l'altro, per visualizzare graficamente il materiale disponibile su Internet. I browser comunicano tra il computer dell'utente (cliente) ed il computer a distanza in cui sono memorizzate le informazioni (web server). I browser spesso trasmettono al web server più informazioni di quelle strettamente necessarie per stabilire la comunicazione. I browser classici trasmetteranno automaticamente al web server visitato il tipo ed il linguaggio del browser, il nome degli altri programmi software installati sul PC dell'utente ed il sistema operativo, la pagina di riferimento, i cookies, ecc. Tali dati possono anche essere trasmessi sistematicamente a terzi dal browser software in modo invisibile.

Queste tecniche permettono di creare "clicktrails" riguardanti l'utente Internet. I clicktrails sono costituiti da informazioni su comportamento, identità, strade seguite o scelte effettuate da questi durante la visita di un sito web. Essi contengono i collegamenti che un utente ha seguito e sono registrati nel web server.

Le direttive europee 95/46/CE e 97/66/CE sulla protezione dei dati contengono disposizioni particolareggiate per la tutela delle persone con riguardo al trattamento dei dati personali. Entrambe le direttive sono pertinenti alle situazioni di cui trattasi nella presente raccomandazione, in quanto i dati personali relativi agli utenti Internet sono trattati in tale contesto.

I cookies o i browser possono contenere o trattare successivamente dati che consentono l'identificazione diretta e indiretta di un singolo utente Internet.

L'applicazione delle disposizioni sul corretto trattamento, le basi legittime del trattamento ed il diritto del soggetto dei dati di decidere sul trattamento dei propri dati portano alla raccomandazione di cui sopra.

Il gruppo di lavoro è particolarmente preoccupato dei rischi inerenti al trattamento dei dati personali riguardanti soggetti di dati che sono completamente all'oscuro di tale trattamento. I progettisti del software e dell'hardware sono quindi invitati a prendere in considerazione e a rispettare i principi di queste direttive al fine di rafforzare la privacy degli utenti Internet.

Fatto a Bruxelles, il 23 febbraio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni

5005/99/def.

WP 18

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni

Adottata il 3 maggio 1999

**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 1995¹⁷,

Considerando gli artt. 29 e 30, paragrafi 1 e 3, della suddetta direttiva¹⁸,

Considerando il suo regolamento interno, in particolare gli artt. 12 e 14 di quest'ultimo,

Ha adottato la presente raccomandazione:

L'obiettivo della raccomandazione è di ricordare l'applicazione alle misure adottate a livello europeo in materia di intercettazione delle telecomunicazioni dei principi di tutela dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare della loro vita privata e della riservatezza della corrispondenza.

Il campo d'applicazione della presente raccomandazione copre le intercettazioni in senso lato, vale a dire l'intercettazione del contenuto delle telecomunicazioni ma anche i dati attinenti alle telecomunicazioni, e in particolare eventuali misure preparatorie (quali il "monitoring" e il "data-mining" dei dati sul traffico) di cui si terrà conto per decidere l'opportunità dell'intercettazione del contenuto della telecomunicazione¹⁹.

1. Portata delle disposizioni adottate a livello europeo in materia di intercettazione delle telecomunicazioni

a. La risoluzione del Consiglio del 17 gennaio 1995 relativa all'intercettazione legale delle telecomunicazioni²⁰ specifica le condizioni tecniche necessarie per l'intercettazione delle telecomunicazioni, senza affrontare la questione delle condizioni in cui simili intercettazioni devono aver

¹⁷ Direttiva del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U. L 281 del 23.11.1995, pag. 31.

¹⁸ I tre membri che rappresentano rispettivamente il Registertilsynet (Danimarca), la Commission Nationale de l'Informatique et des Libertés (CNIL, Francia) e il Data Protection Registrar (Regno Unito), non hanno partecipato al voto di questa raccomandazione, ritenendo che il soggetto trattato non fosse di competenza del gruppo. Essi sostengono tuttavia in linea di massima la raccomandazione.

¹⁹ Questo carattere esteso della nozione di intercettazione delle telecomunicazioni corrisponde al campo di applicazione della risoluzione del Consiglio del 17 gennaio 1995 relativa all'intercettazione legale delle telecomunicazioni, citata in appresso (Capitolo A.1.), e al quadro generale delle disposizioni giuridiche applicabili in materia (si veda in appresso il Capitolo B.).

La raccomandazione si applica all'intercettazione delle telecomunicazioni non pubbliche su Internet. Un'attenzione particolare è dedicata alla problematica generale del trattamento dei dati personali legati allo sviluppo della rete Internet dal gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, nel quadro dei lavori svolti parallelamente dalla "task force internet" del gruppo.

²⁰ G.U. C329 del 14.11.1996.

luogo. Il testo della Risoluzione stabilisce che gli operatori delle reti e i fornitori di servizi sono tenuti a consegnare ai «servizi autorizzati» i dati intercettati non codificati.

Quanto detto vale per le telefonate sulla rete fissa o tramite cellulare, la posta elettronica, le telecopiatrici e i messaggi telex, il flusso di dati Internet, sia per quanto riguarda la conoscenza del contenuto delle telecomunicazioni che i dati relativi alle telecomunicazioni (questi si riferiscono in particolare ai dati sul traffico, ma anche a qualsiasi altro segnale emesso dalla persona oggetto della sorveglianza - punto 1.4.4. della risoluzione).

I dati riguardano la persona sorvegliata nonché le persone che chiamano o sono chiamate da questa persona²¹.

La risoluzione prevede anche che la localizzazione geografica dell'utilizzatore mobile costituisce un dato al quale i servizi autorizzati devono avere accesso²².

Questa risoluzione del 18 gennaio 1995 forma attualmente l'oggetto di una revisione, e uno dei principali obiettivi è l'adeguamento alle nuove tecnologie di comunicazione. Il progetto di testo specifica in particolare l'applicazione delle misure di intercettazione alle telecomunicazioni via satellite²³.

b. Le riflessioni del gruppo di lavoro hanno per oggetto il campo d'applicazione delle misure previste dalla risoluzione del Consiglio del 17 gennaio 1995. Una versione non pubblicata del documento suddetto e posteriore a questo («dichiarazione d'intenzioni» in data 25 ottobre 1995), prevede che i firmatari del testo potranno mettersi in contatto per quanto concerne le specifiche in materia di intercettazione delle telecomunicazioni con il direttore del «Federal Bureau of Investigation» degli Stati Uniti. Il testo prevede inoltre che, previo consenso dei «partecipanti», altri Stati membri possono partecipare allo scambio di informazioni, alla revisione e all'aggiornamento delle specifiche.

Il gruppo fa osservare, da un lato, che lo statuto giuridico di questo testo - in particolare la sua firma effettiva da parte dei paesi interessati - non è chiaro e che esso non è, ai sensi della giurisprudenza della Corte europea dei diritti dell'uomo citata in appresso, accessibile ai cittadini dato che non forma l'oggetto di alcuna pubblicazione. D'altra parte, da questo testo emerge la volontà di mettere a punto misure tecniche di intercettazione delle telecomunicazioni in concertazione con Stati non soggetti alla convenzione europea dei diritti dell'uomo e alle direttive 95/46/CE e 97/66/CE.

c. Il gruppo di lavoro constata che il testo della risoluzione del Consiglio pretende di disciplinare aspetti tecnici relativi alle modalità di intercettazione delle comunicazioni senza mettere in discussione le disposizioni nazionali che regolamentano le intercettazioni da un punto di vista giuridico. Tuttavia, talune misure previste dalla risoluzione intese ad estendere le possibilità di intercettazione delle comunicazioni sono in contraddizione con le disposizioni nazionali, più protettive, di taluni paesi dell'Unione europea (in particolare: punto 1.4, comunicazione dei dati relativi alle chiamate, inclusi quelli relativi alla telefonia mobile, senza tener conto dei servizi anonimi e prepagati attualmente disponibili; punto 1.5, localizzazione geografica degli utenti mobili; punto 5.1,

²¹ Art. 1.4 dell'allegato della risoluzione del Consiglio del 17 gennaio 1995.

²² Art. 1.5, op. cit.

²³ Documento 10951/1/98, Enfopol 98 Rev 1 (<http://www.heise.de/tp/deutsch/special/enfo/6332/1.htm>). Una versione ancora più recente sembra essere stata approvata dal gruppo di lavoro "cooperazione di polizia" del Consiglio ed essere stata trasmessa al Parlamento europeo affinché questo possa adottarla o modificarla. La nuova risoluzione dovrebbe essere adottata dal Consiglio il 27-28 maggio 1999 (si veda il "Datenschutz-Berater, 15.02.99, pag. 5, che menziona una versione non pubblicata del 20.01.99). La commissione giuridica e dei diritti dei cittadini del Parlamento europeo ha raccomandato alla commissione per le libertà pubbliche e gli affari interni (capofila) di respingere il progetto di revisione della raccomandazione del Consiglio nella versione proposta in ENFOPOL 98, fra l'altro per motivi di tutela della vita privata e l'imminente entrata in vigore del Trattato di Amsterdam (si veda la relazione del sig. Florio). La commissione per le libertà pubbliche non ha accolto questa raccomandazione e proporrà quindi in seduta plenaria di approvare ENFOPOL 98 sulla base della relazione del sig. Schmid. Il Parlamento europeo adotterà una decisione all'inizio di maggio.

divieto agli operatori di rivelare a posteriori le intercettazioni realizzate).

d. Anche se la risoluzione del Consiglio persegue l'obiettivo della «tutela degli interessi nazionali, della sicurezza nazionale e di indagine sulla criminalità grave», il gruppo attira l'attenzione sui rischi dovuti ad un'estensione ad un numero crescente di paesi - in parte paesi terzi - delle tecniche di intercettazione e di decifrazione delle telecomunicazioni.

Una dichiarazione ufficiale del Parlamento europeo del 16 settembre 1998 relativa alle relazioni transatlantiche²¹, «ritiene che l'importanza crescente della rete Internet, e più in generale, delle telecomunicazioni a livello mondiale e in particolare il sistema Echelon, nonché i rischi di una loro utilizzazione abusiva, richiedono l'adozione di misure di protezione delle informazioni economiche e di una crittografia efficace.»

Queste considerazioni evidenziano i rischi legati ad un'intercettazione delle telecomunicazioni che non sono limitati solo a questioni di sicurezza nazionale e non riguardano unicamente l'Unione europea. Esse mettono in dubbio la loro legittimità, in particolare alla luce degli obblighi derivanti dal diritto comunitario in materia di tutela dei diritti e delle libertà fondamentali delle persone fisiche, e soprattutto della loro vita privata.

e. Il gruppo sottolinea infine che l'entrata in vigore del trattato di Amsterdam comporterà un cambiamento della base giuridica a livello europeo per quanto riguarda le misure di intercettazione delle telecomunicazioni. La competenza attuale del Consiglio per elaborare il testo della risoluzione, basata sugli artt. K.1, paragrafo 9, e K.3, paragrafo 2, del trattato relativi alla cooperazione di polizia e giudiziaria, sarà sostituita da un competenza d'iniziativa della Commissione europea basata sul nuovo art. K.6, paragrafo 2.

2. Quadro giuridico generale

f. Il gruppo ricorda che ogni intercettazione delle telecomunicazioni, intesa come la presa di conoscenza da parte di un terzo del contenuto e/o dei dati riguardanti le telecomunicazioni private tra due o più corrispondenti, in particolare i dati del traffico legati all'utilizzazione dei servizi di telecomunicazione, costituisce una violazione del diritto alla vita privata degli individui e della riservatezza della corrispondenza. Un'intercettazione è ammissibile solamente se soddisfa tre esigenze fondamentali, in conformità all'art. 8, paragrafo 2, della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950²² e all'interpretazione di questa disposizione da parte della Corte europea dei diritti dell'uomo: una base giuridica, la necessità della misura in una società democratica e la conformità ad uno degli obiettivi legittimi enumerati nella convenzione²³.

La base giuridica dovrà definire con precisione i limiti e le modalità del suo esercizio, grazie a norme chiare e dettagliate, che sono necessarie se si tiene conto del perfezionamento continuo dei mezzi tecnici disponibili²⁴. Il testo della legge dev'essere accessibile al pubblico affinché i cittadini possano conoscere le conseguenze del loro comportamento²⁵.

In un simile contesto giuridico dev'essere vietata una sorveglianza generale o a campione

²¹ Sessione plenaria, processo verbale parte II, B4-0803, 0805, 0806 e 0809/98.

²² Va sottolineato che le garanzie fondamentali riconosciute dal Consiglio d'Europa in materia d'intercettazione delle comunicazioni comportano alcuni obblighi per gli Stati, indipendentemente dalle distinzioni esistenti a livello dell'Unione europea in funzione del carattere comunitario o intergovernativo delle questioni affrontate.

²³ La Convenzione n°108 del Consiglio d'Europa prevede anche che un'ingerenza è tollerata unicamente se si tratta di una misura necessaria in una società democratica alla tutela degli interessi nazionali enumerati al suo art. 9, paragrafo 2 (si osservi che gli interessi nazionali enumerati nella convenzione 108 e nella convenzione per la tutela dei diritti dell'uomo non sono esattamente gli stessi), e se essa si limita unicamente al perseguimento di questo obiettivo.

²⁴ Si vedano in appresso gli obblighi previsti dall'art. 4 della raccomandazione n° 4 del Consiglio d'Europa del 7 febbraio 1995 sulla tutela dei dati personali nelle telecomunicazioni, e in particolare nei servizi telefonici.

²⁵ Sentenze Huvig e Kruslin contro la Francia del 25 aprile 1990, serie A n° 176 A e B, pag. 15 e segg.

delle telecomunicazioni²⁹.

g. Nell'Unione Europea, la direttiva 95/46/CE³⁰ sancisce il principio della tutela del diritto alla vita previsto dalla legislazione degli Stati membri. Questa direttiva precisa i principi contenuti nella convenzione europea per la tutela dei diritti dell'uomo del 4 novembre 1950 e nella convenzione del 28 gennaio 1981 del Consiglio d'Europa per la tutela delle persone con riguardo all'elaborazione automatica dei dati personali. La direttiva 97/66/CE³¹ concretizza le disposizioni di tale direttiva precisando l'obbligo che incombe agli Stati membri di garantire la riservatezza delle comunicazioni tramite leggi nazionali che assicurino la riservatezza delle comunicazioni effettuate tramite una rete pubblica di telecomunicazioni o di servizi di telecomunicazioni accessibili al pubblico.

Ai sensi dell'art. 13, paragrafo 1, della direttiva 95/46/CE, uno Stato membro può adottare misure legislative intese a limitare la portata di taluni obblighi (ad esempio, relativi alla raccolta dei dati) e di taluni diritti (ad esempio, il diritto di essere informati in merito ad una raccolta di dati) previsti dalla direttiva³². Tali eccezioni sono dettagliatamente enumerate: la limitazione deve costituire una misura necessaria per tutelare gli interessi pubblici enumerati in modo esaustivo nei paragrafi da a) a g) di tale articolo, quali la sicurezza dello Stato, la difesa, la pubblica sicurezza, per la prevenzione, l'indagine, individuazione e le procedure contro i reati.

Anche la direttiva 97/66/CE stabilisce all'art. 14, paragrafo 1, che gli Stati membri possono limitare l'obbligo della riservatezza delle comunicazioni sulle reti pubbliche unicamente se questa misura è necessaria per tutelare la sicurezza dello Stato, la difesa, la pubblica sicurezza, la prevenzione, l'indagine, l'individuazione e le procedure contro i reati.

3. Obblighi degli operatori e dei fornitori dei servizi di telecomunicazione

h. È opportuno osservare che gli obblighi relativi alla sicurezza e alla riservatezza dei dati cui sono soggetti gli operatori e i fornitori di telecomunicazioni - nonché gli Stati membri - rispettivamente sulla base degli artt. 17, paragrafi 1 e 2, della direttiva 95/46 e sulla base degli artt. 4, 5 e 6 della direttiva 97/66/CE, costituiscono il principio e non l'eccezione.

²⁹ Si vedano in particolare le sentenze Klass, del 6 settembre 1978, serie A n°28, pag. 23 e segg., e Malone, del 2 agosto 1984, serie A n°82, pag. 30 e segg.

Sia la sentenza Klass che la sentenza Leander del 25 febbraio 1987 ribadiscono la necessità di "garanzie sufficienti contro gli abusi dato che un sistema di sorveglianza segreto inteso a proteggere la sicurezza nazionale comporta il rischio di indebolire o anche distruggere la democrazia col pretesto di difenderla" (Sentenza Leander, serie A n°116, pag. 14 e segg.).

Nella sentenza Klass, la Corte osserva (paragrafi 50 e segg.) che la valutazione dell'esistenza di garanzie adeguate e sufficienti contro gli abusi dipende dalle circostanze del caso. Nella sentenza in questione essa ritiene che le misure di sorveglianza previste dalla legislazione tedesca non autorizzano la sorveglianza generale o per campione e non trasgrediscono l'art. 8 della Convenzione europea per la tutela dei diritti dell'uomo. Le garanzie previste dalla legge tedesca sono le seguenti: le misure di sorveglianza sono consentite solamente se alcuni indizi consentono di sospettare che qualcuno progetta, compie o ha compiuto taluni reati gravi; esse sono consentite solo se non è possibile stabilire i fatti in altro modo o con un onere considerevolmente superiore; anche in tal caso, la sorveglianza può riguardare unicamente la persona sospetta o le persone che si ritiene possano avere contatti con tale sospetto.

³⁰ L'art. 3 della direttiva 95/46/CE esclude dal suo campo d'applicazione il trattamento di dati personali per l'esercizio di attività che non rientrano nel campo d'applicazione del diritto comunitario, nonché il trattamento dei dati ai fini della sicurezza pubblica, della difesa, della sicurezza dello Stato e le attività dello Stato nel campo del diritto penale. La maggior parte delle leggi nazionali per il recepimento di questa direttiva valgono anche per attività non coperte dal diritto comunitario.

A partire dal momento in cui un trattamento dei dati è realizzato nel quadro della direttiva (ad esempio, elenco delle chiamate registrate da un operatore ai fini della fatturazione), ma forma in un secondo tempo l'oggetto di un trattamento consistente in una intercettazione di tali dati, devono essere applicate le disposizioni del diritto comunitario. La direttiva 95/46/CE prevede a tal fine una serie di garanzie che devono essere rispettate nel quadro di tali intercettazioni, che saranno illustrate in appresso.

³¹ Direttiva del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, G.U. L 24 del 30 gennaio 1998, pag.1.

³² PreVisto all'art. 6, paragrafo 1 - principi relativi alla qualità dei dati, all'art. 10, all'art. 11, paragrafo 1, - informazione delle persone interessate, e agli artt. 12 - diritto d'accesso e 21 - pubblicità dei trattamenti.

Il gruppo ricorda che tali obblighi valgono in modo generale anche per gli operatori in virtù dell'art. 7 della convenzione del Consiglio d'Europa n°108 relativa alla tutela delle persone con riguardo al trattamento dei dati personali del 28 gennaio 1981, e dell'art. 4 della raccomandazione del Consiglio d'Europa n°4 sulla tutela dei dati personali nei servizi di telecomunicazione, in particolare per quanto riguarda i servizi telefonici, del 7 febbraio 1995³³.

i. Questi obblighi comportano che gli operatori delle telecomunicazioni e i fornitori di servizi possono trattare i dati relativi al traffico e alla fatturazione delle telecomunicazioni unicamente se sono soddisfatte talune condizioni: partendo dal principio che i dati relativi al traffico concernente gli abbonati e utilizzatori devono essere cancellati o resi anonimi subito dopo la fine della comunicazione, ne segue che gli scopi per cui i dati possono essere trattati, la durata della loro eventuale conservazione nonché l'accesso a tali dati sono rigorosamente limitati³⁴.

j. Inoltre, gli operatori delle telecomunicazioni e i fornitori di servizi di telecomunicazione devono prendere le misure necessarie per rendere tecnicamente difficile o impossibile, tenuto conto dello stato attuale della tecnica, l'intercettazione delle telecomunicazioni da parte di chi non è autorizzato dalla legge.

Il gruppo sottolinea a tale proposito che la realizzazione di strumenti efficaci per l'intercettazione delle comunicazioni per scopi legittimi, che utilizzano le tecniche più avanzate, non deve comportare un abbassamento del livello generale della riservatezza delle comunicazioni e della tutela della vita privata delle persone fisiche.

Questi obblighi assumono un significato particolare nel caso in cui le telecomunicazioni tra persone situate sul territorio degli Stati membri transitano o possono transitare all'esterno del territorio europeo, in particolare nel caso dell'utilizzazione di satelliti o di Internet.

k. Ai sensi della direttiva 95/46/CE, il fatto di rendere accessibili tali telecomunicazioni all'esterno dell'Unione europea potrebbe inoltre costituire una violazione dell'art. 25 della direttiva, dato che le autorità straniere che le intercettano potrebbero non essere in grado di assicurare un adeguato livello di protezione dei dati.

4. Rispetto delle libertà fondamentali da parte delle pubbliche autorità nel quadro delle intercettazioni

l. È importante che il diritto nazionale precisi in modo rigoroso e nel rispetto di tutte le disposizioni summenzionate:

³³ "4.1. I dati personali raccolti e trattati dagli operatori delle reti o dai fornitori di servizi non devono essere divulgati, a meno che l'abbonato in questione non abbia espressamente acconsentito per iscritto e l'informazione divulgata non consenta l'identificazione dell'abbonato.

L'abbonato può ritirare il suo consenso in qualsiasi momento, ma non retroattivamente.

4.2. I dati personali raccolti e trattati dai gestori della rete o dai fornitori di servizi possono essere comunicati alle pubbliche autorità se tale comunicazione è prevista dalla legge e costituisce una misura necessaria in una società democratica:

a. per tutelare la sicurezza dello Stato, la pubblica sicurezza, gli interessi monetari dello Stato o nell'ambito di un procedimento contro un reato;

b. per la tutela della persona interessata e dei diritti e delle libertà altrui.

4.3. Nel caso di una comunicazione di dati personali alle pubbliche autorità, il diritto interno dovrebbe regolamentare:

a. l'esercizio dei diritti di accesso e di rettifica da parte della persona interessata;

b. le condizioni alle quali le pubbliche autorità competenti potranno negare le informazioni alla persona interessata o rinviarne la consegna;

c. la conservazione o la distruzione di tali dati."

³⁴ Si vedano in particolare gli obblighi previsti dall'art. 6 della direttiva 97/66/CE.

Tali obblighi fanno sorgere dei dubbi per quanto riguarda le pratiche diffuse presso i gestori dei servizi di telecomunicazione che consentono un esame generale e preliminare dei dati del traffico degli abbonati, al fine di individuare il comportamento sospetto di taluni abbonati - ed eventualmente consentire l'intercettazione mirata del contenuto di talune telecomunicazioni.

- le autorità autorizzate a consentire l'intercettazione legale delle telecomunicazioni, i servizi autorizzati a procedere alle intercettazioni e la base giuridica del loro intervento,
- gli scopi per cui tali intercettazioni possono esser effettuate, per poter valutare se la misura è adeguata tenuto conto degli interessi nazionali in gioco,
- il divieto di qualsiasi sorveglianza per campione o generale delle telecomunicazioni su vasta scala,
- le circostanze e le condizioni precise (ad esempio, gli elementi che giustificano la misura, la durata della misura) che si applicano alle intercettazioni, nel rispetto del principio di specificità che deve rispettare qualsiasi ingerenza nella vita privata altrui³⁵,
- il rispetto di questo principio di specificità, corollario del divieto di qualsiasi sorveglianza per campione o generale, implica, in particolare per quanto riguarda i dati sul traffico, che le pubbliche autorità possono avere accesso a tali dati solo in casi specifici, e non in modo generale e attivo.
- le misure di sicurezza per quanto riguarda il trattamento e la memorizzazione dei dati, nonché la durata della loro conservazione,
- per quanto riguarda le persone coinvolte indirettamente o aleatoriamente³⁶ nelle intercettazioni, le garanzie particolari che si applicano al trattamento di dati personali: in particolare, i criteri che giustificano la conservazione dei dati, e le condizioni della comunicazione di tali dati a terzi,
- l'informazione della persona sotto sorveglianza, appena questa è possibile³⁷,
- i tipi di ricorso cui possono ricorrere le persone sotto sorveglianza³⁸,
- le modalità di sorveglianza di questi servizi da parte di un'autorità di controllo indipendente³⁹,
- la pubblicità - ad esempio sotto forma di relazioni statistiche regolari - della politica d'intercettazione delle telecomunicazioni effettivamente attuata⁴⁰,
- le condizioni precise per la comunicazione dei dati a terzi nel quadro di accordi bi- o multilaterali.

Fatto a Bruxelles, addì 3 maggio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

³⁵ Cfr. la precedente nota 13.

³⁶ I dati in questione si riferiscono a persone che non formano l'oggetto di misure di sorveglianza, ma il cui corrispondente è oggetto di tali misure; ad esempio: numero di telefono composto dalla persona sorvegliata e relativo ad un parente di quest'ultimo; localizzazione geografica di talune persone in contatto tramite telefonia mobile con la persona sotto sorveglianza.

³⁷ La persona sotto sorveglianza dovrebbe infatti essere informata a partire dal momento in cui l'informazione non danneggia o non danneggia più l'indagine.

³⁸ La summenzionata sentenza nella causa Leander fa presente che l'istituzione dinanzi alla quale può essere presentato il ricorso "non deve essere necessariamente un'istituzione giudiziaria stricto sensu, ma che si deve tener conto dei suoi poteri e delle sue garanzie procedurali nella valutazione dell'efficacia del ricorso". Questo ricorso "deve essere possibilmente efficace, tenuto conto delle limitazioni inerenti ad ogni sistema di sorveglianza segreta volta a proteggere la sicurezza nazionale" (paragrafi 83 e 84).

³⁹ La sentenza nella causa Leander prevede il controllo democratico delle intercettazioni specificando che "è compito del Parlamento e delle istituzioni indipendenti [del governo] vigilare sul corretto funzionamento del sistema" (paragrafo 64).

⁴⁰ Questa esigenza di pubblicità, come anche la necessità di un controllo delle intercettazioni da parte di un'autorità indipendente, sono menzionate nella "Common position on public accountability in relation to interception of private communications" adottata a Hong Kong il 15 aprile 1998 dal gruppo internazionale di lavoro sulla tutela dei dati nel settore delle telecomunicazioni.

Raccomandazione 3/99: La conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari

5085/99/IT/definitivo

WP 25

Gruppo di lavoro per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 3/99: La conservazione dei dati sulle comunicazioni da parte dei fornitori di
servizi Internet a fini giudiziari

Approvata il 7 settembre 1999

Introduzione

La lotta alla criminalità elettronica costituisce un problema che sta richiamando crescente attenzione internazionale.⁴¹ I paesi G8⁴² hanno approvato un piano d'azione⁴³ articolato su dieci punti, attualmente in fase di realizzazione grazie a un sottogruppo specializzato in materia di criminalità elettronica costituito dai rappresentanti delle autorità di polizia dei paesi G8. Uno dei problemi più controversi è costituito dalla conservazione dei dati sul "traffico" (comunicazioni) passato e futuro da parte dei fornitori di servizi Internet a fini giudiziari e di polizia, con trasmissione dei dati stessi alle autorità competenti. Il sottogruppo G8 sulla criminalità elettronica intende formulare raccomandazioni per garantire la possibilità di conservare ed esaminare tali dati. I ministri della Giustizia e degli Interni dei paesi G8 potranno discutere tali raccomandazioni nella riunione di Mosca del 19 - 20 ottobre 1999.

Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali⁴⁴ è consapevole del ruolo importante che può essere svolto dai dati di traffico nel contesto delle indagini su reati commessi via Internet, ma desidera peraltro richiamare l'attenzione dei governi nazionali sui principi relativi alla protezione dei diritti e delle libertà fondamentali dei cittadini, con particolare riferimento alla riservatezza e al segreto postale, principi di cui è necessario tenere conto in questo contesto.

Il gruppo di lavoro è dell'opinione che i ministri della Giustizia e degli Interni G8 potrebbero richiedere un'interpretazione equilibrata delle due direttive UE sulla protezione dei dati⁴⁵ a livello di attuazione onde tenere conto delle esigenze di controllo unitamente a quelle attinenti alla riservatezza.

⁴¹ Vedi ad esempio "COMCRIME Study" "Legal Aspects of computer-related Crime in the Information Society- COMCRIME Study, January 1997 - Presentato nell'ambito del piano d'azione UE contro la criminalità organizzata - Disponibile sul sito web del Comitato consultivo giuridico: <http://www2.echo.lu/legal/en/comcrime/sieber.html>. Il Consiglio d'Europa sta lavorando su un progetto di convenzione in materia di criminalità cibernetica. Il Consiglio dell'UE ha manifestato il proprio sostegno a tale iniziativa il 27 maggio 1999. Per criminalità elettronica si intendono tutti i reati commessi su reti elettroniche, come ad esempio attacchi mediante computer, pubblicazione di materiale illecito su siti web, e attività commesse dalla criminalità transnazionale organizzata (ad es. traffico di narcotici, pornografia infantile).

⁴² Canada, Francia, Germania, Italia, Giappone, Regno Unito, Stati Uniti d'America e Russia.

⁴³ "Meeting of Justice and Interior Ministers of the Eight, December 9-10, 1997, Communiqué, Washington D.C. December 10, Communiqué Annex: Principles and Action Plan to Combat High-tech Crime"

⁴⁴ Istituito in virtù dell'art. 29 della 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, GU L 281 del 23.11.1995, p. 31. Disponibile su: <http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm>

⁴⁵ Direttiva 95/46/CE, e 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, 30 gennaio 1998, p. 1. Indirizzo Internet: vedi nota 4.

Il gruppo di lavoro è altresì consapevole del potenziale onere per operatori di telecomunicazioni e fornitori di servizi Internet.

L'obiettivo della presente Raccomandazione, pertanto, è di contribuire ad una applicazione uniforme delle Direttive 95/46/CE e 97/66/CE, grazie alla definizione di condizioni chiare e prevedibili per gli operatori di telecomunicazioni e fornitori di servizi Internet, come pure per le autorità di controllo, nel rispetto del diritto alla riservatezza.

Situazione giuridica

Nell'ambito dell'Unione europea, la Direttiva 95/46/CE ha permesso di armonizzare la protezione della riservatezza assicurata dai sistemi giuridici degli Stati membri. La direttiva concretizza e amplifica i principi della Convenzione europea per la Protezione dei Diritti umani del 4 novembre 1950 e della Convenzione No. 108 del Consiglio d'Europa del 28 gennaio 1981 per la tutela delle persone con riguardo al trattamento automatico dei dati personali. La Direttiva 97/66/CE precisa le norme di cui sopra nel settore delle telecomunicazioni. Ambedue le direttive si applicano al trattamento dei dati personali, ivi compresi i dati Internet relativi ad abbonati e utenti.⁴⁶

In particolare, gli artt. 6, 7, 13, 17 (1) e (2) della Direttiva 95/46/CE, e gli artt. 4, 5, 6 e 14 della Direttiva 97/66/CE vertono sulla legalità di tali trattamenti da parte di operatori di telecomunicazioni e fornitori di servizi.

Tali norme consentono ai citati operatori e fornitori di effettuare il trattamento dei dati in determinate condizioni espressamente specificate.

L'art. 6 (1) lettera b) dispone che i dati possano essere raccolti unicamente per finalità determinate, esplicite e legittime, e che non possano essere ulteriormente trattati in modo incompatibile con le finalità originali. L'art. 6 (1) lettera e) dispone che i dati personali non possano essere conservati per un arco di tempo superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti o successivamente trattati. L'art. 13 consente agli Stati membri di limitare fra l'altro la portata dell'art. 6 (1) qualora tale restrizione costituisca una misura necessaria alla salvaguardia della sicurezza dello Stato o della pubblica sicurezza, o alla prevenzione, ricerca, accertamento e perseguimento di fenomeni a carattere penale.

L'applicazione dei principi in questione è ulteriormente specificata dagli artt. 5 e 6, paragrafi 2-5, della Direttiva 97/66/CE. L'art. 5 garantisce la riservatezza delle comunicazioni effettuate attraverso le reti pubbliche di telecomunicazione e i servizi di telecomunicazione offerti al pubblico. Gli Stati membri sono tenuti a vietare l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti senza il consenso di questi ultimi, eccetto quando tali attività siano autorizzate a norma di legge in virtù dell'art. 14, paragrafo 1.

Come regola generale, i dati sul traffico devono essere cancellati o resi anonimi al termine della comunicazione (Art. 6, paragrafo 1, della Direttiva 97/66/CE). Ciò si deve alla delicatezza di tali dati, che possono consentire l'elaborazione di profili individuali di comunicazione, ivi comprese le fonti delle informazioni e la località geografica dell'utente di telefoni fissi o mobili, e ai pericoli per la riservatezza che derivano dalla raccolta, trasmissione o ulteriore utilizzazione di tali dati. L'art. 6 (2) prevede un'eccezione concernente il trattamento di taluni dati ai fini delle attività di fatturazione agli abbonati e della riscossione dei canoni di interconnessione, ma solo entro il termine del periodo durante il quale le bollette possono essere legalmente impugnate, o possono essere riscossi i pagamenti.

L'art. 14 (1) consente agli Stati membri di adottare disposizioni volte a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'art. 6, qualora tali limitazioni costituiscano una misura necessaria alla salvaguardia della sicurezza dello Stato, ed alla prevenzione, ricerca, accertamento e perseguimento di attività a carattere penale, come previsto dall'art. 13 (1) della Direttiva 95/46/CE.

Ne deriva che gli operatori e fornitori di servizi Internet non hanno facoltà di raccogliere e

⁴⁶ Vedi "Working document: Processing of Personal Data on the Internet", approvato il 23 febbraio 1999, disponibile all'indirizzo di cui alla nota 1.

memorizzare dati esclusivamente a fini giudiziari, se non in virtù delle eccezioni ed alle condizioni di cui sopra. Ciò coincide con la prassi tradizionale di molti Stati membri, nei quali l'applicazione dei principi nazionali per la protezione dei dati si è tradotta nel divieto al settore privato di mantenere dati personali unicamente in ragione di possibili esigenze di polizia o sicurezza.

In questo contesto, merita rilevare che, ai fini delle esigenze di polizia ed alle condizioni di cui agli artt. 13 della Direttiva 95/46/CE e 14 della Direttiva 97/66/CE, la legislazione di molti Stati membri definisce le precise condizioni alle quali le forze di polizia e di sicurezza possono avere accesso ai dati memorizzati dagli operatori privati di telecomunicazioni e dai fornitori di servizi Internet per proprie finalità a carattere civile.

Come già rilevato dal Gruppo di lavoro nella Raccomandazione 2/99 sulla tutela della riservatezza nel contesto dell'intercettazione di telecomunicazioni, adottata il 3 maggio 1999²⁷, il fatto che una terza parte acquisisca conoscenze concernenti i dati sul traffico relativo all'utilizzazione dei servizi di telecomunicazione è stato generalmente considerato una forma di intercettazione delle telecomunicazioni, e costituisce pertanto una violazione del diritto degli individui alla riservatezza e del segreto epistolare, così come tali diritti sono garantiti dall'art. 5 della Direttiva 97/66/CE²⁸. Inoltre, l'accesso a tali dati è incompatibile con l'art. 6 della direttiva citata.

Qualsiasi violazione di questi diritti e obblighi è inaccettabile se non soddisfa tre criteri fondamentali, in conformità all'art. 8 (2) della Convenzione europea per la Protezione dei Diritti umani e delle Libertà fondamentali del 4 novembre 1950 ed in virtù dell'interpretazione della Corte europea dei Diritti dell'uomo: l'esistenza di una idonea base giuridica, la necessità dell'intervento in una società democratica, e la conformità ad uno dei legittimi obiettivi elencati dalla Convenzione. La base giuridica deve definire con precisione i limiti e le modalità di applicazione del provvedimento: i fini ai quali i dati possono essere trattati, il periodo di tempo durante il quale i dati possono essere (eventualmente) mantenuti, e le caratteristiche dell'accesso devono essere strettamente limitati. Le attività generali di esplorazione o sorveglianza su vasta scala devono essere vietate²⁹. Ne consegue che le autorità pubbliche possono avere accesso ai dati soltanto caso per caso, e mai proattivamente, o in via generale.

Questi criteri coincidono con i citati disposti dell'art. 13 della Direttiva 95/46/CE e dell'art. 14 della Direttiva 97/66/CE.

Divergenza delle norme nazionali³⁰

Per quanto riguarda il periodo durante il quale i dati sul traffico possono essere memoriz-

²⁷ Disponibile all'indirizzo di cui alla nota 1.

²⁸ Le autorità giudiziarie richiedono inoltre l'accesso alle informazioni sui collegamenti in tempo reale, e ai dati concernenti i collegamenti attivi (cosiddetti "futuro traffico dati").

²⁹ Vedi in particolare la sentenza Klass del 6 settembre 1978, serie A N°28, pp.23 e seguenti, e la sentenza Malone del 2 agosto 1984, serie A N°82, pp. 30 e seguenti.

La sentenza Klass, in base a quella Leander del 25 febbraio 1987, insiste sulla necessità di "efficaci garanzie contro gli abusi" "in vista del rischio che un sistema di sorveglianza segreta per la tutela della sicurezza nazionale possa minare o persino distruggere la democrazia, col pretesto di difenderla". (Sentenza Leander, serie A N°116, pp. 14 e seguenti).

La Corte rileva, nella sentenza Klass (par. 50 e seguenti) che la valutazione dell'esistenza di garanzie adeguate ed effettive contro gli abusi dipende da tutte le circostanze del caso. Nella fattispecie, la Corte ritiene che i provvedimenti di sorveglianza previsti dalla legislazione tedesca non permettano una sorveglianza generale o esplorativa e non siano incompatibili con l'art. 8 della Convenzione europea per la Protezione dei Diritti umani. La legislazione tedesca fornisce le seguenti garanzie: la sorveglianza è limitata ai casi in cui vi sono indicazioni tali da legittimare il sospetto che un individuo stia preparando, commettendo o abbia commesso taluni gravi atti criminosi; i provvedimenti possono essere ordinati soltanto se l'accertamento dei fatti con altri metodi sia privo di prospettive di successo, o molto più difficile; ed anche in tal caso, le attività di sorveglianza possono interessare soltanto la persona dell' indagato, o i suoi presunti "contatti".

³⁰ La Commissione sta attualmente analizzando la legislazione degli Stati membri che hanno notificato provvedimenti nazionali di recepimento della Direttiva 97/66/CE e della Direttiva 95/46/CE. Vedi la tabella di recepimento per quanto riguarda la Direttiva 95/46/CE, disponibile all'indirizzo di cui alla nota 4.

zati, la Direttiva 97/66/CE ne consente la conservazione unicamente a fini di fatturazione³¹ e soltanto fino alla fine del periodo durante il quale è legalmente possibile impugnare la fattura. Questo periodo, tuttavia, varia considerevolmente negli Stati membri. In Germania, ad esempio, gli operatori delle telecomunicazioni e i fornitori di servizi di telecomunicazione hanno facoltà di memorizzare i dati necessari per la fatturazione fino a un massimo di 80 giorni, al fine di giustificare la correttezza delle fatture³². In Francia, dipende dallo status dell'operatore: gli operatori "tradizionali" di telecomunicazioni hanno facoltà di memorizzare i dati di traffico fino a un massimo di un anno, in base alla legge che definisce il periodo durante il quale possono essere contestate le fatture. Questo periodo è fissato a 10 anni per altri operatori. In Austria, la legge sulle telecomunicazioni non fissa un periodo preciso durante il quale i dati sul traffico possono essere memorizzati a fini di fatturazione, ma limita tale periodo a quello durante il quale le fatture possono essere contestate, o i pagamenti possono essere riscossi. Nel Regno Unito, secondo la legge, le fatture possono essere impugnate per un periodo di 6 anni, ma gli operatori e fornitori di servizi conservano i relativi dati per circa 18 mesi. In Belgio, la legge non definisce il periodo in questione, ma il principale fornitore di servizi di telecomunicazione lo ha fissato a 3 mesi nelle proprie condizioni generali. In Portogallo la prassi è ancora diversa, poiché, dato che il periodo non è fissato per legge, l'autorità nazionale per la protezione dei dati decide caso per caso. E' interessante notare che in Norvegia il periodo è di 14 giorni.

Anche la pratica attuale dei fornitori di servizi Internet non è omogenea: sembrerebbe che i fornitori più piccoli mantengano i dati sul traffico per periodi brevissimi (poche ore) per mancanza di capacità di memoria. I fornitori più grandi, con maggiori capacità, possono mantenere i dati per qualche mese (ma la durata può dipendere dalle rispettive politiche di fatturazione: in base al tempo di collegamento, o a quota fissa).

A fini giudiziari, la legge olandese sulle telecomunicazioni obbliga gli operatori e i fornitori di servizi a raccogliere e memorizzare i dati sul traffico per tre mesi.

Ostacoli al funzionamento del Mercato interno

Queste variazioni sollevano potenziali ostacoli in seno al Mercato interno dal punto di vista della prestazione transnazionale di servizi Internet e di telecomunicazione, ma anche l'efficacia delle attività giudiziarie può essere ridotta per lo stesso motivo. Si potrebbe sostenere che un fornitore di servizi Internet con sede in uno Stato membro non ha facoltà di memorizzare i dati per un periodo superiore a quello previsto dallo Stato membro in cui l'utente risiede e utilizza il servizio. Alternativamente, un fornitore potrebbe essere obbligato a mantenere i dati per un periodo superiore a quello consentito dal proprio Stato membro in ragione della legislazione del paese di residenza degli utenti. Nel caso di fatture per comunicazioni transnazionali tramite telefoni cellulari, l'incasso non viene effettuato dall'operatore estero, ma dall'operatore nazionale degli abbonati in questione. La diversa durata dei periodi di memorizzazione può quindi comportare gli stessi problemi illustrati per i fornitori di servizi Internet. Il disposto sulla legge applicabile di cui all'art. 4 della Direttiva 95/46/CE risolve il problema soltanto nella misura in cui il fornitore di servizi Internet esercita direttamente il controllo, ed ha sede soltanto in uno Stato membro, ma non nei casi in cui è insediato in Stati membri diversi, che applicano periodi diversi, o laddove effettua il trattamento dei dati sul traffico per conto di autorità di controllo.

Raccomandazione

Alla luce di quanto precede, il Gruppo di lavoro ritiene che il mezzo più efficace per limitare inaccettabili pericoli alla riservatezza nella salvaguardia delle esigenze delle autorità giudiziarie consista nell'evitare che i dati sul traffico siano mantenuti esclusivamente a fini giudiziari, e che le leggi nazionali costringano gli operatori delle telecomunicazioni, i servizi di telecomunicazione e

³¹ E, ove necessario, per il pagamento delle tariffe di intercollegamento fra operatori delle telecomunicazioni, vedi art. 6, paragrafo 2, della Direttiva 97/66/CE.

³² Se una fattura viene contestata durante tale periodo, i relativi dati, naturalmente, possono essere mantenuti fino al termine della vertenza.

i fornitori di servizi Internet a mantenere dati sul traffico per un periodo di tempo superiore a quello necessario ai fini di fatturazione.

Il Gruppo di lavoro raccomanda che la Commissione europea proponga opportuni provvedimenti per un'ulteriore armonizzazione del periodo durante il quale gli operatori delle telecomunicazioni, i servizi di telecomunicazione e i fornitori di servizi Internet hanno facoltà di mantenere i dati sul traffico ai fini di fatturazione e di riscossione dei canoni di intercollegamento⁵³. Il Gruppo di lavoro è del parere che tale periodo debba essere sufficiente per consentire ai consumatori di contestare le fatture, ma che debba essere più breve possibile per non creare un carico eccessivo per gli operatori e i fornitori di servizi e per rispettare i principi di proporzionalità e specificità nell'ambito del diritto alla riservatezza. Il periodo in questione dovrebbe essere allineato sulla base dello standard di tutela più elevato che si riscontri negli Stati membri. Il Gruppo richiama l'attenzione sul fatto che, in diversi Stati membri, sono stati felicemente applicati periodi non superiori a tre mesi.

Il Gruppo di lavoro raccomanda altresì che i governi nazionali tengano conto delle presenti considerazioni.

Fatto a Bruxelles, addì 7 settembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

⁵³ In vista di questo obiettivo, non vi è motivo di effettuare distinzioni fra operatori pubblici o privati.

Documento di lavoro: Trattamento dei dati personali su Internet5013/99/IT/final
WP 16

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Documento di lavoro: Trattamento dei dati personali su Internet

Adottato dal gruppo di lavoro il 23 febbraio 1999

Introduzione

Ogni nuova fase nel processo di sviluppo tecnologico pone problemi per la tutela dei dati personali e il diritto alla vita privata, come dimostra l'esperienza del passato per quanto riguarda ad esempio la distribuzione di personal computer, le prime applicazioni della telematica ecc. Internet rientra in tale contesto almeno per le seguenti ragioni:

- L'impiego delle infrastrutture si basa spesso direttamente sull'elaborazione di dati personali, come alcuni indirizzi del protocollo Internet.
- I servizi forniti per mezzo di queste infrastrutture offrono nuove possibilità, in particolare per quanto riguarda la distribuzione d'informazioni contenenti dati personali (ad es. indirizzari, gruppi di discussione, accesso alle basi dati ecc.).
- Gli strumenti tecnici sono nuovi, come nel caso dei programmi informatici di *browsing*, ed evolvono rapidamente.
- Molti operatori si trovano ad affrontare per la prima volta le nuove attività commerciali in linea che comportano il trattamento di dati personali ed anche i confini tradizionali tra le diverse professioni sono in rapida fase di ridefinizione.
- Uno degli usi più stimolanti di Internet è lo svolgimento di un'attività commerciale in linea: il commercio elettronico consiste in particolar modo nella vendita diretta dall'impresa ai consumatori senza alcuna intermediazione, grazie a nuovi metodi d'individuazione degli obiettivi commerciali e nuovi mezzi di pagamento.
- La dimensione globale si presenta fin dagli inizi.

In questo contesto complesso e, sotto il profilo della protezione dei dati, controverso lavorano concretamente da circa tre anni le autorità nazionali incaricate della tutela dei dati, la cui esperienza si è gradualmente consolidata (vedi ad es. i loro rapporti annuali).

Analogamente il gruppo^{*} ha iniziato ad occuparsi in modo pragmatico e in base all'urgenza dell'argomento discusso a livello europeo o internazionale delle questioni riguardanti l'applicazione al trattamento dei dati personali su Internet dei principi che reggono la tutela dei dati.

Alcuni esempi:

^{*} Istituito dall'articolo 29 della Direttiva 95/46/EC 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, GU L 281 del 23 novembre 1995, p. 31. Disponibile all'indirizzo: <http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

- l'anonimato su Internet⁵⁵;
- il sostegno al "Memorandum di Berlino e Budapest" del gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni⁵⁶;
- un primo parere sul progetto P3P del Consorzio World Wide Web⁵⁷;
- la Raccomandazione 1/99 sul "Trattamento invisibile e automatico dei dati personali su Internet mediante software e hardware", adottata il 23 febbraio 1999⁵⁸.

La questione della protezione dei dati e della vita privata su Internet viene discussa anche in organismi internazionali quali il Consiglio d'Europa⁵⁹ e l'OCSE⁶⁰. In merito alla proposta dell'Unione europea di giungere a soluzioni globali nel quadro dell'OMC, tale organizzazione ha accettato d'includere la tutela dei dati nel suo programma di lavoro relativo ad aspetti del commercio elettronico attinenti alla compravendita. Il tema verrà discusso dal Consiglio per gli scambi di servizi, che si riunisce regolarmente per poter arrivare a presentare una relazione entro il giugno 1999. L'obiettivo è quello di concludere un accordo su principi fondamentali e vincolanti che consentano la libera circolazione dei dati personali nell'ambito del commercio elettronico mondiale, rispettando nel contempo il diritto dei singoli alla vita privata e che assicurino quindi l'affidabilità del commercio elettronico.

La conferenza europea dei commissari responsabili per la protezione dei dati, tenutasi a Dublino il 23 e il 24 aprile 1998, ha auspicato che il gruppo potesse sviluppare il tema in modo più sistematico al fine di chiarire quali fossero le questioni in causa e fornire soluzioni volte a contribuire a uno sviluppo d'Internet e dei servizi ad esso attinenti che rispetti il diritto dell'utente alla vita privata e garantisca l'affidabilità sia per le applicazioni commerciali che per quelle private. I commissari hanno ricordato che quanto disposto dalla legislazione dell'UE in tema di tutela dei dati si applica pienamente, secondo le modalità del caso, al trattamento dei dati personali su Internet, a prescindere dagli strumenti tecnici utilizzati.

La pertinenza delle direttive sulla protezione dei dati

Il gruppo condivide il parere espresso in occasione della conferenza europea dei commissari responsabili per la protezione dei dati. Sotto il profilo giuridico Internet non opera nel vuoto: il trattamento dei dati personali su Internet deve pertanto rispettare i principi della tutela dei dati così come avviene al di fuori della rete⁶¹. Ciò non limita assolutamente il ricorso ad Internet, ma al contrario fa parte degli elementi fondamentali volti ad assicurare la fiducia degli utenti nel funzionamento di Internet e dei servizi forniti da esso. La tutela dei dati su Internet è quindi una condizione indispensabile per l'accettazione del commercio elettronico.

La direttiva generale relativa alla protezione dei dati 95/46/EC si applica a qualsiasi trattamento di dati personali che rientri nel suo ambito a prescindere dai mezzi tecnici utilizzati. Per questo motivo il trattamento dei dati personali su Internet rientra nel campo d'applicazione della direttiva.

⁵⁵ Si veda la Raccomandazione del gruppo 3/97 "L'anonimato su Internet", adottata il 3 dicembre 1997, disponibile all'indirizzo: vedi nota 1.

⁵⁶ Si veda la Raccomandazione del gruppo 2/97 "Rapporto e orientamenti del gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni ("Memorandum di Berlino e Budapest sulla protezione dei dati e della vita privata su Internet"), adottata il 3 dicembre 1997, disponibile all'indirizzo: vedi nota 1.

⁵⁷ Si veda il Parere del gruppo 1/98 "Piattaforma in materia di rispetto della vita privata (P3P) e lo Standard di definizione di profili aperti (OPS)", adottato il 16 giugno 1998, disponibile all'indirizzo: vedi nota 1.

⁵⁸ Disponibile all'indirizzo: vedi nota 1.

⁵⁹ Il Consiglio d'Europa è in procinto di adottare linee guida in materia di protezione della vita privata sulle autostrade dell'informazione.

⁶⁰ Si vedano i risultati della conferenza di Ottawa dell'ottobre 1998: disponibile all'indirizzo <http://www.oecd.org>.

⁶¹ Si veda anche la dichiarazione ministeriale del Convegno sulle reti globali d'informazione, tenutosi a Bonn nel luglio del 1997, disponibile all'indirizzo: <http://www2.echo.lu/bonn/conference.html>.

La direttiva specifica 97/66/EC relativa alla tutela della vita privata e dei dati personali nel settore delle telecomunicazioni⁴² integra la direttiva generale 95/46/EC introducendovi norme specifiche in ambito tecnico e giuridico.⁴³

Internet è una rete di computer aperta a tutti e forma dunque parte del settore pubblico delle telecomunicazioni. Le disposizioni della direttiva 97/66/EC si applicano perciò al trattamento dei dati personali con riferimento alla fornitura di servizi di telecomunicazione disponibili al pubblico mediante reti pubbliche di telecomunicazioni all'interno della Comunità⁴⁴.

La task force Internet

Il gruppo è consapevole del fatto che l'applicazione omogenea delle direttive relative alla protezione dei dati nell'ambito del trattamento dei dati personali su Internet richiede un'analisi che tenga in considerazione soprattutto gli aspetti tecnici e giuridici. Il gruppo intende inoltre contribuire a dar risposta ai molteplici e dettagliati quesiti che potranno essere posti a questo riguardo.

Al fine di assicurare un approccio coerente e omogeneo al trattamento dei dati su Internet il gruppo ha istituito una task force interdisciplinare il cui compito è quello d'identificare le problematiche relative a Internet da discutere ed elaborare i pareri del gruppo a questo riguardo.

La task force di Internet ha già preparato la Raccomandazione 1/99 del gruppo relativa al trattamento invisibile e automatico dei dati personali su Internet mediante software e hardware⁴⁵.

La task force Internet continuerà a lavorare più generalmente sull'applicazione delle due direttive al trattamento dei dati personali su Internet e presenterà proposte riguardanti le modalità per attuarle in modo omogeneo le prescrizioni per quanto riguarda, ad esempio, i servizi di posta elettronica (e-mail) e i dati relativi al traffico su Internet.

Fatto a Bruxelles, addì 23 febbraio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

⁴² A norma dell'articolo 14 paragrafo 3 della Direttiva 97/66/EC, il gruppo Istituito dalla Direttiva 95/46/EC deve svolgere le sue funzioni anche per quanto concerne la tutela dei diritti e delle libertà fondamentali nonché dei legittimi interessi nel settore delle telecomunicazioni, che sono oggetto della Direttiva 97/66/EC.

⁴³ Per quanto riguarda tutti gli aspetti non specificamente regolati dalla Direttiva 97/66/EC, quali gli obblighi del controllore e i diritti delle persone fisiche o i servizi di telecomunicazione non offerti al pubblico, si applica la Direttiva 95/46/EC (si veda il punto 11 del preambolo della Direttiva 97/66/EC).

⁴⁴ Si veda l'articolo 3 paragrafo 1 della Direttiva 97/66/EC.

⁴⁵ Adottata il 23 febbraio 1999. Disponibile all'indirizzo: vedi nota 1.

6.3.4.: Informazione nel settore pubblico**Parere 3/99 relativo a: L'informazione del settore pubblico e la protezione dei dati personali**

WP 20

Gruppo di protezione delle persone
rispetto al trattamento dei dati personali

Parere 3/99 relativo a: L'informazione del settore pubblico e la protezione dei dati personali

Contributo alla consultazione iniziata con il libro verde della Commissione europea intitolato
"L'informazione del settore pubblico: una risorsa fondamentale per l'Europa", COM (1998) 585

Adottato il 3 maggio 1999

Introduzione e osservazioni preliminari:

La Commissione europea ha sottoposto alla consultazione pubblica un libro verde su "informazione del settore pubblico: una risorsa fondamentale per l'Europa"*. L'oggetto principale del libro consiste nel promuovere una discussione sul modo di agevolare l'accesso delle informazioni detenute dal settore pubblico ai cittadini ed alle imprese nonché sulla necessità o no di armonizzare le norme nazionali in questo settore. Sembra che il documento si sia ampiamente ispirato alla rivendicazione degli operatori privati che desiderano accedere al minimo costo alle informazioni pubbliche e contestano il mantenimento dei monopoli pubblici nel campo in questione.

Una delle poste in gioco del libro verde riguarda dunque la messa a disposizione dell'informazione del settore pubblico, vale a dire di una categoria particolare di dati detti "pubblici", quelli che, essendo detenuti da organismi del settore pubblico, verrebbero resi pubblici in virtù di norme o di un uso⁶⁷ il cui fondamento implicito ed esplicito può trovarsi in una volontà di trasparenza dello stato nei confronti dei cittadini⁶⁸.

La protezione dei dati personali non è affatto ignorata da questo documento sebbene non ne rappresenti a prima vista la problematica più importante.

Il punto 111 (II. 7, pag. 17) menziona in modo esplicito che la direttiva 95/46/CE relativa alla protezione dei dati personali⁶⁹ "stabilisce norme obbligatorie per i settori pubblico e privato e [...] si applica pienamente nel caso in cui dati personali siano detenuti dal settore pubblico".

Il punto 114 sottolinea che "l'emergere della società dell'informazione potrebbe comportare nuovi rischi per la vita privata degli individui se alcuni registri pubblici diventassero accessibili sotto forma elettronica (in particolare online, su Internet, e in grandi quantità)".

Il libro verde, nel complesso, porta alla luce, tuttavia, diverse ambiguità sulla forza di tale convinzione.

* Com 1998 – 585, disponibile al seguente indirizzo : <http://www.echo.lu/legal/en/access.htm>.

⁶⁷ Sembra che una distinzione possa essere fatta fra la pubblicazione derivante da disposizioni di legge, l'accesso all'informazione autorizzato dalla legge, e situazioni nelle quali la questione della pubblicità o dell'accesso si pone in seguito a una domanda formulata da privati o imprese senza che entrino in gioco particolari disposizioni di legge.

⁶⁸ Il presente parere non tratta pertanto dell'altra accezione - più ampia - del concetto di dati "pubblici": l'insieme dei dati gestiti dal settore pubblico.

⁶⁹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla protezione delle persone fisiche in relazione all'elaborazione dei dati a carattere personale e alla libera circolazione di tali dati, GU L 281, 23 novembre 1995, p. 31. Disponibile all'indirizzo seguente: <http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.htm>.

In primo luogo l'impiego (nella versione inglese) del termine "publicly available" (disponibile pubblicamente) è propizio al concetto secondo il quale i dati resi pubblici sarebbero di conseguenza disponibili per qualsiasi uso. Si noterà che il principio di finalità, pilastro delle nostre legislazioni sulla protezione dei dati, s'adatta male all'aggettivo "disponibile". Il principio della lealtà della raccolta, inoltre, garantito soprattutto dall'esigenza di sicurezza dei trattamenti, potrebbe essere danneggiato per il fatto che un dato venga reso pubblico senza riflessioni né precauzioni. Per questo motivo l'espressione "publicly available" andrebbe allontanata a vantaggio di un'altra formulazione più adeguata e scevra di ambiguità (ad esempio « publicly accessible »).

In secondo luogo la domanda n 7 ("le considerazioni relative al rispetto della vita privata meritano un'attenzione particolare per quanto riguarda lo sfruttamento dell'informazione del settore pubblico?", pagina 17) potrebbe far pensare che il richiamo delle disposizioni dettate dalla direttiva 95/46/CE non porta a precise e salde conclusioni al riguardo, allorché si precisa (punto 111) che la direttiva 95/46/CE "realizza l'equilibrio necessario tra il principio dell'accesso all'informazione del settore pubblico e la protezione dei dati personali". Occorre eliminare tali ambiguità.

In tale contesto il presente parere ha per obiettivo nutrire la riflessione sulla dimensione della protezione dei dati personali, che è essenziale quando ci s'impegna ad agevolare l'accesso ai dati del settore pubblico dal momento che questi riguardano le persone fisiche. Non ha tuttavia la pretesa di fornire tutte le risposte alle domande sollevate dalla conciliazione tra l'obiettivo di agevolare l'accesso ai dati del settore pubblico, fondata sulla volontà di rafforzare la trasparenza degli Stati nei riguardi del cittadino, e la protezione dei dati personali così com'è definita dalla direttiva europea 95/46/CE.

Tale parere non tratterà quindi interrogativi sollevati dal libro verde che sembrano superare la messa a disposizione di terzi dell'informazione del settore pubblico, come ad esempio il punto di vista espresso al punto 56 (II ; 2, pagina 10) secondo cui « l'impiego delle nuove tecnologie può accrescere in modo considerevole l'efficacia della raccolta d'informazione. Esso offre agli organismi pubblici la possibilità di condividere l'informazione disponibile, quando conforme alle norme sulla protezione dei dati ».

Lo scopo è di fornire, sulla base della direttiva 95/46/CE e di esperienze concrete a fini pedagogici nel campo dei registri più conosciuti dei dati a carattere personale resi pubblici, un primo insieme di punti di riferimento che occorre prendere in considerazione all'atto di adozione di decisioni concrete. Questi punti di riferimento e esempi concreti provenienti da diversi Stati membri sono destinati ad illustrare come, nella società dell'informazione, devono essere prese in considerazione le norme di protezione dei dati in relazione a quelli derivati da registri pubblici, nonché alcune misure d'ordine tecnico o organizzativo che possono contribuire (senza tuttavia pretendere di garantire una tutela senza difetti) a conciliare la pubblicità di questi dati e il rispetto delle disposizioni di protezione dei dati a carattere personale e in particolare quelle relative al principio fondamentale in materia, ossia il principio della finalità per la quale i dati vengono, nel nostro caso, resi pubblici.

(I) Le norme di protezione dei dati si applicano ai dati a carattere personale resi pubblici

L'accessibilità delle informazioni che dipendono dal settore pubblico, in particolare mediante informatizzazione, raccomandata dal libro verde, pone il problema di sapere in quali modi verranno utilizzate le informazioni. Il loro utilizzo non può essere vietato, perché ciò è in contrasto con l'evoluzione delle nostre società. Non è quello il senso delle nostre legislazioni di protezione dei dati, che si fanno garanti della tutela dell'informatizzazione della società, e non del suo divieto.

D'altra parte, l'applicabilità delle nostre leggi di protezione dei dati ai dati personali resi pubblici, è soltanto l'espressione di un elemento che deriva dai testi stessi sulla protezione dei dati: un dato a carattere personale, anche reso pubblico, resta un dato a carattere personale e merita, di conseguenza, la dovuta protezione.

Questa dichiarazione implica necessariamente una definizione della protezione che viene offerta al dato a carattere personale reso pubblico. A tale riguardo, la direttiva 95/46/CE fornisce fin d'ora alcune risposte.

A. La direttiva 95/46/CE relativa alla protezione delle persone fisiche in relazione all'elaborazione dei dati a carattere personale e alla libera circolazione di questi dati

La direttiva permette di prendere in considerazione, nell'attuazione delle norme previste, il principio del diritto d'accesso del pubblico ai documenti amministrativi⁷⁰ ed anche altri elementi pertinenti⁷¹.

In tal modo, il principio della finalità esige che i dati a carattere personale siano raccolti per finalità determinate, esplicite e legittime, e non possono essere successivamente trattati in modo incompatibile con tali finalità⁷². Questo principio svolge un ruolo fondamentale per l'accesso dei dati a carattere personale detenuti dal settore pubblico.

Occorre in particolare determinare caso per caso in quale misura una legge esige o autorizza la pubblicazione o l'accesso da parte del pubblico a dati a carattere personale: si tratta forse di un'accessibilità integrale e illimitata nel tempo, di un utilizzo dei questi dati a qualsiasi fine, indipendentemente dalla finalità iniziale, o, al contrario, di un'accessibilità soltanto parziale e/o di un utilizzo vincolato alle finalità per le quali i dati sono stati resi pubblici? Di conseguenza, non esiste un'unica categoria di dati a carattere personale destinati a essere resi pubblici, e che dovrebbero essere trattati uniformemente dal punto di vista della protezione, ma occorre piuttosto procedere ad una analisi per gradi dei diritti dell'individuo interessato e, rispettivamente, dei diritti di accesso del pubblico. Benché l'accesso ai dati possa essere pubblico, esso può essere sottoposto ad una serie di condizioni (come la dimostrazione di un interesse legittimo) mentre lo sfruttamento dei dati, ad esempio a fini commerciali o da parte dei mass media, può essere limitato. Gli esempi che seguono illustrano questi interrogativi.

È poi utile ricordare che, indipendentemente dalla pubblicazione o meno dei dati a carattere personale, l'interessato ha sempre il diritto di accedere ai dati che lo riguardano, e il diritto di esigere, se necessario, la correzione o cancellazione di dati la cui gestione non è conforme alla direttiva, in particolare a causa di un loro possibile carattere incompleto o inesatto⁷³.

Indubbiamente, diverse disposizioni della direttiva fanno esplicitamente riferimento al carattere pubblico dei dati. Due di queste disposizioni meritano di essere citate con tutte le sfumature.

L'articolo 18.3, che impone un obbligo di notificazione all'autorità di controllo per quanto riguarda i trattamenti a cui vengono sottoposti i dati, permette di fare eccezione a quest'obbligo per la compilazione di registri "i quali, in forza di disposizioni legislative o regolamentari (... siano) predisposti per l'informazione del pubblico e siano aperti alla consultazione del pubblico". Ma i considerando 50 e 51 della direttiva precisano che queste deroghe o semplificazioni si applicano soltanto ai trattamenti il cui scopo (prima condizione) è di mantenere un registro destinato, nel rispetto del diritto nazionale, all'informazione del pubblico (2a condizione) e che sia aperto alla consulta-

⁷⁰ Vedi considerando 72. Occorre notare che la direttiva non contiene definizioni del termine "documenti amministrativi", ma che tale termine può essere inteso in senso ampio che permette di coprire almeno le "informazioni amministrative" previste dal libro verde nella proposta di classificazione (punto 73 e seguente, pagina 12).

⁷¹ Vedi l'articolo 10 e il considerando 37 della direttiva 95/46/CE sulla conciliazione del diritto alla vita privata con le norme che disciplinano la libertà d'espressione. Vedi anche la raccomandazione 1/97 del Gruppo su "Legislazione sulla protezione dei dati e mass media", adottata il 25.2.1997 (documento 5012/9, disponibile nelle 11 lingue ufficiali all'indirizzo indicato in nota alla pagina 2).

⁷² Vedi in particolare l'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/EC.

⁷³ Vedi articolo 12 della direttiva 95/46/EC.

zione del pubblico o di chiunque possa dimostrare un interesse legittimo (3a condizione), per cui tali deroghe non dispensano il responsabile del trattamento da alcuno degli altri obblighi che derivano dalla direttiva.

Infine, l'articolo 26.1. f consente una deroga all'esigenza di un livello adeguato di protezione per i dati che sono oggetto di un trasferimento verso paesi terzi quando il trasferimento dei dati stessi verso un paese che non offre lo stesso livello di garanzia è realizzato "a partire da un registro aperto alla consultazione del pubblico". Tuttavia, il considerando 58 della direttiva limita la portata del trasferimento precisando che non deve riguardare la totalità dei dati né intere categorie di dati contenuti nel registro, e che, eventualmente, il trasferimento deve essere effettuato soltanto su richiesta di persone che hanno un interesse legittimo in proposito.

Ma deriva chiaramente da queste disposizioni e precisazioni che se la protezione dei dati a carattere personale non deve ostacolare il diritto dei cittadini di avere accesso ai documenti amministrativi alle condizioni previste da ogni legislazione nazionale, la direttiva non ha inteso privare i dati accessibili al pubblico di qualsiasi protezione.

La discussione sul problema di sapere se c'è bisogno di armonizzare le norme nazionali sull'accesso all'informazione del settore pubblico deve comunque tenere conto delle norme armonizzate sulla protezione dei dati a carattere nazionale, come pure delle misure nazionali che le recepiscono.

Oltre alla missione della Commissione di vigilare sull'applicazione della direttiva, spetta inoltre al Gruppo Istituito dall'articolo 29 della direttiva di apprezzare concretamente la portata delle disposizioni nazionali adottate in applicazione della direttiva stessa nei casi precisi in cui potrebbero risultare divergenze sul piano nazionale.⁷¹

B. Esempi di conciliazione delle norme sulla protezione dei dati personali e sull'accesso alle informazioni del settore pubblico

Alcune legislazioni subordinano la diffusione di informazioni detenute dal settore pubblico a talune finalità che possono comportare un divieto d'accesso ad alcuni dati, il divieto di alcune utilizzazioni, o comunque particolari condizioni di accesso.

Ma la digitalizzazione delle informazioni e le possibilità di ricerca a testo integrale possono moltiplicare all'infinito le possibilità d'interrogazione e di selezione, mentre la diffusione di Internet aumenta i rischi di cattura e deviazione dei dati. Inoltre, la combinazione di dati del settore pubblico di provenienza diversa, una volta pubblicati, è grandemente facilitata dalla digitalizzazione dei dati stessi, e permette, in particolare, la creazione di profili sulle condizioni di vita o il comportamento degli individui⁷². Inoltre, occorre prestare un'attenzione particolare al fatto che, mettendo i dati a carattere personale a disposizione del pubblico, si alimentano in vasta misura le nuove tecniche di "data warehousing" e di "data mining". Questi metodi permettono di raccogliere dati senza alcuna indicazione preliminare delle relative finalità, che vengono definite soltanto alla fase di sfruttamento. Di conseguenza, occorre tenere attentamente conto di tutto ciò che è tecnicamente possibile fare con i dati⁷³.

È per questo che occorre verificare, caso per caso, quali potrebbero essere le ripercussioni negative sull'individuo prima di qualsiasi decisione di diffusione su supporto numerico. A seconda dei casi, occorre o decidere di non diffondere taluni dati a carattere personale, oppure sottoporre la diffusione alla decisione dell'interessato, o ad altre condizioni.

⁷¹ Vedi gli articoli 29 e 30 della direttiva 95/46/CE.

⁷² Si noti che l'utilizzazione di queste tecnologie permette anche allo Stato di elaborare siffatti profili.

⁷³ Altro esempio: grazie al controllo elettronico di due banche dati, si possono ottenere più facilmente informazioni negative su questa o quella persona, ad esempio: il vaglio del registro della popolazione (quando esiste) e degli elenchi elettorali permette di identificare le persone che non hanno diritto di voto.

Le basi dati derivanti da decisioni dell'autorità giudiziaria:

Il punto 74 del libro verde (pagina 11) che fa riferimento alle sentenze dei tribunali, per illustrare il concetto d'informazione fondamentale al funzionamento della democrazia, solleva un interrogativo di fondo. Infatti, è lecito ritenere che tutte le sentenze di tutte le giurisdizioni possano essere disponibili su Internet senza recare pregiudizio alle persone.

Strumento di documentazione giuridica, le basi dati sulla giurisprudenza possono diventare, in mancanza di precauzioni particolari, schedari informativi sui cittadini se vengono consultate non per conoscere la giurisprudenza ma ad esempio per identificare tutte le procedure giudiziarie che si riferiscono ad una stessa persona.

La Commissione per la Protezione della Vita Privata (Belgio), in un parere del 23 dicembre 1997, lo ha sottolineato con forza: "l'evoluzione tecnologica deve accompagnarsi ad una maggiore prudenza quando si tratta di identificare le parti nelle cronache giudiziarie". Essa propone che, in mancanza di una completa anonimità, le decisioni giudiziarie accessibili al pubblico non siano indicizzate in base al nome delle parti, per impedire eventuali ricerche sulla base di questo criterio.

La Commissione per la protezione dei dati personali italiana⁷⁷ ha intenzione di proporre a livello nazionale che le parti dispongano di un diritto d'opposizione alla pubblicazione del loro nome nelle basi dati della giurisprudenza. Questo diritto dovrebbe essere esercitabile in qualsiasi momento, e dovrebbe essere tenuto presente in occasione dell'aggiornamento delle basi dati diffuse su supporto magnetico. L'esercizio di questo diritto non avrebbe effetto retroattivo sulle pubblicazioni su carta.

In Francia, il ministero della giustizia, che desidera diffondere le basi dati della giurisprudenza su Internet, ha imposto, nel relativo capitolato d'oneri, l'anonimità delle decisioni.

Alcuni testi ufficiali:

La diffusione di informazioni su Internet implica una massa enorme di informazioni su scala mondiale, ed una moltiplicazione delle relative fonti. Questo cambiamento di scala geografica può comportare un rischio particolare. Infatti, è possibile che la diffusione di un'informazione legittimamente pubblica in un determinato paese possa causare, a livello mondiale, danni gravi alla vita privata o all'integrità fisica delle persone. Ciò avviene quando, ad esempio, le decisioni in materia di naturalizzazione (cittadinanza) sono oggetto di pubblicazione ufficiale obbligatoria. Tale è il caso della Francia, dove, secondo il parere della Commissione Nazionale dell'Informatica e delle Libertà (CNIL), il Governo francese, in occasione della pubblicazione su Internet della Gazzetta Ufficiale, ha escluso questo tipo di testi per evitare ad alcuni cittadini che hanno abbandonato la nazionalità d'origine il rischio di incorrere in eventuali rappresaglie.

Così, in alcuni casi, la volontà di trasparenza di uno Stato, ed in particolare dei suoi cittadini, può adattarsi male alla diffusione planetaria delle informazioni.

Altri esempi di diffusione di dati personali resi pubblici e sottoposti a condizioni miranti a proteggere gli interessati:

Le condizioni d'accesso ai dati a carattere personale contenuti nei registri possono essere molto varie, a seconda della regolamentazione: ad esempio, accesso parziale ai dati del registro, necessità di dimostrare un interesse legittimo, o divieto di impieghi commerciali.

Così, in Germania, gli elenchi dei candidati alle elezioni federali devono comportare cognome, nome, professione, giorno e luogo di nascita e indirizzo. Tuttavia, sugli elenchi resi pubblici prima dello voto dal responsabile locale o del Land incaricato dello svolgimento delle elezioni federali, il giorno di nascita è sostituito dall'anno di nascita.

In Italia, la legislazione relativa al registro della popolazione, tenuto da ogni municipio, prevede il divieto della comunicazione dei dati agli enti privi e l'obbligo di qualsiasi amministrazione che chiede la comunicazione dei dati stessi di dimostrare un congruo interesse pubblico.

⁷⁷ Garante per la protezione dei dati personali

In Francia, le liste elettorali sono pubbliche a fini del controllo della regolarità. La legge ne permette l'utilizzazione a fini politici da parte di tutti i candidati e tutti i partiti, ma ne proibisce l'impiego commerciale. Non sarebbe concepibile, in queste condizioni, che gli elenchi elettorali possano essere diffusi su Internet.

Inoltre in Francia, i dati a carattere personale contenuti nel catasto sono pubblici, ma è vietato farne un impiego commerciale.

In Grecia, il presente sistema del catasto organizzato in base ad un registro alfabetico dei proprietari di beni immobiliari sarà sostituito da un registro basato sull'identificazione dei beni immobili per impedire che le ricerche riguardino l'insieme dei beni immobiliari che appartengono ad una stessa persona. L'accesso al catasto è sottoposto alla dimostrazione di un interesse legittimo.

(II) Le nuove tecnologie possono contribuire a conciliare la protezione dei dati personali e la loro pubblicazione

Le nuove tecnologie, e talune misure amministrative di accompagnamento, pur favorendo l'accesso ai dati pubblici, in particolare con la "messa on-line", sono anche in grado di facilitare il rispetto dei principi principali di protezione dei dati, come il principio della finalità, quello dell'informazione e del diritto di opposizione, e quello della sicurezza. Tuttavia, l'utilizzazione di queste tecnologie non presenta una garanzia assoluta contro il rischio di abusi e di deviazioni dai principi di protezione dei dati personali che abbiamo descritto.

A Le condizioni tecniche d'accesso alle informazioni provenienti dal settore pubblico devono contribuire al rispetto del principio di finalità

Tenuto conto delle condizioni d'accessibilità numerica del pubblico, è certamente molto difficile garantire nella pratica la specificazione della finalità, ma un ricorso ragionato e determinato alla tecnica deve contribuire a raggiungere quest'obiettivo. Occorre per ciò verificare e definire in ogni caso le condizioni di interrogazione. A tale riguardo, si dovrebbe applicare il principio seguente: "chiunque può leggere qualsiasi dato, preso singolarmente, nella misura autorizzata, ma non tutti i dati nel loro insieme". La scelta dei criteri di ricerca deve escludere ogni possibilità di abuso in situazioni normali. Occorre inoltre verificare se non è possibile aggirare l'ostacolo ottenendo informazioni complementari presso altre fonti.

È per questo che la consultazione on-line di banche dati può essere oggetto di restrizioni tali da impedire la deviazione dalle finalità per le quali i dati vengono resi pubblici. Queste misure, da definire caso per caso, possono consistere, ad esempio, nel limitare il campo o i criteri d'interrogazione.

Così, in Francia, gli estratti dell'atto di nascita sono accessibili a chiunque dispone dell'identità, della data e del luogo di nascita di una persona. La CNIL ha subordinato la consultazione on-line di questi estratti alla condizione che la relativa richiesta elettronica comporti tutte queste informazioni. In tal modo, utilizzando gli opportuni criteri restrittivi per l'interrogazione delle basi dati, la raccolta su vasta scala di queste informazioni a scopi di utilizzo commerciale può essere evitata, e la finalità dell'accesso rispettata.

In Francia, allo stesso modo, l'elenco telefonico pubblicato su supporto telematico poteva essere interrogato a partire dalle prime lettere del cognome, il che ne rendeva più facile la teletrasmissione e l'utilizzo commerciale contro la volontà di alcuni abbonati che si erano opposti a tale impiego. Ma il blocco su Minitel e Internet di questo tipo d'interrogazione ha permesso di evitare eventuali deviazioni di finalità con questo mezzo.

Nei Paesi Bassi, i CD-Rom destinati alla diffusione dell'elenco del telefono sono stati concepiti in modo da impedire il reperimento del nome e dell'indirizzo di una persona a partire dal relativo numero di telefono (non è possibile l'interrogazione della base dati esclusivamente sul campo costituito dal numero di telefono).

Inoltre le basi dati relative ai registri delle imprese non possono essere interrogate in base al nome di una persona, il che potrebbe permettere una ricerca del complesso di imprese nelle quali una stessa persona è presente.

B Promuovere il ricorso ai mezzi tecnici che tendono ad impedire la cattura automatizzata dei dati accessibili on-line

Si può citare il protocollo di esclusione dei motori di ricerca (Robots Exclusion Protocol) che permette di evitare l'indicizzazione automatica totale o parziale delle pagine di un sito. In ogni caso, questi metodi possono essere efficaci soltanto se i progettisti dei siti e i navigatori internet sono informati della loro esistenza, e se i motori di ricerca li rispettano. Alcune società che producono motori di ricerca dichiarano di rispettare questo protocollo.

(III) Utilizzazione commerciale

I dati a carattere personale detenuti dal settore pubblico sono stati inizialmente raccolti ed elaborati con finalità precise, e, normalmente, in base ad una regolamentazione. A volte la raccolta era obbligatoria, a volte una condizione per accedere ad un servizio pubblico. Il cittadino, pertanto, non si aspetta che i dati che lo riguardano siano resi pubblici e utilizzati a fini commerciali. È per questo che, fra l'altro, alcune legislazioni nazionali permettono l'accesso pur proibendo l'utilizzo commerciale delle informazioni del settore pubblico, compresi i dati a carattere personale⁷⁹.

Dal punto di vista della direttiva 95/46/CE⁸⁰, si pone il problema di sapere se l'utilizzo commerciale deve essere considerato come finalità incompatibile con quella per cui i dati sono stati raccolti inizialmente, e, in caso affermativo, a quali condizioni potrebbe essere consentito un tale utilizzo.

Se la pubblicazione e la commercializzazione delle informazioni derivanti dal settore pubblico sono ammesse⁸¹, occorre rispettare alcune regole, e quindi porsi il problema, caso per caso, di come conciliare effettivamente il rispetto della vita privata con gli interessi commerciali degli operatori.

La direttiva 95/46/CE riconosce il diritto degli interessati di essere informati sul trattamento dei relativi dati, ed anche un diritto di opporsi a trattamenti sia pure legittimi. Le persone devono dunque essere informate della finalità di commercializzazione, e potere opporsi a tale utilizzo con mezzi semplici e efficaci⁸².

Su questo punto, c'è ancora molto da fare. La molteplicità delle fonti di diffusione dei dati, il grande numero di operatori, la possibilità di teletrasmissione, tutto ciò concorre a sostenere l'idea di uno sportello unico per la protezione dei dati, affinché i cittadini non siano costretti a molteplici azioni presso tutti gli operatori. È il caso, in molti paesi, degli elenchi degli abbonati al telefono.

Per la stessa ragione, la CNIL⁸³ ha raccomandato agli editori di guide di identificare su tutti i relativi supporti (carta, CD-ROM, Minitel o Internet) gli abbonati che hanno esercitato il diritto di opporsi all'utilizzazione dei loro dati a fini commerciali.

Questa idea dello sportello unico sembra essenziale, tanto per il rispetto dei diritti delle persone che per gli operatori commerciali che desiderano utilizzare dati a carattere personale.

La conciliazione del diritto alla vita privata e degli interessi commerciali degli operatori potrebbe anche portare al fatto che il consenso dell'interessato⁸⁴, e persino provvedimenti legislativi o normativi, siano necessari, come illustrato dall'esempio seguente:

In un parere relativo alla commercializzazione dei dati derivanti dalle licenze edilizie, la Commissione belga per la protezione della vita privata ha ritenuto che una diversa finalità (cioè la

⁷⁹ Vedi allegato 1 del libro verde : Situazione attuale negli Stati membri per quanto riguarda la legislazione e le politiche relative all'accesso all'informazione proveniente dal settore pubblico, p. 21 e seguenti.

⁸⁰ Vedi articolo 6 paragrafo 1 b della direttiva 95/46/CE.

⁸¹ Merita sottolineare che, secondo alcuni, siccome la riunione di dati diversi permette di elaborare profili personali, si deve proibire l'utilizzazione commerciale dei dati a carattere personale, o almeno limitarla, con opportune penali in caso di infrazioni. Per quanto riguarda i dati a carattere personale ricavati da fonti ufficiali, non dovrebbero sussistere eccezioni all'obbligo di informare l'interessato (articolo 11 della direttiva).

⁸² Vedi articoli 10, 11 e 14 della direttiva 95/46/CE.

⁸³ Commissione Nazionale dell'Informatica e delle Libertà, Francia.

⁸⁴ Vedi i articoli 2 h), 7a e 8 della direttiva 95/46/CE concernenti la definizione di "consenso" nonché l'esigenza di forme specifiche del consenso a seconda dei casi.

commercializzazione dei trattamenti effettuati delle autorità pubbliche) per essere consentita, debba essere legittimata da una base normativa o giuridica che definisca in modo sufficientemente preciso questa nuova finalità. In mancanza di tale legittimazione, la Commissione ha ritenuto che l'interesse costituito dalla comunicazione dei dati a terzi non prevalga sul diritto al rispetto della vita privata della persona i cui dati sono comunicati. Una terza possibilità consiste nel chiedere il permesso dell'interessato per la finalità di commercializzazione. Questo consenso deve essere dato esplicitamente e con cognizione di causa, tenendo conto del fatto che chi chiede una licenza edilizia è costretto a presentare una pratica che risponde a tutta una serie di prescrizioni.

Più oltre, nello stesso parere, la Commissione belga fa riferimento all'informazione degli interessati insistendo in particolare sull'esistenza di un diritto di opposizione automatico e gratuito, se i dati sono stati ottenuti a fini di marketing diretto.

Conclusione:

Il legislatore, quando auspica che un dato sia reso accessibile al pubblico, non intende però che esso diventi *res nullius*. Tale è la filosofia dell'insieme delle nostre legislazioni. Il carattere pubblico di un dato a carattere personale, che deriva da una regolamentazione o dalla volontà della persona interessata, non priva per ciò e definitivamente la persona della tutela che le garantisce la legge ai sensi dei principi fondamentali di tutela dell'identità umana.

Nel dibattito condotto nel quadro della consultazione sul libro verde, e nelle conclusioni che saranno ricavate, occorre dunque tenere conto in particolare degli aspetti e questioni seguenti per conciliare il rispetto del diritto alla vita privata e alla protezione dei dati a carattere personale dei cittadini con il diritto di accedere alle informazioni derivanti dal settore pubblico:

- valutazione caso per caso del problema di sapere se un dato a carattere personale può essere pubblicato/reso accessibile o meno, e, in caso affermativo, a quali condizioni e su quali supporti (digitali o meno, diffusione Internet, ecc.),
- principi di finalità e di legittimità,
- informazione degli interessati,
- diritto di opposizione degli interessati,
- utilizzazione delle nuove tecnologie per contribuire al rispetto del diritto alla vita privata.

Questi principi fondamentali si impongono non soltanto nelle situazioni nelle quali esiste una regolamentazione riguardante la pubblicazione o l'accesso, ma anche in quelle in cui non sembrano essere necessarie misure a carattere normativo per soddisfare la domanda di accedere alle informazioni provenienti dal settore pubblico, compresi i dati a carattere personale⁴⁴.

In attesa delle conclusioni che la Commissione europea potrà ricavare dalla consultazione in corso, il Gruppo esprime fin d'ora il massimo interesse a continuare a contribuire ai lavori previsti in proposito, nonché agli interrogativi che esulano, in senso stretto, dal quadro del libro verde per quanto riguarda la messa a disposizione di terzi delle informazioni provenienti dal settore pubblico⁴⁵.

Fatto a Bruxelles, addì 3 maggio 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

⁴⁴ Vedi nota in fondo a p. 2.

⁴⁵ Vedi ad esempio, sopra, le osservazioni concernenti il punto 56 (p. 9 del libro verde) sulla possibilità di raccolta e di distribuzione di informazioni, come pure il punto 123 (p. 19) sulle proposte d'azione per lo scambio di informazioni fra entità del settore pubblico.

6.3.5. Trasferimenti di dati verso Paesi terzi.**Parere 5/99 concernente il livello di tutela dei dati personali in Svizzera**

5054/99/def.

WP 22

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Parere 5/99 concernente il livello di tutela dei dati personali in Svizzera.

Adottato il 7 giugno 1999

**PARERE 5/99 CONCERNENTE IL LIVELLO DI TUTELA
DEI DATI PERSONALI IN SVIZZERA**

Il Gruppo* è stato informato dell'elaborazione da parte della Commissione europea di un progetto di decisione basata sull'art. 25, paragrafo 6, della direttiva 95/46/CE, che constata che la Svizzera, a motivo della sua legislazione interna, garantisce un livello di tutela adeguato ai sensi dell'art. 25, paragrafo 2, della direttiva suddetta.

Per fornire un parere alla Commissione europea, assistita dal Comitato istituito con l'art. 31 della direttiva 95/46/CE, il Gruppo ha effettuato un'analisi delle disposizioni di protezione dei dati applicabili in Svizzera⁷.

Al riguardo, occorre operare una distinzione tra la situazione legislativa vigente a livello federale - disciplinata dalla legge sulla tutela dei dati del 19 giugno 1992, successivamente modificata ed integrata dall'ordinanza del Consiglio federale del 14 giugno 1993- e la situazione esistente a livello cantonale.

Avuto riguardo alla ripartizione delle competenze tra la Confederazione e i Cantoni, la legge federale si applica ai trattamenti di dati personali effettuati nell'insieme del settore privato svizzero nonché ai trattamenti effettuati dalle autorità pubbliche federali; dal canto loro, le disposizioni cantonali disciplinano i trattamenti di dati personali operati dal settore pubblico cantonale o comunale. Per esempio, rientrano nelle competenze dei Cantoni i trattamenti operati nel settore della polizia, della scuola, della sanità e, più particolarmente, degli ospedali pubblici. In uno scrupolo di precisione va rilevato che anche i Cantoni sono indotti ad effettuare taluni trattamenti di dati personali in attuazione del diritto federale, per esempio per la riscossione delle imposte federali.

Prima di prevedere norme legislative federali e cantonali occorre rilevare in via preliminare che le norme federali e cantonali dovrebbero essere in armonia con le normative risultanti:

- da una parte, dalla Convenzione del Consiglio d'Europa per la tutela delle persone fisiche con riguardo al trattamento automatizzato dei dati personali (Convenzione n° 108), Convenzione ratificata dalla Svizzera il 2 ottobre 1997, e che, senza essere direttamente applicabile, stabilisce impegni internazionali a carico sia della federazione che dei Cantoni;
- d'altra parte, dalla Costituzione federale (modificata con voto popolare in data 18 aprile

* Istituito dall'art. 29 della 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, GU L 281 del 23 novembre 1995, pag. 31, disponibile al seguente indirizzo: <http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.htm>.

⁷ Nell'intento di disporre di informazioni maggiormente precise su taluni punti, il Presidente del Gruppo ha inviato una lettera al preposto federale per la tutela dei dati in data 15 marzo 1999. Quest'ultimo ha risposto in data 24 marzo 1999. Inoltre, il segretario del Gruppo ha stabilito contatti informali con il preposto federale.

scorso), nell'interpretazione data dalla giurisprudenza del Tribunale federale. Va rilevato che il nuovo testo costituzionale dà a chiunque il diritto al rispetto della sua vita privata e, in particolare, il diritto di essere tutelato contro l'utilizzazione abusiva dei dati che lo riguardano (art. 13 relativo alla tutela della sfera privata).

1. Secondo il parere del Gruppo, la legge federale sulla tutela dei dati garantisce un livello di tutela adeguato.

Nel documento di lavoro adottato il 24 luglio 1998 relativo ai trasferimenti di dati personali verso paesi terzi⁸, il Gruppo ha fornito delucidazioni sulle esigenze della direttiva ed enumerato gli elementi concreti che dovrebbero essere presi in considerazione ai fini della valutazione del livello di protezione consono. Alla luce di una tabella di corrispondenza tra le esigenze della direttiva e le disposizioni della legge federale⁹, emerge che la legge federale, che si applica ai trattamenti automatizzati di dati ed ai trattamenti manuali, prevede il complesso dei principi elencati nel documento di lavoro succitato, a prescindere dal fatto che si tratti dei principi della protezione delle persone o dei meccanismi volti a garantire un'effettiva applicazione dei principi di base.

È peraltro necessario formulare delle precisazioni inerenti al principio di trasparenza ed alla tutela dei dati sensibili.

Si rileverà che il principio di trasparenza è previsto espressamente per il caso particolare di raccolta sistematica di dati da parte di un organo federale. In generale, tuttavia, tale principio si evince dalla prassi di buona fede di cui all'art. 4, comma 2, della legge¹⁰.

La legge non contempla certamente il divieto del trattamento dei dati sensibili, ma pone disposizioni specifiche quanto al loro trattamento come d'altronde per i profili di personalità assoggettati alle stesse regole di tutela: l'art. 17 dispone che tali dati possano essere trattati da organi federali soltanto qualora la legge lo preveda espressamente o se eccezionalmente un compito definito in una legge lo esiga assolutamente, il Consiglio federale l'abbia autorizzato, la persona vi abbia acconsentito o abbia reso i dati accessibili a ciascuno. Per quanto riguarda il settore privato, l'art. 13, paragrafo 1, subordina il trattamento di qualsiasi dato al consenso da parte della persona, a un interesse pubblico o privato preponderante o a un'autorizzazione legale; l'art. 12 fa divieto di comunicare a terzi dati sensibili, salvo motivi giustificati. Infine, la protezione dei dati sensibili è corroborata dall'art. 35 della legge che prevede sanzioni penali nei riguardi di chiunque violi il dovere di discrezione rivelando tali dati illecitamente.

2. La situazione a livello cantonale è di difficile comprensione.¹¹

Alla luce dello studio condotto su richiesta dei servizi della Commissione¹² che verte più particolarmente sulla legislazione di vari Cantoni e delle indicazioni fornite dall'incaricato federale emergono i seguenti elementi di valutazione:

- le legislazioni adottate dai Cantoni si ispirano ampiamente alla convenzione 108, osservazione evidentemente coerente con gli impegni assunti dalla Svizzera in esito alla ratifica della convenzione;

⁸ Disponibile sul sito indicato in nota a piè di pagina n° 1.

⁹ Documento 5007/99, disponibile presso i servizi della Commissione europea, Direzione generale XV « Mercato interno e servizi finanziari », Unità E1 « Libera circolazione dell'informazione, protezione dei dati », Rue de la Loi 200, B - 1049 Bruxelles.

¹⁰ Siffatta interpretazione è stata confermata dal Preposto federale nei contatti informali con il segretariato del gruppo.

¹¹ Si rileva che, sui 26 Cantoni che conta la Confederazione:

- 17 dispongono di una legislazione in materia di protezione dei dati (...), tre dei quali hanno inoltre introdotto una disposizione di tutela dei dati nella rispettiva costituzione cantonale;
- 4 hanno adottato direttive governative, due dei quali hanno altresì introdotto una disposizione nella relativa costituzione cantonale; uno ha elaborato un progetto di legge;
- gli altri cantoni non presentano normative cantonali specifiche (tre di loro stanno mettendo a punto un progetto di legge).

¹² Disponibile presso i servizi della Commissione europea (cfr. indirizzo supra nota a piè pagina 4).

- i trattamenti di dati personali devono rispondere ai principi generali derivanti dalla giurisprudenza del tribunale federale relativa in particolare all'art. 4 della Costituzione federale (parità di trattamento) ed alla libertà personale che determina una norma minima in materia di tutela dei dati (segnatamente per quanto attiene i principi di qualità dei dati stessi - in particolare legalità, buona fede, finalità, proporzionalità o esattezza dei dati), il diritto d'accesso, il diritto di rettifica o di distruzione dei dati. E' probabile che tale giurisprudenza venga confermata, se non addirittura rafforzata sulla scorta del succitato testo costituzionale;
- quando non è assoggettato a disposizioni cantonali in materia di protezione dei dati, il trattamento di dati personali da parte di organi cantonali effettuato in esecuzione del diritto federale è disciplinato dalla legge federale. Inoltre, per detti trattamenti, i Cantoni devono dotarsi di un organo incaricato di vigilare sul rispetto della tutela dei dati e che fruisce delle stesse competenze dell'incaricato federale. È il caso in particolare dell'elaborazione dei dati a fini di sicurezza sociale, dei trattamenti di dati nei settori del diritto degli stranieri o dell'asilo, dell'imposta federale o della statistica;
- taluni trattamenti di dati sono soggetti a norme specifiche di riservatezza, come per esempio l'elaborazione di dati medici negli ospedali pubblici sottoposto a segreto medico.

Conclusione

Il Gruppo raccomanda alla Commissione e al comitato Istituito in virtù dell'art. 31 della direttiva 95/46/CE di constatare che la Svizzera garantisce un livello di tutela adeguato ai sensi dell'art. 25, paragrafo 6 di detta direttiva.

Fatto a Bruxelles, addì 7 giugno 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

**Parere 6/99 relativo al livello di protezione dei dati personali in Ungheria**

5070/IT/99/def.

WP 24

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Parere 6/99 relativo al livello di protezione dei dati personali in Ungheria

Adottato il 7 settembre 1999

**PARERE 6/99 RELATIVO AL LIVELLO DI PROTEZIONE
DEI DATI PERSONALI IN UNGHERIA**

Il Gruppo⁹⁾ è stato informato dell'elaborazione da parte della Commissione europea di un progetto di decisione basata sull'art. 25, paragrafo 6 della direttiva 95/46/CE, che constata che l'Ungheria garantisce, tramite la sua legislazione interna, un livello di protezione adeguato ai sensi dell'art. 25, paragrafo 2 di detta direttiva.

Per fornire un parere alla Commissione europea, assistita dal comitato istituito in virtù dell'articolo 31 della direttiva 95/46/CE, il Gruppo ha effettuato un'analisi delle disposizioni di protezione dei dati applicabili in Ungheria¹⁰⁾.

1. La situazione legislativa in materia di protezione dei dati personali è disciplinata dalla legge LXIII promulgata il 17 novembre 1992, entrata in vigore il 1° maggio 1993 e successivamente modificata¹¹⁾. Il campo d'applicazione di detta legge è più vasto della protezione dei dati personali dato che la legge stabilisce altresì il regime applicabile all'accesso del pubblico ai documenti amministrativi. Il difensore civico (Ombudsman), i cui poteri vengono fissati dalla legge e che è stato nominato dal Parlamento il 20 giugno 1995, è competente per il controllo dell'applicazione delle due normative.

In materia di tutela dei dati personali è altresì opportuno osservare quanto segue:

- gli impegni internazionali dell'Ungheria, derivanti dalla ratifica, in data 8 ottobre 1997, della convenzione del Consiglio d'Europa per la tutela delle persone fisiche con riguardo al trattamento automatizzato dei dati personali (convenzione n. 108),
- la tutela a livello costituzionale della vita privata, con particolare riguardo al trattamento dei dati personali¹²⁾,

⁹⁾ Istituito con l'art. 29 della 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, GU L 281 del 23 novembre 1995, pag. 31. Disponibile al seguente indirizzo: <http://www.europa.eu.int/comm/dg15/fr/media/dataprot/index.htm>.

¹⁰⁾ Nell'intento di ottenere informazioni più precise su taluni punti di è svolto uno scambio di corrispondenza tra il presidente del gruppo e l'Ombudsman ungherese (lettere del 22 marzo e del 19 aprile 1999 e risposte rispettivamente del 25 marzo e del 23 aprile 1999).

¹¹⁾ Cfr. da ultimo la legge n. LXXII del 22 giugno 1999 che introduce il concetto di "subfornitore" nella legislazione ungherese.

¹²⁾ La traduzione inglese effettuata dalle autorità ungheresi dell'articolo 59 della costituzione recita come segue : « (1) In the Republic of Hungary everyone is entitled to the protection of his or her reputation and to privacy of the home, of personal effects, particulars, papers, records and data, and to the privacy of personal affairs and secrets. (2) For the acceptance of the law on the protection of the security of personal data and records, the votes of two thirds of the MPs present are necessary. »

- l'esistenza di leggi settoriali che hanno ripreso disposizioni in materia di protezione dei dati personali in settori tanto disparati quanto i servizi segreti, le statistiche, la prospezione commerciale, la ricerca scientifica e, recentemente, il settore sanitario.

2. Secondo il parere del gruppo la legge ungherese sulla protezione dei dati garantisce un livello di tutela adeguato.

Nel suo documento di lavoro adottato il 24 luglio 1998 relativo ai trasferimenti di dati personali verso paesi terzi⁹⁷, il Gruppo ha spiegato le esigenze della direttiva ed elencato gli elementi concreti che dovrebbero essere presi in considerazione per la valutazione del livello di tutela adeguato.

Alla luce di una tabella di corrispondenza tra le esigenze della direttiva e le disposizioni della legge ungherese⁹⁸, emerge che la legge magiara, che si applica ai trattamenti automatizzati di dati ed ai trattamenti manuali⁹⁹, prevede l'insieme dei principi elencati nel documento di lavoro succitato, a prescindere dal fatto che si tratti dei principi della tutela delle persone fisiche o dei meccanismi volti a garantire un'applicazione effettiva dei principi di base.¹⁰⁰

Conclusione

Il Gruppo raccomanda alla Commissione e al Comitato Istituito in forza dell'articolo 31 della direttiva 95/46/EC di constatare che l'Ungheria garantisce un livello di tutela adeguato ai sensi dell'art. 25, paragrafo 6 di detta direttiva.

Fatto a Bruxelles, addì 7 settembre 1999

Per il Gruppo
Il presidente
Peter J. HUSTINX

⁹⁷ Disponibile sul sito indicato nella note in calce di pagina 1.

⁹⁸ Documento 5002/99, disponibile presso i servizi della Commissione europea, Direzione generale XV "Mercato interno e servizi finanziari", Unità E1 "Libera circolazione dell'informazione, protezione dei dati", Rue de la Loi 200, B - 1049 Bruxelles.

⁹⁹ È stato chiarito che la definizione del trattamento comprende la raccolta dei dati (« adatok felvétele » in ungherese).

¹⁰⁰ Dalle informazioni fornite dall'Ombudsman emerge in particolare quanto segue:

- l'appartenenza sindacale, benché non figuri nell'elenco dei dati sensibili di cui all'articolo 2, paragrafo 1 della legge, è considerata in pratica alla stregua di un dato sensibile a motivo delle opinioni politiche che rivela;
- l'Ombudsman dispone di poteri come quello di agire in giustizia o davanti alle autorità competenti quando constata un'infrazione penale o una mancanza disciplinare;
- secondo gli articoli 4 e 16 della legge deroghe ai diritti delle persone possono risultare soltanto da un atto legislativo. Al riguardo sono stati forniti i testi di legge relativi alla polizia (legge XXXIV del 1994), ai servizi competenti per la sicurezza nazionale ed al regime fiscale;
- in caso di raccolta di dati personali sulla base di uno schedario esistente, l'informazione delle persone interessate può essere garantita, in base all'articolo 6, secondo paragrafo, seconda frase della legge, dalla pubblicazione sulla Gazzetta ufficiale della Repubblica ungherese.

6.4 AUTORITÀ COMUNE DI CONTROLLO SCHENGEN

6.4.1. 3ª RELAZIONE DI ATTIVITÀ (Marzo 1998 – Febbraio 1999)

Indice

Nota di sintesi

Parte I: INTRODUZIONE

Parte II: UN ANNO DI ATTIVITÀ DELL'ACC

Capitolo I: PARERI E RACCOMANDAZIONI DELL'ACC

Capitolo II: ATTIVITÀ DI CONTROLLO

Capitolo III: CAMPAGNA DI INFORMAZIONE

Capitolo IV: INTEGRAZIONE NELL'UNIONE EUROPEA E ACQUIS DELL'ACC

Capitolo V: FUNZIONAMENTO DELL'ACC

Parte III: RELAZIONI DELL'ACC ALL'INTERNO E AL DI FUORI DELLA STRUTTURA SCHENGEN

Parte IV: REAZIONI DELLE AUTORITÀ SCHENGEN ALLA RELAZIONE ANNUALE DELL'ACC

Parte V: IL FUTURO DELL'ACC NEL NUOVO QUADRO ISTITUZIONALE

Parte VI: ALLEGATI

1. I compiti dell'ACC previsti dalla Convenzione
2. Pareri e raccomandazioni dell'ACC durante il periodo 1998-1999
3. Quadro dei pareri dell'ACC e reazioni degli organi esecutivi tecnici
4. Promemoria
Le Autorità comuni competenti per l'applicazione della Convenzione
Obiettivi e architettura del SIS
Uffici SIRENE
Protezione dei dati personali
5. Organigramma dei gruppi di lavoro Schengen
6. Dichiarazione universale dei Diritti dell'uomo
7. Elenco dei pareri, decisioni e raccomandazioni nella prospettiva dell'integrazione nell'Unione europea

8. Regolamento interno dell'ACC
9. Principi generali applicabili alle visite e ai controlli del C.SIS
10. Elenco dei membri dell'ACC
11. Segnalazioni nel SIS
12. Indice cronologico
13. Protocollo del Trattato di Amsterdam relativo a Schengen

DECLARATION OF THE JSA OBSERVER STATES

Having observer status in the JSA, the Nordic countries share the concerns of the full members as expressed in the annual report. They also share the main viewpoints expressed in the opinions referred. Among other things, it is of greatest importance that the advice and opinions given is observed and respected by the central as well as the national bodies in the Schengen system.

The presence of the Nordic national data and privacy protection commissions in the JSA is of utmost importance in the efforts aiming at ensuring common, public acceptance and support of the important work done in accordance with the Schengen Convention. The Nordic observers are of the opinion that the JSA need to have its resources strengthened in the future and hope that the integration in EU will enable this, without compromising the JSA status as an independent authority.

NOTA DI SINTESI

La presentazione della terza relazione annuale dell'Autorità di controllo comune di Schengen (marzo 1998 – febbraio 1999) coincide con un anno di trasformazione del quadro istituzionale dell'applicazione della Convenzione di Schengen, dovuta all'entrata in vigore del Trattato di Amsterdam.

Ciò implica nuove regole, nuovi diritti e maggiore trasparenza nella struttura organizzativa di Schengen e nel funzionamento del sistema d'informazione.

Sulla scia degli anni precedenti, il 1998 è stato un anno che ha visto affermarsi l'indipendenza dell'Autorità di controllo comune quale organo competente a tutelare i diritti dei cittadini nei confronti della Convenzione di applicazione dell'Accordo di Schengen, in particolar modo per quanto riguarda la protezione dei dati personali.

L'ACC ha lanciato una battaglia a tutto campo per la trasparenza e l'informazione dando ampia pubblicità alla sua relazione annuale, varando in diversi paesi la campagna "Il Sistema d'informazione Schengen vi riguarda", diffondendo un manifesto e opuscoli informativi sui diritti del cittadino, promuovendo il primo colloquio sui "Diritti dei cittadini nei confronti dei sistemi d'informazione di polizia" ed organizzando una conferenza stampa per la presentazione della relazione.

I garanti per la protezione dati nazionali hanno sottoposto la relazione annuale dell'ACC ai parlamenti nazionali e taluni l'hanno pubblicata nei rispettivi siti Internet. Tale relazione è stata presentata anche alla Autorità Schengen e trasmessa al Parlamento europeo.

L'ACC ha proposto nuovi meccanismi di interazione e cooperazione con gli organi esecutivi di Schengen, volti a snellire le procedure di informazione reciproca, e, per la prima volta, ha avuto modo di far valere il suo punto di vista in una riunione del Comitato esecutivo.

Le linee direttrici tracciate all'inizio dell'anno sono state rispettate: l'ACC ha emesso una serie di pareri, è stata informata sullo studio e sullo sviluppo tecnico del futuro sistema d'informazione, ha proceduto per la prima volta ad un'azione globale di controllo presso tutti gli uffici SIRENE formulando raccomandazioni in materia di rafforzamento della sicurezza nello scambio di

informazioni complementari, ha reso pubbliche le sue attività e diffuso informazioni sui diritti dei cittadini ed ha insistito e fatto tutto il possibile per l'efficacia del funzionamento di Schengen.

Nel quadro delle proprie attribuzioni, l'ACC ha inoltre deciso di procedere ad un controllo specifico del sistema centrale.

Malgrado le sue numerose iniziative e proposte, l'ACC non è riuscita a far adottare dal Comitato esecutivo le misure di rafforzamento delle risorse umane, tecniche e finanziarie promesse. Ai fini di un controllo democratico non basta l'esistenza formale di un'autorità indipendente: è altresì indispensabile che questa funzioni con mezzi e strumenti necessari. Ciò assume particolare rilevanza nel quadro dell'evoluzione dei sistemi d'informazione di polizia europei (Europol, Eurodac, Sistema d'informazione doganale) e del potenziamento delle misure di cooperazione nella lotta alla grande criminalità organizzata.

E' necessario a tal fine perfezionare i meccanismi di cooperazione tra le autorità di controllo, incaricate, per ognuno di questi sistemi, di tutelare i valori fondamentali della libertà e della cittadinanza. E' altresì fondamentale trovare, nel quadro dell'Unione europea, un equilibrio ottimale che consenta di mantenere un alto livello di sicurezza nel SIS e di assicurare un controllo indipendente ed efficace del sistema.

E' auspicabile che l'integrazione dell'Autorità di controllo comune nell'Unione europea avvenga in un modo armonioso, che garantisca un controllo continuo ed indipendente. L'esperienza e l'acquis dell'ACC sono necessari per il futuro dei sistemi di polizia europei.

In questo anno di profondi cambiamenti, ringrazio tutti coloro che hanno preso parte alle attività dell'Autorità di controllo comune, le autorità di controllo nazionali, i rappresentanti degli Stati in seno al Comitato esecutivo e al Gruppo centrale, i gruppi tecnici e il Segretariato Schengen per questi anni di lavoro comune.

Lavoro che valeva la pena realizzare per la costruzione europea, per la libertà, per i diritti della cittadinanza e per la sicurezza comune.

Marzo 1999

Il Presidente
João Labescat

Parte I
Introduzione

L'Autorità di controllo comune è stata istituita il 26 marzo 1995. Questi quattro anni di funzionamento continuo costituiscono la prima esperienza di un'entità indipendente di controllo comune di un sistema di polizia europeo. Le attività che sin dall'inizio l'ACC ha svolto in difesa dei cittadini assumono particolare rilevanza in quest'anno 1998, nel quale si celebra il 50° anniversario della Dichiarazione universale dei diritti dell'uomo.

Le attività dell'ACC hanno accompagnato le vicissitudini del funzionamento del sistema di informazione che contiene attualmente i dati di Germania, Austria, Belgio, Spagna, Francia, Grecia, Italia, Lussemburgo, Paesi Bassi e Portogallo. I compiti che gli Stati hanno affidato all'ACC sono stati assolti. Ne è la prova questo ultimo anno di attività.

Sin dal giugno 1992, una decisione ministeriale ha istituito un'autorità di controllo comune provvisoria (ACCP), organo che ha compiuto i primi passi nella preparazione dell'applicazione dei principi della protezione dei dati.

Scopo della Convenzione di applicazione dell'Accordo di Schengen è consentire l'abolizione dei controlli alle frontiere interne degli Stati membri al fine di creare un grande spazio di libera circolazione delle persone garantendo nel contempo, all'interno di tale spazio, un livello di sicurezza almeno pari a quello esistente in precedenza.

Tra le misure compensative previste dalla Convenzione per conseguire questo obiettivo figurano l'armonizzazione della politica dei visti, una politica comune in materia di determinazione dello Stato responsabile dell'esame di una domanda di asilo, il miglioramento della cooperazione di polizia e giudiziaria, l'intensificazione della lotta al traffico illecito di stupefacenti, l'armonizzazione del livello dei controlli alle frontiere esterne del territorio Schengen e la creazione di un sistema d'informazione Schengen (SIS).

Il sistema comune collega tutti i paesi che applicano la Convenzione di applicazione dell'Accordo di Schengen e consente ai suoi utenti (uffici con compiti di polizia, ambasciate e consolati, uffici stranieri, ecc.) di disporre in tempo reale delle informazioni necessarie all'esercizio dei loro compiti rispettivi inserite da un altro Stato che applica la Convenzione.

Tali informazioni riguardano le persone (ricercate per arresto estradizionale, non ammissibili nel territorio, scomparse o oggetto di una sorveglianza discreta) e gli oggetti (veicoli, armi, documenti, banconote rubate, sottratte o smarrite).

Il funzionamento del Sistema d'informazione Schengen presuppone obbligatoriamente la costituzione e il funzionamento di un'Autorità di controllo comune per la protezione dei dati personali (ACC), incaricata di vigilare, segnatamente, sul rispetto delle disposizioni della Convenzione relative all'unità di supporto tecnico del SIS (articolo 115). Questo organo, composto di due rappresentanti di ogni autorità di controllo nazionale delle Parti contraenti, si è visto inoltre attribuire un compito di consulenza ed armonizzazione delle prassi e delle dottrine nazionali.

Sono membri dell'ACC i rappresentanti delle autorità di controllo dei dieci Stati che partecipano al sistema. Le autorità di Danimarca, Finlandia, Islanda, Norvegia e Svezia partecipano alle attività dell'ACC con lo status di osservatori.

Nel 1998, in esecuzione del programma d'azione approvato, l'ACC ha incentrato le proprie attività sui seguenti settori:

- per la prima volta ha realizzato un controllo globale in tutti gli uffici SIRENE e formulato una serie di raccomandazioni volte al miglioramento della sicurezza;
- ha preparato il controllo specifico del sistema centrale che avrà luogo nel primo semestre del 1999;
- ha seguito le attività di sviluppo del SIS I+ e gli studi preliminari sul SIS II;
- ha definito un acquis comunitario nella prospettiva dell'integrazione di Schengen nell'Unione europea;
- ha lanciato la campagna "Il Sistema d'informazione Schengen vi riguarda" e distribuito poster e opuscoli informativi sui diritti del cittadino nei punti di ingresso dello spazio Schengen (aeroporti, frontiere marittime, ecc.);

- ha formulato pareri, in particolare sull'accesso ai dati del sistema Schengen da parte degli uffici della motorizzazione.
- ha promosso il primo colloquio sui "Diritti dei cittadini nei confronti dei sistemi di polizia" tenutosi a Lisbona;

E' stata preoccupazione costante dell'ACC garantire la trasparenza e l'informazione in merito alle proprie attività e ai diritti dei cittadini. Ha tentato inoltre di istituire un meccanismo agile di informazione reciproca tra le autorità di controllo nazionali e gli organi Schengen. A tal fine ha invitato più volte responsabili di vari gruppi di lavoro.

Il SIS conta attualmente circa nove milioni di dati, consultabili a partire da migliaia di terminali della polizia e delle autorità giudiziarie di dieci paesi dell'Unione europea. Nel 1998, l'integrazione di Austria, Italia e Grecia ha portato ad un aumento del volume di dati. Nel nuovo quadro istituzionale dell'Unione europea sarà necessario che il sistema d'informazione mantenga un alto livello di sicurezza in tutti i suoi componenti e di controllo indipendente.

Parte II

UN ANNO DI ATTIVITA' DELL'ACC

Capitolo I

PARERI E RACCOMANDAZIONI

Sicurezza degli uffici SIRENE : un'azione coordinata in tutti i paesi

Il 12 dicembre 1997, l'Autorità di controllo comune ha deciso di procedere ad una verifica delle misure di sicurezza adottate dagli uffici SIRENE. Tale decisione è stata adottata a seguito di una fuga di documenti e di informazioni prodottasi nel mese di novembre presso un ufficio SIRENE.

I garanti per la protezione dati dei 10 paesi che applicano la Convenzione hanno pertanto effettuato verifiche presso i rispettivi SIRENE.

In collaborazione con il garante belga, il 31 marzo 1998 il presidente dell'ACC ha inoltre preso parte ad una riunione con i responsabili del coordinamento dell'informazione di polizia dell'ufficio SIRENE belga. Nel quadro della riunione le autorità belghe hanno informato l'ACC in merito alle misure adottate e alle misure previste per migliorare la sicurezza.

Avvalendosi delle relazioni nazionali, l'ACC ha elaborato un documento di sintesi relativo alla sicurezza degli uffici SIRENE. Il ruolo dell'ACC in questo settore è risultato benefico per stimolare un'armonizzazione delle misure di sicurezza in ogni Stato.

L'ACC ha sottolineato che la rete inter-SIRENE deve soddisfare, in materia di sicurezza, tutti i requisiti imposti dall'articolo 118 della Convenzione di Schengen.

L'ACC ha proposto una serie di raccomandazioni. Tra queste:

- necessità di mantenere il più alto livello possibile di sicurezza fisica, garantendo, in particolare, che l'accesso ai dati sia limitato al solo personale autorizzato;
- cifratura dei dati in caso di scambio di informazioni e di archiviazione, definizione di norme comuni di sicurezza applicabili al personale dei SIRENE e designazione di un funzionario responsabile della sicurezza;
- promozione di azioni di formazione specifica sulla sicurezza dell'informazione destinate agli utenti del sistema;
- regolare elaborazione di relazioni sulla sicurezza da sottoporre ai rispettivi garanti per la protezione dati nazionali.

L'ACC ha posto l'accento sull'eccellente cooperazione prestata da tutte le autorità nazionali coinvolte ed ha manifestato la propria soddisfazione per il fatto che questa azione di controllo, coordinata in tutti i paesi, ha contribuito a migliorare significativamente la sicurezza delle informazioni, condizione indispensabile per garantire la fiducia del cittadino e delle istituzioni democratiche nel funzionamento del Sistema d'informazione Schengen.

Le raccomandazioni e la relazione di sintesi sono state approvate l'11 dicembre 1998. La sintesi è stata trasmessa l'8 gennaio 1999 al Comitato esecutivo, al Gruppo centrale e al gruppo di lavoro SIRENE. E' stato inoltre pubblicato un comunicato stampa che richiama brevemente il contenuto del documento di sintesi. L'ACC è ora in attesa della reazione degli organi esecutivi Schengen.

Parere sull'accesso ai dati SIS da parte degli uffici della motorizzazione

Il 16 giugno 1998, il Gruppo centrale ha trasmesso all'ACC una richiesta di parere formulata dal Gruppo di lavoro "SIRENE". Tale richiesta verteva sulle condizioni d'accesso degli uffici della motorizzazione ai dati SIS. Si pregava l'ACC di precisare la sua interpretazione del concetto di dato di natura personale. Secondo il gruppo SIRENE, il numero di telaio di un veicolo non rientra nella definizione di questo concetto.

La richiesta trae origine da un progetto teso ad autorizzare gli uffici della motorizzazione a consultare il SIS allo scopo di individuare veicoli rubati, immatricolati nello spazio Schengen, al momento di una nuova immatricolazione nel paese di prima immatricolazione o in un altro paese Schengen.

Nel suo parere, approvato il 6 novembre 1998, l'ACC constata che l'accesso ai dati SIS da parte degli uffici della motorizzazione e il raffronto di archivi costituirebbero in diversi Stati Schengen una violazione degli articoli 101, commi 2 e 4 e 102 della Convenzione di Schengen. L'ACC ritiene tuttavia che tale accesso sia ammissibile se gli uffici della motorizzazione soddisfino le condizioni di competenza e di finalità previste dalla Convenzione e siano in grado di applicare le misure di sicurezza di cui all'articolo 118.

Il parere è stato trasmesso al Gruppo centrale (parere 98/5).

Capitolo II

ATTIVITA' DI CONTROLLO

Principi generali relativi alle visite di controllo dell'ACC al C.SIS

L'ACC e il Ministero dell'Interno francese hanno elaborato in comune un insieme di principi destinati a chiarire le modalità delle visite di controllo presso l'impianto del sistema centrale (C.SIS). La definizione di questi principi si inquadra nei compiti previsti dall'articolo 115 della Convenzione.

Al termine di un lungo processo di consultazioni reciproche e dopo una riunione tenutasi a Parigi tra membri dell'ACC ed esponenti del Ministero dell'Interno francese, è stato possibile presentare una proposta concreta. Questa è stata esaminata il 29 giugno 1998 in presenza di rappresentanti del Ministero dell'Interno francese.

Poiché questi hanno a loro volta suggerito una serie di modifiche, l'ACC ha nuovamente discusso ed approvato il documento l'11 settembre 1998. Il 6 novembre, il Ministero dell'Interno francese ha a sua volta approvato il testo e lo ha sottoposto agli altri Stati Schengen per informazione.

Il documento "Principi generali applicabili alle visite e controlli presso il C.SIS" (in allegato) definisce i tipi di visite (di carattere generale o di controllo), i meccanismi di informazione del Ministero dell'Interno, la composizione dei gruppi di visita o di controllo, la definizione del programma di lavoro, il regime di accesso ai documenti, il sistema di valutazione delle relazioni tecniche e la garanzia della loro riservatezza.

Il testo definitivo mira a porre termine alle interpretazioni restrittive della funzione di controllo dell'ACC ed è conforme allo spirito di cooperazione che ha sempre caratterizzato le relazioni con il Ministero dell'Interno francese.

Il documento ha formato oggetto di una comunicazione al Gruppo centrale nel corso della riunione del 19 febbraio 1999.

Controllo del C.SIS

Nel corso del 1998 l'ACC ha preparato, di concerto con il Ministero dell'Interno francese, i principi applicabili alle visite e al controllo presso il C.SIS (v. sopra). Il periodo di tempo trascorso dopo l'ultimo controllo e l'integrazione di tre paesi (Austria, Grecia e Italia) rendeva necessaria la realizzazione di un nuovo controllo. L'ACC ha deciso a tal fine di istituire un gruppo di lavoro tecnico, coordinato dal rappresentante lussemburghese. Gli esperti si sono riuniti in diverse occasioni per preparare la visita di controllo che avrà luogo nel primo semestre del 1999. Il gruppo di lavoro ha elaborato una lista contenente gli elementi del C.SIS da sottoporre a controllo.

Gruppi tecnici ed esperti

Il 27 aprile 1998, i presidenti del Comitato di orientamento SIS e del PWP hanno presentato lo stato di avanzamento dei lavori relativi al rinnovo e al miglioramento del SIS (installazione della rete SIRENE fase II e preparazione del SIS I+ e del SIS II). In conformità di quanto stabilito nel corso della riunione, nel giugno 1998 l'ACC ha ricevuto una cospicua documentazione amministrativa e tecnica sulla rete SIRENE fase II ed un CD-Rom sul C.SIS I.

I membri dell'ACC hanno constatato con rammarico che, secondo il presidente del Comitato di orientamento SIS, al momento in cui l'Autorità di controllo comune ha chiesto di essere associata alle attività, non era più possibile modificare le specifiche tecniche per tener conto delle sue richieste. E' stato comunicato che queste verranno tuttavia prese in debita considerazione al momento della messa in servizio del sistema.

Sono stati inoltre informati del fatto che, per evitare ritardi ed un aumento dei costi, non è stata richiesta la certificazione di sicurezza dell'intero sistema SIS II. Sarà tuttavia possibile richiedere successivamente la certificazione di ogni singola componente del sistema.

Il 20 novembre 1998, esperti dell'ACC hanno preso parte ad una riunione informativa con esponenti di IBM ed esperti dei gruppi tecnici di Schengen interessati al SIS II. I periti di IBM hanno presentato le varie opzioni relative alla futura architettura del sistema e i criteri di valutazione. Gli esperti dell'ACC non hanno tuttavia ricevuto informazioni di carattere tecnico, informazioni sulla sicurezza né i motivi alla base della scelta di tre architetture tra le dodici presentate. Hanno potuto constatare che, alla data della presentazione, non era possibile prefigurare le scelte future ed hanno deplorato che IBM non avesse ancora potuto esaminare in modo approfondito gli aspetti legati alla sicurezza.

Sulla base del resoconto presentato dai propri esperti, l'ACC ha chiesto spiegazioni in merito ai motivi che hanno portato alla scelta delle tre architetture e la trasmissione di documentazione tecnica supplementare.

I coordinatori del progetto hanno risposto all'invito dell'ACC l'11 dicembre 1998, presentando una relazione orale sullo stato di avanzamento dello studio preliminare sul SIS II. Hanno riassunto le tappe preparatorie della procedura di aggiudicazione dello studio preliminare. Sono state date alle delegazioni informazioni dettagliate sul contenuto degli studi di IBM e sulle varie soluzioni prospettate. Per quanto riguarda l'usurpazione di identità, problema sollevato dall'ACC e oggetto di un parere, è stato annunciato che la soluzione sarà integrata nel SIS I+.

L'ACC attende ora di poter prendere conoscenza del capitolato d'oneri per conoscere i criteri che hanno portato alla scelta delle architetture prese in considerazione e i criteri di sicurezza. Dovrebbe essere presa una decisione sulla base dello studio che sarà disponibile il 22 dicembre 1998. Alla fine di febbraio 1999, questa informazione non era ancora giunta all'ACC.

Capitolo III CAMPAGNA D'INFORMAZIONE

Campagna d'informazione sui diritti dei cittadini nei confronti del SIS

Nel 1997, l'ACC aveva deciso di varare in tutti i paesi una campagna d'informazione destinata ai cittadini dal titolo "Il Sistema d'informazione Schengen vi riguarda". L'ACC ha infatti constatato un insufficiente esercizio dei diritti del cittadino e soprattutto del diritto di accesso e di verifica dei dati. Uno dei motivi di questo deficit è la mancanza di un'informazione diretta al pubblico.

Per tale motivo, nel programma di lavoro e nel bilancio dell'ACC è stata prevista la realizzazione di una campagna con un duplice obiettivo: da un lato, informare i cittadini in merito ai diritti loro riconosciuti dalla Convenzione di Schengen e, d'altro lato, contribuire ad una maggiore trasparenza e conoscenza di Schengen.

L'ACC ha realizzato manifesti ed opuscoli prevedendone la diffusione alle frontiere esterne di Schengen ad opera degli organi nazionali competenti. Il materiale informativo è stato presentato in occasione della sessione annuale di Lisbona, nel giugno 1998.

Per ragioni pratiche, le campagne d'informazione nazionali non sono state lanciate immediatamente. Sono state avviate tra il mese di dicembre 1998 e l'inizio del 1999 in taluni paesi (Spagna, Grecia, Germania, Portogallo e Austria). Si annuncia l'avvio di tali campagne in Belgio, Lussemburgo e Italia mentre nei Paesi Bassi si incontrano difficoltà legate al loro finanziamento. Per quanto riguarda l'autorità di controllo francese, si è vista rifiutare ogni collaborazione da parte delle autorità competenti.

Va ricordato che la campagna di informazione dell'ACC ha beneficiato del sostegno del Gruppo centrale, sia per quanto riguarda la stampa degli opuscoli che la loro distribuzione.

Pagina Internet dell'ACC

Mossa dalla stessa volontà di informare il cittadino sui suoi diritti, nel 1998 l'ACC ha deciso di creare una pagina Internet. Il cittadino vi troverà informazioni sui suoi diritti e sulle attività dell'ACC. Il sito dovrebbe essere ultimato nel corso del 1999.

Presentazione della relazione annuale alla conferenza stampa di Bruxelles e Sessione annuale

L'ACC ha presentato la propria relazione annuale nel quadro di una conferenza stampa tenutasi presso il Palais d'Egmont di Bruxelles il 28 aprile 1998. Erano presenti giornalisti di diverse agenzie di stampa internazionali e di due reti televisive. Era stata comunicata prima ai rappresentanti del Gruppo centrale.

La Sessione annuale dell'ACC si è tenuta a Lisbona il 29 e 30 giugno 1998. L'ACC mirava innanzi tutto a contribuire ad una maggiore trasparenza nel funzionamento del Sistema d'informazione Schengen, soprattutto sotto il profilo dei diritti del cittadino. In questa occasione, la relazione annuale dell'ACC è stata presentata alla stampa.

In collaborazione con il garante per la protezione dati portoghese, il 30 giugno l'ACC ha organizzato un colloquio sui "Diritti del cittadino nei confronti dei sistemi d'informazione di polizia - Il modello Schengen".

I relatori hanno posto l'accento sul ruolo dell'ACC, sull'integrazione di Schengen nell'Unione europea, sulla cooperazione tra Stati membri, sullo scambio di informazioni inter-SIRENE, sull'integrazione dei sistemi d'informazione di polizia, sulla protezione dei dati e su Europol e i sistemi d'informazione di polizia dell'Unione europea. Ha preso parte alla sessione di apertura il Segretario di Stato aggiunto del Ministero dell'Amministrazione interna portoghese, sig. Armando Vara. Oltre all'esponente del governo portoghese, sono intervenuti il presidente del Gruppo centrale, il Direttore generale GAI del Consiglio dell'Unione europea, il coordinatore aggiunto di Europol, il presidente del garante per la protezione dati portoghese e il presidente dell'ACC. Sono

inoltre intervenuti il Direttore generale della polizia giudiziaria portoghese, la coordinatrice dell'ufficio SIRENE Portogallo e il coordinatore portoghese per la libera circolazione delle persone nello spazio europeo. La sessione, aperta agli organi di stampa, ha beneficiato di una certa eco nei giornali e alla televisione ed i suoi atti sono stati pubblicati su Internet. Al colloquio hanno preso parte circa un centinaio di persone. Oltre alle alte personalità dello Stato portoghese (Provveditore alla Giustizia, Segretario di Stato per l'inserimento delle minoranze, Viceprocuratore generale della Repubblica, Ispettore generale dell'amministrazione interna, Comandanti generali della polizia), hanno assistito al colloquio anche i rappresentanti del Gruppo centrale di vari paesi ed esponenti del Ministero della Giustizia di Italia, Austria Norvegia e Svezia.

Il garante per la protezione dati portoghese ha pubblicato gli atti del colloquio in portoghese ed in inglese.

Capitolo IV

INTEGRAZIONE NELL'UNIONE EUROPEA E ACQUIS DELL'ACC

Su richiesta del Gruppo centrale, l'ACC ha elaborato l'elenco dell'acquis in previsione dell'integrazione dell'acquis di Schengen nell'Unione europea. Si tratta infatti di definire l'insieme delle decisioni adottate nel quadro di Schengen, che faranno parte dell'insieme delle regole che disciplinano il funzionamento dell'ACC.

L'elaborazione di tale elenco e la sua trasmissione diretta dell'ACC alle autorità europee sono state precedute il 14 febbraio da una riunione tra il presidente dell'ACC e il Direttore generale della direzione Giustizia e Affari interni (GAI) dell'Unione europea. L'elenco dei documenti che costituiscono l'acquis dell'ACC, esaminato nella riunione dell'ACC del 27 aprile 1998, è stato trasmesso al Consiglio dell'UE (Presidenza e DG GAI) il 18 maggio 1998. Copia del documento è stata inoltre comunicata al presidente del Gruppo centrale.

L'elenco contiene i pareri formulati e una serie di principi approvati che l'ACC considera costitutivi dell'acquis. Si tratta, in particolare, dei pareri emessi in occasione della verifica della corretta esecuzione delle disposizioni della Convenzione relative al SIS o in occasione dell'esame delle difficoltà di applicazione o di interpretazione che possono sorgere nella gestione del SIS, nonché di una serie di principi, approvati dagli organi Schengen, che sanciscono l'indipendenza dell'ACC. Tra gli atti costitutivi dell'acquis dell'ACC figura anche la relazione riservata elaborata a seguito della visita di controllo al C.SIS.

Per quanto riguarda la prevista integrazione del personale del Segretariato Schengen nell'Unione europea, l'Autorità di controllo comune si è pronunciata perché questo trasferimento avvenga in modo equilibrato e giusto. L'ACC ha sottolineato che in futuro sarà importante conservare il livello di conoscenze e di esperienza acquisito dal personale nel corso degli anni, conoscenze ed esperienza che l'ACC considera fondamentali per l'assolvimento dei suoi compiti.

In occasione della sua riunione dell'11 settembre 1998, l'ACC è stata informata del fatto che i suoi pareri e raccomandazioni non faranno parte dell'acquis Schengen in quanto tali ma potranno essere confermati mediante una successiva decisione. Alla fine di febbraio 1999, l'ACC non ha ancora ricevuto informazioni ufficiali.

Si sottolinea che, ai sensi del Protocollo Schengen allegato al Trattato di Amsterdam, le decisioni e dichiarazioni del Comitato esecutivo e gli atti adottati ai fini dell'applicazione della Convenzione da parte di autorità alle quali il Comitato esecutivo ha conferito potere decisionale, costituiscono acquis comunitario. Diverse di queste decisioni riguardano l'ACC, in particolare quelle che riconoscono la sua indipendenza, l'autonomia della sua linea di bilancio, i bilanci annuali e l'accesso alla documentazione e alle informazioni Schengen.

L'11 dicembre 1998, l'ACC ha approvato una nota relativa al suo acquis istituzionale e funzionale e l'ha trasmessa al Gruppo centrale e al Comitato esecutivo (con copia al Consiglio) affinché sia sottoposta all'esame del gruppo "Acquis Schengen" dell'UE all'inizio del 1999. L'ACC ha inoltre conferito al presidente il mandato di illustrare la portata di questa nota dinanzi al Comitato esecutivo. Come indicato in precedenza, il Comitato esecutivo del mese di dicembre 1998 ha affidato l'esame del documento al Gruppo centrale.

Capitolo V FUNZIONAMENTO DELL' ACC

Riunioni

L'ACC si è riunita sette volte in sessione plenaria tra marzo 1998 e marzo 1999. Sono state organizzate due riunioni di due giorni, una a Bruxelles e l'altra a Lisbona.

Sono state inoltre organizzate riunioni tecniche per preparare la visita di controllo al C.SIS e incontri tra gli esperti dell'ACC e i responsabili dell'elaborazione dello studio preliminare sul SIS II (Lisbona e Bruxelles).

Il presidente dell'ACC ha preso parte a riunioni del Gruppo centrale (Strasburgo e Ostenda) e del Comitato esecutivo (Berlino).

Elezioni del Presidente e del Vicepresidente

L'11 dicembre 1998, sono stati rieletti all'unanimità il Presidente (sig. João Labescat) e il Vicepresidente (sig. Bart De Schutter).

Bilancio dell'ACC e sostegno del Segretariato

La linea di bilancio specifica destinata all'ACC è un principio sancito da una decisione del Comitato esecutivo del 1997 e, in quanto tale, costituisce un acquis nella prospettiva dell'integrazione di Schengen nell'Unione europea.

In occasione della sua riunione del 27 aprile 1998, l'ACC ha approvato il progetto di bilancio. Questo prevedeva una voce supplementare relativa al rafforzamento del supporto amministrativo mediante l'assunzione di una persona a tempo pieno ed era improntato al rigore e al contenimento delle spese.

Il bilancio dell'Autorità di controllo comune e il sostegno da parte del Segretariato sono aspetti fondamentali per l'efficacia delle sue attività e per l'esercizio delle sue competenze. Gli organi esecutivi di Schengen hanno rifiutato di dotare l'ACC dei mezzi indispensabili al suo funzionamento indipendente¹.

In occasione della riunione di Lisbona del 29 giugno, l'ACC ha preso atto del fatto che la sua domanda di bilancio per il 1999 era stata trasmessa al gruppo di lavoro competente che l'aveva in seguito iscritta all'ordine del giorno del Gruppo centrale, consapevole delle conseguenze di un'eventuale integrazione del Segretariato Schengen nel Segretariato generale del Consiglio dell'UE nel corso del 1999. Il bilancio dell'ACC doveva, secondo l'ACC, essere approvato lasciando impregiudicate le conseguenze budgetarie dell'eventuale integrazione, vale a dire la necessità di prevedere la copertura delle spese attualmente imputate al bilancio generale.

Benché in occasione dell'incontro con la presidenza dell'ACC, la presidenza tedesca di Schengen si fosse impegnata a sostenere la richiesta, l'ACC ha preso conoscenza del fatto in dicembre 1998 che il Gruppo centrale aveva approvato il bilancio dell'ACC per il 1999 ma non l'assunzione di una persona supplementare per il supporto amministrativo. L'ACC ha quindi incaricato il

¹ Nel 1997, il bilancio dell'ACC (70.400,52 EURO) corrispondeva allo 0,011 % del bilancio globale del Segretariato Schengen (6.258.493,45 EURO).

Nel 1998, il bilancio del Segretariato ha conosciuto un aumento (6.753.336,77 EURO) e quello dell'ACC vi contribuiva a concorrenza dello 0,012 %.

Nel 1999, la proposta dell'ACC (137.580,91 EURO) corrispondeva allo 0,021 % del bilancio globale del Segretariato Schengen.

Il bilancio dell'ACC approvato corrisponde al primo semestre 1999 e ammonta a 43.381,37 EURO. La chiave di ripartizione è la seguente : Gruppo 1 (Germania, Grecia, Spagna, Francia, Italia, Austria e Portogallo) : 4.333,80 EURO ; Gruppo 2 (Belgio e Paesi Bassi) : 2.101,84 EURO + Lussemburgo 130,12 EURO ; Gruppo 3 (Danimarca, Norvegia, Finlandia e Svezia) : 2.166,91 EURO + Islanda 43,38 EURO.

suo presidente di partecipare alla riunione del Comitato esecutivo di Berlino, il 16 dicembre 1998, per difendere questa richiesta. Ha avuto modo di illustrare le ragioni che giustificano la richiesta di bilancio supplementare dell'ACC volto a rafforzare il sostegno amministrativo attualmente prestato dal Segretariato. Il presidente ha inoltre presentato una nota relativa al costo totale di funzionamento dell'ACC, facendo astrazione delle economie di scala di cui beneficiano le riunioni Schengen che si tengono sinora nell'edificio Benelux (acquis istituzionale e funzionale, v. sopra). Il Comitato esecutivo ha respinto la richiesta di bilancio supplementare.

Nonostante ammontasse a meno dell'1% del bilancio generale, la proposta è stata respinta. A ciò si aggiunge il fatto che, rispetto agli accordi presi nel 1997/1998 con la presidenza Schengen, il sostegno all'ACC da parte del Segretariato è diminuito. In un organico totale del Segretariato di circa 70 persone, l'ACC può contare su un unico amministratore (disponibile per appena 1/5 del suo tempo), responsabile contemporaneamente di altri gruppi di lavoro.

Nelle sue decisioni il Comitato esecutivo non ha tenuto conto delle competenze dell'ACC attribuite dalla Convenzione.

Preoccupata per tale assenza palese di sostegno degli organi esecutivi di Schengen, l'ACC continua a sostenere di dover disporre delle risorse umane, tecniche e finanziarie necessarie alle sue competenze, ora e nel futuro quadro istituzionale.

Regolamento interno

Il 27 aprile 1998, l'ACC ha proceduto alla revisione del proprio regolamento interno per iscriverci il principio dell'indipendenza del proprio bilancio. Il regolamento è stato integrato da un nuovo articolo 11 dal titolo "Bilancio" (v. doc. SCH/Aut-cont (95) 25, 6a rev.). Il testo consacra il principio approvato dal Comitato esecutivo dell'esistenza di una linea di bilancio autonoma la cui dotazione deve corrispondere all'attività annuale dell'ACC.

Parte III

RELAZIONI DELL'ACC ALL'INTERNO E AL DI FUORI DELLA STRUTTURA SCHENGEN

Relazioni con la Commissione delle libertà pubbliche del Parlamento europeo

Già nel 1997, il presidente in carica dell'ACC aveva proposto alla presidenza della Commissione delle libertà pubbliche del Parlamento europeo di presentare la sua relazione annuale. La proposta è stata reiterata nel 1998 ma è rimasta lettera morta. Una serie di esemplari della relazione annuale sono stati comunque inviati alla Commissione del Parlamento europeo.

Relazioni con il Gruppo centrale e il Comitato esecutivo

Una delegazione dell'ACC è stata invitata dalla presidenza Schengen ad una riunione del Gruppo centrale tenutasi a Strasburgo il 4 marzo 1998, a margine di una visita al C.SIS. Tale riunione ha consentito di prendere conoscenza dello stato di avanzamento dei lavori relativi al rinnovo del SIS e all'implementazione della rete SIRENE fase II.

In una lettera del 12 marzo 1998 (doc. SCH/Aut-cont-lettre (98) 4) il presidente dell'ACC ha ringraziato il presidente del Gruppo centrale dell'invito. Si trattava del primo incontro dell'ACC con il Gruppo centrale in sessione plenaria. L'incontro ha consentito all'ACC di far conoscere la sua posizione sul ruolo che questa intende svolgere nei confronti degli organi Schengen, soprattutto per quanto riguarda le prospettive future del SIS.

Il Gruppo centrale ha accettato di associare l'ACC alle attività sullo studio preliminare della rete SIRENE fase II e sul SIS I+. L'ACC potrà in tal modo accertarsi che il sistema futuro compren-

derà specifiche tecniche che consentiranno di esercitare i controlli previsti dalla Convenzione.

L'ACC ha confermato che avrebbe continuato, come in passato, a trasmettere i propri pareri e raccomandazioni alla presidenza del Gruppo centrale con tempestività dopo la loro approvazione. Anche i processi verbali, una volta approvati dall'ACC, saranno a disposizione del Gruppo centrale.

Dal canto loro, il Gruppo centrale e i gruppi tecnici provvederanno a mettere a disposizione il maggior numero di documenti possibile, elaborando in particolare una lista dei documenti tecnici approvati dai gruppi di lavoro suscettibili di interessare l'ACC.

Il 27 aprile 1998, l'ACC ha invitato la trioca del Gruppo centrale ma alla riunione ha preso parte solo il presidente.

Questi ha confermato l'importanza che attribuiva alle attività dell'ACC ed ha dichiarato di voler sostenere la campagna d'informazione destinata all'opinione pubblica. Ha dichiarato che avrebbe provveduto a far sì che i pareri e le raccomandazioni dell'ACC siano esaminati dai gruppi di lavoro competenti ed ha annunciato l'imminente trasmissione di una relazione di risposta ai pareri e raccomandazioni dell'autorità (in particolare quelli formulati a seguito del controllo del C.SIS nel 1996), già approvata dal Gruppo centrale il 20 aprile 1998. Il presidente del Gruppo centrale ha inoltre dichiarato che avrebbe appoggiato la richiesta dell'ACC di disporre di mezzi supplementari, richiesta che ha richiamato l'attenzione del Gruppo centrale e il cui esame è stato affidato al gruppo di esperti finanziari competente.

Su invito della presidenza del Gruppo centrale, il presidente dell'ACC ha partecipato al "Workshop SIS" organizzato ad Ostenda il 24 giugno 1998. Ha potuto così integrare le informazioni già fornite dal presidente del Comitato di orientamento SIS ai paesi PECO in merito alle esigenze della Convenzione in materia di dati di natura personale e all'esistenza di un'autorità di controllo nazionale indipendente.

Il presidente dell'ACC ha preso parte alla riunione del Comitato esecutivo di Berlino il 16 dicembre 1998. Ha avuto modo di presentare ai Ministri degli Stati Schengen una serie di documenti dell'ACC (richiesta di bilancio supplementare per beneficiare di un maggiore supporto amministrativo da parte del Segretariato e documento sull'acquis organizzativo dell'ACC). Come indicato in precedenza, la prima richiesta non è stata accolta mentre il documento sull'acquis organizzativo, che l'ACC chiedeva di approvare e trasmettere al gruppo "Acquis Schengen" dell'Unione europea, è stato sottoposto al Gruppo centrale.

Commissione permanente di applicazione della Convenzione

Il Comitato esecutivo ha istituito una commissione di vista incaricata di verificare la corretta applicazione della Convenzione da parte degli Stati Schengen. La Germania sarà il primo paese a ricevere le visite di detta Commissione. Uno dei gruppi di visita appositamente istituiti procederà ad una serie di verifiche presso il SIRENE Germania e sui terminali SIS. L'ACC ha ricordato al Gruppo centrale le competenze attribuitegli dalla Convenzione ed ha pertanto chiesto di essere associata ai controlli. Nella sua risposta, il Gruppo centrale invita il presidente dell'ACC ad assistere all'incontro che si terrà tra l'autorità di controllo tedesca e il gruppo di visita SIS.

In occasione della riunione del 12 febbraio 1999, l'ACC ha deciso di insistere presso la presidenza del Gruppo centrale affinché rappresentanti del Garante per la protezione dati tedesco possano accompagnare la Commissione durante tutta la sua missione. Le verifiche vertono infatti su aspetti connessi con gli articoli 126 e successivi della Convenzione, materie per le quali la competenza dell'autorità di controllo nazionale è indiscutibile. Nella sua riunione del 19 febbraio 1999, il Gruppo centrale ha tuttavia respinto questa richiesta.

Di fronte al rifiuto del Gruppo centrale, l'ACC ha protestato ufficialmente nei confronti del presidente del Comitato esecutivo, richiamando l'attenzione sul fatto che è stata istituita una Commissione ad hoc con poteri di controllo nel settore dei dati personali, dimenticando che la Convenzione prevede già un proprio sistema destinato a garantire l'osservanza di questi principi. Si effettuano controlli e verifiche senza tener conto degli organi competenti ad effettuare tali controlli e verifiche. Controlli e verifiche che non possono essere visti come mera somma delle parti,

bensi come un insieme che comprende gli N.SIS, il C.SIS e gli uffici SIRENE.

L'ACC ha espresso il suo stupore in merito al fatto che delegazioni di paesi che non partecipano ancora al sistema e che non hanno pertanto inserito dati possano avere accesso ad informazioni di natura personale, mentre l'Autorità di controllo comune e i Garanti per la protezione dati nazionali, organi indipendenti, sono esclusi dai controlli effettuati nell'ambito della Commissione permanente.

Parte IV

REAZIONI DELLE AUTORITÀ SCHENGEN ALLA RELAZIONE ANNUALE DELL'ACC

Nel 1998 il Gruppo centrale ha risposto alla relazione annuale dell'ACC indicando, per alcune raccomandazioni, che i gruppi di lavoro non avevano ancora ultimato la loro riflessione, e precisando l'esito riservato alle altre raccomandazioni. Da questa situazione emergeva chiaramente che molti pareri dell'ACC sollevavano problemi tecnici che sarebbe stato possibile risolvere solo mediante un rinnovo del SIS. L'ACC ha preferito evitare una sterile polemica e si è limitata a prendere conoscenza della relazione di risposta.

Rimane il fatto che tale relazione di risposta della presidenza belga elaborata durante il 1° semestre 1998 è stata comunicata un anno dopo la trasmissione della relazione annuale agli organi esecutivi Schengen, termine di risposta considerato eccessivo. Alcune raccomandazioni relative al controllo del C.SIS effettuato in ottobre 1996 sono state discusse dal Comitato di orientamento SIS solo il 22 luglio 1997 e solo nove mesi più tardi l'ACC è stata informata di questo esame tecnico. Si osserva che molte delle raccomandazioni dell'ACC non sono ancora state attuate col pretesto di problemi tecnici e finanziari (anche se, stando alle informazioni disponibili, tali raccomandazioni sono state prese in considerazione nei lavori di sviluppo del nuovo sistema).

Per quanto riguarda lo stato dell'esame delle sue raccomandazioni, l'ACC ritiene di dover disporre delle risposte in tempo utile e di non poter attendere un anno prima di conoscere eventuali decisioni in merito alle sue proposte. La missione di controllo dell'ACC è incompatibile con tempi di risposta così lunghi.

L'ACC si è stupita del fatto che il Gruppo centrale abbia adottato il principio della risposta annuale, come avviene al Consiglio d'Europa. Il Sistema d'informazione Schengen, infatti, funziona 24 ore su 24, 365 giorni l'anno e l'ACC è chiamata ad esercitare un potere di controllo sul sistema. L'ACC non è un organo consultivo, ma un'autorità.

L'ACC considera che le decisioni che riguardano le sue missioni devono esserle comunicate rapidamente, non appena adottate dai gruppi Schengen competenti.

Il presidente dell'ACC ha fatto presente questa posizione in occasione della riunione del Gruppo centrale tenutasi a Bonn il 5 novembre 1998.

L'11 dicembre 1998, l'ACC ha preso conoscenza della relazione del Comitato di orientamento SIS in risposta alla sua seconda relazione annuale (doc. SCH/OR.SIS (98) 133, 2a rev. - marzo 1997/marzo 1998). Tale relazione è stata approvata dal Gruppo centrale il 24 novembre 1998.

L'ACC ha potuto constatare che la relazione contiene diverse inesattezze. Il Comitato di orientamento SIS, ad esempio, nega che l'ACC abbia una competenza in materia di riavvicinamento delle prassi nazionali, quando una tale competenza è riconosciuta dall'articolo 115, comma 3 della Convenzione. Il Comitato di orientamento considera invece di essere l'organo investito di questa competenza.

Nella relazione, il Comitato di orientamento SIS indica inoltre che la Convenzione non prevede l'obbligo di dare esecuzione alle raccomandazioni dell'ACC e rifiuta di mettere a disposizione di questa un conto utente proprio, limitato alla funzione di audit del sistema. Tutto ciò è in contraddizione con l'articolo 115, comma 2. E' invece fondamentale, per un sistema come il SIS, che esista una vera funzione di audit, esigenza di un sistema di controllo indipendente, pena la creazione di un sistema di controllo sempre subordinato all'azione di chi è controllato.

L'ACC ha elaborato una risposta trasmessa il 3 febbraio 1999 al Gruppo centrale (doc. SCH/Aut-cont-lettre (99) 1).

La lettera riafferma che è inaccettabile che le risposte degli organi esecutivi giungano all'ACC dodici mesi dopo l'elaborazione della relazione annuale dell'ACC, come avvenuto per la risposta alla relazione 1996, o otto mesi dopo come per la relazione 1997.

Parte V

IL FUTURO DELL'ACC NEL NUOVO QUADRO ISTITUZIONALE

Tra circa due mesi entrerà in vigore il Trattato di Amsterdam. Verrà così modificato in modo positivo il quadro istituzionale del funzionamento di Schengen con il rafforzamento dei diritti del cittadino, il controllo democratico da parte del Parlamento europeo e l'effettiva competenza giurisdizionale della Corte di giustizia europea. Si tratta di un passo avanti importante sulla strada della cittadinanza europea e della sicurezza comune.

Nel quadro dell'Unione europea sono ancora in discussione le modifiche al funzionamento dei sistemi di informazione di polizia e del rispettivo controllo indipendente.

In risposta ad un'apposita richiesta, l'ACC ha presentato all'Unione europea e al Gruppo centrale un rapporto sulle materie che considera far parte dell'acquis comunitario. Ha inoltre comunicato ai suddetti organi il proprio programma di lavoro per i prossimi mesi, accompagnandolo di una stima di bilancio, della richiesta di un sostegno amministrativo e del numero di riunioni annuali.

In materia di acquis, si sottolinea che una parte sostanziale delle materie riguardanti il funzionamento dell'ACC sono un effetto giuridico diretto della Convenzione di applicazione (in particolare le sue attribuzioni e le sue competenze) o sono fondate su decisioni del Comitato esecutivo (ad es.: linea di bilancio autonoma, bilancio compatibile con le sue attribuzioni, accesso alla documentazione e all'informazione).

L'integrazione del SIS nella struttura dell'Unione europea deve garantire la continuità del controllo indipendente ad opera dell'ACC e le attività di quest'ultima non devono patire di tale integrazione. Stando alle dichiarazioni di un esponente della DG GAI (Direzione generale "Giustizia e Affari interni") dell'Unione europea, presente ad una riunione dell'ACC, sarebbe garantita un'integrazione armoniosa in questo senso.

Va ricordato che i sistemi d'informazione europei subiranno una significativa evoluzione nel prossimo anno. Essendo imminente, infatti, l'applicazione della Convenzione Europol, del Sistema d'informazione doganale e del sistema Eurodac risulta importantissimo definire modalità ottimali che consentano a tutti i sistemi di funzionare in armonia con un controllo indipendente ed effettivo.

Il quadro legislativo della protezione dei dati attraversa, in tutti gli Stati membri dell'Unione europea, un processo di profondo cambiamento.

L'armonizzazione legislativa in Europa e l'approfondimento della cooperazione tra le autorità di controllo nazionali e tra queste e l'UE condurranno senza dubbio ad una maggiore efficacia del funzionamento dei sistemi e ad un regime più coerente di tutela dei diritti.

Parte VI

ALLEGATI

1. I COMPITI DELL'ACC PREVISTI DALLA CONVENZIONE

Gli Stati che hanno ratificato la Convenzione hanno attribuito all'ACC il compito principale di controllare l'unità di supporto tecnico del SIS, compito che solo questa può realizzare (articolo 115, comma 2). Spetta inoltre all'ACC formulare pareri e vigilare sull'armonizzazione delle prassi o delle dottrine nazionali.

Alla luce della sua composizione e delle sue attribuzioni, l'ACC è un'entità indipendente

dalla struttura Schengen che gode di veri poteri di autorità come quelli risultanti dal controllo del C.SIS (accesso, verifica di legalità, elaborazione di relazioni).

La Convenzione di applicazione dell'Accordo di Schengen precisa i compiti dell'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 106, comma 3);
- analizza le difficoltà di applicazione o di interpretazione che possono sorgere nell'utilizzo del SIS;
- esamina i problemi che possono sorgere durante il controllo indipendente effettuato dalle autorità di controllo nazionali delle Parti contraenti;
- 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, comma 3);
- elabora relazioni che vengono trasmesse alle autorità alle quali pervengono le relazioni delle autorità di controllo nazionali (articolo 115, comma 4);

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 (articolo 118, comma 2).

Per quanto riguarda gli scambi di informazioni non riguardanti il SIS:

- può, su richiesta delle Parti contraenti, formulare un parere sulle difficoltà di applicazione e di interpretazione dell'articolo 126 relativo al trattamento dei dati trasmessi, al di fuori del SIS, in applicazione della Convenzione (articolo 126, comma 3, lettera f);
- può, alle condizioni e secondo le modalità previste all'articolo 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 (articolo 127, comma 1).

2. PARERI E RACCOMANDAZIONI DELL'ACC

Nella precedente relazione annuale (marzo 1997 – marzo 1998) è stata inserita la maggior parte dei pareri formulati dall'ACC nel 1998. Malgrado la loro attualità, tali pareri non sono stati inseriti nella presente relazione.

Vi figurano invece il parere relativo all'accesso al SIS da parte degli uffici della motorizzazione e la relazione sulla sicurezza degli uffici SIRENE.

PARERE N° 98/5 DELL'AUTORITÀ DI CONTROLLO COMUNE DESTINATO AL COMITATO ESECUTIVO

Oggetto: accesso al Sistema d'Informazione Schengen (SIS) da parte degli uffici della motorizzazione

A norma dell'articolo 93 della Convenzione di Schengen, il Sistema d'Informazione Schengen ha lo scopo, innanzi tutto, di preservare l'ordine pubblico e la sicurezza pubblica nel territorio delle Parti contraenti. Il sistema viene inoltre utilizzato per la procedura in materia di visti, il rilascio di titoli di soggiorno e l'attuazione della legislazione sugli stranieri nel quadro dell'applicazione della Convenzione.

A norma dell'articolo 101, 4° comma della Convenzione, ciascuna Parte contraente deve comunicare al Comitato esecutivo l'elenco delle autorità autorizzate alla consultazione. Tale elenco deve essere redatto nel rispetto dei criteri definiti all'articolo 101, 1° e 2° commi per quanto riguarda la qualificazione delle autorità interessate e i compiti attribuiti a livello nazionale. In concreto, il diritto d'interrogare direttamente i dati è riservato esclusivamente alle autorità competenti in materia di controlli di frontiera e di altre verifiche di polizia e doganali nonché, ai sensi dell'articolo 96, del rilascio dei visti e dei titoli di soggiorno e dell'amministrazione degli stranieri.

Non sono finora compresi in questo elenco gli uffici della motorizzazione, in quanto si trat-

ta, nella maggior parte degli Stati membri, di autorità amministrative con una diversa sfera di competenza. Gli uffici in questione di almeno alcuni Stati Schengen chiedono ora che anche ad essi sia consentito l'accesso ai dati relativi agli oggetti ricercati di cui all'articolo 100: ritengono che altrimenti si creerebbe una lacuna quanto alla possibilità di verificare, in sede di immatricolazione di veicoli, se si tratta di veicoli rubati all'estero. E' indubbio che l'accesso al SIS da parte di tali uffici costituisca un'esigenza reale.

VALUTAZIONE GIURIDICA

Dati in questione: va innanzi tutto ricordato che i dati relativi agli oggetti ricercati di cui all'articolo 100 comprendono anche il numero di telaio. L'autorità di controllo comune ha affermato, in un parere del 7 marzo 1997, che le informazioni relative a determinati caratteri distintivi dei veicoli quali, per esempio, la marca, il tipo, il colore e le caratteristiche tecniche degli stessi, non vanno considerati come dati di natura personale a condizione che non vi sia un nesso tra tali informazioni e la targa, il suo proprietario o il conducente del veicolo. Nel parere dell'ACC del 3 febbraio 1998 n. 98/3, lettera f), il numero di telaio viene tuttavia annoverato tra i dati di natura personale, in quanto può portare all'identificazione del proprietario o del conducente del veicolo.

L'ACC ritiene che il numero di telaio, qualora non possa essere messo in relazione con il proprietario del veicolo, non costituisca di per sé un dato a carattere personale. Tuttavia, le disposizioni che disciplinano la consultazione e l'uso del sistema (Capitolo II, Titolo IV della Convenzione) si applicano a prescindere dall'eventuale carattere personale dei dati, vale a dire che, anche se il destinatario non è in grado di identificare una persona, è comunque salva l'applicazione dell'articolo 101 che determina le autorità aventi la competenza esclusiva per la consultazione diretta del SIS.

Autorità abilitate a consultare il SIS: Per la maggior parte degli Stati membri è indubbio che l'accesso da parte degli uffici della motorizzazione ai dati del Sistema d'informazione Schengen sarebbe illecito. A norma dell'articolo 101, 1° comma della Convenzione, l'accesso ai dati inseriti nel SIS è riservato esclusivamente alle autorità competenti in materia di controlli alle frontiere e di altri controlli di polizia e doganali effettuati all'interno del Paese e relativo coordinamento. Nella maggior parte degli Stati membri, gli uffici della motorizzazione non sono competenti ad effettuare verifiche di polizia, ma sono autorità prettamente amministrative.

Finalità dell'interrogazione del SIS: ai sensi dell'articolo 102, 4° comma, i dati non possono essere utilizzati a scopi amministrativi. La Convenzione prevede inoltre "misure da adottare" per ogni tipo di segnalazione. Ne consegue che, per non contravvenire al principio di finalità, solo le autorità competenti a prendere tali misure devono essere autorizzate a interrogare il SIS. Stando agli elementi a conoscenza dell'ACC, le verifiche che gli uffici della motorizzazione desiderano effettuare grazie alla consultazione del SIS sono di natura amministrativa. Tali uffici non sono competenti a prendere le misure indicate e non ne avrebbero del resto la possibilità concreta.

CONCLUSIONI

L'accesso ai dati contenuti nel SIS da parte degli uffici della motorizzazione e il raffronto degli archivi sarebbero contrari al disposto degli articoli 101, 102, 2° comma e 102, 4° comma della Convenzione di Schengen.

Tuttavia, se gli uffici di alcuni Stati membri soddisfano le condizioni di competenza e di finalità imposte dalla Convenzione e sono in grado di applicare le misure di sicurezza imposte dall'articolo 118 della Convenzione, l'ACC ritiene ammissibile il principio di tale accesso, purché tali dati siano utilizzati per i fini previsti dall'articolo 100.

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.

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.

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 ;
2. cifratura delle comunicazioni tra il SIRENE e l'N.SIS e controllo della cifratura da parte dei membri delle autorità di controllo ;
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 i 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. incoraggiamento 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.

3. QUADRO DEI PARERI DELL'ACC E REAZIONI DEGLI ORGANI ESECUTIVI E TECNICI

Contenuto	Attività	Osservazioni
Controllo del C.SIS (marzo 1994) e parere del 18 maggio 1994	- La Francia ha adottato le misure ritenute più adeguate. - Il 4 marzo 1998, in occasione di una visita al C.SIS da parte del Gruppo centrale e del presidente dell'ACC, sono stati presentati alcuni lavori di adattamento del sito.	Stando alle informazioni in possesso dell'ACC questi lavori non sono stati realizzati.
Parere del 22 febbraio 1995 sul fondamento giuridico degli uffici SIRENE	Il 27 giugno 1996, il Gruppo centrale ha ritenuto che la base giuridica esiste, che i metodi di lavoro, la struttura e lo statuto formale degli uffici SIRENE sono disciplinati dal diritto interno degli Stati Schengen e che le autorità di controllo nazionali garantiscono il controllo del funzionamento del SIS e degli uffici SIRENE e provvedono all'informazione dell'ACC.	Quindici mesi dopo essere stato adito, il Gruppo centrale respinge l'argomentazione dell'ACC.
Visita di controllo al C.SIS del mese di ottobre 1996: Raccomandazione n. 1	Definizione di una nuova procedura di confronto dei dati che non evidenzia più le differenze riscontrate dall'ACC.	Nel 1998 è annunciata una nuova procedura di confronto dei dati.

Raccomandazione n. 2	Procedere ad una certificazione ITSEM/ITSEC del sistema informatico ed applicare le misure di sicurezza raccomandate o garantire almeno il livello di sicurezza previsto.	- Impossibilità di realizzare a posteriori la certificazione del sistema attuale. Impossibilità di attivare le funzioni di tracciatura. - Le specifiche tecniche definite nell'ambito della procedura di appalto per il rinnovo del C.SIS prevederanno che ogni componente del nuovo sistema debba obbligatoriamente essere conforme ai criteri ITSEC e alla norma 4-C2/E2. I sistemi saranno certificati o potranno esserlo su richiesta degli Stati Schengen.	Il Gruppo centrale dichiara che non è possibile procedere alla certificazione del sistema attuale. Il futuro sistema potrà essere certificato.
Raccomandazione n. 3	Ridurre il numero di "super utenti" del C.SIS che usufruiscono di un accesso privilegiato al sistema che consente loro di accedere a qualsiasi archivio registrato nel sistema informatico, di modificarne il contenuto e di cancellare qualsiasi traccia del loro intervento.	- Il personale del C.SIS è oggetto di severissime procedure di assunzione e di controllo di sicurezza. - Nelle specifiche dei nuovi sistemi sarà prevista una ripartizione precisa dei compiti di gestione affinché le funzioni possano essere attribuite sulla base di tali compiti. - Questa misura dovrebbe permettere di ridurre il numero di "super utenti" necessari.	L'ACC è stata informata del fatto che in futuro il numero di "super utenti" sarà ridotto.

Raccomandazione n. 4	Attivare le funzioni di tracciatura che consentono di verificare a posteriori le azioni effettuate dai vari utenti, a prescindere dal loro profilo.	Le specifiche tecniche definite nell'ambito della procedura di appalto per il rinnovo del C.SIS prevederanno che le ditte offerenti dovranno indicare le risorse supplementari necessarie perché i criteri di prestazione del sistema siano rispettati in caso di attivazione delle funzioni di tracciatura. Le specifiche prevedono inoltre che siano realizzati test con le funzioni di tracciatura attivate, allo scopo di verificare che il sistema operativo sia in grado di funzionare anche con le funzioni di tracciatura attivate. Le specifiche tecniche e l'offerta selezionata saranno trasmesse all'ACC perché questa possa prendere posizione.	

Raccomandazione n. 5	Gestione e trasporto dei supporti magnetici. Ricorrere sistematicamente alla cifratura in caso di registrazione dei dati su supporto magnetico per fini di trasporto o stoccaggio. L'ACC ha in effetti constatato che le misure di sicurezza adottate dagli Stati Schengen nella gestione e nel trasporto dei supporti magnetici sui quali sono registrati i dati SIS sono insufficienti.	Gli esporti del PWP hanno esaminato nel 1998 una soluzione che consiste nel trasmettere dati cifrati on-line. Questa soluzione consentirebbe una protezione equivalente a quella delle trasmissioni tra C.SIS e N.SIS ed eviterebbe i rischi di smarrimento, furto o sostituzione.	
Parere del 7 marzo 1997 sul progetto pilota relativo ai veicoli rubati, formulato su invito del Gruppo centrale del 10 febbraio 1997.	Rifiutare l'accesso al SIS da parte degli Stati Schengen che non applicano ancora la Convenzione. L'ACC ha ricordato che le disposizioni della Convenzione autorizzano l'accesso al SIS dei soli Stati che applicano la Convenzione stessa. Ha tuttavia indicato che tali paesi potevano essere associati al progetto mediante meccanismi di cooperazione bilaterale o multilaterale disciplinati dalle legislazioni nazionali in materia di protezione dei dati e assoggettati al controllo delle autorità di controllo nazionali. Alla data di realizzazione del progetto, l'Austria, l'Italia e la Grecia non applicavano ancora la Convenzione.	Il progetto pilota è stato portato avanti evitando che gli Stati che non applicavano la Convenzione avessero accesso ai dati. I meccanismi di cooperazione bilaterale o multilaterale proposti dall'ACC hanno consentito di associare questi paesi al progetto pilota.	

Parere del 7 marzo 1997 sul progetto di accordo sulle infrazioni stradali.	Richiamare nel testo dell'accordo le disposizioni relative alla protezione dei dati personali.	Il gruppo di lavoro competente ha adattato il progetto come richiesto dall'ACC.	
Parere 97/1 del 22 maggio 1997 sulla duplicazione di una parte delle segnalazioni SIS (per consentire il trasporto delle copie verso le rappresentanze diplomatiche e consolari, articolo 118, 2° comma della Convenzione).	Vigilare sulla sicurezza durante il trasporto delle copie. Provvedere alla registrazione di almeno il 10% delle consultazioni di questi supporti per consentire alle autorità di controllo di verificare se tali consultazioni erano autorizzate.	Nel 1998 la questione era ancora allo studio del Comitato di orientamento SIS.	
	Poiché l'uso di copie non aggiornate può recare pregiudizio ai diritti del cittadino, in attesa della creazione di un sistema di consultazione diretta, gli Stati membri debbono procedere a verifiche supplementari in tempo reale per garantire l'attualità di una segnalazione che figura su una copia ed accettare la propria responsabilità in caso di rilascio di un visto ad una persona segnalata nel SIS dopo duplicazione dei dati.		
Parere 98/1 sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione.	Procedere alla distruzione fisica dei dossier relativi ad una segnalazione dopo cancellazione della stessa. Modificare in questo senso il Manuale SIRENE.	Il 13 gennaio 1999, il Gruppo centrale ha trasmesso all'ACC la risposta del gruppo di lavoro competente, stando al quale la conservazione dei dossier è disciplinata dal diritto nazionale.	

Parere 98/2 sulla segnalazione nel SIS di persone vittime di un'usurpazione di identità.	Adottare una soluzione che consenta di indicare che si tratta di un'identità usurpata al fine di tutelare i diritti della vittima di tale usurpazione di identità.	Al momento non è ancora stata trovata una soluzione al problema. Il SIS II dovrebbe consentire di risolvere il problema. Nel mese di marzo 1998, il Gruppo centrale ha annunciato che esisteva una decisione in materia.	Il problema dovrebbe essere risolto entro il 2000.
Parere 98/3 sulle eventuali relazioni tra il SIS e il progetto di sistema "ASF - veicoli rubati" (Automated Search Facility) di Interpol	Non autorizzare la trasmissione di dati personali dal SIS verso Stati non Schengen.	Il Gruppo centrale ha seguito il parere dell'ACC.	
Parere 98/4 sulla registrazione delle consultazioni ai sensi dell'articolo 103 della Convenzione.	Rispettare le regole comuni per garantire che sia registrato il 10% delle consultazioni del SIS.	Il Gruppo centrale non ha seguito il parere dell'ACC ritenendo che la questione è di competenza degli Stati membri.	
Parere 98/5 sull'accesso al SIS da parte degli uffici della motorizzazione.	Rifiutare l'accesso al Sistema d'informazione Schengen da parte degli uffici della motorizzazione. L'ACC considera tuttavia che l'accesso è ammissibile nei casi in cui l'ufficio della motorizzazione soddisfa le condizioni di competenza e di finalità previste dalla Convenzione ed è in grado di applicare le misure di sicurezza di cui all'articolo 118 della Convenzione stessa.		

4. PROMEMORIA

GLI ORGANI COMUNI PREPOSTI ALL'APPLICAZIONE DELLA CONVENZIONE

Ai fini dell'applicazione della Convenzione, le Parti contraenti hanno istituito due organi:

- il Comitato esecutivo, composto dei ministri competenti per l'attuazione della Convenzione in ogni Stato parte, ha per compito generale di vigilare alla corretta applicazione della Convenzione e dispone di una serie di competenze specifiche (articolo 131);
- l'Autorità di controllo comune (ACC), composta di due rappresentanti di ogni autorità nazionale di controllo, ha il compito di verificare la corretta esecuzione delle disposizioni della Convenzione per quanto riguarda l'unità di supporto tecnico del SIS (articolo 115). Dispone inoltre di competenze più generali in materia di protezione dei dati.

Oltre a questi due organi, il sistema Schengen gravita attorno al Gruppo centrale, dal quale dipendono un Comitato di orientamento SIS nonché diversi gruppi di lavoro, alcuni dei quali istituiti dalla stessa Convenzione.

Gli organi Schengen sono assistiti da un Segretariato. Questo compito è svolto dal Segretariato generale dell'Unione economica del Benelux, la cui sede è a Bruxelles.

L'organigramma figura in allegato.

OBIETTIVI ED ARCHITETTURA DEL SISTEMA D'INFORMAZIONE SCHENGEN

Il Titolo IV della Convenzione è interamente dedicato al Sistema d'Informazione Schengen (SIS).

L'articolo 93 della Convenzione precisa che il SIS "avvalendosi delle informazioni trasmesse per il suo tramite, ha lo scopo di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza dello Stato, e di assicurare l'applicazione delle disposizioni sulla circolazione delle persone stabilite nella presente Convenzione".

Le informazioni registrate nel sistema

L'articolo 94 elenca limitativamente le categorie di dati che possono essere registrati nel sistema. Gli articoli da 95 a 100 precisano i motivi che giustificano l'inserimento delle segnalazioni. Le categorie di dati riguardano le persone, gli oggetti e i veicoli.

Per quanto riguarda le persone, nel sistema possono essere inseriti cognome e nome, alias, segni fisici particolari, oggettivi ed inalterabili, indicazione eventuale del fatto che la persona è armata o violenta e linea di condotta da eseguire in caso di individuazione della persona in questione.

E' vietato menzionare informazioni dette "sensibili" quali la razza, le opinioni politiche, la confessione religiosa o altre convinzioni nonché informazioni relative allo stato di salute o la vita sessuale.

Le finalità che giustificano l'inserimento di una segnalazione nel SIS sono le seguenti:

a. a prescindere dalla cittadinanza della persona:

- arresto per fini di estradizione (articolo 95);
- ricerca in caso di scomparsa, ricerca di minori o di persone che devono essere internate per decisione di un'autorità competente (articolo 97);
- arresto ai fini di comparizione dinanzi all'autorità giudiziaria, anche in qualità di testimone, nell'ambito di un procedimento penale o dell'esecuzione di una pena privativa della libertà (articolo 98);
- sorveglianza discreta e controllo specifico ai fini della repressione di reati penali o della prevenzione di minacce gravi per la sicurezza dello Stato (articolo 99);

b. per gli stranieri, ossia chiunque non sia cittadino di uno Stato membro delle Comunità europee (v. definizione all'articolo 1, 6° comma):

- non ammissione nel territorio a seguito di un provvedimento amministrativo o giudiziario adottato nel rispetto delle regole procedurali nazionali o fondato su un rischio per l'ordine pubblico e la sicurezza pubblica o la sicurezza nazionale o sul fatto che lo straniero in questione abbia violato la normativa nazionale relativa all'ingresso e al soggiorno degli stranieri (articolo 96).

Per quanto riguarda gli oggetti, nel sistema possono essere inseriti solo dati relativi al nome del proprietario di veicoli, armi da fuoco, documenti e banconote rubati, sottratti o smarriti, ricercati per fini di sequestro o di prova nell'ambito di un procedimento penale (articolo 100).

Per quanto riguarda i veicoli, possono essere registrati dati relativi a quei veicoli ricercati per fini di sorveglianza discreta o di controllo specifico (articolo 99 già citato). Questa categoria permette di registrare informazioni relative al conducente e ai passeggeri del veicolo sorvegliato.

Destinatari delle informazioni

Gli articoli 92 e 101 della Convenzione precisano che le autorità designate dalle Parti contraenti possono accedere, mediante consultazione automatizzata o non automatizzata:

- all'insieme dei dati inseriti nel SIS in occasione dei controlli di frontiera e degli accertamenti e di altri controlli di polizia e di dogana effettuati all'interno del territorio in conformità del diritto nazionale;
- alla sola categoria di segnalazioni per fini di non ammissione in caso di rilascio di visti e permessi di soggiorno e di amministrazione degli stranieri nel quadro delle disposizioni della Convenzione relative alla circolazione degli stranieri.

L'elenco delle autorità abilitate a consultare direttamente i dati inseriti nel SIS deve essere comunicato al Comitato esecutivo (articolo 101, 4° comma).

Architettura del Sistema d'Informazione Schengen

Numerosi articoli del Titolo IV prescrivono il rispetto di diverse misure di ordine tecnico ma la descrizione generale del sistema figura all'articolo 92.

Il Sistema d'informazione Schengen (SIS) si compone di una sezione nazionale (N.SIS) presso ogni Parte contraente e di un'unità di supporto tecnico (C.SIS) istituita e mantenuta in comune, la cui responsabilità incombe alla Repubblica francese.

L'unità di supporto tecnico ha sede a Strasburgo ed ha il compito di rendere materialmente identico il contenuto di tutti gli N.SIS. A tal fine, il C.SIS contiene un archivio di dati che garantisce l'identità degli archivi nazionali mediante la trasmissione di informazioni on-line.

La trasmissione dei dati avviene nel rispetto dei protocolli e delle procedure definiti in comune dalle Parti contraenti per l'unità di supporto tecnico.

L'articolo 118, 4° comma prevede le misure di sicurezza necessarie per l'unità di supporto tecnico. Tali misure sono identiche a quelle richieste per ogni N.SIS (articolo 118, 1°, 2° e 3° comma).

GLI UFFICI SIRENE

Gli uffici SIRENE (Supplementi d'informazione richiesti per l'ingresso nazionale) sono una creazione degli Stati parte non esplicitamente prevista dalla Convenzione.

In ogni Stato Schengen, l'ufficio SIRENE è stato incaricato di procedere, sulla base del SIS, allo scambio di informazioni supplementari e funge da intermediario nelle consultazioni tra i vari Stati sulla condotta da adottare in caso di esecuzione di una segnalazione.

Compiti e attività degli uffici SIRENE sono concretamente definiti in un manuale comune detto "Manuale SIRENE". Il loro ruolo consiste essenzialmente nel procedere a consultazioni preliminari alla creazione di segnalazioni, a scambi di informazioni, al controllo delle segnalazioni multiple e alla definizione di ordini di priorità.

Nel 1998, i membri dell'ACC degli Stati che applicano la Convenzione hanno realizzato visite di controllo nei rispettivi uffici SIRENE ed hanno trasmesso le relazioni su tali visite al Segretariato dell'Autorità di controllo comune (doc. SCH/Aut-cont (98) 9 (Francia), 13 e 40 (Belgio), 15 (Italia), 21 (Germania), 28 (Grecia), 31 (Portogallo), 33 (Paesi Bassi), 35 (Spagna) e 36 (Austria). Anche il Lussemburgo e i Paesi Bassi hanno presentato una relazione sulla sicurezza dei rispettivi uffici SIRENE).

Il livello di sicurezza degli uffici SIRENE non deve 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:

- 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 ;
- cifratura delle comunicazioni tra il SIRENE e l'N.SIS e controllo della cifratura da parte dei membri delle autorità di controllo ;
 - 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;
- limitazione e controllo dell'accesso agli archivi manuali dei dossier;
- cifratura delle informazioni contenute su supporto informatico ;
- 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 i password ;
- verifica regolare dei motivi di una interrogazione del SIS;
- designazione di un funzionario responsabile della sicurezza e definizione delle norme di sicurezza comuni ai vari uffici SIRENE, applicabili al loro personale;
- 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 ;
- incoraggiamento dell'organizzazione di corsi di formazione incentrati sulla sicurezza dei dati per gli utenti degli uffici SIRENE ;
- raccomandazione dell'elaborazione da parte degli N.SIS e degli uffici SIRENE di relazioni sulla sicurezza, a intervalli regolari, per esempio ogni anno.

PROTEZIONE DEI DATI PERSONALI

UNA LEGGE ED UN'AUTORITÀ DI CONTROLLO NAZIONALE: CONDIZIONI PRELIMINARI PER L'APPLICAZIONE DELLA CONVENZIONE

Gli Stati parte hanno posto diverse condizioni preliminari all'applicazione della Convenzione nei rispettivi territori. L'Atto finale richiama il carattere imperativo di queste condizioni.

Tra di esse figura l'obbligo, per ogni Stato parte, di dotarsi, prima di procedere alla trasmissione di dati personali, di un'autorità nazionale di controllo indipendente (articoli 114 e 128) e di una legge sulla protezione dei dati.

Per quanto riguarda il trattamento automatizzato o meno dei dati trasmessi, la Convenzione prevede le seguenti disposizioni:

- a. Trattamento automatizzato di dati trasmessi in applicazione del Titolo IV relativo al SIS:

ARTICOLO 117

Ciascuna Parte contraente prenderà, al più tardi al momento dell'entrata in vigore della Convenzione, le disposizioni nazionali necessarie per raggiungere un livello di protezione dei dati di natura personale almeno pari a quello derivante dai principi della Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone nei riguardi del trattamento automatizzato dei dati di natura personale, nel rispetto della Raccomandazione R 15 (87) del 17 settembre 1987 del Comitato dei Ministri del Consiglio d'Europa tendente a regolare l'uso dei dati di natura personale nel settore della polizia.

La trasmissione di dati di natura personale potrà avvenire soltanto quando le disposizioni di protezione dei dati personali saranno entrate in vigore nel territorio delle Parti contraenti interessate dalla trasmissione.

- b. Trattamento automatizzato di altri dati trasmessi in applicazione della Convenzione, ad eccezione di quelli relativi alle domande di asilo:

ARTICOLO 126

Esigenza, al momento dell'entrata in vigore della Convenzione, di un livello di protezione dei dati di natura personale almeno pari a quello derivante dai principi della già citata Convenzione del Consiglio d'Europa e trasmissione dei dati subordinata all'efficacia di tale protezione nel territorio delle Parti contraenti interessate dalla trasmissione.

ARTICOLO 129

Per quanto riguarda la trasmissione dei soli dati relativi alla cooperazione di polizia, le Parti contraenti debbono raggiungere un livello di protezione dei dati di natura personale che rispetti i principi della già citata Raccomandazione R (87) 15 del 17 settembre 1987 del Comitato dei Ministri del Consiglio d'Europa.

- c. Dati trasmessi in applicazione della Convenzione provenienti da un archivio o registrati in un archivio, ad eccezione di quelli relativi alle domande di asilo, al SIS o all'assistenza giudiziaria in materia penale:

ARTICOLO 127

Applicazione del disposto dell'articolo 126 e, per quanto riguarda la trasmissione di dati relativi alla cooperazione di polizia, livello di protezione dei dati che rispetti i principi della già citata Raccomandazione R (87) 15.

- d. Infine, ai dati che figurano nei dossier si applicano esclusivamente, salvo un'unica eccezione, le disposizioni specifiche di protezione dei dati di cui all'articolo 126, 3° comma sotto il controllo, se del caso, dell'autorità nazionale competente (articolo 128, 2° comma).

SFERE D'APPLICAZIONE RISPETTIVE DELLA CONVENZIONE E DEL DIRITTO NAZIONALE

La Convenzione opera, in materia di protezione dei dati di natura personale, una complessa suddivisione tra la sfera di applicazione delle proprie disposizioni e la sfera di applicazione del diritto nazionale degli Stati parte.

Diritti delle persone rispetto al SIS

La norma può essere illustrata in questi termini: laddove la Convenzione non prevede disposizioni particolari, è di applicazione il diritto di ogni Parte contraente.

La Convenzione precisa i diritti riconosciuti alle persone e i loro eventuali limiti. Fermo restando il rispetto di tali disposizioni, le persone esercitano i loro diritti in conformità della legislazione di ogni Stato parte.

Diritto di accesso e di comunicazione (articolo 109)

Chiunque può avere accesso alle informazioni contenute nel SIS che lo riguardano. A tal fine, la persona può presentare una richiesta presso le autorità competenti di ogni Stato parte.

Se il diritto nazionale lo prevede, l'autore della domanda può ricevere le informazioni che lo riguardano. Tuttavia, in applicazione del principio della "proprietà dei dati", la comunicazione di queste informazioni è subordinata al fatto che lo Stato in cui è stata presentata la domanda ma che non è l'autore dell'inserimento della segnalazione dia preliminarmente allo Stato autore della segnalazione l'occasione di prendere posizione in merito.

La comunicazione delle informazioni può essere rifiutata se può nuocere all'esecuzione della segnalazione o se ciò risulta necessario ai fini della tutela dei diritti e delle libertà altrui. La comunicazione viene in ogni caso respinta se la persona è segnalata ai fini di sorveglianza discreta.

Diritto di rettifica (articolo 110)

Chiunque può far rettificare dati contenenti errori di fatto o far cancellare dati contenenti errori di diritto che lo riguardano. Nella prassi, l'esercizio di questo diritto è ampiamente facilitato dalla comunicazione delle informazioni contenute nel sistema.

Diritto di avviare un'azione di rettifica, cancellazione, informazione o indennizzo (articolo 111)

Chiunque deve poter adire, nel territorio di ciascuna Parte contraente, la giurisdizione o l'autorità competente relativamente ad una segnalazione che lo riguarda. L'esecuzione delle decisioni definitive avviene ad opera dello Stato parte interessato.

Diritto di chiedere una verifica dei dati (articolo 114, 2° comma)

Chiunque ha il diritto di chiedere alle autorità di controllo nazionali di verificare i dati inseriti nel Sistema d'Informazione Schengen che lo riguardano nonché l'utilizzazione che ne viene fatta.

Se i dati sono stati inseriti da uno Stato diverso da quello nel quale viene presentata la domanda, il controllo è effettuato in stretto coordinamento con l'autorità di controllo dello Stato autore della segnalazione.

Nonostante non sia ancora stato elaborato l'elenco delle domande presentate negli Stati Schengen relative all'esercizio dei diritti summenzionati, dagli elementi d'informazione di cui dispone l'ACC emerge che, per ogni Stato, il numero di tali richieste varia da uno a quaranta per i due anni trascorsi.

Controllo del Sistema d'Informazione Schengen

La Convenzione stabilisce i principi della protezione dei dati che, fatto salvo il diritto interno di ogni Parte contraente, sono applicabili in caso di trattamento dei dati inseriti nel SIS (articolo 104). Per quanto riguarda il controllo del rispetto di tali principi, la Convenzione opera una ripartizione di competenze tra l'Autorità di controllo comune e le autorità di controllo nazionali (articoli 114 e 115).

La Convenzione elenca i seguenti principi:

- a. Principio della finalità della registrazione dei dati e, salvo eccezioni limitativamente elencate, del loro utilizzo: estradizione, non ammissione, persone scomparse, testimoni, persone citate o condannate, oggetti rubati, persone e veicoli oggetto di sorveglianza discreta o controllo specifico (articoli da 94 a 100 e 102 già citati).
- b. Divieto di trattare dati sensibili ed enumerazione limitativa dei dati registrati (articolo 94 già citato).
- c. Definizione dei destinatari: accesso limitato alle autorità nazionali competenti in determinati settori e solo per l'adempimento delle loro missioni (articolo 101 già citato).
- d. Divieto di copiare le segnalazioni di un'altra Parte contraente in un archivio nazionale e limitazione delle duplicazioni per scopi tecnici (articolo 102).
- e. Obbligo di registrazione di ogni decima trasmissione di dati per fini di controllo dell'ammissibilità (articolo 103).
- f. Determinazione di una durata di conservazione dei dati (articoli 112 e 113).
- g. Obbligo di conservare i dati cancellati per un anno presso l'unità di supporto tecnico per fini di controllo a posteriori della loro esattezza e della liceità del loro inserimento (articolo 113, 2° comma).

Per quanto riguarda il controllo del sistema, la Convenzione stabilisce che ogni Stato parte debba incaricare un'autorità nazionale di procedere al controllo, in modo indipendente e nel rispetto della legislazione nazionale (articolo 114), dell'archivio della sezione nazionale del Sistema d'informazione Schengen (N.SIS). E' compito di tali autorità accertare il rispetto delle disposizioni sulla protezione dei dati della Convenzione e, se, del caso, delle disposizioni aggiuntive del diritto nazionale.

Il controllo dell'unità di supporto tecnico (C.SIS) è invece affidato all'Autorità di controllo comune. Questa deve operare nell'osservanza della Convenzione di Schengen, della Convenzione del Consiglio d'Europa sulla protezione dei dati, della Raccomandazione del Consiglio d'Europa sui dati di polizia e del diritto francese.

SCAMBI DI INFORMAZIONI AL DI FUORI DEL SIS

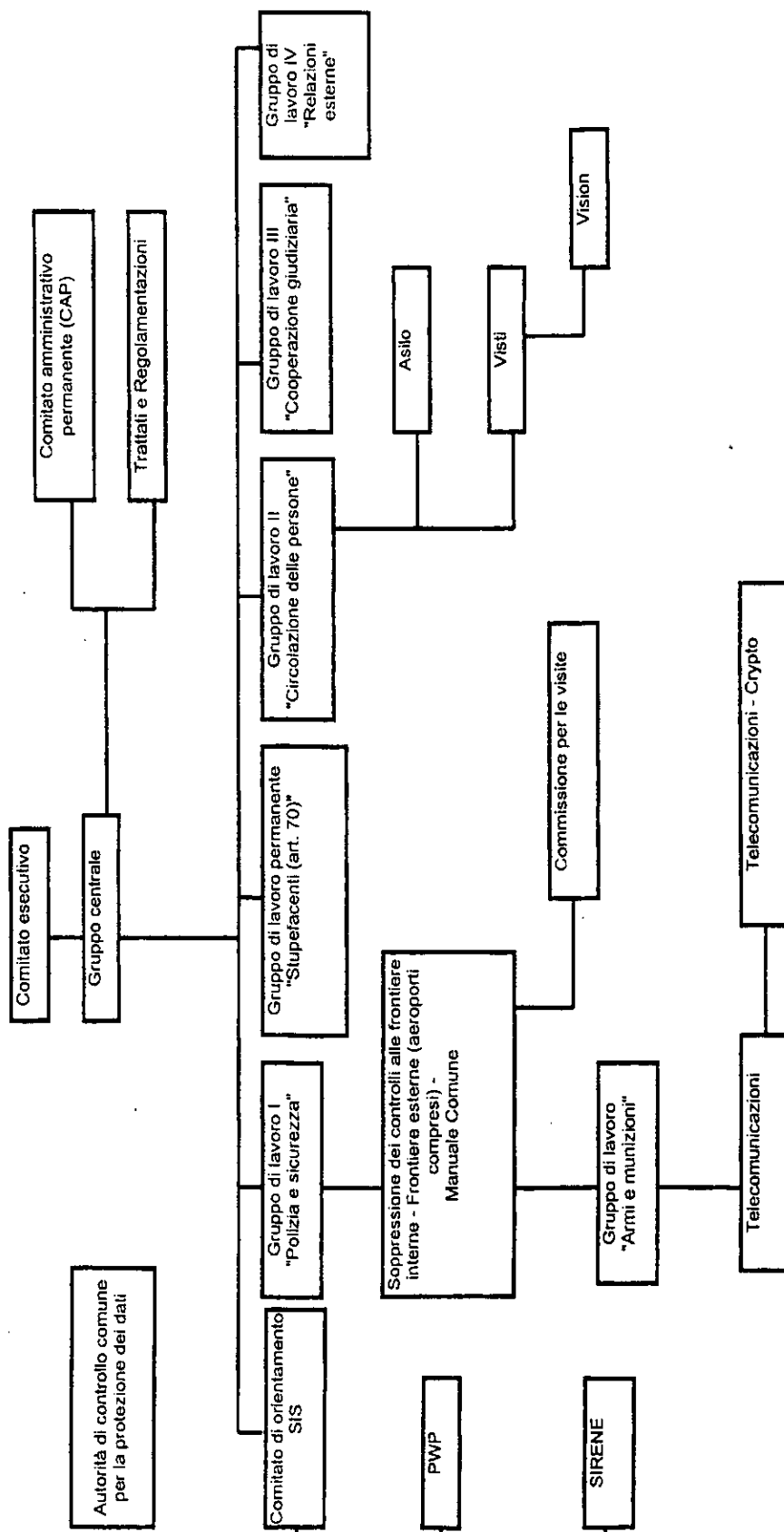
Il Titolo VI della Convenzione (articolo 126 e successivi), intitolato "Protezione dei dati di natura personale" è dedicato alle regole applicabili agli scambi di informazioni che non danno luogo ad una segnalazione nel SIS ma avvengono nel quadro dell'applicazione della Convenzione (v. punti 2.1.b e 2.1.c).

I principi definiti (finalità, limitazione dei destinatari, esattezza dei dati, ...) sono applicabili ferme restando le disposizioni della legislazione nazionale in materia di protezione dei dati, legislazione che disciplina in particolare l'esercizio dei diritti delle persone interessate.

Il controllo del rispetto delle regole enunciate dalla Convenzione è di competenza delle autorità nazionali.

Il ruolo dell'ACC è complementare: l'Autorità di controllo comune può, su richiesta delle Parti contraenti, formulare un parere sulle difficoltà di applicazione e di interpretazione poste da queste regole.

5. ORGANIGRAMMA DEI GRUPPI DI LAVORO SCHENGEN



6. 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.

7. ELENCO DELLE DECISIONI, DELLE RACCOMANDAZIONI, DEI PARERI E DELLE RELAZIONI DELL'AUTORITÀ DI CONTROLLO COMUNE SCHENGEN CHE COSTITUIRANNO L'ACQUIS SCHENGEN IN CONFORMITÀ DEL PROTOCOLLO RELATIVO ALL'INCORPORAZIONE DELL'ACQUIS SCHENGEN NELL'AMBITO DELL'UNIONE EUROPEA PREVISTO NEL TRATTATO DI AMSTERDAM

Documento	Argomento	Rif. documento Schengen
Regolamento interno	Il Regolamento garantisce l'indipendenza dell'ACC e ne definisce la composizione, le modalità di elezione della presidenza, le regole di funzionamento e i compiti da assolvere.	SCH/Aut-cont (95) 25, 6a rev.
Linea di bilancio autonoma	Garantisce nel quadro del bilancio generale di Schengen una linea autonoma dell'ACC, come proposto da quest'ultima.	SCH/Com-ex (97) PV 1 riv. (riunione del Comitato esecutivo del 25 aprile 1997); SCH/Com-ex (97) 1 (decisione del Comitato esecutivo del 25 aprile 1997); SCH/Com-ex (98) 9 (progetto di decisione del Comitato esecutivo del 21 aprile 1998)
Bilancio dell'ACC 1997 e 1998.	Stabilisce fondi e criteri di ripartizione adeguati per l'assolvimento dei compiti.	SCH/Aut-cont (96) 4a rev. + SCH/Aut-cont (98) budget 1
Decisione dell'ACC relativa alle leggi sulla protezione dei dati della Grecia	Dichiarazione dell'ACC sull'entrata in vigore delle leggi sulla protezione dei dati della Grecia.	SCH/Aut-cont (97) PV 3 (riunione dell'ACC del 27 marzo 1997) e SCH/Aut-cont (97) 1. 5
Decisione dell'ACC relativa alle leggi sulla protezione dei dati dell'Italia	Dichiarazione dell'ACC sull'entrata in vigore delle leggi sulla protezione dei dati dell'Italia	SCH/Aut-cont (97) PV 7 (riunione dell'ACC del 4 luglio 1997) e SCH/Aut-cont (97) 35
Elenco delle autorità autorizzate a consultare direttamente i dati inseriti nel SIS	Articolo 101, 4° comma della Convenzione. Decisione dell'ACCP.	SCH/Aut-cont (95) PV 1 (riunione dell'ACCP del 22 febbraio 1995)

Documento	Argomento	Rif. documento Schengen
Raccomandazioni dell'ACCP sul C.SIS	Raccomandazioni relative alla sicurezza presso il C.SIS, all'affidabilità delle trasmissioni tra gli N.SIS e il sistema centrale.	SCH/Aut-cont (94) dec. 1 (18 maggio 1994)
Parere sull'esercizio del diritto di accesso e sui principi di cooperazione nella verifica dei dati	Definisce i principi di cooperazione tra le autorità di controllo nazionali, nel quadro dell'esercizio dei diritti di accesso e di verifica.	SCH/Aut-cont (96) 16, 2a rev.
Raccomandazioni dell'ACC sul funzionamento del sistema d'informazione	Raccomandazioni sulla sicurezza del SIS contenute nella Relazione a carattere riservato del 27 marzo 1997 e riprodotte in parte nella relazione di attività 1995-1997.	- SCH/Aut-cont (96) 40, 2a rev. (dicembre 1996, versione definitiva del 27 marzo 1997) - (RISERVATO) - SCH/Aut-cont (97) 27, 2a rev. (Relazione di attività 1995-1997 del 17 marzo 1997) - pagg. 24-28
Parere sul progetto pilota relativo ai veicoli rubati	Principi da rispettare in materia di scambio di informazioni provenienti dal SIS, nell'ambito di operazioni tra Stati Schengen, con paesi che non applicano ancora la Convenzione.	Parere del 7 marzo 1997 (SCH/Aut-cont (96) 22 riv.)
Parere sull'Accordo di cooperazione nella contestazione delle infrazioni stradali e nell'esecuzione delle relative sanzioni pecuniarie	Enumerazione delle menzioni relative alla protezione dei dati (diritti delle persone, principio di cooperazione tra autorità nazionali e competenze dell'ACC) che devono figurare nell'Accordo.	Parere del 7 marzo 1997 (SCH/Aut-cont (96) 19 riv.)
Relazione sulle attività dell'ACC - marzo 1995/marzo 1997	Attività dell'ACC da marzo 1995 a marzo 1997 (Approvata e distribuita ai sensi dell'articolo 115, 4° comma della Convenzione di applicazione).	SCH/Aut-cont (97) 27, 2a rev. del 17 marzo 1997
Relazione sulle attività dell'ACC - marzo 1997/marzo 1998	Attività dell'ACC da marzo 1997 a marzo 1998 (Approvata e distribuita ai sensi dell'articolo 115, 4° comma della Convenzione di applicazione).	SCH/Aut-cont (98) 5, 5a rev., pubblicato il 28 aprile 1998

Documento	Argomento	Rif. documento Schengen
Decisione sulla composizione dell'Autorità	Decisione sul riconoscimento dello status di osservatori ai rappresentanti della Danimarca, della Finlandia, della Norvegia, dell'Islanda e della Svezia.	SCH/Aut-cont (97) PV 1 (verbale della riunione del 10 e 11 febbraio 1997 a Strasburgo)
Decisioni sulla composizione dell'Autorità	Decisione sul riconoscimento della qualità di membri dell'ACC ai rappresentanti dell'Austria, della Grecia e dell'Italia.	SCH/Aut-cont (97) PV 11 (verbale della riunione dell'ACC del 12 dicembre 1997)
Parere sulla duplicazione di una parte delle segnalazioni SIS	Utilizzazione di supporti tecnici di duplicazione ai fini della consultazione delle segnalazioni ex articolo 96 della Convenzione di applicazione degli Accordi di Schengen da parte delle Rappresentanze diplomatiche e consolari di alcuni Stati Schengen all'estero	Parere 97/1 del 22 maggio 1997 (SCH/Aut-cont (97) 38 riv.)
Parere sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione	Cancellazione dei dati ai sensi dell'articolo 112. Revisione del Manuale Sirene.	Parere 98/1 del 3 febbraio 1998 (SCH/Aut-cont (97) 55, 2a rev.)
Parere sulla segnalazione nel SIS di persone la cui identità è stata usurpata	Denuncia da parte dell'ACC della situazione attuale e proposta di collaborazione ai fini della ricerca di una soluzione che non rechi pregiudizio ai diritti del legittimo titolare dell'identità usurpata.	Parere 98/2 del 3 febbraio 1998 (SCH/Aut-cont (97) 42, 2a rev.)
Parere sulle eventuali relazioni tra il SIS e il progetto "ASF - Veicoli rubati" di Interpol.	Tipo di dati che possono essere trasmessi dal SIS verso la banca dati d'Interpol ASF.	Parere 98/3 del 3 febbraio 1998 (SCH/Aut-cont (97) 50, 2a rev.)
Parere sulla registrazione delle consultazioni prevista all'articolo 103	Enumerazione dei criteri da rispettare al momento della registrazione di cui all'articolo 103.	Parere 98/4 del 3 febbraio 1998 (SCH/Aut-cont (97) 70 riv.)

Documento	Argomento	Rif. documento Schengen
Comunicazione all'ACC dei documenti di altri gruppi Schengen	Messa a disposizione dell'ACC dei documenti relativi alle attività legate al SIS perché questa possa verificare se vengono prese in considerazione le sue raccomandazioni tecniche.	Lettera del Presidente del Gruppo centrale all'ACC del 12 gennaio 1998 (SCH/Aut-cont (98) 11)
Assistenza del Segretariato all'ACC	Rafforzamento del sostegno del Segretariato all'ACC affinché questa possa assolvere i propri compiti.	• Regolamento interno dell'ACC (art. 10) (SCH/Aut-cont (95) 25, 6a rev.) • SCH/Aut-cont (97) PV 6 (riunione del 16 giugno 1997 tra i rappresentanti dell'ACC, del Gruppo centrale e del Ministero dell'Interno francese) • SCH/Aut-cont (97) 2 (lettera del Presidente del Gruppo centrale del 14 gennaio 1997) • SCH/Aut-cont (97) PV 1 (riunione del Gruppo centrale del 23 febbraio 1998)

Nota: la relazione del 27 marzo 1997 sul controllo del C.SIS contiene raccomandazioni sulla sicurezza del SIS nonché la reazione del Ministero dell'Interno francese ad alcune di esse (SCH/Aut-cont (96) 40, 2a rev.).

Tale documento è considerato **riservato** dall'ACC e dal Gruppo centrale. E' stato pertanto trasmesso dall'ACC al presidente del Comitato esecutivo e ai membri del Gruppo centrale che l'hanno trasmesso a loro volta ai propri esperti interessati.

Estratti di tale relazione sono ripresi alle pagine 24-28 della relazione sulle attività 1995/1997 SCH/Aut-cont (97) 27, 2a rev.

8. REGOLAMENTO INTERNO DELL'AUTORITA' DI CONTROLLO COMUNE

approvato dall'ACC il 2 febbraio 1996
modificato all'articolo 2 per decisione adottata dall'ACC nella riunione del 4.7.1997
modificato il 27 aprile 1998 con l'aggiunta di un nuovo articolo 11

L'Autorità di controllo comune,

visto l'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 relativo alla eliminazione graduale dei controlli alle frontiere comuni, firmato il 19 giugno 1990, denominata in appresso "la Convenzione", adotta il 19 ottobre 1995 il seguente regolamento interno:

**Articolo 1
COMPITI**

1. L'Autorità di controllo comune assolve, conformemente al presente regolamento interno, i compiti previsti dalla Convenzione e qualsiasi altro compito relativo alla protezione dei dati di natura personale che essa ritenga connesso con l'applicazione della Convenzione.
2. Nell'esercizio dei suoi compiti, l'Autorità di controllo comune può intervenire d'ufficio, o su richiesta di un'Autorità di controllo nazionale di uno Stato Schengen o di una Parte contraente o di un organo del Sistema Schengen, secondo le disposizioni della Convenzione.

**Articolo 2
COMPOSIZIONE**

1. L'Autorità di controllo comune si compone, in conformità dell'articolo 115 della Convenzione, di due rappresentanti dell'Autorità di controllo nazionale di cui all'articolo 114 della Convenzione di ogni Parte contraente in cui è entrata in vigore la Convenzione, in conformità dell'articolo 140. E' considerata Parte contraente anche la Parte che ha concluso con le Parti dell'Accordo e della Convenzione di Schengen un accordo di cooperazione relativo alla soppressione dei controlli delle persone alle frontiere interne definite all'articolo 1 della Convenzione, a condizione che tale accordo di cooperazione sia entrato in vigore. Ciascuna delegazione dispone di un voto deliberante.
2. L'Autorità di controllo comune può, su decisione presa all'unanimità, concedere lo status di osservatore senza voto deliberante ai rappresentanti delle Autorità di controllo nazionali di cui all'articolo 114 della Convenzione o agli esperti indipendenti delle Parti contraenti che non soddisfano ancora il disposto dell'articolo 140, 2° comma, ultima frase. E' considerata Parte contraente anche la Parte che ha concluso con le Parti dell'Accordo e della Convenzione di Schengen un accordo di cooperazione relativo alla soppressione dei controlli delle persone alle frontiere interne definite all'articolo 1 della Convenzione, a condizione che tale accordo di cooperazione sia stato ratificato, accettato o approvato da tutte le Parti, ma non ancora entrato in vigore.
3. I membri dell'Autorità di controllo comune, nonché gli osservatori, non possono essere membri di un gruppo di lavoro o di un'autorità - che non sia l'autorità di controllo nazionale per la protezione dei dati di natura personale - istituiti in virtù della Convenzione. Possono tuttavia aggregarsi alle delegazioni nazionali in qualità di esperti.
4. Un membro dell'Autorità di controllo comune che si trovi nell'impossibilità di partecipare ad una riunione può farsi sostituire da una persona designata dall'Autorità di controllo nazionale in conformità del presente articolo.
5. I membri dell'Autorità di controllo comune possono farsi accompagnare da un esperto che li assiste.

Articolo 3 PRESIDENZA

1. L'Autorità di controllo comune elegge il presidente e il vicepresidente tra i suoi membri. Essi sono eletti a maggioranza dei due terzi delle delegazioni di cui all'articolo 2, par. 1. Il loro mandato ha una durata di un anno, rinnovabile una volta.
2. Il vicepresidente fa parte di una delegazione che non è quella del presidente ; sostituisce il presidente in caso di assenza o di impedimento.
3. In caso di vacanza prima dello scadere del mandato del presidente o del vicepresidente, si provvederà alla sua sostituzione. Il membro eletto per sostituire il presidente o il vicepresidente assicura le sue funzioni per la restante durata del mandato.

Articolo 4 RUOLO DEL PRESIDENTE

1. Il presidente rappresenta l'Autorità di controllo comune. Vigila sul suo buon funzionamento. Convoca l'Autorità di controllo comune e stabilisce il luogo, il giorno e l'ora delle riunioni. Apre e chiude le riunioni. Dirige le discussioni. Il presidente stabilisce l'ordine del giorno provvisorio.
2. Al fine di preparare le deliberazioni dell'Autorità di controllo comune, il presidente può designare, per un determinato tema, uno o più relatori tra i membri.

Articolo 5 FUNZIONAMENTO

1. L'Autorità di controllo comune si riunirà non meno di due volte l'anno. Si riunisce anche su iniziativa del presidente, in caso di richiesta motivata, scritta o orale, fatta in sede di riunione, di almeno tre delegazioni di cui all'articolo 2, par. 1. Si riunisce inoltre nei casi previsti dalla Convenzione.
2. Tranne nei casi ritenuti urgenti dal presidente, le convocazioni sono inviate almeno 14 giorni prima della riunione. La convocazione comprende l'ordine del giorno provvisorio della riunione e, eventualmente, la relativa documentazione.
3. L'Autorità di controllo comune adotta l'ordine del giorno definitivo all'inizio di ogni riunione.

Articolo 6 QUORUM E REGOLE DI MAGGIORANZA

1. L'Autorità di controllo comune può tenere una riunione valida solo se sono presenti almeno due terzi delle delegazioni di cui all'articolo 2, par. 1.
2. Fatte salve le disposizioni dell'articolo 13, le deliberazioni dell'Autorità di controllo comune sono adottate allorché la metà più uno delle delegazioni presenti di cui all'articolo 2, par. 1 si esprimono favorevolmente.
3. Ogni delegazione dispone della possibilità di depositare una nota esplicativa del voto.
4. L'Autorità di controllo comune delibera in base a documenti e progetti redatti nelle lingue nazionali degli Stati Schengen.

Articolo 7**PUBBLICITÀ E DESTINATARI DELLE DELIBERAZIONI**

1. Le riunioni dell'Autorità di controllo comune non sono pubbliche, salvo decisione contraria dell'Autorità di controllo comune.
2. L'Autorità di controllo comune stabilisce a chi trasmettere le sue deliberazioni nonché le modalità di una loro eventuale pubblicazione, fatto salvo il disposto dell'articolo 115, paragrafo 4 della Convenzione.

Articolo 8**PROCEDURA SCRITTA**

1. Le deliberazioni dell'Autorità di controllo comune possono essere adottate mediante una procedura scritta, a condizione che tutte le delegazioni ne abbiano accettato il principio nel corso di una riunione.
2. Il presidente può ricorrere d'ufficio alla procedura scritta in caso di urgenza.
3. In entrambi i casi, il presidente invia il progetto a tutti i membri dell'Autorità di controllo comune. Qualora le delegazioni non si oppongano a tale progetto entro un termine fissato dal presidente di almeno quattordici giorni, a decorrere dalla ricezione del progetto di deliberazione, esso verrà considerato approvato.
4. La procedura scritta nel caso di cui al paragrafo 2 del presente articolo cessa qualora una delegazione chieda, entro un termine di cinque giorni lavorativi, a decorrere dalla data di ricezione del progetto, di poterne discutere in seno all'Autorità di controllo comune.

Articolo 9**GRUPPI DI LAVORO, ESPERTI, VERIFICHE IN LOCO**

1. L'Autorità di controllo comune può istituire gruppi di lavoro definendone i compiti.
2. L'Autorità di controllo comune può far ricorso a esperti. Può elaborare un elenco di esperti ai quali si fa ricorso in via prioritaria.
3. Per quanto concerne il controllo della funzione di supporto tecnico, l'Autorità di controllo comune può designare uno o più dei suoi membri al fine di procedere a verifiche in loco. Se lo ritiene urgente, il presidente può procedere d'ufficio a tale designazione. In tal caso, ne informa senza indugio i membri dell'Autorità di controllo comune. I membri incaricati di effettuare verifiche possono farsi assistere da esperti che figurano nel summenzionato elenco.
4. I gruppi di lavoro, gli esperti e i membri dell'Autorità incaricati di procedere a verifiche riferiscono sull'esito delle stesse all'Autorità di controllo comune.

Articolo 10**SEGRETIARIATO**

1. Il Segretariato dell'Autorità di controllo comune è assicurato sotto la responsabilità del presidente dalle persone e dai servizi messi a disposizione dall'autorità competente della cooperazione Schengen.
2. Il Segretariato tiene un registro delle deliberazioni adottate dall'Autorità di controllo comune.
3. La corrispondenza destinata all'Autorità di controllo comune è indirizzata al Segretariato, all'attenzione del presidente.

Articolo 11 BILANCIO DELL'AUTORITÀ DI CONTROLLO COMUNE

All'Autorità di controllo comune è assegnato un bilancio, iscritto come linea autonoma nel bilancio Schengen, che le consente di realizzare il suo programma di lavoro annuale nel quadro delle attribuzioni che le sono conferite dalla Convenzione.

Articolo 12 VERBALI

1. E' redatto un verbale di ogni riunione dell'Autorità di controllo comune.
2. Sotto la responsabilità della presidenza, il Segretariato elabora il progetto di verbale. Tale progetto è sottoposto all'Autorità di controllo comune per approvazione nel corso della riunione successiva.
3. I membri e gli osservatori possono fare rettificare il verbale in un secondo tempo secondo le osservazioni da loro formulate nella relativa riunione.

Articolo 13 RISERVATEZZA

Fatta salva l'applicazione dell'articolo 7, paragrafo 2 i membri dell'Autorità di controllo comune, gli osservatori, gli esperti e i membri del Segretariato hanno l'obbligo della riservatezza. Tale obbligo non vige nei confronti delle autorità di controllo nazionali, né delle Autorità nazionali cui i membri e gli osservatori debbono riferire sulle loro attività secondo il diritto nazionale.

Articolo 14 MODIFICA DEL REGOLAMENTO

Le modifiche del presente regolamento sono adottate all'unanimità dall'Autorità di controllo comune. Tali modifiche entrano in vigore una settimana dopo la loro adozione salvo disposizioni contrarie.

9. PRINCIPI GENERALI APPLICABILI ALLE VISITE ED AI CONTROLLI DEL C.SIS

Scopo dei presenti principi è chiarire le modalità delle visite e dei controlli dell'Autorità di controllo comune (ACC) sul sito del C.SIS a Strasburgo.

Tali visite si collocano nel quadro dei compiti derivanti dall'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen (Convenzione di Schengen).

1) Tipi di visite

Le visite possono essere raccolte in due categorie:

- la visita d'informazione che, in generale, comprende la visita degli edifici, la presentazione generale del SIS e l'attività del C.SIS senza vera e propria consultazione della base dati. Può essere effettuata dall'ACC nella sua composizione plenaria;
- la visita di controllo che ha lo scopo di verificare la corretta esecuzione delle disposizioni della Convenzione di Schengen e che, in principio, viene effettuata da un gruppo ristretto di persone appositamente incaricato di tale compito dall'ACC.
- Tale gruppo di controllo è incaricato di verificare l'integrità, la qualità, la continuità, l'esclusività e la riservatezza del C.SIS nel quadro della Convenzione.

2) Informazione del Ministero dell'Interno

L'ACC informa il Ministero dell'Interno (direzione generale della polizia nazionale, direzione delle libertà pubbliche e degli affari giuridici, direzione delle trasmissioni e dell'informatica) della sua visita al C.SIS a Strasburgo.

L'ACC precisa la natura della visita, lo scopo, la lingua di lavoro e le soluzioni previste per ovviare alle difficoltà di ordine linguistico, la data prevista e la composizione del gruppo che effettua la visita.

3) Composizione del gruppo che effettua la visita

L'ACC determina la composizione del gruppo che effettua la visita o il controllo che può essere composto delle seguenti tre categorie di persone:

- membri dell'ACC e del Segretariato generale,
- membri e agenti delle autorità di controllo nazionali preposte alla protezione dei dati; --
- esperti esterni.

Un elenco nominativo, completo, viene trasmesso al Ministero dell'Interno. Alle visite di controllo possono partecipare solo i membri effettivi dell'ACC, il Segretariato generale e le persone abilitate e mandate dall'ACC.

In caso di ricorso ad esperti esterni che non figurano nell'elenco di cui all'articolo 9 del Regolamento interno dell'ACC, questa ne informa il Ministero dell'Interno con un mese d'anticipo.

4) Svolgimento della visita di controllo

All'inizio della visita di controllo il programma di lavoro preliminarmente stabilito dall'ACC viene comunicato ai responsabili del sito al fine di consentire loro di prendere le disposizioni del caso per rispondere alle domande poste dall'ACC.

5) Consultazione del sistema informatico

Il gestore del C.SIS impiega tutti i mezzi necessari per soddisfare in tempo reale le richieste di consultazione del sistema informatico formulate dall'Autorità di controllo comune. Provvede in particolare a mettere a sua disposizione un tecnico incaricato di procedere a operazioni manuali necessarie per soddisfare le summenzionate richieste.

6) Accesso ai documenti

L'ACC ha accesso a tutti i documenti riguardanti il C.SIS utili al suo compito.

Essa rispetta il carattere riservato dei documenti.

I documenti classificati "*secret défense*" debbono rimanere nella sede del C.SIS, ma sono accessibili all'ACC.

La consegna di copie di documenti è subordinata alla firma di una ricevuta.

7) Relazioni tecniche

Le relazioni tecniche sono e rimangono riservate nella misura in cui potrebbero rivelare aspetti operativi del sistema.

Prima di essere trasmesse alle autorità Schengen, esse vengono trasmesse ai responsabili del C.SIS perché formulino eventuali osservazioni.

10. COMPOSIZIONE DELLE DELEGAZIONI DELL'AUTORITÀ DI CONTROLLO COMUNE

Belgique

M. B. DE SCHUTTER

Commissie voor de bescherming van de persoonlijke levenssfeer

C/o Vrije Universiteit Brussel

Pleinlaan 2 – 1050 Brussel

Tel : 00 32 2 629 26 31

Fax : 00 32 2 629 26 62

Mme B. HAVELANGE

Commission de la protection de la vie privée

Bld de Waterloo 115 – 1000 Bruxelles

Tel : 00 32 2 542 72 00

Fax : 00 32 2 542 72 12

Pays-Bas

MM. P.J. HUSTINX & P.A. MICHAEL

Registratiekamer

Prins Clauslaan 20

Postbus 93374

25090 AJ's-Gravenhage

Tel : 00 31 70 381 13 00

Fax : 00 31 70 381 13 01

Espagne

M. D. Juan Manuel Fernandez LOPEZ

M. Miguel Angel Lopez HERRERO

Agence de Protection des Données

Paseo de la Castellana 41

28046 Madrid

Tel : 00 34 91 308 39 68/308 47 02

Fax : 00 34 91 308 46 92

Allemagne

M. J. JACOB, commissaire fédéral à la protection des données

Représenté par :

M. W. von POMMER ESCHÉ

Chef du département auprès du commissaire fédéral à la protection des données

Riemenschneiderstraße, 11

Tel : 00 49 228 81 99 50

Fax : 00 49 228 81 99 550

M. R. HAMM, commissaire du Land de Hesse à la protection des données

Représenté par :

Mme A. SCHRIEVER-STEINBERG

Uhlandstr. 4

65189 Wiesbaden

Tel : 00 49 611 1408 0

Fax : 00 49 611 37 85 79

France

M. A. TÜRK et Mme F. FOURETS

Suppléant M. O. COUTOR

CNIL

Rue Saint Guillaume, 21

75340 Paris Cedex 07

Tel : 00 33 1 53 73 22 22

Fax : 00 33 1 53 73 22 00

Portugal

M. J.A.M. LABESCAT da SILVA

M. Nuno Albuquerque MORAIS SARMENTO

Rua de S. Bento 148 3º Andar

1200 Lisbonne

Tel : 00 351 1 392 84 00

Fax : 00 351 1 397 68 32

Luxembourg

M. R. FABER et M. J.P. REITER, représentants effectifs

M. J. WAGNER et M. G. WIVENES, représentants suppléants

Secrétariat de l'Autorité de contrôle « Police »

Ministère de la Justice

L-2934 Luxembourg

Tel : 00 352 478 45 62

Fax : 00 352 227 661

Autriche

Mme W. KOTSCHY

Mme E. SOUHRADA-KIRCHMAYER

Ballhausplatz 1

A – 1014 Wien

Österreich

Tel : 00 43 1 531 15/2525

Fax : 00 43 1 53 115/2690

Italie

M. S. Neri

Tel : 00 390 667 60 46 93

Fax : 00 390 95 62 12 20

Fax : 00 390 6 676 096 78

M. BUTTARELLI

Garante per la protezione dei dati personali

Secretary general

Largo del Teatro Valle, 6

00186 Roma

Tel : 00 39 06 68 18 61

Fax : 00 39 06 68 18 669

Grèce

M. C. DAFERMOS

Suppléant M. G. DELYANNIS – D. KRINTZALIS

Autorité de protection des données à caractère personnel

Av. Omirou 8

Athenes 11 527
Tel : 00 301 33 52 604/5
Fax : 00 301 33 52 617

Islande : en tant qu'observateur

Ms. S. JÖHANNESDÓTTIR
Mr. T. ÖRLYGSSON
Data protection Commission
Ministry of Justice
Armarhvoll
150 Reykjavik
Islande
Tel : 00 354 560 90 10
Fax : 00 354 552 73 40

Danemark : en tant qu'observateur

Ms. Lotte N. JØRGENSEN
Registertilsynet
Christians Brygge 28 – 1553 KØBENHAVN V
Danemark
Tel : 00 45 33 14 38 44
Fax : 00 45 33 13 38 43

Suède : en tant qu'observateur

M. Ulf WIDEBÄCK
General-Director
Ms. B.M. WESTER
Supervisory Director
Datainspektionen
Box 8114
S – 104 20 Stockholm
Sweden
Tel : 00 46 8 657 61 00
Fax : 00 46 8 650 86 13

Norvège : en tant qu'observateur

M. G. APENES & Mme G. SLETTE MARK
Datatilsynet
Postboks 8177 Dep. 00 34 Oslo
Tel : 00 47 22 39 69 00
Fax : 00 47 22 42 23 50

Finlande : en tant qu'observateur

Mr. AARNIO – Head of Finnish delegation
Ms. M. KLEEMOLA
Office of the Data Protection Ombudsman
PL 315 Finland 00 181 Helsinki
Tel : 00 358 9 18 251
Fax : 00 358 9 18 25 7835

SCH.Aut-Cont (99) 8, 2a rev.

11. DATI INSERITI NEL SIS
DATI DA INSERIRE NEL SISTEMA D'INFORMAZIONE SCHENGEN (5 marzo 1999)

SEGNALAZIONI AGGIORNATE	AUSTRIA	BELGIO	GERMANIA	SPAGNA	FRANCIA	GRECIA	ITALIA	LUSS.	PAESI BASSI	PORT.	TOTALE
Banconote (BK)	47	0	210841	0	534310	0	77147	246	658	87	823336
Doc. Intatti (DB)	58	1242	58888	9366	7362	81	4940	5	166	96	82204
Armi (FA)	913	993	118030	16000	57584	8329	0	683	674	10219	2134425
Doc. d'identità (IC)	53961	1565	1531072	11306	1583359	749	1668496	3109	435691	4498	5293806
Veicoli (VE)	8500	31524	233897	121523	232820	37289	448852	1737	41315	17573	1175030
Personale ricercate (WP)	30276	4852	726205	22574	166403	48305	227812	730	9879	2019	1239055
TOTALE	93755	40176	2878933	180769	2581838	94753	2427247	6510	488383	93755	8826856

SCH.Aut-Cont (99) 8, 2a rev.

DATI INSERITI NEL SISTEMA D'INFORMAZIONE SCHENGEN (5 marzo 1999)

SEGNALAZIONI AGGIORNATE	TOTALE
BANCONOTE (BK)	823 336
DOCUMENTI INTATTI (DB)	82 204
ARMI (FA)	213 425
DOCUMENTI D'IDENTITA' (ID)	5 293 806
VEICOLI (VE)	1 175 030
PERSONE RICERCATE (WP)	1 239 055
TOTALE	8 826 856

12. INDICE CRONOLOGICO

1985

L'Accordo di Schengen è firmato il 14 giugno 1985 dai governi degli Stati dell'Unione economica del Benelux, della Repubblica federale di Germania e della Repubblica francese. E' provvisoriamente applicato il giorno successivo a quello della firma (articolo 32) ed entra in vigore il 2 marzo 1986.

1990

La Convenzione di applicazione dell'Accordo di Schengen, firmata dalle stesse Parti contraenti il 19 giugno 1990, sviluppa, per fini legati ai controlli alle frontiere esterne comuni, la cooperazione di polizia, doganale e giudiziaria.

Una delle misure fondamentali del dispositivo di cooperazione è la creazione di un sistema di informazione comune, il Sistema d'informazione Schengen (Titolo IV della Convenzione).

L'istituzione di questo sistema induce la creazione di un'autorità di controllo comune, sull'esempio di modelli nazionali di autorità di controllo indipendenti competenti in questo settore.

1992

E' istituita un'Autorità di controllo comune provvisoria (ACCP), presieduta dal sig. Faber (Lussemburgo) e composta di uno o due rappresentanti delle autorità di controllo nazionali dei cinque Stati fondatori e di uno o due esperti indipendenti designati dagli Stati aderenti sul cui territorio la Convenzione non è ancora stata messa in applicazione.

L'ACCP si riunisce dodici volte a Bruxelles tra il 29 giugno 1992 e il 22 febbraio 1995.

1993

Il Portogallo e la Spagna ratificano l'Accordo e la Convenzione di applicazione di Schengen.

1994

L'Autorità di controllo comune effettua la prima visita al sistema centrale di Strasburgo.

E' elaborato un questionario sulle norme di protezione dei dati applicabili negli Stati Schengen.

Viene eletto alla presidenza il sig. Von Pommer Esche (Germania), Capo di dipartimento presso il garante federale per la protezione dei dati.

1995

Il 26 marzo la Convenzione viene messa in applicazione nel territorio di sette paesi: Germania, Belgio, Spagna, Francia, Lussemburgo, Paesi Bassi e Portogallo. Lo stesso giorno viene istituita l'Autorità di controllo comune. Il Sistema d'informazione Schengen entra in servizio.

Tra il 17 maggio e il 14 dicembre dello stesso anno, l'ACC si riunisce 5 volte sotto la presidenza del sig. Von Pommer Esche.

Il 14 dicembre, il sig. Turk (Francia), senatore e membro della Commissione nazionale dell'Informatica e delle Libertà (CNIL), e il sig. Labescat (Portogallo), avvocato e membro della Commissione nazionale per la protezione dei dati, sono eletti rispettivamente presidente e vicepresidente dell'ACC.

1996

Il 2 febbraio è approvato il Regolamento interno dell'Autorità di controllo comune.

Il 19 dicembre, Danimarca, Finlandia e Svezia firmano l'Accordo di adesione a Schengen. Islanda e Norvegia siglano un Accordo di cooperazione in forza al quale la Convenzione di Schengen può essere applicata nel loro territorio. L'ACC si riunisce nove volte nel corso dell'anno. Partecipano ai lavori, con lo status di osservatori, rappresentanti indipendenti di Austria, Italia e Grecia.

L'ACC approva i principi di cooperazione tra le autorità nazionali di controllo in materia di esercizio del diritto di accesso.

1997

L'ACC si riunisce dieci volte tra il mese di marzo 1997 e il mese di marzo 1998. Fatta eccezione per la sessione annuale tenutasi a Lisbona in aprile 1997, tutte le riunioni si svolgono a Bruxelles.

Oltre alle riunioni plenarie, l'ACC si riunisce cinque volte in cerchia ristretta. Si tengono inoltre incontri tra rappresentanti dell'ACC ed esponenti del Ministero dell'Interno francese.

L'ACC vede riconoscere l'importanza del suo ruolo da parte degli organi esecutivi di Schengen. Viene dotata di un bilancio mediante una linea di gestione finanziaria autonoma e riceve con maggiore regolarità le informazioni necessarie per l'esercizio delle sue funzioni.

L'11 febbraio ha luogo il controllo presso il sistema centrale di Strasburgo, a seguito del quale l'ACC elabora una relazione contenente una serie di raccomandazioni sul funzionamento del sistema.

L'ACC elabora pareri sul progetto pilota relativo ai veicoli rubati, sull'accordo di cooperazione in materia di contestazione delle infrazioni stradali e di esecuzione delle relative sanzioni pecuniarie e sulla duplicazione di una parte delle segnalazioni SIS.

L'ACC approva la sua prima relazione di attività (marzo 1995 - marzo 1997) e la presenta al pubblico in aprile, nel quadro di una conferenza stampa organizzata a Lisbona.

Alla fine del 1997, il numero dei paesi che applicano la Convenzione passa a dieci: Germania, Austria, Belgio, Spagna, Francia, Grecia, Italia, Lussemburgo, Paesi Bassi e Portogallo. I rappresentanti delle autorità di controllo nazionali degli Stati nordici (Danimarca, Finlandia, Islanda, Norvegia e Svezia) partecipano ai lavori dell'ACC nella qualità di osservatori.

Il Sig. J. Labescat e B. De Schutter sono eletti rispettivamente presidente e vicepresidente dell'ACC.

1998

L'ACC formula pareri sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione, sull'usurpazione di identità e le conseguenze, per quanto riguarda il SIS, per il legittimo titolare dell'identità usurpata, sulla trasmissione di dati relativi ai veicoli rubati (dal SIS alla banca dati di Interpol), sul controllo di ammissibilità delle consultazioni SIS e sull'accesso ai dati SIS da parte degli uffici della motorizzazione.

Per la prima volta viene realizzato un controllo globale presso tutti gli uffici SIRENE, seguito da una serie di raccomandazioni relative al rafforzamento della sicurezza.

L'ACC segue i lavori di sviluppo del SIS I+ e gli studi preliminari sul SIS II.

Definisce un acquis comunitario nella prospettiva dell'integrazione di Schengen nell'Unione europea.

Promuove il primo colloquio sui "Diritti dei cittadini nei confronti dei sistemi d'informazione di polizia" ed una conferenza stampa a Lisbona.

Lancia la campagna "Il Sistema d'informazione Schengen vi riguarda" che prevede la distribuzione di poster e opuscoli informativi sui diritti dei cittadini nei punti di ingresso dello spazio Schengen (aeroporti, frontiere marittime, ecc.).

Il presidente dell'ACC partecipa per la prima volta ad una riunione del Comitato esecutivo ed assiste ad una riunione del Gruppo centrale a Strasburgo.

13. PROTOCOLLO DEL TRATTATO DI AMSTERDAM RELATIVO A SCHENGEN

LE ALTE PARTI CONTRAENTI,

RILEVANDO che gli accordi relativi all'eliminazione graduale dei controlli alle frontiere comuni firmati da alcuni Stati membri dell'Unione europea a Schengen il 14 giugno 1985 e il 19 giugno 1990, nonché gli accordi connessi e le norme adottate sulla base dei suddetti accordi mirano a promuovere l'integrazione europea e, in particolare, a consentire all'Unione europea di trasformarsi più rapidamente in uno spazio di libertà, di sicurezza e di giustizia;

DESIDEROSI di incorporare gli accordi e le norme summenzionati nel quadro dell'Unione europea,

CONFERMANDO che le disposizioni dell'*acquis* di Schengen sono applicabili solo se e nella misura in cui essi sono compatibili con l'Unione e il diritto comunitario;

TENENDO CONTO della particolare posizione della Danimarca;

TENENDO CONTO del fatto che l'Irlanda e il Regno Unito di Gran Bretagna e Irlanda del Nord non sono parti dei suddetti accordi e non li hanno firmati; che dovrebbero tuttavia essere previste disposizioni per consentire a tali Stati di accettare, in tutto o in parte, le disposizioni di tali accordi;

RICONOSCENDO che, pertanto, è necessario avvalersi delle disposizioni del trattato sull'Unione europea e del trattato che istituisce la Comunità europea relative ad una cooperazione rafforzata tra alcuni Stati membri e che a tali disposizioni si dovrebbe fare ricorso solo in ultima istanza;

TENENDO CONTO della necessità di mantenere un rapporto speciale con la Repubblica d'Islanda e il Regno di Norvegia, Stati che hanno entrambi confermato la loro intenzione di essere vincolati dalle disposizioni summenzionate, in base all'accordo firmato a Lussemburgo il 19 dicembre 1996,

HANNO CONVENUTO le seguenti disposizioni, che sono allegate al trattato sull'Unione europea e al trattato che istituisce la Comunità europea;

ARTICOLO 1

Il Regno del Belgio, il Regno di Danimarca, la Repubblica federale di Germania, la Repubblica ellenica, il Regno di Spagna, la Repubblica francese, la Repubblica italiana, il Granducato di Lussemburgo, il Regno dei Paesi Bassi, la Repubblica d'Austria, la Repubblica portoghese, la Repubblica di Finlandia e il Regno di Svezia, firmatari degli accordi di Schengen, sono autorizzati a instaurare tra loro una cooperazione rafforzata nel campo di applicazione di tali accordi e delle disposizioni collegate, quali sono elencati nell'allegato del presente protocollo, in prosieguo denominato *acquis* di Schengen. Tale cooperazione è realizzata nell'ambito istituzionale e giuridico dell'Unione europea e nel rispetto delle pertinenti disposizioni del trattato sull'Unione europea e del trattato che istituisce la Comunità europea.

ARTICOLO 2

1. A decorrere dall'entrata in vigore del trattato di Amsterdam, l'*acquis* di Schengen, incluse le decisioni del Comitato esecutivo istituito dagli accordi di Schengen che sono state adottate anteriormente a tale data, si applica immediatamente ai tredici Stati membri di cui all'articolo 1, fatte salve le disposizioni del paragrafo 2 del presente articolo. A decorrere dalla medesima data, il Consiglio si sostituirà al suddetto Comitato esecutivo.

Il Consiglio, deliberando all'unanimità dei membri di cui all'articolo 1, adotta le disposizioni necessarie per l'attuazione del presente paragrafo. Il Consiglio, deliberando all'unanimità, determina, in base alle pertinenti disposizioni dei trattati, la base giuridica di ciascuna delle disposizioni o decisioni che costituiscono l'*acquis* di Schengen.

Relativamente a tali disposizioni e decisioni e in base a detta determinazione delle basi giuridiche, la Corte di giustizia delle Comunità europee esercita le competenze conferitele dalle pertinenti disposizioni applicabili dei trattati. La Corte di giustizia non è comunque competente per quanto concerne le misure e le decisioni relative al mantenimento dell'ordine pubblico e alla salvaguardia

della sicurezza interna.

Fino all'adozione delle misure di cui sopra è fatto salvo l'articolo 5, paragrafo 2, le disposizioni o decisioni che costituiscono l'*acquis* di Schengen sono considerate atti fondati sul titolo VI del trattato sull'Unione europea.

2. Le disposizioni del paragrafo 1 si applicano agli Stati membri che hanno firmato protocolli di adesione agli accordi di Schengen a decorrere dalle date stabilite dal Consiglio, che delibera all'unanimità dei Membri di cui all'articolo 1, a meno che le condizioni per l'adesione di uno di tali Stati all'*acquis* di Schengen siano soddisfatte prima dell'entrata in vigore del trattato di Amsterdam.

ARTICOLO 3

A seguito della determinazione di cui all'articolo 2, paragrafo 1, secondo comma, la Danimarca mantiene rispetto agli altri firmatari degli accordi di Schengen gli stessi diritti e gli stessi obblighi che aveva anteriormente a detta determinazione per quanto concerne le parti dell'*acquis* di Schengen la cui base giuridica è individuata nel titolo III bis del trattato che istituisce la Comunità europea.

Per quanto attiene alle parti dell'*acquis* di Schengen la cui base giuridica è individuata nel titolo VI del trattato sull'Unione europea, la Danimarca mantiene gli stessi diritti e gli stessi obblighi degli altri firmatari degli accordi di Schengen.

ARTICOLO 4

L'Irlanda e il Regno Unito di Gran Bretagna e Irlanda del Nord, i quali non sono vincolati dall'*acquis* di Schengen, possono, in qualsiasi momento, chiedere di partecipare, in tutto o in parte, alle disposizioni di detto *acquis*.

Il Consiglio decide in merito a tale richiesta all'unanimità dei suoi membri di cui all'articolo 1 e del rappresentante del governo dello Stato interessato.

ARTICOLO 5

1. Le proposte e le iniziative che si baseranno sull'*acquis* di Schengen sono soggette alle pertinenti disposizioni dei trattati.

In tale contesto, laddove l'Irlanda o il Regno Unito, o entrambi, non abbiano notificato per iscritto al Presidente del Consiglio, entro un congruo periodo di tempo, che desiderano partecipare, l'autorizzazione di cui all'articolo 5 A del trattato che istituisce la Comunità europea o all'articolo K.12 del trattato sull'Unione europea si considera concessa agli Stati membri di cui all'articolo 1 nonché all'Irlanda e al Regno Unito, laddove uno di essi desideri partecipare ai settori di cooperazione in questione.

2. Le pertinenti disposizioni dei trattati di cui al paragrafo 1, primo comma, si applicano anche nel caso in cui il Consiglio non abbia adottato le misure di cui all'articolo 2, paragrafo 1, secondo comma.

ARTICOLO 6

La Repubblica di Islanda e il Regno di Norvegia sono associati all'attuazione dell'*acquis* di Schengen e al suo ulteriore sviluppo, in base all'accordo firmato a Lussemburgo il 19 dicembre 1996. A tal fine vengono concordate procedure appropriate in un accordo che sarà concluso con tali Stati dal Consiglio, che delibera all'unanimità dei suoi membri di cui all'articolo 1. Tale accordo include disposizioni relative al contributo dell'Islanda e della Norvegia ad ogni conseguenza finanziaria derivante dall'attuazione del presente protocollo.

Il Consiglio, deliberando all'unanimità, conclude con l'Islanda e la Norvegia un accordo separato, al fine di stabilire i diritti e gli obblighi fra l'Irlanda e il Regno Unito di Gran Bretagna e Irlanda del Nord, da un lato, e l'Islanda e la Norvegia, dall'altro, nei settori dell'*acquis* di Schengen che riguardano tali Stati.

ARTICOLO 7

Il Consiglio, che delibera a maggioranza qualificata, adotta le modalità relative all'integrazione del Segretariato Schengen nel Segretariato Generale del Consiglio.

ARTICOLO 8

Ai fini dei negoziati relativi all'adesione di nuovi Stati membri all'Unione europea, l'*acquis* di Schengen e le ulteriori misure adottate dalle istituzioni nell'ambito del suo campo d'applicazione sono considerati un *acquis* che deve essere accettato integralmente da tutti gli Stati candidati all'adesione.

ALLEGATO

ACQUIS DI SCHENGEN

1. L'accordo, firmato a Schengen il 14 giugno 1985, tra i Governi degli Stati dell'Unione economica del Benelux, la Repubblica federale di Germania e la Repubblica francese, relativo all'eliminazione graduale dei controlli alle frontiere comuni.
2. La Convenzione, firmata a Schengen il 19 giugno 1990, tra il Regno del Belgio, la Repubblica federale di Germania, la Repubblica francese, il Granducato di Lussemburgo e il Regno dei Paesi Bassi, recante applicazione dell'accordo relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmato a Schengen il 14 giugno 1985, nonché l'atto finale e le dichiarazioni comuni relativi.
3. I protocolli e gli accordi di adesione all'accordo del 1985 e la Convenzione di applicazione del 1990 con l'Italia (firmata a Parigi il 27 novembre 1990), la Spagna e il Portogallo (entrambe firmate a Bonn il 25 giugno 1991), la Grecia (firmata a Madrid il 6 novembre 1992), l'Austria (firmata a Bruxelles il 28 aprile 1995) e la Danimarca, la Finlandia e la Svezia (tutte firmate a Lussemburgo il 19 dicembre 1996), con i relativi atti finali e dichiarazioni.
4. Le decisioni e le dichiarazioni adottate dal Comitato esecutivo istituito dalla Convenzione di applicazione del 1990, nonché gli atti per l'attuazione della Convenzione adottati dagli organi cui il Comitato esecutivo ha conferito poteri decisionali.

PAGINA BIANCA

6.5. AUTORITÀ COMUNE DI CONTROLLO EUROPOL

6.5.1. ATTO N. 1/99 DELL'AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL del 22 aprile 1999 che stabilisce il proprio regolamento interno (1999/C 149/01)

L'Autorità di controllo comune
vista la convenzione, basata sull'articolo K.3 del trattato sull'Unione europea, che istituisce un ufficio europeo di polizia (convenzione Europol)(1), in particolare l'articolo 24, paragrafo 7, considerando che spetta all'autorità di controllo comune stabilire, con decisione presa all'unanimità, il proprio regolamento interno, ha adottato il seguente regolamento interno:

Regolamento interno dell'Autorità di controllo comune dell'Europol

SOMMARIO

Titolo I

FUNZIONI E COMPETENZE DELL'AUTORITÀ DI CONTROLLO COMUNE

Articolo 1

FUNZIONI

1. L'autorità di controllo comune è incaricata di vigilare, nel rispetto della convenzione, sull'attività dell'Europol per accertarsi che la memorizzazione, il trattamento e l'utilizzazione dei dati in possesso dei servizi dell'Europol non ledano i diritti della persona. Essa controlla inoltre la legittimità della trasmissione dei dati provenienti dall'Europol (articolo 24, paragrafo 1, prima e seconda frase, della convenzione).

2. A tal fine, l'autorità di controllo comune svolge in particolare le seguenti funzioni:

- a) esame delle decisioni costitutive degli archivi (articolo 12, paragrafo 1, seconda frase, e paragrafo 2, terza frase, della convenzione);
- b) esame delle disposizioni relative alla stesura delle relazioni sul richiamo di dati di carattere personale (articolo 16, prima frase, della convenzione);
- c) esame delle norme generali per la trasmissione di dati di carattere personale da parte dell'Europol agli Stati e ad organismi terzi (articolo 18, paragrafo 2, seconda frase, della convenzione);
- d) esame delle questioni relative a:
 - applicazione e interpretazione della convenzione connesse con l'attività dell'Europol per quanto riguarda il trattamento e l'utilizzazione di dati di carattere personale (articolo 24, paragrafo 3, primo caso, della convenzione),
 - controllo indipendente effettuato dalle autorità di controllo degli Stati membri (articolo 24, paragrafo 3, secondo caso, della convenzione),
 - esercizio del diritto all'informazione (articolo 24, paragrafo 3, terzo caso, della convenzione),
 - elaborazione di proposte armonizzate in vista di soluzioni comuni ai problemi che si presentano (articolo 24, paragrafo 3, quarto caso, della convenzione);
- e) verifica della legittimità e della correttezza dell'eventuale memorizzazione, rilevamento, trattamento ed utilizzazione di dati di carattere personale da parte dell'Europol su richiesta dell'interessato (articolo 24, paragrafo 4, della convenzione);
- f) stesura periodica di relazioni di attività (articolo 24, paragrafo 6, della convenzione).

Articolo 2**COMPETENZE**

1. Nello svolgimento delle sue mansioni, l'autorità di controllo comune è dotata delle competenze conferitele dalla convenzione.

2. In particolare, l'autorità di controllo comune è autorizzata ad ottenere informazioni dall'Europol, ad ottenere l'accesso a tutti i documenti e agli archivi cartacei, nonché a qualsiasi altra informazione memorizzata dall'Europol, nonché ad ottenere libero accesso in qualsiasi momento a tutti i locali dell'Europol (articolo 24, paragrafo 2, della convenzione). Ciò include l'informazione su hardware e software e l'accesso ai medesimi, ogniqualvolta sia necessario per lo svolgimento delle funzioni dell'autorità di controllo comune. Le modalità possono essere fissate in accordi tra l'autorità di controllo comune e il consiglio di amministrazione dell'Europol.

Articolo 3**Comitati**

1. L'autorità di controllo comune istituisce il comitato di cui all'articolo 24, paragrafo 7, della convenzione.

2. Può istituire una o più commissioni interne e determinarne la composizione e le competenze (articolo 24, paragrafo 8, della convenzione).

Titolo II**REGOLAMENTO INTERNO DELL'AUTORITÀ DI CONTROLLO COMUNE****Articolo 4****COMPOSIZIONE**

1. L'autorità di controllo comune è composta da al massimo due membri o rappresentanti di ciascuna delle autorità di controllo nazionali che costituiscono una delegazione. Ciascun membro può avere un supplente. I membri dell'autorità di controllo comune e i loro supplenti sono nominati per cinque anni dai rispettivi Stati membri (articolo 24, paragrafo 1, terza frase, della convenzione); tale mandato è rinnovabile.

2. I membri dell'autorità di controllo comune e i loro supplenti sono indipendenti, non ricevono istruzioni nello svolgimento delle loro mansioni e sono soggetti soltanto alla legge. In particolare, essi non devono essere contemporaneamente membri di un altro organismo istituito secondo la convenzione o far parte del personale dell'Europol.

In casi di conflitto di interessi, la persona interessata notifica tale interesse e non partecipa alle discussioni e alle decisioni sul caso e può, ove necessario, essere esclusa a maggioranza dei voti espressi a scrutinio segreto dalle delegazioni che partecipano alla riunione. La persona interessata viene ascoltata prima che si proceda all'esclusione, ma non partecipa alla decisione. Una persona che si ritiri o venga esclusa può farsi sostituire dal supplente.

3. Possono essere nominati membri dell'autorità di controllo comune o supplenti solo coloro che posseggono le capacità richieste (articolo 24, paragrafo 1, terza frase, della convenzione). Particolare attenzione viene rivolta ai requisiti relativi alla designazione del comitato per i ricorsi.

4. Qualora un membro dell'autorità di controllo comune non possa assistere ad una riunione, può farsi rappresentare dal suo supplente.

5. La carica di membro dell'autorità di controllo comune termina quando la persona in questione si dimette o cessa di essere membro o rappresentante dell'autorità di controllo nazionale, a meno che il suo mandato sia confermato dallo Stato membro interessato. La nomina a membro non può essere revocata se non in base alla legislazione nazionale. La presente disposizione si applica, con gli opportuni adattamenti, anche ai supplenti.

Articolo 5**PRESIDENZA**

1. L'autorità di controllo comune elegge al suo interno un presidente e un vicepresidente a maggioranza di due terzi dei voti espressi, a scrutinio segreto, dalle delegazioni presenti. Il vice-

presidente non può essere membro della delegazione del presidente. Se nessuno dei candidati ottiene la maggioranza richiesta nel primo turno di votazione, si procede a un secondo turno tra i due candidati che hanno ottenuto il maggior numero di voti. Il presidente e il vicepresidente sono eletti per un periodo di due anni, prorogabile per un secondo mandato di un anno.

2. Il presidente rappresenta l'autorità di controllo comune e ne presiede le riunioni. Egli vigila sul corretto andamento dei lavori; convoca le riunioni dell'autorità di controllo comune e ne fissa il luogo, la data e l'ora. Apre e chiude le sedute, prepara l'ordine del giorno provvisorio e assicura l'esecuzione delle decisioni dell'autorità di controllo comune.

3. In caso di assenza del presidente, il vicepresidente ne fa le veci. In assenza del vicepresidente, il membro più anziano in termini di età fa le veci del vicepresidente. La prima riunione dell'autorità di controllo comune è convocata e presieduta dal membro più anziano in termini di età sino all'elezione del presidente.

4. L'autorità di controllo comune può, al fine di preparare i propri lavori in merito a questioni particolari, nominare tra i propri membri, su proposta del presidente, uno o più relatori. In caso d'urgenza, il presidente può procedere a tale nomina direttamente. In tal caso egli ne informa senza indugio i membri dell'autorità di controllo comune.

5. Il presidente o la maggioranza delle delegazioni possono chiedere la presenza del direttore alle riunioni e invitare ad esse membri del personale dell'Europol, esperti nazionali, ufficiali di collegamento e altre persone.

Articolo 6

METODI DI LAVORO

1. L'autorità di controllo comune si riunisce almeno quattro volte all'anno. Si riunisce altresì su iniziativa del presidente e ogniqualvolta almeno tre delegazioni presentino una richiesta scritta motivata ovvero una proposta orale nel corso di una precedente riunione. Il presidente del consiglio di amministrazione e il direttore dell'Europol possono proporre punti da iscrivere all'ordine del giorno e proporre la convocazione dell'autorità di controllo comune.

2. Ad eccezione dei casi ritenuti urgenti dal presidente, la notifica della convenzione della riunione deve giungere almeno due settimane prima della riunione e ad essa vengono acclusi l'ordine del giorno provvisorio e i documenti necessari per la riunione, a meno che la natura dei documenti stessi non lo consenta. L'ordine del giorno definitivo viene adottato all'inizio di ogni riunione.

3. Le riunioni dell'autorità di controllo comune sono valide solo se vi partecipano almeno i due terzi delle delegazioni. Le decisioni vengono adottate a maggioranza semplice delle delegazioni presenti, salvo che il presente regolamento interno disponga diversamente. Ciascuna delegazione ha diritto a un voto. In caso di parità, prevale il voto del presidente.

4. Le riunioni dell'autorità di controllo comune non sono pubbliche. I suoi documenti sono riservati, a meno che l'autorità di controllo comune disponga diversamente. Tuttavia, i documenti trasmessi dall'Europol sono soggetti alle norme sulla segretezza di cui all'articolo 31, paragrafo 1, della convenzione.

5. L'autorità di controllo comune si riunisce sulla base di documenti e progetti redatti in tutte le lingue ufficiali delle istituzioni dell'Unione europea. Sono ammesse deroghe a tale regola solo in casi di urgenza. Tuttavia, ogni delegazione ha il diritto di chiedere una traduzione nella propria lingua.

6. Le decisioni dell'autorità di controllo comune possono essere adottate tramite procedura scritta, sempreché tale procedura sia stata approvata da tutte le delegazioni in riunione. In casi urgenti il presidente è autorizzato a ricorrere alla procedura scritta. In entrambi i casi il presidente trasmette un progetto di decisione ai membri dell'autorità di controllo comune. Se le delegazioni non si oppongono al progetto di decisione, tradotto nelle rispettive lingue ufficiali, entro un termine stabilito dal presidente e non inferiore a 14 giorni dalla notifica, la proposta è considerata adottata. Qualora entro cinque giorni lavorativi dalla notifica del progetto di decisione, una delegazione chieda un dibattito orale in sede di autorità di controllo comune, la procedura scritta viene sospesa.

Articolo 7**CONTROLLI IN LOCO ED ESPERTI**

1. Nell'ambito delle competenze conferite dall'articolo 24 della convenzione, l'autorità di controllo comune può eseguire controlli sulla protezione dei dati presso l'Europol.

2. L'autorità di controllo comune può nominare uno o più membri incaricati di eseguire questi controlli. Tali membri possono essere assistiti da esperti, nel modo ritenuto appropriato dall'autorità di controllo comune. Tali esperti sono selezionati unicamente da un elenco preventivamente stilato dall'autorità di controllo comune e da essa comunicato all'Europol. Gli esperti figuranti in tale elenco devono provenire dalle autorità di controllo nazionali e da organismi delle amministrazioni pubbliche, tranne nel caso in cui siffatti esperti non siano disponibili. Tutti gli esperti devono soddisfare i requisiti di sicurezza in vigore secondo i rispettivi diritti nazionali.

3. Per motivi di urgenza, il presidente può procedere alla nomina di tali membri ed esperti direttamente. In questo caso ne informa senza indugio i membri dell'autorità di controllo comune.

4. I membri dell'autorità di controllo comune incaricati di effettuare un controllo riferiscono alla medesima in merito ai risultati della loro attività.

Articolo 8**PROCEDURA IN CASO DI VIOLAZIONI**

Qualora l'autorità di controllo comune constati violazioni di disposizioni della convenzione per quanto riguarda la memorizzazione, il trattamento o l'utilizzazione di dati di carattere personale, ne informa il direttore dell'Europol e gli chiede una risposta scritta entro un termine stabilito. L'autorità di controllo comune, se ritiene che la risposta non sia sufficiente o non sia stata trasmessa per tempo, ovvero se sorgono altre difficoltà, interpella per iscritto il consiglio di amministrazione (articolo 24, paragrafo 5, terza frase della convenzione). La mancata esecuzione di una decisione definitiva del comitato per i ricorsi è considerata una violazione della convenzione.

Articolo 9**PROCESSO VERBALE**

Di ogni riunione dell'autorità di controllo comune è redatto un processo verbale. Il progetto di verbale è preparato dal segretariato sotto la direzione del presidente e sottoposto all'autorità di controllo comune per l'adozione nella successiva riunione. Ciascun membro ha il diritto di far modificare il processo verbale affinché rispecchi le osservazioni da esso formulate nel corso della riunione.

Articolo 10**RELAZIONE DI ATTIVITÀ**

1. L'autorità di controllo comune redige una relazione di attività almeno ogni due anni. Almeno un mese prima che tale relazione sia trasmessa al Consiglio, il consiglio di amministrazione ha la possibilità di esprimere un parere, che viene allegato alla relazione (articolo 24, paragrafo 6 della convenzione).

2. L'autorità di controllo comune decide di pubblicare o meno la relazione di attività e, nel primo caso, decide in merito alle modalità della pubblicazione.

Titolo III**REGOLAMENTO INTERNO DEL COMITATO PER I RICORSI****Articolo 11****FUNZIONI DEL COMITATO PER I RICORSI**

1. Il comitato per i ricorsi (in prosieguo denominato "il comitato") esamina i ricorsi previsti nell'articolo 19, paragrafi 6, 7 e 8, nell'articolo 20, paragrafo 4, e nell'articolo 22, paragrafo 3, della convenzione.

2. Il comitato adotta le decisioni definitive in merito alle questioni di cui al paragrafo 1.

3. Oltre alle competenze di cui all'articolo 2, paragrafo 2, il comitato è dotato dei poteri previsti dal presente capitolo.

Articolo 12**Composizione**

1. Il comitato è composto da un membro di ciascuna delegazione dell'autorità di controllo comune. Ogni membro può avere un supplente. I membri del comitato e i loro supplenti sono nominati per un periodo di cinque anni dall'autorità di controllo comune, su designazione della delegazione interessata. Il loro mandato è rinnovabile.

2. I membri del comitato e i loro supplenti devono possedere le qualifiche necessarie per esaminare e deliberare in merito ai ricorso di cui all'articolo 1, paragrafo 1, che comprendono tra l'altro conoscenze specialistiche in campo giuridico ed esperienza in materia di risoluzione delle controversie e di protezione dei dati.

3. Qualora un membro del comitato non possa assistere ad una riunione, egli può farsi rappresentare dal suo supplente.

4. La qualifica di membro del comitato viene meno quando la persona interessata si dimette o cessa di essere membro dell'autorità di controllo comune. Tale disposizione si applica altresì ai supplenti.

Articolo 13**INDIPENDENZA E IMPARZIALITÀ**

1. Nello svolgimento delle loro mansioni i membri del comitato sono indipendenti e imparziali, non sono vincolati dalle istruzioni dell'autorità di controllo comune o di chiunque altro e sono soggetti soltanto alla legge. Per tutta la durata del loro mandato essi non possono svolgere attività incompatibili con i requisiti di indipendenza e imparzialità prescritti loro in quanto membri del comitato o con la disponibilità richiesta a tale fine. Le attività che sono o sono state svolte per conto dell'autorità nazionale di controllo non sono considerate incompatibili con l'attività svolta nel comitato. Le disposizioni del presente paragrafo si applicano altresì ai supplenti.

2. Qualora un membro del comitato o un supplente sia stato coinvolto nel caso in modo tale da dare adito a seri dubbi in ordine alla sua imparzialità, o in qualsiasi altra circostanza che possa recare pregiudizio alla corretta deliberazione su un ricorso, egli rende nota la sua posizione e si ritira dal caso.

3. Se una parte ricusa un membro o un supplente per i motivi di cui ai paragrafi 1 e 2, il comitato ascolta la persona interessata nonché le altre parti, quindi decide sulla questione in assenza della persona interessata e a scrutinio segreto.

4. Qualora una persona si dimetta o venga esclusa dal caso a norma del paragrafo 3, essa viene sostituita dal supplente.

Articolo 14**PRESIDENZA**

1. Il comitato elegge al suo interno un presidente e un vicepresidente a maggioranza di due terzi dei voti espressi, a scrutinio segreto, dai membri presenti. Qualora nessun candidato ottenga la maggioranza richiesta al primo turno di votazioni, ha luogo un secondo turno tra i due candidati che hanno ricevuto il maggior numero di voti. Il presidente o il vicepresidente dell'autorità di controllo comune non può essere eletto presidente o vicepresidente del comitato né essere membro della stessa delegazione. Il presidente e il vicepresidente vengono eletti per un periodo di due anni. Essi possono essere eletti per un secondo mandato di un anno.

2. Il presidente presiede le riunioni e vigila sul corretto andamento dei lavori. Convoca le riunioni del comitato, ne fissa il luogo, la data e l'ora e prepara l'ordine del giorno provvisorio.

3. In caso di assenza del presidente, il vicepresidente ne fa le veci. In assenza del vicepresidente, il membro più anziano in termini di età fa le veci del vicepresidente. La prima riunione del comitato è convocata e presieduta dal membro più anziano in termini di età fino all'elezione del presidente.

4. Il comitato può, al fine di preparare le sue deliberazioni, nominare tra i propri membri, su proposta del presidente, uno o più relatori. In tali casi, il membro designato quale relatore appartiene in linea di massima allo Stato membro da cui proviene il ricorrente oppure, se il ricorrente proviene da uno Stato terzo, allo Stato membro cui il caso è più strettamente connesso. In caso d'urgenza, il presidente può procedere a tale nomina direttamente. In tal caso egli ne informa senza indugio i membri del comitato. Il relatore esamina il ricorso e presenta al comitato una relazione sulla sua ammissibilità nonché una proposta relativa ad ulteriori procedimenti con particolare riguardo alle misure preparatorie necessarie.

Articolo 15**RAPPRESENTANZA**

Il ricorrente può essere assistito o rappresentato da un avvocato o da un altro consulente. Il comitato può decidere di escludere dal procedimento un avvocato o un consulente in caso di comportamento gravemente scorretto. In caso di esclusione il presidente fissa un termine per consentire alla parte interessata di designare un altro avvocato o consulente; il procedimento è sospeso fino alla scadenza di tale termine. L'avvocato o il consulente esibisce, su richiesta del comitato, il mandato conferitogli dal ricorrente.

Articolo 16**LINGUE**

1. I lavori vengono svolti in una delle lingue ufficiali delle istituzioni dell'Unione europea. Il ricorrente sceglie la lingua ufficiale del procedimento. Questa è utilizzata nelle dichiarazioni orali e nei documenti scritti delle parti, nonché nei processi verbali e nelle decisioni del comitato.

2. I documenti redatti in una lingua diversa da quella del procedimento sono corredati di una traduzione in tale lingua. In caso di documenti molto lunghi, la traduzione può limitarsi a estratti o sunti. Il comitato può trasmettere in qualsiasi momento, in virtù delle sue competenze o su richiesta di una delle parti, una traduzione completa.

3. Se necessario, i servizi di interpretazione e traduzione vengono forniti, a titolo gratuito, a ogni membro del comitato e alle parti. Le decisioni del comitato sono tradotte in tutte le lingue ufficiali delle istituzioni dell'Unione europea.

4. Qualora il ricorrente non conosca nessuna delle lingue ufficiali delle istituzioni dell'Unione europea, la denuncia può essere presentata in un'altra lingua. Il ricorrente è tenuto a presentare un sunto in una delle lingue ufficiali. Il presidente o il relatore fa tradurre la denuncia nella lingua scelta.

Articolo 17**ISTRUZIONE DELLA PROCEDURA**

1. Il ricorso viene introdotto mediante denuncia scritta depositata presso il segretario dell'autorità di controllo comune entro tre mesi dalla data di ricezione della decisione dell'Europol da parte del ricorrente. In mancanza di una decisione, il ricorso è introdotto entro tre mesi dalla data di scadenza dei termini di cui all'articolo 19, paragrafo 6, all'articolo 20, paragrafo 4, e all'articolo 22, paragrafo 3, della convenzione. Qualsiasi dubbio in merito all'osservanza dei termini è risolto a favore del ricorrente.

2. Il ricorrente espone i motivi del ricorso. Nella denuncia devono risultare chiari l'identità del ricorrente, l'oggetto del ricorso e le motivazioni. La denuncia è corredata dell'eventuale documentazione giustificativa disponibile. Il ricorrente può ritirare la denuncia in qualsiasi momento.

3. Il segretario notifica l'avvenuto ricevimento della denuncia entro quattro settimane e fornisce informazioni generali sullo svolgimento futuro del procedimento.

4. Se la denuncia non soddisfa i requisiti di cui al paragrafo 2, prima e seconda frase, e all'articolo 16, paragrafo 4, seconda frase, il segretario invita il ricorrente a rettificare eventuali omissioni entro quattro settimane.

5. Il comitato respinge, su proposta del presidente o del relatore, i ricorsi che non soddisfino i requisiti previsti. Un ricorso presentato oltre i termini di cui al paragrafo 1 può essere accolto qualora il ritardo sia dovuto a circostanze particolari.

Articolo 18**ESAME PRELIMINARE**

1. Se la denuncia soddisfa i requisiti stabiliti, essa viene esaminata dal comitato in base alle disposizioni seguenti, che tengono conto della convenzione, in particolare degli articoli 19, 20 e 22.

2. Copia della denuncia viene trasmessa all'Europol affinché comunichi le proprie osservazioni, che vengono presentate entro quattro settimane, prorogabili di altre due settimane.

3. Il comitato può decidere, in singoli casi, di coinvolgere nella procedura di ricorso anche una o più unità nazionali. Il ricorrente e l'Europol sono informati della decisione. Copia delle osservazioni dell'Europol e del ricorrente è in tal caso trasmessa alle pertinenti unità nazionali affinché, entro quat-

tro settimane, prorogabili di altre due settimane, possano presentare le proprie osservazioni.

4. Una volta ricevute le osservazioni o scaduti i termini, il comitato dispone di tre mesi di tempo per esaminare la denuncia.

Articolo 19

INFORMAZIONI SUPPLEMENTARI

1. Il comitato può chiedere al ricorrente, all'Europol, alle unità nazionali, alle autorità di controllo nazionali o ad altri organi di fornirgli informazioni, elementi di prova o osservazioni. Le parti hanno il diritto di presentare al comitato suggerimenti riguardo all'assunzione delle prove o di chiedere l'ammissione degli elementi di prova. Il comitato esamina attentamente tali suggerimenti e richieste di ammissione nella misura necessaria all'esame del caso.

2. Il comitato può anche decidere di effettuare ispezioni in loco presso l'Europol. Si applica parimenti l'articolo 7. In tal caso il ricorrente o il suo consulente sono informati dell'esito delle ispezioni.

Articolo 20

ACCESSO AGLI ATTI DEL PROCEDIMENTO

1. Tutte le parti hanno, se lo desiderano, accesso agli atti del procedimento e possono chiedere al segretariato dell'autorità di controllo comune di fornire loro, a proprie spese, estratti o fotocopie. L'accesso è negato qualora ciò sia necessario:

- per il corretto svolgimento delle funzioni dell'Europol;
 - per la tutela della sicurezza e dell'ordine pubblico negli Stati membri o per la prevenzione della criminalità;
 - per la protezione dei diritti e delle libertà di terzi,
- tutti casi nei quali non possono essere invocati gli interessi della persona in questione.

2. L'Europol, le unità nazionali e le autorità di controllo nazionali possono indicare in quale misura le informazioni da essi fornite non debbano essere messe a disposizione del ricorrente, specificando le ragioni di tale limitazione. Il comitato può chiedere ulteriori motivazioni. Se il comitato ritiene accettabili tali motivazioni, le informazioni in questione non vengono trasmesse. Il comitato può decidere diversamente, all'unanimità, solo in assenza di motivi accettabili. In tal caso il comitato può decidere di richiedere un sunto da mettere a disposizione del ricorrente o chiedere che talune informazioni vengano fornite a quest'ultimo.

Articolo 21

AUDIZIONI

1. Le parti, qualora ne facciano richiesta, sono sentite dal comitato. Il comitato informa debitamente le parti del loro diritto di essere sentite. Tale diritto si esercita per iscritto. Il comitato decide di ricorrere a una audizione orale su richiesta di una delle parti del procedimento, nella misura ritenuta necessaria per l'esame del caso. Il comitato informa debitamente le parti del loro diritto di essere sentite. Tutte le parti vengono informate a tempo debito dell'audizione orale e hanno il diritto di presenziarvi.

2. L'audizione è pubblica a meno che il comitato decida, d'ufficio o su richiesta di una delle parti, di escludere totalmente o parzialmente il pubblico qualora lo rendano necessario motivi di pubblica sicurezza, in particolare i motivi di cui all'articolo 19, paragrafo 3, della convenzione, o la tutela della vita privata di una persona, oppure nella misura strettamente necessaria, a giudizio del comitato, in particolari circostanze in cui la pubblicità potrebbe recare pregiudizio alla corretta decisione del ricorso. Qualora uno Stato membro coinvolto nella procedura oppure l'Europol richiedano di non ammettere il pubblico, il comitato può decidere diversamente, all'unanimità, solo in assenza dei motivi menzionati alla frase 1.

3. Il comitato può decidere, su richiesta di una parte o di propria iniziativa, di sentire una parte senza la presenza di terzi, qualora sia necessario per assicurare il corretto funzionamento dell'Europol, per tutelare la sicurezza di uno Stato membro o per proteggere gli interessi del ricorrente o di un terzo. Le parti assenti vengono informate dei lavori svolti in loro assenza.

Articolo 22**AUDIZIONE DI TESTIMONI ED ESPERTI**

1. Il comitato può decidere, su richiesta di una parte o di propria iniziativa, di sentire testimoni. Tutte le parti e i testimoni interessati vengono informati a tempo debito dell'audizione. Si applica altresì l'articolo 21, paragrafi 2 e 3.

2. I testimoni convocati dal comitato hanno diritto al rimborso delle spese di viaggio e di alloggio e ad una compensazione per il mancato guadagno nella misura ritenuta equa dal comitato. Essi possono ricevere i necessari anticipi. Tutti i pagamenti sono a carico del bilancio dell'autorità di controllo comune.

3. I testimoni sono sentiti dal comitato. I membri del comitato possono interrogare i testimoni. Con l'autorizzazione del presidente, le parti possono interrogare i testimoni. Prima dell'inizio dell'udienza, il presidente rammenta ai testimoni che sono tenuti a dire la verità.

4. Il comitato può nominare esperti e definire i loro compiti. Gli esperti hanno diritto ad un compenso per il lavoro svolto. Il comitato può decidere di sentire gli esperti. Si applicano inoltre le regole relative all'audizione dei testimoni.

Articolo 23**DICHIARAZIONI CONCLUSIVE**

Prima di prendere una decisione definitiva, il comitato invita tutte le parti a fare dichiarazioni conclusive.

Articolo 24**PROCESSO VERBALE**

1. Il comitato redige un processo verbale dei procedimenti che rispecchia l'andamento di ogni audizione e le dichiarazioni rilasciate nel corso della stessa. Le parti possono richiedere che taluni documenti o talune dichiarazioni vengano inclusi, integralmente o in parte, nel processo verbale. Il processo verbale viene firmato dal presidente, trasmesso alle parti e allegato agli atti del procedimento. Nei casi di cui all'articolo 21, paragrafo 2, o all'articolo 2, o all'articolo 22, paragrafo 1, il comitato impone alcune limitazioni.

2. L'articolo 9 si applica altresì a tutte le riunioni del comitato alle quali le parti non partecipano.

Articolo 25**DECISIONI E RISERVATEZZA**

1. Le riunioni del comitato sono valide solo se vi partecipano i quattro quinti dei membri o dei loro supplenti.

2. Le decisioni vengono adottate a maggioranza semplice dei membri o supplenti presenti alla riunione, salvo che il presente regolamento o la convenzione dispongano diversamente. In caso di parità, prevale il voto del presidente. Tutti coloro che prendono parte alla decisione definitiva devono aver partecipato ad una audizione.

3. Le deliberazioni del comitato rimangono riservate.

4. Nella decisione definitiva del comitato figurano i nomi delle parti e dei loro rappresentanti, i nomi dei membri del comitato che hanno partecipato alla decisione, la data nella quale la decisione è pronunciata, la parte dispositiva della decisione, una breve esposizione dei fatti del caso e le motivazioni. La decisione viene pronunciata in una sessione pubblica e notificata alle parti. Copia della decisione è trasmessa all'autorità di controllo comune.

Articolo 26**NOTIFICAZIONI**

Le notificazioni e le altre comunicazioni alle parti, ai testimoni e agli esperti vengono trasmesse con mezzi tali da garantire che i destinatari vengano debitamente informati e che, se necessario, ciò possa essere verificato.

Articolo 27**SPESE**

1. Il comitato decide in merito alle spese del procedimento nella sua decisione definitiva. Il procedimento dinanzi al comitato è gratuito. In caso di proposizione del ricorso, le spese necessarie sostenute dal ricorrente per la presentazione e il procedimento sono imputate, interamente o in parte, all'Europol, nella misura ritenuta equa dal comitato.

2. Al ricorrente che non sia in grado di sostenere in tutto o in parte le spese del procedimento può essere concesso in qualsiasi momento, su richiesta, un contributo per coprire tali spese. All'atto della presentazione della domanda egli acclude alla stessa i documenti attestanti il suo stato di necessità. Il comitato può revocare in qualsiasi momento il contributo, qualora i requisiti in base ai quali esso è stato concesso mutino nel corso del procedimento. In caso di approvazione del contributo, le spese sono imputate al bilancio dell'autorità di controllo comune. Se ciò è giustificato, la decisione definitiva può prescrivere ad una parte di restituire al bilancio dell'autorità di controllo comune gli anticipi concessi. Nel presentare la domanda il ricorrente dichiara di acconsentire al pagamento delle spese, ove prescritto dalla decisione definitiva.

Articolo 28**REGOLARITÀ DELLE PROCEDURE**

Nei casi non contemplati dal presente regolamento interno, il comitato provvede a che lo svolgimento del procedimento sia conforme ai principi generali del diritto comunitario di cui all'articolo F, paragrafo 2, del trattato sull'Unione europea.

Titolo IV**DISPOSIZIONI FINALI****Articolo 29****SEGRETARIATO**

1. Nello svolgimento delle sue mansioni l'autorità di controllo comune è assistita da un segretariato situato presso la sua sede. Il segretariato è un organo permanente, i cui membri sono assunti unicamente in base alla competenza. I membri agiscono esclusivamente nel vero interesse dell'autorità di controllo comune, sono totalmente indipendenti dall'Europol e non accettano istruzioni da nessun'altra autorità. Le assunzioni o i distacchi del personale del segretariato avvengono su proposta dell'autorità di controllo comune. I membri del personale del segretariato non svolgono altre attività lavorative senza l'autorizzazione del presidente dell'autorità di controllo comune.

2. Il segretariato è posto sotto la direzione del presidente dell'autorità di controllo comune in base alle norme stabilite da detta autorità. Il segretariato fornisce inoltre servizi al comitato per i ricorsi. Nell'esercizio di tali funzioni esso è posto sotto la direzione del presidente di detto comitato. Il segretariato tiene un registro dei ricorsi e di ogni altro documento.

3. Il segretariato assicura inoltre che gli obblighi di cui all'articolo 32 della convenzione siano rispettati nei lavori dell'autorità di controllo comune.

Articolo 30**RISERVATEZZA**

1. I membri dell'autorità di controllo comune, i supplenti, gli esperti e i membri del segretariato sono tenuti a trattare in maniera riservata le informazioni di cui siano venuti a conoscenza nell'ambito della loro attività, a meno che il corretto svolgimento delle loro mansioni richieda altrimenti. Tale obbligo sussiste anche dopo la cessazione dall'incarico.

2. All'atto della loro nomina, i membri dell'autorità di controllo comune, i supplenti, gli esperti e i membri del segretariato dichiarano di accettare detti obblighi.

3. Nel caso di violazioni dell'obbligo di riservatezza, un membro dell'autorità di controllo comune o il suo supplente può essere sospeso a maggioranza dei due terzi delle votazioni espresse a scrutinio segreto dalle delegazioni che partecipano a una riunione dell'auto-

rità di controllo comune. L'interessato è ascoltato prima che sia presa la decisione, ma non partecipa alla stessa. La presente disposizione si applica allo stesso modo al comitato per i ricorsi, qualora la violazione dell'obbligo di riservatezza interessi i lavori di quel comitato. In tal caso l'autorità di controllo comune è informata senza indugio.

Se un membro viene sospeso, esso è sostituito dal suo supplente. La decisione di sospensione è comunicata all'autorità di controllo nazionale che ha nominato il membro sospeso.

Articolo 31

BILANCIO E SPESE

1. Il segretariato prepara il progetto di bilancio annuale da sottoporre all'autorità di controllo comune; una volta approvato, il progetto viene trasmesso al consiglio di amministrazione prima delle consultazioni previste dall'articolo 24, paragrafo 9, della convenzione.

2. L'autorità di controllo comune decide circa l'erogazione dei fondi di bilancio ad essa destinati, che vengono amministrati dal segretariato.

3. Le spese dell'autorità di controllo comune e del comitato per i ricorsi, comprese le spese per i membri di detto comitato ed i loro supplenti, necessarie al corretto esercizio delle loro funzioni, sono a carico del bilancio dell'autorità di controllo comune in base alle norme da essa stabilite.

Articolo 32

MODIFICA DEL REGOLAMENTO INTERNO

Le modifiche del presente regolamento interno vengono adottate all'unanimità dall'autorità di controllo comune e sottoposte all'approvazione unanime del Consiglio (articolo 24, paragrafo 7, prima frase, della convenzione).

Articolo 33

VALUTAZIONE

Il presente regolamento interno è sottoposto ad una valutazione da parte dell'autorità di controllo comune entro tre anni dopo la sua entrata in vigore.

Articolo 34

ENTRATA IN VIGORE DEL REGOLAMENTO INTERNO

Il presente regolamento interno entra in vigore il giorno successivo a quello dell'approvazione da parte del Consiglio, a norma dell'articolo 24, paragrafo 7, della convenzione(2).

Fatto a Bruxelles, addì 22 aprile 1999.

Per l'autorità di controllo comune

Il presidente

Fergus GLAVEY

(1) GU C 316 del 27.11.1995, pag. 1.

(2) Il regolamento interno è stato approvato dal Consiglio il 21 aprile 1999.

DICHIARAZIONE DEL CONSIGLIO

sull'articolo 4, paragrafo 5, e sull'articolo 12, paragrafo 4, adottata all'atto dell'approvazione del regolamento interno dell'autorità di controllo comune dell'Europol

Gli Stati membri concordano sul fatto che la cessazione della carica di membro o di supplente dell'autorità di controllo comune prima del termine previsto non possa verificarsi in particolare per motivi riguardanti lo svolgimento della funzione nell'ambito del comitato per i ricorsi.

6.6. CONSIGLIO D'EUROPA

- 6.6.1. **Amendments to the convention for the protection of individuals with regard to automatic processing of personal data (ets no. 108) allowing the european communities to accede (adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999)**

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 and have transferred their competencies to the European Communities in the field concerned. In this case, those member States of the Communities do not vote, and the other member States may vote. 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 non member State 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."

**6.6.2. DRAFT ADDITIONAL PROTOCOL TO CONVENTION ETS N° 108
ON SUPERVISORY AUTHORITIES AND TRANSBORDER DATA FLOWS**

(Provisionally adopted by the Consultative Committee of Convention ETS N° 108

on 18 June 1999

for the purpose of transmission for opinion

from the Parliamentary Assembly of the Council of Europe)

PREAMBLE

The Parties to this additional 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")

Convinced that supervisory authorities, exercising their functions in complete independence, are an essential component of the effective protection of individuals with regard to the processing of personal data,

Considering the importance of the flow of information between peoples,

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, within its territory, with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. To this end, the said 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 fundamental freedoms in regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

5. In accordance with the provisions of Chapter IV and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Article 2

**TRANSBORDER FLOWS OF PERSONAL DATA TO A RECIPIENT WHICH IS NOT SUBJECT
TO THE JURISDICTION OF A PARTY TO THE CONVENTION**

1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1, 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 satisfaction of the competent authorities according to domestic law.

Article 3

FINAL PROVISIONS

1. The provisions of Articles 1 and 2 of this Protocol shall be regarded by the Parties 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 States Signatories to the Convention. After acceding to the Convention under the conditions provided by it, the European Communities may sign this Protocol. This Protocol is subject to ratification, acceptance or approval. A Signatory to this Protocol may not ratify, accept or approve it unless it has previously or simultaneously ratified, accepted or approved the Convention or has acceded to it. Instruments of ratification, acceptance or approval of this Protocol 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 expiry of a period of three months after the date on which 5 of its Signatories have expressed their consent to be bound by the Protocol in accordance with the provisions of the previous paragraph.
In respect of any Signatory to this Protocol 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 expiry of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.
4. After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the 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 expiry 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 expiry of a period of three months after the date of its deposit.
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 acceded to this Protocol of:
 - a. any signature;
 - b. the deposit of any instrument of ratification, acceptance or approval;
 - 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 Strasbourg, 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 any State invited to accede to the Convention.