Relazione 2001

Nuovi diritti, riservatezza,
dignità della persona.
8 maggio 2002:
a cinque anni dalla legge 675

www.garanteprivacy.it

Indice

Elenco delle abbreviazioni XII

I Stato di attuazione della legge n. 675/1996

Le principali novità sul piano normativo

1. Il completamento della disciplina: una nuova legge-delega e un testo unico 3
2. Altre attività normative 6
3. Iniziative legislative 7
4. L'attività consultiva del Garante sugli atti del Governo 9

Pubblica amministrazione

5. Profili generali 11
6. Informazioni sensibili e altri dati particolari 12
7. Trasparenza dell'attività amministrativa 15
8. Accesso ai documenti amministrativi 17
9. Banche dati di rilevanti dimensioni e censimento della popolazione 19
10. Carta d'identità elettronica e tessera elettorale 22
11. Documentazione anagrafica e materia elettorale 25
12. Enti locali 27
13. Canone radiotelevisivo 28

Attività giudiziarie e di polizia

14. Premesse 32
15. Trattamento di dati nell'ambito dell'attività giudiziaria 33
16. Notificazione di atti e comunicazioni 35
17. Attività di polizia 36
18. Sistema di informazione Schengen 38

Sanità

19. Considerazioni generali 39
20. Informazioni genetiche 42
21. Aids 43

Rapporto di lavoro

22. Tutela dei dati personali dei lavoratori e dati valutativi 44
23. Informative e controllo a distanza del personale 47
24. Annunci di lavoro 48
25. Sistemi informativi in materia di lavoro 50

Indice

Statistica, ricerca scientifica e ricerca storica

26. Statistica e ricerca scientifica 51
27. Ricerca storica 52

Associazioni, movimenti politici e partiti

28. Trattamento dei dati e realtà associative 54
29. L'uso di dati per finalità politico-elettorali 55
30. Condomini 56

Attività forense, investigazione privata e liberi professionisti

31. Liberi professionisti e albi professionali 57
32. La raccolta di dati per finalità di difesa e di indagine difensiva 58
33. I codici deontologici 59

Settore del credito, finanziario ed assicurativo

34. Profili generali 60
35. Perizie medico-legali 63
36. Raccolte di dati in ambito assicurativo e banca dati Isvap 64
37. Centrali rischi 65
38. Anagrafe degli assegni bancari e postali 68

Attività giornalistiche e mezzi di informazione

39. Attività giornalistica e rispetto dei principi della legge n. 675/1996 69
40. Tutela dei minori 71
41. Cronache giudiziarie 73
42. Dignità della persona e dati idonei a rivelare lo stato di salute 75

Sorveglianza e sistemi biometrici

43. Videosorveglianza 76
44. Rilevazioni biometriche 78
45. Braccialetto elettronico 80

Marketing

46. *Marketing* e diritti dell'interessato 81

Telefonia e reti di comunicazione

47. Profili generali 82
48. Accesso ai dati di traffico telefonico 83
49. Attivazione di nuovi servizi e consenso dell'interessato 84
50. Elenchi abbonati e diritto alla riservatezza 85

51. Comunicazioni indesiderate su utenze telefoniche mobili 86

Trattamento dei dati personali in *Internet*

52. Profili generali 87
53. Comunicazioni indesiderate ed utilizzo dei nomi di dominio *Internet* 88
54. Il codice deontologico 89

Sicurezza dei dati e dei sistemi

55. Le misure di sicurezza: casi applicativi 90

I trasferimenti all'estero di dati

56. Paesi che offrono una protezione adeguata 91
57. "*Safe Harbor*" 93
58. Clausole contrattuali standard 95

II Il Garante

La nuova composizione del collegio

59. La continuità nell'attività dell'Autorità 99

La trattazione dei ricorsi

60. Principali problemi esaminati 100
61. Profili procedurali e procedimenti instaurati autonomamente 102
62. Impugnazione dei provvedimenti dell'Autorità 104

Attività ispettive e applicazione di sanzioni amministrative

63. La programmazione delle ispezioni e i risultati 105
64. L'attività sanzionatoria del Garante 107

L'attività di informazione e comunicazione

65. Profili generali 109
66. Seminari, convegni ed altre iniziative 111
67. Il sito *Internet* dell'Autorità 113

La gestione amministrativa dell'Ufficio

68. I regolamenti del Garante e la nuova organizzazione dell'Ufficio 114
69. Il bilancio, gli impegni di spesa e l'attività contrattuale 116
70. Lo sviluppo del sistema informativo 118
71. Biblioteca e centro di documentazione 120
72. Il personale e i collaboratori esterni 122

Indice

Il registro dei trattamenti

73. Organizzazione e futuri sviluppi 124

Dati statistici

74. Prospetto analitico 126

III Attività comunitarie e internazionali

Il recepimento delle direttive comunitarie

75. Le direttive sulla protezione dei dati 131
76. Stato di recepimento delle direttive 95/46/CE e 97/66/CE negli Stati menbri 132
77. *Privacy* nelle telecomunicazioni 133

Altre novità nel diritto comunitario e nel settore giustizia-affari interni

78. Profili generali 134

La cooperazione tra Autorità garanti in Europa

79. Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali 135
80. La partecipazione ad altri comitati e gruppi di lavoro 136

L'Autorità di controllo comune Schengen

81. Il rapporto per il 2000-2001 138

Europol

82. L'attività dell'Autorità di controllo comune e i primi casi di contenzioso 139

Il controllo sul Sistema informativo doganale

83. La creazione dell'Autorità di controllo 140

Eurodac

84. Collaborazione tra Stati membri e garanzie per gli interessati 141

Consiglio d'Europa

85. La Convenzione sul *cybercrime* 142
86. L'attività dei gruppi di esperti 143
87. Linee-guida in materia di sorveglianza 145

O.C.S.E.

88. I risultati conseguiti nel 2001 146
89. Ulteriori iniziative 147

IV Documentazione

Testi

Disposizioni normative

90. Legge 31 dicembre 1996, n. 675 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali 151
91. Decreto Legislativo 28 dicembre 2001, n. 467 - Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'art. 1 della legge 24 marzo 2001, n. 127 175
92. Legge 24 marzo 2001, n. 127 - Differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali 182
93. Legge 28 marzo 2001, n. 145 - Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano riguardo all'applicazione della biologia e della medicina: Convenzione sui diritti dell'uomo e sulla biomedicina, fatta a Oviedo il 4 aprile 1997, nonché del Protocollo addizionale del 12 gennaio 1998, n. 168, sul divieto di clonazione di esseri umani 183

Provvedimenti del Garante

94. Autorizzazione n. 1/2002 al trattamento dei dati sensibili nei rapporti di lavoro 184
95. Autorizzazione n. 2/2002 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale 189
96. Autorizzazione n. 3/2002 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni 195
97. Autorizzazione n. 4/2002 al trattamento dei dati sensibili da parte dei liberi professionisti 199

Indice

98. Autorizzazione n. 5/2002 al trattamento dei dati sensibili da parte di diverse categorie di titolari 203
99. Autorizzazione n. 6/2002 al trattamento di dati sensibili da parte degli investigatori privati 210
100. Autorizzazione n. 7/2002 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici 215
101. Autorizzazione al trasferimento di dati personali verso organizzazioni aventi sede negli Stati Uniti secondo i "Principi di approdo sicuro in materia di riservatezza" - 10 ottobre 2001 221
102. Autorizzazione al trasferimento di dati personali verso Paesi terzi in conformità alle clausole contrattuali standard approvate dalla Commissione europea - 10 ottobre 2001 223
103. Autorizzazione al trasferimento di dati personali verso Paesi extra-europei in conformità alle clausole contrattuali tipo di cui alla decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/CE - 10 aprile 2002 225
104. Autorizzazione al trasferimento di dati personali verso l'Ungheria - 17 ottobre 2001
Autorizzazione al trasferimento di dati personali verso la Svizzera - 17 ottobre 2001 227
105. Provvedimento del 7 marzo 2001 - Partiti e movimenti politici - Un "decalogo" per l'utilizzazione di dati da parte di partiti e movimenti politici nella propaganda elettorale 231
106. Provvedimento in materia di codici di deontologia e di buona condotta - 10 aprile 2002 235

Commissione europea

107. Decisione della Commissione del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso Paesi terzi a norma della direttiva 95/46/CE 238
108. Decisione della Commissione del 27 dicembre 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in Paesi terzi, a norma della direttiva 95/46/CE 251

Consiglio d'Europa

109. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows - Strasbourg, 8.11.2001 262
110. Council of Europe Convention on *Cybercrime* - Budapest, 23.11.2001 265

Autorità di controllo comune Schengen

111. Quinta relazione di attività dell'Autorità di controllo comune: marzo 2000 - dicembre 2001 286

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (art. 29 direttiva 95/46/CE)

112. Raccomandazione 1/2001 concernente i dati relativi alla valutazione del personale - Adottata il 22.3.2001 312
113. Raccomandazione relativa ai requisiti minimi per la raccolta di dati *on-line* nell'Unione europea 314
114. Parere 8/2001 del Gruppo di lavoro "Articolo 29" sul trattamento dei dati nel contesto lavorativo - Adottato il 13 settembre 2001 322

Richiami ipertestuali

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (art. 29 direttiva 95/46/CE)

115. Parere 1/2001 sul progetto di decisione della Commissione ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso Paesi terzi in conformità all'articolo 26(4) della direttiva 328
116. Parere 2/2001 sul livello di adeguatezza del Personal Information and Electronic Documents Act (legge sui dati personali e i documenti elettronici) canadese 329
117. Parere 3/2001 sul livello di protezione della legge 2000 di modifica della legge australiana sulla tutela della vita privata (settore privato) 330
118. Parere 4/2001 sul progetto di Convenzione sulla cybercriminalità del Consiglio d'Europa 331
119. Parere 5/2001 sulla relazione speciale del Mediatore europeo al Parlamento europeo a seguito del progetto di raccomandazione alla Commissione europea nella denuncia 713/98/IJH. 332
120. Quarta relazione annuale sulla situazione relativa alla tutela delle persone con riguardo al trattamento dei dati personali e alla vita privata nella Comunità e nei Paesi terzi concernente l'anno 1999 333
121. Parere 7/2001 sul progetto di decisione della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili di attività di elaborazione con sede in Paesi terzi ai sensi dell'articolo 26(4) della direttiva 95/46/CE 334

Indice

122. Prassi raccomandata IATA n. 1774 - Protezione della riservatezza e dei flussi transfrontalieri di dati personali utilizzati per il trasporto aereo internazionale di passeggeri e merci 335
123. Parere 9/2001 sulla comunicazione della Commissione intitolata «Creare una società dell'informazione più sicura rafforzando la sicurezza delle infrastrutture dell'informazione e lottando contro la criminalità informatica» 336
124. Parere 10/2001 sulla necessità di un approccio equilibrato alla lotta contro il terrorismo 337
125. Quinta relazione annuale sulla situazione relativa alla tutela delle persone con riguardo al trattamento dei dati personali e alla vita privata nell'Unione europea e nei Paesi terzi concernente l'anno 2000 338

Unione europea

126. Posizione comune adottata dal Consiglio il 28 gennaio 2002 in vista dell'adozione della direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche 340
127. Comunicazione della Commissione europea al Parlamento europeo sulla Posizione comune del Consiglio in merito all'adozione della direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, del 30 gennaio 2002 341

Commissione europea

128. Decisione della Commissione europea, del 26 luglio 2000, sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal dipartimento del commercio degli Stati Uniti (con rettifica) 342
129. Decisione della Commissione europea, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati in Ungheria 343
130. Decisione della Commissione europea, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati in Svizzera 344
131. Decisione della Commissione del 20 dicembre 2001 conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act) 345

132. Documento di lavoro dei servizi della Commissione sull'applicazione della decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal dipartimento del commercio degli Stati Uniti 346
133. Proposta di decisione del Parlamento europeo, del Consiglio e della Commissione relativa allo statuto e alle condizioni generali d'esercizio delle funzioni di garante europeo della protezione dei dati COM(2001) 411 347

Consiglio d'Europa

134. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine 348
135. Additional Protocol to the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine on the Prohibition of Cloning Human Beings 349
136. Protection of Personal Data with regard to Surveillance 350

Indice

Elenco delle abbreviazioni

La presente Relazione è riferita al 2001 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 24 aprile 2002, relative a sviluppi significativi che si è ritenuto opportuno menzionare.

art. articolo

Bollettino Bollettino del Garante per la protezione dei dati personali

"Cittadini e Società dell'Informazione"

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

Provv. provvedimento

Relazione Relazione del Garante per la protezione dei dati personali

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

Stato di attuazione della legge n. 675/1996

Le principali novità sul piano normativo

1 Il completamento della disciplina: una nuova legge-delega e un testo unico

Anche il 2001 è stato contraddistinto da interventi normativi di particolare importanza nella tematica del trattamento dei dati personali.

Il Parlamento ha conferito una nuova delega al Governo (la terza da quando è stata approvata la legge n. 675/1996: v. le leggi nn. 676/1996 e 344/1998) al fine di completare ed armonizzare la disciplina in materia.

Il legislatore ha così confermato l'attenzione manifestata più volte per le istanze di tutela dei diritti fondamentali della personalità connessi all'utilizzo delle informazioni di carattere personale, e ha anche ridefinito in termini più ampi il contenuto della delega, prevedendo l'emanazione di un testo unico delle disposizioni normative in materia di protezione dei dati personali volto a ricomprendere le diverse disposizioni generali e speciali (l. 24 marzo 2001, n. 127, in *G.U.* 19 aprile 2001, n. 91).

La prima fase di attuazione di tale legge si è conclusa con l'emanazione, a fine anno, di un decreto legislativo recante "*Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'articolo 1 della legge 24 marzo 2001, n. 127*" (d.lg. 28 dicembre 2001, n. 467, in *G.U.* 16 gennaio 2002, n. 13).

Tra le novità più significative introdotte da tale decreto si segnalano diverse soluzioni normative dirette a semplificare e a razionalizzare alcuni adempimenti e requisiti per il trattamento, all'esito della prima fase di applicazione della legge, e che hanno al contempo rafforzato il connesso quadro di garanzie per gli interessati.

Per quanto attiene ad esempio alla notificazione al Garante è stata invertita, nei limiti consentiti dalla normativa comunitaria, la logica del sistema, e si è prefigurato il passaggio da un regime in cui era previsto un obbligo generale di notificazione, salvi i casi di esonero o di possibile utilizzazione di una notificazione semplificata, ad uno in cui il quadro di trasparenza viene valorizzato in modo da concentrare l'istituto della notificazione alle sole ipotesi in cui il trattamento, in ragione delle modalità o della natura dei dati personali, sia suscettibile di arrecare pregiudizio ai diritti ed alle libertà dell'interessato, nei casi e con le modalità individuati con regolamento del Governo.

Una ulteriore semplificazione ha interessato le modalità di indicazione nell'informativa delle coordinate identificative del responsabile del trattamento, rese più agevoli soprattutto in riferimento ai casi di designazione di un numero rilevante di responsabili da parte di un medesimo titolare del trattamento.

Di particolare rilievo sono, poi, alcune disposizioni che attribuiscono importanti compiti al Garante in attuazione di specifiche previsioni comunitarie. Si fa riferimento, ad esempio, al principio del *bilanciamento di interessi* nell'individuazione dei casi di esclusione del consenso (art. 7, lett. *f*), direttiva n. 95/46/CE) ed all'istituto del *prior checking* (art. 20 direttiva n. 95/46/CE).

Quanto al primo profilo, è di specifico interesse la previsione di una norma di chiusura, all'art. 12, comma 1, lett. *h-bis*) della legge n. 675, che introduce un elemento di flessibilità nell'individuazione delle possibili situazioni in cui il trattamento di dati personali "comuni" potrà essere effettuato anche senza il consenso degli interessati, demandando al Garante il compito di individuarle, sulla base dei principi sanciti dalla legge, qualora ricorra un legittimo interesse del titolare del trattamento – o di un terzo al quale i dati sono comunicati – e non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato. Per questa via, il principio di bilanciamento di interessi assurge quindi ad ulteriore parametro di liceità del trattamento.

Con riguardo al secondo profilo, va sottolineato che con l'introduzione dell'istituto del *prior checking* il trat-

1

tamento dei dati che può comportare specifici rischi per i diritti e le libertà dei soggetti cui si riferiscono le informazioni trattate, in riferimento a dati diversi da quelli "*sensibili*" e da quelli "*comuni*", dovrà rispettare eventuali misure ed accorgimenti prescritti dal Garante a seguito di una verifica preliminare.

Sia in relazione al *prior checking*, sia con riferimento al menzionato *bilanciamento di interessi*, il decreto attribuisce a questa Autorità, sulla base dei principi contenuti nelle leggi vigenti, il compito di individuare anche con provvedimenti di carattere generale i casi in cui i nuovi istituti devono trovare applicazione, nonché alcuni accorgimenti e misure da rispettare a garanzia degli interessati, semplificando, così, l'attuazione degli istituti medesimi.

Come precisato nel corso dell'esame dello schema di decreto legislativo da parte della Commissione giustizia del Senato, tali soluzioni rispondono all'esigenza di evitare lacune e incertezze applicative in ambiti nei quali sono coinvolti diritti e libertà fondamentali della persona e vengono in considerazione condotte talvolta sanzionate anche penalmente.

I casi in cui i soggetti privati possono trattare dati personali anche senza il consenso dell'interessato sono stati integrati anche in riferimento ad altre realtà (es., attuazione di obblighi contrattuali o precontrattuali) e, in materia di dati "sensibili", in relazione alle c.d. investigazioni difensive e all'esercizio di un diritto in sede giudiziaria.

Il decreto legislativo ha poi assegnato particolare rilievo all'adozione di nuovi codici di deontologia e di buona condotta quale strumento di sperimentata efficacia per dare integrale attuazione ai principi sanciti dalla legge n. 675/1996 e alle Raccomandazioni del Consiglio d'Europa in diversi settori espressamente indicati (servizi di comunicazione offerti per via telematica e in particolare attraverso *Internet; direct marketing;* gestione del rapporto di lavoro; informazione commerciale; sistemi informativi gestiti da "centrali-rischi" private; strumenti automatizzati di rilevazione di immagini; dati provenienti da archivi pubblici), fornendo alle categorie interessate l'opportunità di contribuire attivamente, nel rispetto del principio di rappresentatività, all'introduzione di vere e proprie fonti normative atipiche recanti regole rilevanti per stabilire se il trattamento dei dati è lecito e corretto.

In questa prospettiva, nel corso del 2001 è stato varato l'importante codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici (v. il *Provv.* del Garante n. 8/P/2001, in *G.U.* 5 aprile 2001, n. 80) la cui adozione era stata prevista dal decreto legislativo 30 luglio 1999, n. 281. Il codice è diretto a garantire che l'utilizzazione dei dati di carattere personale acquisiti nell'ambito della ricerca storica, dell'esercizio del diritto allo studio e all'informazione e nell'attività archivistica si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e all'identità personale, senza pregiudicare ed anzi favorendo lo svolgimento delle attività considerate.

È pressoché completato, poi, il procedimento per l'adozione del codice per l'attività statistica e per la ricerca scientifica svolte al di fuori del Sistema statistico nazionale, e sono proficuamente in avanzata fase di redazione i codici per il trattamento dei dati da parte dei difensori e degli investigatori privati.

Il decreto n. 467/2001 ha infine rimodulato il quadro sanzionatorio della legge n. 675/1996 trasformando la natura di alcune sanzioni (legate in particolare a violazioni formali concernenti la notificazione dei trattamenti) e iniziando ad introdurre, ove possibile, meccanismi di "ravvedimento operoso" (per le violazioni in materia di misure minime di sicurezza).

Al tempo stesso, è stato ampliato l'ambito della punibilità in sede penale dell'inosservanza di importanti provvedimenti adottati dal Garante, nell'ambito del più generale intervento che, in linea con la direttiva europea, ha rafforzato i poteri di verifica dell'Autorità sui trattamenti effettuati (articolo 31, comma 1, lett. *c)*, della legge n. 675/1996).

È stato in questo quadro introdotto il presidio della sanzione penale per gravi fatti di falsa dichiarazione o comunicazione nei rapporti con l'Autorità ed è stato anche aggiornato l'importo di alcune sanzioni amministrative pecuniarie.

Infine, il decreto reca alcune disposizioni per migliorare l'attuazione della direttiva n. 97/66/CE attraverso mirate integrazioni al decreto legislativo n. 171 del 1998 in materia di tutela della vita privata nelle telecomunicazioni, anche a seguito di sollecitazioni della Commissione europea alla quale è stata data poi notizia delle utili soluzioni adottate.

Si segnalano, in particolare, le disposizioni che tendono a rendere effettivo l'uso delle modalità di pagamento alternative alla fatturazione, in modo da assicurare l'anonimato dell'utente, e quelle che hanno introdotto l'obbligo per i fornitori di servizi di telecomunicazione di informare adeguatamente il pubblico circa il servizio di identificazione della linea chiamante e di assicurare la disattivazione di tale servizio in relazione alle chiamate di emergenza.

Il processo di completamento della normativa in materia non si è ancora concluso, stante la prevista adozione entro il 31 dicembre 2002 del citato testo unico (su cui è impegnata una commissione di esperti istituita presso la Presidenza del Consiglio dei Ministri-Dipartimento per la funzione pubblica), il quale potrà introdurre ulteriori integrazioni ed eventuali modifiche di coordinamento o finalizzate alla migliore attuazione della vigente disciplina, anche nei settori, come quelli relativi alle attività giudiziarie e di polizia, sulle quali è avvertita l'esigenza di completare il percorso previsto dalle leggi-delega intervenute a decorrere dal 1996.

2 Altre attività normative

Nei mesi conclusivi della XIII legislatura e in questo primo scorcio della XIV, altri provvedimenti normativi hanno riguardato aspetti d'interesse, anche indiretto, per la materia del trattamento dei dati personali. Si segnalano i più rilevanti:

a) la legge 1 marzo 2002, n. 39 (Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee – *Legge comunitaria 2001*), che prevede l'attuazione di quattro direttive comunitarie di possibile rilievo per la protezione dei dati personali: la direttiva sul commercio elettronico, la direttiva sulla moneta elettronica, quella sul divieto di discriminazione per motivi di razza o etnia e la direttiva sull'assicurazione obbligatoria in materia di responsabilità civile da circolazione di autoveicoli. Il testo approvato, inoltre, contiene disposizioni in materia di televendite e di trasmissioni televisive, che prevedono anche particolari forme di tutela per i minori;

b) la legge 27 dicembre 2001, n. 459, in materia di *diritto di voto dei cittadini all'estero*, il cui art. 5 realizza l'elenco aggiornato dei cittadini residenti all'estero finalizzato alla predisposizione delle liste elettorali, mediante unificazione dei dati contenuti nell'A.I.R.E. e negli schedari consolari;

c) il decreto-legge 25 settembre 2001, n. 350, convertito dalla legge 23 novembre 2001, n. 409 (*Disposizioni urgenti in vista dell'introduzione dell'euro*: provvedimento sul c.d. "rientro dei capitali dall'estero"), il cui articolo 13 reca disposizioni in ordine ad una dichiarazione riservata da rendere ai competenti uffici;

d) la legge 29 marzo 2001, n.135, recante la riforma della legislazione sul turismo, il cui articolo 8 apporta alcune modifiche all'articolo 109 del testo unico delle leggi di pubblica sicurezza (r.d. 18 giugno 1931, n.773) in materia di "*schedine d'albergo*". Il testo in vigore prima della modifica apportata dalla legge n.135/2001 prevedeva che le schede fossero conservate per dodici mesi nella struttura ricettiva, a disposizione degli ufficiali o agenti di pubblica sicurezza, e che ne fosse trasmessa copia giornalmente agli uffici di p.s. anche con mezzi telematici. Il testo novellato prevede, invece, che il gestore comunichi all'autorità le generalità degli alloggiati mediante consegna di copia di scheda o, in alternativa, i dati nominativi delle predette schede mediante la loro comunicazione in via informatica o telematica, secondo modalità stabilite con decreto del Ministro dell'interno. Il testo non reca disposizioni specifiche sulle modalità e sui limiti del trattamento dei dati personali acquisiti dagli organi di polizia, diversamente da quanto previsto nella versione approvata dal Senato;

e) il decreto ministeriale 2 febbraio 2001, relativo alla descrizione dei tipi e delle caratteristiche, nonché alle modalità di installazione e di uso dei mezzi elettronici e degli strumenti tecnici destinati al *controllo delle persone sottoposte agli arresti domiciliari o alla detenzione domiciliare* previsti dagli articoli 275-*bis* c.p.p. e 47-*ter*, comma 4-*bis*, della l. 26 luglio 1975, n. 354 (c.d. "braccialetto elettronico"). L'art. 4 del decreto, relativo al trattamento dei dati personali, prevede che l'applicazione dei mezzi e degli strumenti avvenga nel rispetto della dignità dell'interessato, che sia delimitato il tempo di conservazione dei dati e che siano individuate le persone legittimate a trattarli nel rispetto delle misure di sicurezza ai sensi dell'art. 15 della legge n. 675/1996.

3 Iniziative legislative

L'Autorità ha seguito i lavori relativi ad altre iniziative parlamentari rilevanti per la tematica della protezione dei dati personali.

Tra le più importanti occorre ricordare:

a) il disegno di legge sulle *notifiche degli atti del processo* e sulle *notifiche e comunicazioni in sede amministrativa*, di iniziativa del sen. Caruso (AS 556), analogo a quello approvato da un ramo del Parlamento nella XIII legislatura (cfr. *Relazione 2000*, par. 17, p. 27). Il disegno mira ad aggiornare la disciplina di queste materie in relazione ai vigenti principi in tema di diritti della personalità e contiene alcune disposizioni che recepiscono, nella sostanza, anche alcune indicazioni formulate dall'Autorità;

b) talune proposte di legge sul *contrasto alla pedofilia,* in discussione presso la Commissione giustizia della Camera (AC 311 ed abb.) Nel corso dei relativi lavori sono state richiamate alcune mozioni approvate dalla Camera nel novembre scorso, nonché il parere espresso dalla medesima Commissione sullo schema di decreto delegato in materia di protezione dei dati personali (cfr. par. 1), nei quali si chiede al Governo di predisporre strumenti normativi per disciplinare l'obbligo dei *provider* di conservare per un certo tempo i *log–file* a fini di giustizia. In collegamento con i lavori della Commissione giustizia si muove l'indagine conoscitiva in materia di tutela dei minori presso la Commissione bicamerale per l'infanzia. A quest'ultima, il Garante ha inviato una nota informativa nella quale, fra l'altro, si sono espresse perplessità circa la raccolta generalizzata di informazioni (*log-file*) e la loro conservazione per tempi lunghi, tenuto conto anche della loro presumibile relativa efficacia a fini di prevenzione e repressione degli illeciti;

c) un disegno di legge in materia di uso dei *dati contenuti nei registri immobiliari* (AS 512), in discussione presso la Commissione giustizia del Senato. Il 7 febbraio u.s. vi è stata un'audizione informale del Garante sulla materia – con specifico riferimento alla Raccomandazione (91) 10 del Consiglio d'Europa, da attuare ai sensi del recente decreto legislativo n. 467/2001 – nella quale si è sottolineata l'importanza di un lavoro di approfondimento preliminare che consenta di perfezionare i testi normativi in linea con i principi in materia di protezione dei dati personali. L'audizione si è rivelata proficua e l'Autorità si è dichiarata disponibile per analoghe forme di collaborazione con il Parlamento riferite ad altre iniziative normative;

d) un disegno di legge del Governo che disciplina l'*esercizio del diritto di voto da parte di elettori affetti da gravi infermità* (AS 236). L'Autorità ha fornito al Ministero dell'interno, su richiesta, alcune indicazioni per la presentazione di emendamenti finalizzati ad una più elevata tutela della riservatezza degli interessati. Le novità sono state recepite dal Ministero ed accolte dalla competente commissione parlamentare;

e) la riforma della disciplina delle attività trasfusionali e della produzione di emoderivati (attualmente contenuta nella legge 4 maggio 1990, n. 107), esaminata dalla Commissione igiene e sanità del Senato. La materia presenta aspetti che riguardano anche la protezione dei dati personali. Le attività concernenti le *trasfusioni di sangue umano* svolte in ambito sanitario possono infatti comportare il trattamento di dati sensibili idonei a rivelare lo stato di salute delle persone, donatori di sangue o soggetti a emotrasfusioni e sono ricomprese, in base al d.lg. n. 135 del 1999, fra quelle di *rilevante interesse pubblico* per le quali è consentito ai soggetti pubblici l'uso dei dati personali sullo stato di salute degli interessati (art. 17, comma 1, lett. *g*), d.lg. n. 135/1999);

f) il disegno di legge di ratifica della *Convenzione europea di assistenza giudiziaria in materia penale* (AC 2372), esaminato presso le Commissioni giustizia ed esteri della Camera. Il Governo ha recepito le indicazioni fornite dal Garante per una efficace protezione dei dati personali trattati;

g) un disegno di legge "collegato" con la legge 27 dicembre 2001, n. 459 sul voto degli italiani all'estero, che tende a modificare le modalità di *rilevazione dei cittadini* residenti all'estero, nell'ambito del quale si pre-

vedono flussi di dati in via informatica fra diversi soggetti istituzionali (AS 470).

Sono stati inoltre seguiti i lavori relativi ad alcune indagini conoscitive su altre tematiche d'interesse. Oltre a quella in materia di tutela dell'infanzia cui si è fatto cenno, vanno ricordate:

- l'*indagine conoscitiva sul futuro dell'Unione europea*, presso le competenti commissioni della Camera e del Senato, riguardante, fra l'altro, anche l'attuazione della Carta dei diritti fondamentali dell'Unione europea adottata a Nizza nel 2000;
- l'indagine conoscitiva sugli effetti nell'ordinamento delle revisioni apportate al Titolo V della Parte II della Costituzione dalla legge n. 3/2001 sul *federalismo*, nell'ambito della quale è stata svolta in data 30 ottobre 2001 l'audizione del Presidente dell'Autorità, prof. Rodotà.

4 L'attività consultiva del Garante sugli atti del Governo

L'art. 31, comma 2, della legge n. 675/1996, prevede che il Presidente del Consiglio dei ministri e ciascun ministro debbano consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere in materia di protezione di dati personali.

In relazione a tale attribuzione, nel corso dell'anno (nonostante l'intervallo connesso al rinnovo delle Camere) sono pervenute al Garante varie richieste di parere.

Fra gli atti consultivi adottati si segnalano, in particolare, quelli riguardanti:

a) il decreto recante regole procedurali per la tenuta dei *registri informatizzati dell'amministrazione della giustizia* (decreto del Ministro della giustizia 24 maggio 2001);

b) il regolamento di attuazione della legge 22 dicembre 1999, n. 512 sull'istituzione del *Fondo di rotazione per la solidarietà alle vittime dei reati di tipo mafioso* (d.P.R. 28 maggio 2001, n. 284);

c) l'approvazione dei modelli di *scheda anagrafica e professionale del lavoratore*, ai sensi dell'art. 4, comma 3, del d.P.R. 7 luglio 2000, n. 442 (decreti ministeriali 30 maggio 2001);

d) il regolamento per la semplificazione dei procedimenti in materia di *infermità da causa di servizio, pensione privilegiata ed equo indennizzo*, adottato ai sensi della l. 340/2000 all. A, n. 63. In base alle indicazioni fornite dall'Autorità, l'art. 4 del d.P.R. 29 ottobre 2001, n. 461 reca disposizioni per il trattamento dei dati sensibili e in particolare di quelli riguardanti lo stato di salute;

e) il decreto concernente il regolamento sul funzionamento dell'*archivio informatizzato degli assegni bancari e postali* (decreto del Ministro della giustizia 7 novembre 2001, n. 458);

f) il regolamento riguardante la redazione della *documentazione caratteristica del personale appartenente all'Esercito, alla Marina e all'Aeronautica* (parere del 24 aprile 2001);

g) il regolamento recante criteri e modalità per l'espletamento da parte delle amministrazioni aggiudicatrici di *procedure ad evidenza pubblica attraverso l'utilizzo di sistemi elettronici e telematici di negoziazione* per l'approvvigionamento di beni e servizi, adottato ai sensi dell'art. 24, comma 4, l. 340/2000 (parere del 14 giugno 2001);

h) il decreto per l'aggiornamento del 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. 8, comma 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

i) il d.P.R. concernente l'istituzione del *sistema di comunicazione degli enti locali*, ai sensi degli artt. 3, comma 153, l. n. 662/1996 e 9 d.l. n. 557/1993 (parere del 27 giugno 2001);

l) l'adeguamento da parte dei soggetti pubblici all'art. 5 del d.lg. n. 135 del 1999 in ordine all'adozione delle disposizioni regolamentari in materia di *trattamenti di dati sensibili nella pubblica amministrazione* (parere del 17 gennaio 2002);

m) il regolamento (decreto 13 dicembre 2001, n. 489, in *G.U.* del 12 aprile 2002) concernente l'integrazione delle norme relative alla *vigilanza sull'adempimento dell'obbligo scolastico* (parere del 15 giugno 2001).

4

A fronte dei diversi pareri richiesti ed espressi, si deve però segnalare nuovamente il problema della mancata consultazione del Garante che si è verificato in altre occasioni, in particolare nella decorsa legislatura. Ciò sebbene il Garante abbia in passato rappresentato il persistere di varie omissioni dei ministeri nel consultare questa Autorità, evidenziando più volte che i provvedimenti adottati in assenza del parere sono viziati ed annullabili per violazione di legge.

Fra i casi più rilevanti di mancata consultazione vanno fra gli altri menzionati:

a) il regolamento di *attuazione delle direttive nn. 97/51/CE e 98/10/CE*, in materia di telecomunicazioni (d.P.R. 11 gennaio 2001, n. 77, contenente disposizioni anche in materia di elenchi telefonici);

b) il regolamento recante disciplina per l'assegnazione delle *borse di studio in favore delle vittime del terrorismo e della criminalità*, nonché degli orfani e dei figli delle vittime del terrorismo (d.P.R. 14 marzo 2001, n. 318);

c) il decreto riguardante disposizioni per l'uniformità di trattamento sul *diritto agli studi universitari*, a norma dell'art. 4 l. 2 dicembre 1991, n. 390 (d.P.C.M. 9 aprile 2001);

d) il regolamento in materia di accertamento, riscossione e liquidazione del *diritto annuale versato dalle imprese alle camere di commercio*, ai sensi dell'art. 17 l. 23 dicembre 1999, n. 488 (decreto del Ministro dell'industria, del commercio e dell'artigianato 11 maggio 2001, n. 359);

e) il regolamento recante norme in materia di agevolazioni relativamente all'*attribuzione del codice fiscale ed alle modalità di presentazione delle dichiarazione di pagamento delle imposte per i contribuenti residenti all'estero*, ai sensi dell'art. 14 l. 27 luglio 2000, n. 212 (decreto del Ministro delle finanze 17 maggio 2001, n. 281);

f) il regolamento per la semplificazione dei procedimenti relativi ad *autorizzazioni per lo svolgimento di attività disciplinate dal testo unico in materia di pubblica sicurezza,* nonché al riconoscimento della qualifica di agente di pubblica sicurezza (d.P.R. 28 maggio 2001, n. 311);

g) il decreto per l'individuazione di *dati sulle carriere degli studenti e per il rilascio del certificato di supplemento al diploma* destinati all'anagrafe nazionale degli studenti universitari (decreto del Ministro dell'università e della ricerca scientifica 30 maggio 2001) in ordine al quale il Ministero dell'istruzione, dell'università e della ricerca, dopo l'adozione del provvedimento, ha richiesto al Garante eventuali pareri circa la congruità del sistema informativo adottato rispetto alla normativa in materia di protezione dei dati personali e si è dichiarato ora disponibile a porre rimedio al vizio incorso nella procedura;

h) il regolamento recante disposizioni in materia di utilizzo del *servizio di collegamento telematico con l'Agenzia delle entrate* per la presentazione di documenti, atti e istanze previsti dalle disposizioni che disciplinano i singoli tributi, nonché per ottenere certificazioni ed altri servizi connessi ad adempimenti fiscali (d.P.R. 5 ottobre 2001, n. 404). Analoghe tematiche, oggetto di provvedimenti dell'Agenzia delle entrate e dell'Agenzia del territorio, non sono stati sottoposti a previo parere (v., in particolare, dd. 12 dicembre 2001 e 15 marzo 2002, in *G.U.* 20 e 22 dicembre 2001 nn. 295 e 297 e 27 marzo 2002, n. 73, in tema di *voltura degli atti relativi a diritti sugli immobili*, *registrazione telematica dei contratti di locazione* e di affitto di beni immobili e dei dati concernenti *erogazioni liberali per progetti culturali*);

i) il decreto di approvazione del modello di dichiarazione di *emersione del lavoro irregolare*, delle relative istruzioni, nonché delle modalità di presentazione (decreto del Ministro dell'economia e delle finanze del 15 novembre 2001);

l) il regolamento di semplificazione per l'iscrizione negli *elenchi dei coltivatori diretti, coloni e mezzadri a fini previdenziali* (d.P.R. 7 dicembre 2001, n. 476).

Pubblica amministrazione

5 Profili generali

Con riguardo al trattamento di dati personali da parte delle pubbliche amministrazioni, anche nell'anno 2001 è rimasto aperto il delicato problema dell'attuazione, ancora largamente incompleta, delle disposizioni del d.lg. n. 135/1999 relative al trattamento di dati sensibili e giudiziari da parte di soggetti pubblici.

L'anno trascorso è stato caratterizzato anche dalle operazioni di censimento della popolazione che hanno impegnato tutti i comuni italiani, con conseguenti risvolti anche di carattere organizzativo per molte amministrazioni – specie locali – chiamate ad affrontare vari profili di protezione dei dati personali.

Su tali operazioni il Garante è intervenuto fornendo diverse indicazioni in una fase preventiva. Ha ricevuto successivamente segnalazioni e quesiti da parte di cittadini ed ha avviato un ciclo di ispezioni volto a verificare lo stato di attuazione delle prescrizioni in materia di tutela della riservatezza.

L'attività svolta in relazione al censimento ha costituito anche l'occasione per verificare il grado di acquisizione dei principi in materia di protezione dei dati personali da parte delle amministrazioni locali.

Tale verifica, unitamente alla valutazione del contenuto dei numerosi quesiti pervenuti, ha confermato la percezione che in diversi uffici pubblici manchi ancora un'adeguata comprensione delle regole introdotte dalla legge n. 675/1996 e degli effetti che le stesse comportano sul modo di amministrare.

Manca a tutt'oggi, come si è evidenziato anche nella relazione per il 2000, una visione di insieme dei problemi.

Viene poi privilegiato, a volte, un approccio di tutela meramente formale che porta peraltro a burocratizzare inutilmente le garanzie e gli adempimenti posti a tutela dei diritti delle persone e della sicurezza delle informazioni, senza alcun beneficio per gli interessati.

È sicuramente necessario, quindi, un miglioramento dei rapporti fra amministrazione e cittadino sul piano della tutela dei diritti della personalità.

6 Informazioni sensibili e altri dati particolari

Il d.lg. n. 135/1999 ha introdotto una nuova opportunità in termini di trasparenza, attraverso cui i soggetti pubblici possono trattare lecitamente dati sensibili e informazioni di tipo giudiziario.

Accanto all'originaria previsione dell'art. 22, comma 3, l. n. 675/1996, secondo la quale i trattamenti di dati sensibili sono consentiti solo se autorizzati da un'"*espressa norma di legge nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità d'interesse pubblico perseguite*", il decreto del 1999 ha infatti previsto una seconda soluzione che presuppone un ruolo più diretto delle amministrazioni interessate al trattamento.

In particolare, l'art. 5 del d.lg. n. 135, modificando il citato art. 22, ha stabilito che, laddove la legge o, in via transitoria, il Garante, abbiano individuato determinate rilevanti finalità d'interesse pubblico perseguite con un determinato trattamento, i soggetti pubblici possono utilizzare i dati dopo avere, però, previamente individuato e reso noti, "secondo i rispettivi ordinamenti", i tipi di dati e di operazioni di trattamento eseguibili.

Anche nell'anno 2001, gli atti adottati in tal senso dalle amministrazioni sono risultati, purtroppo, in numero assolutamente esiguo e non privi di gravi difetti, lacune ed errori, tanto da giustificare la considerazione che varie disposizioni del d.lg. n. 135/1999 sono rimaste sostanzialmente inapplicate e che diversi trattamenti di dati personali effettuati in ambito pubblico sono proseguiti in modo illecito, dal punto di vista formale e sostanziale.

L'adozione degli atti diretti ad individuare e rendere noti i tipi di dati e di operazioni effettuabili non è sempre avvenuta, poi, consultando preventivamente il Garante, come dovuto per legge, il che ha determinato ulteriori ripercussioni sulla loro validità.

Le rare ipotesi in cui è stato richiesto il parere su schemi di regolamento hanno invece consentito a questa Autorità di fornire alcune indicazioni che contengono utili riferimenti anche per altre amministrazioni (v. da ultimo il regolamento per la semplificazione dei procedimenti in materia di infermità da causa di servizio, pensione privilegiata ed equo indennizzo: d.P.R. 29 ottobre 2001, n. 461).

L'estensione del fenomeno della mancata attuazione del d.lg. n. 135, che è tale da esporre il nostro Paese a rischi di gravi violazioni della disciplina comunitaria, ha indotto il Garante a segnalare nuovamente al Governo, in data 17 gennaio 2002, ai sensi dell'art. 31, comma 1, lett. *m)*, della legge n. 675/1996, la necessità di adottare ogni opportuna iniziativa affinché il trattamento dei dati sensibili e giudiziari da parte dei diversi soggetti pubblici si conformi alle disposizioni vigenti. Con la medesima segnalazione, sono state inoltre enucleate alcune linee-guida alle quali le pubbliche amministrazioni devono uniformarsi nella predisposizione degli atti (in *Bollettino* n. 24, p. 40).

Quanto ai contenuti, il Garante ha ribadito che l'individuazione dei tipi di dati sensibili e giudiziari e delle operazioni di trattamento non rappresenta un adempimento formale di mera ricognizione e legittimazione di prassi esistenti. Presuppone piuttosto una selezione sul piano normativo di una serie di attività, al fine di attuare i princìpi vincolanti affermati dal d.lg. n. 135/1999 con effetti innovativi sui trattamenti già svolti.

È quindi necessaria una ricognizione scrupolosa di tutte le attività materiali che ciascun soggetto pubblico intende proseguire in relazione alle rilevanti finalità di interesse pubblico già individuate. Occorre poi una valutazione organica della stretta pertinenza e necessità dei dati personali e delle operazioni rispetto alle finalità medesime (art. 22, comma 3-*bis*).

La pubblicità che per legge deve essere data a tali provvedimenti, secondo i vari ordinamenti, deve inoltre

porre il cittadino in condizione di conoscere, con un apprezzabile grado di chiarezza, con quali modalità sono utilizzate delicate informazioni che ai sensi della direttiva comunitaria in materia non dovrebbero essere trattate in linea di principio.

Al fine di agevolare il lavoro delle amministrazioni, l'Autorità ha peraltro allegato al citato provvedimento un prospetto schematico da utilizzare come possibile base per la rilevazione delle attività svolte. In proposito, ha anche evidenziato che i dati personali trattati devono essere indicati dalle amministrazioni solo per categorie (es. dati sulla salute; vita sessuale; ecc.), senza, quindi, un eccessivo grado di dettaglio, operando tale ricognizione sulla base del presupposto che le tipologie di dati non così individuate e rese pubbliche non possono essere utilizzate.

Relativamente alla forma che tali provvedimenti promossi dalle amministrazioni pubbliche devono assumere, il Garante ha ribadito quanto affermato in altre circostanze e cioè che deve trattarsi di atti di natura regolamentare e non meramente amministrativa. Ciò trova conferma anche nel fatto che il d.lg. n. 282/1999 ha demandato tale compito, relativamente ai trattamenti di dati in ambito sanitario, proprio ad un regolamento del Ministro della salute. Se si opinasse diversamente, si giungerebbe del resto all'incongrua conclusione che operazioni come la comunicazione e la diffusione continuerebbero a presupporre una previa norma di legge o di regolamento quando sono effettuate su dati "comuni" (art. 27, commi 2 e 3, l. n. 675/1996), mentre verrebbero ad essere paradossalmente legittimate da atti di minor rilievo benché riguardanti la delicata area delle informazioni sensibili o di tipo giudiziario.

La forma regolamentare, poi, in ragione del particolare e più adeguato procedimento di formazione (interno ed esterno ai soggetti pubblici) assicura all'atto-regolamento una maggiore stabilità.

Il Garante, fermo restando il diritto dei cittadini di far valere i propri diritti nelle competenti sedi, anche in relazione agli eventuali danni subiti, si è da ultimo riservato, in presenza di accertate violazioni della disciplina in materia, di adottare specifici provvedimenti di blocco o divieto del trattamento.

Tuttavia, consapevole delle difficoltà che può comportare tale disciplina integrativa di dati sensibili, l'Autorità ha anche intrapreso forme di collaborazione con gli organismi rappresentativi delle autonomie locali, cui si accennerà nel paragrafo dedicato a questo tema (par. 12).

La necessità di prevedere le predette garanzie in riferimento ai tipi di dati e di operazioni eseguibili si è configurato in termini parzialmente differenti nei riguardi degli organismi sanitari pubblici: l'art. 2, comma 1, del citato d.lg. n. 282/1999 ha infatti affidato tale compito ad uno specifico decreto del Ministro della salute (da adottarsi sentiti la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano ed il Garante), che è stato previsto per permettere una disciplina uniforme del settore.

Le riunioni dell'apposito gruppo di lavoro, interrottesi con la legislatura, sono riprese – anche a seguito di diverse sollecitazioni – ma non sono giunte a compimento.

La mancata emanazione del decreto spiega effetti negativi in uno dei settori più delicati di applicazione della normativa sulla protezione dei dati personali. Oltre a privare i cittadini di importanti garanzie a tutela dei propri diritti fondamentali, costringe vari organismi sanitari a sollecitare più volte il consenso a milioni di cittadini, o ad ometterne la richiesta agli interessati, sebbene tale adempimento potrebbe essere estremamente semplificato proprio con le procedure previste dalla legge e che attendono di essere attuate con il decreto.

Sempre in materia di dati sanitari va segnalato il rilascio da parte del Garante della nuova autorizzazione generale n. 2/2002 relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, che trova parziale applicazione anche in ambito pubblico, con poche modifiche sostanziali rispetto a quella adottata in precedenza.

Per quanto concerne i dati a carattere giudiziario, il loro trattamento resta al momento regolato principalmente dall'art. 24 della legge n. 675/1996, il quale non prevede una disciplina differenziata fra soggetti pubblici e privati e stabilisce che il trattamento medesimo possa aver luogo solo se autorizzato da un'espressa norma di legge o da un provvedimento del Garante dal quale risultino le rilevanti finalità d'interesse pubblico perse-

guite dal trattamento, i tipi di dati trattati e le precise operazioni autorizzate.

L'art. 5 del d.lg. n. 135/1999 (come modificato dall'art. 15 del d.lg. n. 281/1999) ha previsto anche per tali dati la possibilità per le amministrazioni pubbliche di specificare i tipi di informazioni utilizzabili e di operazioni eseguibili in relazione alle finalità di rilevante interesse pubblico ivi indicate.

Tali rilevazioni hanno però incontrato i problemi appena ricordati a proposito dei dati sensibili. Anche in questo caso necessita, pertanto, una rapida emanazione dei regolamenti attuativi da parte di tutte le amministrazioni interessate.

Il Garante ha autorizzato detti trattamenti, come già in passato con l'autorizzazione n. 7 (rinnovata ora con scadenza al 30 giugno 2003) rilasciata a favore di soggetti privati e anche pubblici, in relazione ad alcune ulteriori rilevanti finalità di interesse pubblico.

Su un piano più specifico, sempre con riferimento al trattamento di dati giudiziari, merita di essere menzionata la richiesta presentata al Garante nel 2001 da parte di un'amministrazione comunale che chiedeva di essere autorizzata a trattare tali tipi di dati in relazione alle attività di predisposizione e di aggiornamento degli elenchi dei giudici popolari di cui alla legge n. 287/1951, ritenendo che le stesse non fossero comprese nel d.lg. n. 135/1999 o in altri atti autorizzatori del Garante.

Dette attività non risultavano specificamente menzionate in nessuno di tali provvedimenti, ma l'Autorità ha rilevato (v. nota del 30 luglio 2001) che, secondo l'art. 11 della menzionata legge n. 287, l'ufficio di giudice popolare *"è parificato a tutti gli effetti all'esercizio delle funzioni pubbliche elettive*" e che il trattamento dei dati a carattere giudiziario poteva pertanto intendersi autorizzato in termini generali in quanto riconducibile alle attività di rilevante interesse pubblico "*dirette all'applicazione della disciplina in materia di elettorato attivo e passivo…*" (art. 8, comma 1, d.lg. n. 135/1999).

Va infine ricordata, anche in questa sede, l'introduzione dell'istituto del *prior checking*. Il decreto legislativo n. 467/2001 ha previsto che il trattamento dei dati diversi da quelli sensibili ed a carattere giudiziario, qualora presenti rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che esso può determinare, è ammesso solo se è effettuato nel rispetto di specifici accorgimenti e misure a garanzia dell'interessato.

Tali cautele potrebbero essere quindi prescritte dal Garante anche nell'ambito di eventuali trattamenti effettuati da soggetti pubblici, sulla base dei princìpi sanciti dalla legge e nell'ambito di una verifica precedente all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, sulla base di un eventuale interpello del titolare.

7 Trasparenza dell'attività amministrativa

Nelle relazioni annuali presentate negli anni precedenti è stato più volte evidenziato che la normativa sulla tutela dei dati personali non può essere interpretata in una prospettiva di riduzione indiscriminata della trasparenza amministrativa e, in particolare, di quella che ne costituisce la sua più frequente forma di applicazione: il diritto di accesso agli atti amministrativi.

Rimandando al successivo paragrafo una disamina di alcuni aspetti relativi al diritto d'accesso, si intende dar conto di alcune indicazioni di questa Autorità che nell'anno preso in considerazione hanno offerto, in diversi casi, una chiave di lettura nel delicato bilanciamento (tra diritto di accesso ex art. 13 l. n. 675/1996 e diritto di accesso ex l. n. 241/1990) fra esigenze di trasparenza e tutela della riservatezza.

In particolare preme richiamare l'attenzione, come già fatto nella *Relazione 2000*, sull'incidenza che un diverso diritto di accesso, quale quello introdotto dall'art. 13 della legge n. 675/1996, ha avuto in termini di maggiore trasparenza dell'attività della pubblica amministrazione.

Quest'ultima disposizione consente all'interessato di accedere a singole informazioni personali che lo riguardano (anziché a documenti), con modalità tendenzialmente diverse da quelle previste dalla legge n. 241/1990 (visione e copia). Nonostante tale più specifica area di informazioni conoscibili, l'esercizio di questo nuovo diritto da parte degli interessati ha contribuito anch'esso ad una maggiore "apertura" e trasparenza della pubblica amministrazione: si pensi, ad esempio, agli effetti che esso ha avuto nei riguardi della conoscenza delle valutazioni operate sui dipendenti (v. *Provv.* 2 giugno 1999; sul punto v., *amplius*, par. 22).

Le esigenze di trasparenza delle attività pubbliche sono venute nuovamente in evidenza in diverse situazioni nel corso del 2001, anche in riferimento, ad esempio, alle attività dei consigli comunali e, in particolare, alla possibilità che le riunioni consiliari siano riprese da strumenti audiovisivi, specie quando vi sia il rischio che vengano divulgati dati sensibili.

Al riguardo si è rilevato che l'art. 8 del d.lg. n. 135/1999 consente alle amministrazioni pubbliche di trattare taluni dati di carattere sensibile (quali ad esempio quelli desumibili da opinioni espresse dai consiglieri nell'ambito delle sedute), nei limiti in cui ciò risulti necessario ad assicurare il rispetto del principio di pubblicità dell'attività istituzionale e fermo restando il divieto posto dall'art. 23, comma 4, della legge n. 675/1996 di diffondere i dati idonei a rivelare lo stato di salute.

Gli articoli 10 e 38 del testo unico delle leggi sull'ordinamento degli enti locali (d.lg. n. 267/2000) garantiscono, poi, espressamente un regime di pubblicità degli atti e delle sedute del consiglio comunale, rinviando ad un regolamento l'introduzione di eventuali limiti al regime di pubblicità sopra descritto.

Tale tipo di regolamento può costituire la sede idonea per disciplinare le modalità e i limiti di pubblicità delle sedute consiliari, ivi comprese le riprese televisive, nonché per indicare, eventualmente, le procedure attraverso le quali disporre volta per volta determinate limitazioni (v. *Provv.* 17 gennaio 2002). Ciò al fine di assicurare, con riferimento ad alcune informazioni particolarmente "delicate", i diritti della personalità e la dignità dei soggetti presenti alla seduta o che siano oggetto del relativo dibattito.

Invero, rispondendo al quesito di un Comune, il Garante ha affermato che la diffusione delle immagini delle sedute comunali da parte della televisione locale deve ritenersi in generale consentita – anche al di fuori dell'ambito locale ed anche nel caso in cui ad esse vengano aggiunte le opinioni e i commenti del giornalista – sulla base di quanto disposto dall'art. 25 della legge 675/1996 e dal Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica. Ciò purché i presenti siano stati debitamente informati dell'esistenza delle telecamere e della successiva diffusione delle immagini. In ogni caso, devono essere

fatte salve le necessarie cautele per prevenire l'indebita divulgazione di dati sensibili, quali quelli relativi alle condizioni di salute (v. *Newsletter* 11-13 marzo 2002, in *www.garanteprivacy.it*).

Il tema è stato anche affrontato, sotto ulteriori profili, con la pronuncia del 28 maggio 2001, con la quale sono stati forniti ulteriori chiarimenti in merito al problema della diffusione via Internet, tramite *webcam* riproduttive anche del sonoro, di avvenimenti caratterizzati dal tratto della pubblicità, quali le conferenze stampa o lo svolgimento delle sedute pubbliche di organi come il consiglio comunale.

L'Autorità ha avuto modo di puntualizzare che simili fattispecie non pongono particolari problemi dal punto di vista del rispetto delle prescrizioni contenute nella l. n. 675/1996, a patto di osservare alcune cautele. In particolare, occorrerà anzitutto informare tutti i presenti della diffusione delle immagini, anche attraverso l'affissione di avvisi chiari e sintetici e, per i dati sensibili, osservare rigorosamente il principio di stretta necessità di cui all'art. 8 d.lg. 11 maggio 1999, n. 135, evitando in ogni caso, come si è detto, di diffondere dati idonei a rivelare lo stato di salute.

Al contrario, l'uso di simili strumenti risulta non ammissibile sia con riferimento alle riunioni di organi che, in base a leggi o regolamenti, non sono aperte al pubblico (quali ad esempio le riunioni della giunta municipale o di varie commissioni), sia per quanto concerne il ricevimento del pubblico e l'ordinaria attività degli uffici, posto che le pur irrinunciabili finalità di trasparenza non possono essere perseguite imponendo a ciascun cittadino un obbligo di diffondere la propria immagine durante i colloqui con il sindaco o con un altro rappresentante comunale o, addirittura, di rivelare al pubblico il contenuto della conversazione che può riguardare peraltro delicati aspetti personali o familiari. Senza dimenticare, naturalmente, che la riproduzione stabile di immagini può comportare anche un controllo a distanza della qualità o quantità del lavoro dei dipendenti comunali, comunque vietato in base allo Statuto dei lavoratori.

In tema di trasparenza l'Autorità è pervenuta a conclusioni analoghe a quelle complessivamente evidenziate in questo paragrafo affrontando alcuni profili relativi alla pubblicità dei dati relativi agli iscritti negli albi professionali, sui quali si sofferma il par. 31.

Va segnalato da ultimo che l'Autorità ha rappresentato il quadro attuale della normativa italiana in materia di conoscibilità dei dati relativi agli incarichi da parte dei dipendenti pubblici, quale elemento di comparazione da utilizzare, assieme a quello riferito ad altri Paesi, nell'ambito della pronuncia pregiudiziale sollecitata alla Corte di giustizia delle comunità europee in riferimento alla direttiva n. 95/46/CE del 1995 (nota del 13 aprile 2001: fattispecie in tema di conoscibilità dei compensi corrisposti a dipendenti pubblici e di imprese che perseguono un pubblico interesse, se superiori ad una certa soglia).

8 Accesso ai documenti amministrativi

L'Autorità ha continuato ad occuparsi, nel corso dell'anno, del rapporto tra la normativa sul diritto di accesso ai documenti amministrativi e le disposizioni che tutelano il diritto alla riservatezza dei dati personali, anche con riferimento al diritto riconosciuto ai consiglieri comunali e provinciali di accedere agli atti e ai documenti detenuti presso le rispettive amministrazioni locali (legge n. 241/1990 e art. 43 d.lg. n. 267/2000).

Trattasi di un tema delicato e complesso sul quale dottrina e giurisprudenza dibattono da tempo, soprattutto in seguito all'entrata in vigore della legge n. 675/1996 e del d.lg. n. 135/1999 (per una sintetica ricostruzione degli orientamenti giurisprudenziali v. *Relazione 2000*, p. 9).

Il Consiglio di Stato ha tra l'altro sostenuto, sulla base di un'interpretazione dei commi 1 e 2 del citato art. 16 del d.lg. n. 135/1999, la sussistenza di un'autonoma previsione normativa in materia di accesso ai dati sulla salute e sulla vita sessuale (C.d.S. Sez. VI, n. 1882/2001). Secondo tale impostazione, il legislatore del 1999 avrebbe consentito il trattamento dei dati sensibili diversi da quelli sulla salute e sulla vita sessuale, mentre avrebbe condizionato l'accesso ai documenti amministrativi contenenti dati sulla salute e sulla vita sessuale ad un giudizio comparativo tra il diritto da far valere e il diritto alla riservatezza dell'interessato. Il Consiglio di Stato ha inoltre sostenuto che tale valutazione deve essere effettuata in concreto, "in modo da evitare il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica dei diritti in contesa".

Il Garante aveva rilevato già, sin dai primi mesi della propria attività, che la legge n. 675/1996 non ha abrogato la normativa a tutela della trasparenza e dell'accesso agli atti della pubblica amministrazione (art. 43, comma 2, l. n. 675/1996), affermando che l'esistenza di una specifica normativa sulla protezione dei dati personali non può essere invocata per negare o limitare il diritto di accesso e che spetta all'amministrazione destinataria della richiesta valutare in concreto la sussistenza delle condizioni per accedere ai documenti amministrativi previste dalla legge (artt. 22 e ss. l. n. 241/1990; art. 2 d.P.R. n. 352/1992; art. 43 d.lg. n. 267/2000).

Tra i numerosi atti e provvedimenti adottati nel corso dell'anno, con i quali è stato confermato l'orientamento sinteticamente richiamato, si citano, a titolo meramente esemplificativo, il parere espresso a favore del Ministero dei trasporti e della navigazione (del 16 febbraio 2001) e quello reso alla Questura di Roma (del 4 settembre 2001).

Le suddette amministrazioni avevano chiesto un parere su due richieste di accesso loro pervenute, l'una relativa agli atti di una gara d'appalto e l'altra presentata da un avvocato della vedova di una guardia giurata deceduta durante una rapina, avente ad oggetto alcuni atti dell'ente di cui la vittima era dipendente.

In entrambi i pronunciamenti sono state fornite indicazioni utili per la risoluzione dei quesiti formulati, anche sotto il profilo dei limiti normativi al diritto di accesso, e ha specificato che le amministrazioni pubbliche, nel regolamentare le modalità di esercizio di tale diritto, possono definire casi di esclusione di tale diritto in conformità ai criteri normativi specificamente previsti (art. 24, comma 2, lett. *d)*, l. n. 241/1990; art. 8, comma 5, lett. *d)*, d.P.R. n. 352/1992).

In particolare, nel parere alla Questura di Roma si è ricordato che l'amministrazione destinataria della richiesta di accesso deve accertare la sussistenza dell'interesse giuridicamente rilevante e delle altre condizioni previste dalla normativa, anche alla luce delle recenti disposizioni in materia di indagini difensive secondo le quali il difensore può chiedere direttamente i documenti all'amministrazione che ha adottato il provvedimento o che lo detiene stabilmente.

Sul rapporto tra il diritto di conoscere solo i dati personali del richiedente e il diritto di accesso agli atti della pubblica amministrazione il Garante è intervenuto anche nell'ambito di alcune decisioni su ricorsi presentati

ex art. 29 della legge n. 675/1996 (cfr. *Provv.* 27 giugno 2001; 4 luglio 2001; 24 luglio 2001; 28 settembre 2001), con le quali sono stati nuovamente evidenziati alcuni dei caratteri distintivi dei due diritti, talora erroneamente ritenuti simili e riconosciuti a tutela delle medesime situazioni giuridiche soggettive.

In proposito si è registrata una diffusa propensione da parte di soggetti richiedenti e di titolari di trattamenti in ambito pubblico e privato a confondere le distinte condizioni e il diverso ambito di applicazione delle due normative (l. n. 241/1990 e l. n. 675/1996).

Al riguardo il Garante, oltre a soffermarsi sui profili sostanziali delle questioni, ha posto in evidenza un discrimine procedurale, sottolineando che il valido esercizio del diritto tutelato dall'art. 13 della l. n. 675/1996 determina a carico del titolare o del responsabile del trattamento l'obbligo di confermare l'esistenza o meno delle informazioni relative all'interessato e di comunicarle a quest'ultimo senza ritardo, in forma intelligibile, estrapolandole, ove necessario, da archivi, banche dati, atti o documenti che le contengono. Diversamente da quanto previsto dalla normativa sull'accesso agli atti amministrativi, l'adempimento della richiesta di accesso può avvenire anche tramite l'esibizione e/o la consegna in copia della documentazione solo quando l'estrazione dei dati risulti particolarmente difficoltosa e secondo le modalità prescritte dallo stesso art. 13 e dall'art. 17 del d.P.R. n. 501/1998.

9 Banche dati di rilevanti dimensioni e censimento della popolazione

Come si è già sottolineato nelle due relazioni annuali precedenti, la materia della costituzione di grandi banche dati ha registrato di recente un forte sviluppo.

Il ricorso ad archivi di grandi dimensioni continua a presentare vantaggi sul piano dell'efficienza dell'attività amministrativa, per l'elevato numero di informazioni che vi sono detenute e per le più agevoli interconnessioni che possono operarsi.

Per altro verso, tale tendenza alimenta elementi di preoccupazione per i cittadini e induce l'Autorità a rivolgere una particolare attenzione al fenomeno, per valutare l'incidenza degli effetti delle nuove tecnologie sui diritti fondamentali della personalità.

In questo quadro si affacciano all'orizzonte alcune prime iniziative in tema di *e-government*.

In proposito, su invito del Dipartimento del Ministro per l'innovazione e le tecnologie, l'Ufficio del Garante ha collaborato – per gli aspetti di propria competenza – alla redazione di un bando per progetti di *e-government* che verranno presentati nel corso del 2002 ed ha assicurato la propria disponibilità per la loro successiva valutazione sotto il profilo del rispetto della normativa in materia di protezione dei dati personali.

Si è infatti avvertito il rischio che in alcuni programmi volti a migliorare l'efficienza delle pubbliche amministrazioni possano risultare trascurati i profili della protezione dei dati, anche in ragione dell'insufficiente grado di "metabolizzazione" della normativa in materia.

Accanto a questo tipo di attività preventiva rispetto all'inizio dei trattamenti, l'Autorità, sempre con riferimento alla possibile creazione di grandi banche dati, ha prestato particolare attenzione al profilo inerente alle operazioni di censimento, con riguardo a varie fasi del suo svolgimento: da quella consultiva a quella di controllo delle procedure adottate.

Specifica attenzione è stata tra l'altro prestata alla raccolta delle informazioni relative all'appartenenza linguistica nelle province di Trento e Bolzano.

Con riguardo alla prima di queste indagini, tesa a determinare la consistenza e la dislocazione territoriale degli appartenenti alle popolazioni di lingua ladina, mochena e cimbra residenti in quella provincia, l'Autorità, all'atto di rendere il prescritto parere, ha fornito precise indicazioni sul modello predisposto, ponendo l'accento sull'esigenza di rispettare i principi di pertinenza e di non eccedenza con riguardo ad alcune specifiche domande che evidenziavano con precisione il nominativo dell'intervistato e la sua data di nascita. Considerato, poi, che detta rilevazione era da considerarsi di carattere facoltativo per gli interessati, è stato chiesto agli enti competenti di specificare nei modelli che la mancata risposta non avrebbe comportato alcuna conseguenza.

In termini più generali, poi, è stata constatata la mancata previsione di tale rilevazione nel Programma statistico nazionale (PSN), richiesta dall'art. 6-*bis* del d.lg. n. 322/1989 introdotto dall'art. 11 del d.lg. n. 281/1999, e ne ha chiesto quindi l'integrazione.

Analoga inosservanza è stata registrata con riferimento all'indagine condotta nella provincia autonoma di Bolzano relativamente alla determinazione della consistenza dei gruppi linguistici italiano, tedesco e ladino.

Tale ultima rilevazione, per il suo carattere obbligatorio e generalizzato, ha già in passato sollevato forti preoccupazioni in larghi strati dell'opinione pubblica, che in quest'occasione sono state portate all'attenzione del Garante in particolare da un'associazione locale. Il sistema prevede infatti la raccolta, in occasione del censimento generale della popolazione, della dichiarazione di appartenenza linguistica di tutti i cittadini nella provincia di Bolzano, ivi compresi i minori a partire dai 14 anni. Le dichiarazioni sono state conservate presso i locali uffici giudiziari, anche per eventuale documentazione che potrebbe essere rilasciata all'interessato su sua richiesta, per essere presentata in determinate occasioni (partecipazione a concorsi pubblici, candidature alle elezioni, rapporti con le forze di polizia e la magistratura, ecc.).

9

Nell'esaminare contestualmente il reclamo presentato da un'associazione e un progetto di modifica della normativa vigente (art. 18 d.P.R. n. 752/1976), il Garante ha rilevato che la raccolta sistematica delle dichiarazioni di appartenenza linguistica di tutti i cittadini, a fronte di un utilizzo dei dati che si rivela spesso solo occasionale ed eventuale, si pone in contrasto con i principi della legge, della direttiva europea sulla *privacy* e della convenzione-quadro per la tutela delle minoranze nazionali.

Senza entrare nel merito del più ampio problema della c.d. proporzionale etnica, l'Autorità ha osservato come il quadro normativo internazionale, comunitario e nazionale di riferimento sia mutato rispetto al periodo nel quale è stato varato l'attuale meccanismo di raccolta e di utilizzazione delle informazioni sull'appartenenza linguistica. Alla luce di questi mutamenti, la raccolta sistematica di tali dichiarazioni non è risultata conforme ai principi di pertinenza e di non eccedenza del trattamento sanciti dalla normativa sulla *privacy*.

Anche considerando le garanzie attualmente introdotte nel sistema (consegna e conservazione delle dichiarazioni in busta chiusa, utilizzo solo a richiesta dell'interessato o per motivi di giustizia, ecc.), la gestione e la conservazione di un così alto numero di dati sensibili sono apparse quindi potenzialmente lesive del diritto alla riservatezza dei dichiaranti e comunque sproporzionate rispetto agli scopi perseguiti.

Quanto riscontrato dall'Autorità non ha ancora portato ad innovazioni sostanziali sul piano legislativo. Poco dopo il citato pronunciamento il Governo ha trasmesso all'Autorità due schemi normativi volti alla revisione dell'art. 18 del d.P.R. n. 752/1976, il primo dei quali ha stabilito, come principale innovazione al regime previgente, che la consegna e la custodia delle dichiarazioni di appartenenza linguistica vengano effettuate non più presso il tribunale competente per territorio, ma presso il comune di residenza o presso il commissariato del Governo, a scelta dell'interessato.

Tale nuova soluzione, ad avviso dell'Autorità, presenta diversi inconvenienti, quali, ad esempio quello di: *a)* spostare la custodia delle dichiarazioni presso strutture che possono essere meno organizzate dal punto di vista della sicurezza (si pensi ad esempio a piccoli comuni); *b)* rendere più difficile il controllo delle operazioni di distruzione; *c)* agevolare possibili forme di improprio "controllo indiretto" presso le amministrazioni locali, ove si potrebbero effettuare già autonome valutazioni prendendo spunto dalla scelta degli interessati di depositare o meno le dichiarazioni presso di esse; *d)* introdurre, per altro verso, difficoltà supplementari di ordine amministrativo e burocratico, ad esempio in caso di uso delle dichiarazioni per fini di giustizia (l'a.g. dovrà individuare preliminarmente dove venga detenuta la dichiarazione) o in caso di cambio di residenza.

La soluzione prefigurata dal Governo non ha inoltre preso in considerazione uno degli elementi in ordine al quale si era manifestata la preoccupazione del Garante, avendo l'Autorità richiamato l'attenzione anche sul più generale problema dell'effettiva necessità di provvedere ad una raccolta di molteplici dati di siffatto genere.

Ciò premesso, e considerato che uno schema era stato inviato al Garante dopo essere già stato approvato dal Consiglio dei ministri (v. d.lg. 18 gennaio 2002, n. 11, in *G.U.* 20 febbraio 2002, n. 43), l'Autorità ha potuto solo esprimere il proprio auspicio che le norme in parola vengano al più presto integrate e modificate nel senso indicato.

Ha manifestato al contempo l'esigenza di una attenta vigilanza affinché in sede applicativa sia posta sin d'ora la massima attenzione sull'attuazione delle misure di sicurezza e sulla prevenzione di ogni uso improprio dei dati detenuti.

Le medesime necessità di modifica ed integrazione del testo si sono rivelate anche con riferimento al secondo schema presentato all'Autorità, il quale è sembrato anch'esso allontanarsi dalle osservazioni a suo tempo formulate. A parte, infatti, la decisione di evitare la pubblicazione nelle graduatorie finali delle appartenenze ai diversi gruppi linguistici e la previsione di forme volte a ridurre la presentazione delle dichiarazioni in sede concorsuale, sono stati eliminati alcuni articoli della bozza precedente che pure avrebbero esercitato un effetto positivo su alcuni casi di applicazione concreta della normativa vigente.

Da ultimo, il Ministro per gli affari regionali ha formulato con nota del 24 aprile 2002, diretta all'Autorità, l'impegno a ricercare una nuova soluzione che possa riaffrontare il problema ed essere valutata positivamente sul piano che interessa la competenza del Garante, osservando la particolare procedura prevista per le modifiche alle norme di attuazione della regione a statuto speciale, regione nella quale, ha osservato il Ministro, le regole sulla *privacy* devono essere parimenti rispettate così come in tutto il Paese.

Il problema della possibile creazione di una grande banca dati sulla base dell'appartenenza etnico-linguistica si è presentato in altra sede con riguardo alla richiesta, rivolta da alcuni comuni ed associazioni della regione

Friuli-Venezia Giulia, di poter compilare in lingua slovena i questionari relativi al 14° censimento generale della popolazione.

L'Istat si era opposto a tale richiesta, oltre che per alcuni problemi di ordine tecnico, anche per il fatto che in tal modo si sarebbe originata una raccolta di dati idonei a rivelare l'origine etnica degli interessati, essendo ancora non efficace la normativa introdotta dalla legge 23 febbraio n. 2001, n. 38, che prevedeva tale possibilità.

L'Autorità, interpellata al riguardo, ha fatto presente di non ravvisare alcuna incompatibilità di fondo all'introduzione di questionari compilabili anche in sloveno, a condizione che fossero rispettate le specifiche modalità stabilite dal decreto n. 281/1999 per i trattamenti statistici e, in particolare, che fossero previamente indicati nel Piano statistico nazionale (PSN) i dati sensibili oggetto di trattamento, specificando per quali rilevazioni gli stessi sarebbero stati utilizzati, nonché le relative modalità di trattamento.

Verificata la disponibilità dell'Istat, il Governo ha provveduto, con il d.P.C.M. 12 novembre 2001, a modificare il PSN 2001-2003 autorizzando la distribuzione di questionari in lingua slovena.

10 Carta d'identità elettronica e tessera elettorale

La carta d'identità e il documento d'identità elettronico, introdotti in Italia dalla l. 15 maggio 1997, n. 127 e successivamente regolamentati da fonti normative di rango primario e secondario, sono stati oggetto di attenta riflessione e di controllo da parte dell'Autorità sin dai primi mesi della sua attività, come documentato dalle precedenti relazioni annuali.

Essi costituiscono, insieme alla carta sanitaria elettronica, i primi importanti documenti informatici promossi dalla pubblica amministrazione.

La loro istituzione rientra in un importante processo di trasformazione del rapporto tra cittadino e pubblica amministrazione e di ristrutturazione dell'apparato burocratico del paese, in atto a livello nazionale dai primi anni novanta.

I documenti elettronici sono infatti espressione dei principi di semplificazione, snellimento e razionalizzazione dell'attività amministrativa e costituiscono uno sforzo di adeguamento della stessa ai caratteri di diffusa informatizzazione e globalizzazione dell'economia e delle più moderne forme di informazione.

Tale processo deve risultare in linea con gli orientamenti dell'Unione europea che da tempo ha sollecitato le amministrazioni pubbliche nazionali ad avvalersi di nuove tecnologie anche al fine di contribuire ad una rapida affermazione di servizi di interesse pubblico dinamici basati sulla conoscenza.

Il Consiglio e il Parlamento europeo sono infatti da tempo impegnati nell'elaborazione di principi generali comuni per consentire agli Stati membri di regolamentare la materia in modo organico e di contribuire alla creazione di uno spazio europeo economico e normativo.

Vi è peraltro il rischio che la diffusione dei documenti elettronici e l'interconnessione tra le pubbliche amministrazioni degli archivi informatici (cfr., a titolo meramente esemplificativo, l'allineamento dei dati contenuti nelle anagrafi comunali con quelli contenuti nell'archivio dell'Agenzia delle entrate per la carta e il documento d'identità elettronici) possano comportare una riduzione dei diritti della persona e della riservatezza dei dati personali.

Ciò anche in considerazione del fatto che su questi profili l'Italia non è dotata di una legislazione in tutto idonea a contemperare le esigenze di semplificazione e razionalizzazione dell'attività amministrativa con quelle di tutela della persona, anche in attuazione delle prescrizioni e dei principi generali già contenuti nella normativa comunitaria.

Con specifico riferimento alla carta d'identità elettronica occorre ricordare che essa potrebbe svolgere due funzioni: quella tradizionale di documento di riconoscimento personale del titolare e quella tipica delle c.d. *carte intelligenti,* ossia l'idoneità a fornire servizi ai cittadini per via telematica.

La polifunzionalità della carta sembra avere indotto il legislatore a stabilire che essa debba contenere i dati identificativi della persona e il relativo codice fiscale, e che possa, invece, contenere l'indicazione del gruppo sanguigno, le opzioni di carattere sanitario previste dalla legge, alcuni dati biometrici con esclusione del d.n.a., le informazioni occorrenti per la firma elettronica e tutti gli altri dati utili all'esercizio dell'attività amministrativa e all'erogazione dei servizi (art. 36 d.P.R. n. 445/2000).

Al riguardo, l'Autorità, nell'esercizio della funzione consultiva di cui è titolare, ha più volte segnalato, negli anni precedenti, la necessità di individuare con maggiore attenzione e proporzionalità la tipologia dei dati da inserire nei documenti elettronici, i soggetti che possono eventualmente accedere alle varie categorie di dati e

le garanzie per gli interessati, in particolare in relazione al conferimento di delicate informazioni quali i dati sanitari o biometrici.

In un parere espresso alla Presidenza del Consiglio dei Ministri sullo schema di testo unico delle norme in materia di documentazione amministrativa, poi emanato con il citato d.P.R. 28 dicembre 2000, n. 445, il Garante aveva già ribadito la necessità di specificare con maggiore dettaglio, da un lato, le condizioni, le modalità e i limiti nei quali la carta d'identità e il documento elettronico possono contenere i dati sensibili sopra citati; da un altro lato, i casi in cui il cittadino è obbligato a conferire i suddetti dati e i casi in cui il medesimo risulta legittimato ad opporvisi (cfr. parere del 7 settembre 2000). Queste indicazioni non sono state adeguatamente prese in considerazione. Con riferimento poi al piano di sperimentazione dei documenti d'identità elettronici predisposto dal Ministero dell'interno e già in fase di avanzata attuazione, si deve continuare a registrare la mancata consultazione del Garante da parte del Ministero sui singoli progetti, su cui pure erano state fornite ampie assicurazioni (cfr. *Relazione 2000*, p. 14).

In precedenza l'Autorità aveva infatti segnalato la necessità di essere consultata ai sensi dell'art. 31, comma 2, l. n. 675/1996, anche allo scopo di contribuire ad una valutazione omogenea dell'attività svolta dai primi comuni interessati dalla sperimentazione (cfr. *Provv.* 12 luglio 2000), ricevendo, come si è detto, l'impegno del Ministro dell'interno a tenere in massima considerazione, in sede di attuazione del decreto concernente le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione dei documenti d'identità elettronici, le osservazioni del Garante non recepite dal decreto medesimo (cfr. d.m. 19 luglio 2000).

È quindi auspicabile che le nuove iniziative per sperimentare e realizzare a regime la carta d'identità elettronica ed eventuali altri supporti informatici analoghi (v., ora, il d.lg. 23 gennaio 2002, n. 10, art. 8) interagiscano meglio con i principi richiamati più volte dal Garante specie in tema di proporzionalità.

La tessera elettorale, documento sostitutivo e permanente del certificato elettorale, è stato introdotto nel corso dell'anno in forma cartacea (cfr. d.P.R. 8 settembre 2000, n.120), nonostante la previsione legislativa sulla possibilità di adottare tale tessera su supporto informatico, anche attraverso l'utilizzazione congiunta della carta d'identità elettronica (art. 13 l. 30 aprile 1999, n. 120).

Tale questione ha a lungo impegnato l'Autorità lo scorso anno, dapprima in incontri con rappresentanti del Ministero dell'interno, e poi nell'elaborazione di un primo articolato parere espresso sullo schema del regolamento concernente la tessera elettorale (cfr. parere del 17 novembre 1999; v. anche la *Relazione 1999*, p. 29).

In tale occasione il Garante aveva formulato varie osservazioni critiche sull'ipotesi di introdurre, seppure per una fase transitoria, la tessera elettorale in forma cartacea e aveva suggerito di utilizzare direttamente il modello su supporto informatico.

L'Autorità aveva in particolare espresso la preoccupazione che la tessera cartacea, valida per un numero consistente di consultazioni elettorali e/o referendarie e riportante l'indicazione dell'avvenuto voto diversamente dal modello informatico, comportasse una conoscibilità dei dati relativi al comportamento elettorale dell'interessato eccessiva rispetto alle finalità della legge istitutiva (l. n. 120/1999) e non pienamente conforme alla normativa sulla protezione dei dati personali.

Tali osservazioni, qui riportate in estrema sintesi, non sono state accolte nel regolamento emanato con d.P.R. 8 settembre 2000, n. 299, in quanto, come risulta da una relazione del sottosegretario di Stato per l'interno, l'interesse al controllo sull'esercizio del diritto di voto è stato ritenuto prevalente sull'esigenza di tutela della riservatezza dei cittadini (cfr. resoconto stenografico Camera, I commissione, 27 ottobre 1999).

L'Autorità ha però vivamente auspicato un riesame a breve dell'intera questione, anche in considerazione delle aspre e diffuse critiche successivamente intervenute sul documento così come adottato.

In particolare, in occasione delle ultime consultazioni elettorali (12 maggio 2001), l'Autorità ha ribadito che alcuni profili del nuovo modello di tessera elettorale cartaceo non rispettano la disciplina sulla riservatezza dei cittadini e il principio della segretezza del voto, rendendo conoscibile il comportamento elettorale del cittadino. Il Garante ha pertanto sollecitato nuovamente il Ministero ad un complessivo riesame della questione,

segnalando anche alcuni specifici accorgimenti per evitare che l'attuale modalità cartacea di certificazione della partecipazione al voto possa eventualmente evidenziare particolari condizioni dell'elettore, quali la degenza in ospedale e la detenzione in carcere (v. comunicato stampa del 24 aprile 2001, in *Bollettino* n. 19, p. 44). Va peraltro nuovamente evidenziata la collaborazione svoltasi, con esito positivo, con il Ministero dell'interno nel quadro della revisione della disciplina sull'esercizio del diritto di voto da parte degli elettori infermi (v. par. 3 lett. *d)* della presente Relazione).

11 Documentazione anagrafica e materia elettorale

Il Garante ha continuato, nel corso del 2001, a soddisfare numerose richieste di chiarimenti avanzate da enti locali con riferimento alla disciplina, parzialmente diversa, ad essi applicabile pur nell'uniformità del quadro relativo a tutti i soggetti pubblici non economici. Diverse pronunce hanno riguardato in particolare i problemi relativi alla comunicazione e alla diffusione dei dati nell'ambito delle norme riguardanti gli atti anagrafici, lo stato civile e le liste elettorali.

Era stata affrontata già nel corso del 2000 (v. *Provv.* 26 maggio e 5 dicembre 2000, rispettivamente in *Bollettino* n. 13, p. 15 e n. 14/15, p. 22) la delicata questione della creazione di una nuova e più articolata anagrafe regionale della popolazione realizzata integrando con legge della Regione Friuli-Venezia Giulia (n. 11/2000) le disposizioni concernenti l'anagrafe dei beneficiari delle agevolazioni sul prezzo delle benzine.

Sul tema il Garante è tornato con parere del 10 aprile 2001 (*Bollettino* n. 19, p. 6) per ribadire che tali iniziative non sono compatibili con la disciplina anagrafica (tenendo anche conto dei limiti cui soggiace la potestà normativa regionale in materia di protezione dei dati personali) e, conseguentemente, con i principi dell'articolo 27 della legge n. 675/1996. Non sono state ritenute ammissibili, pertanto, né la libera consultazione diretta delle anagrafi (attraverso, ad esempio, l'interrogazione individuale o di massa di qualsiasi dato contenuto negli archivi), né la loro indifferenziata interconnessione con le banche dati del soggetto richiedente le informazioni medesime.

In relazione al quadro relativo all'attività di comunicazione verso i cittadini da parte delle istituzioni comunali, sono state esaminate le segnalazioni di alcuni cittadini di Roma e di Milano che, avendo ricevuto una lettera da parte dei rispettivi sindaci, avevano chiesto all'Autorità di verificare se l'inoltro della comunicazione fosse avvenuto nel rispetto della normativa in materia di trattamento dei dati personali. La voluta personalizzazione delle funzioni dei sindaci ha avuto come conseguenza anche una personalizzazione delle loro comunicazioni, il che ha reso meno agevole tracciare confini netti tra comunicazione "istituzionale" e comunicazione "non istituzionale", generando a volte incertezza nell'opinione pubblica e reazioni da parte di alcuni cittadini.

Il Garante, con due provvedimenti del 19 aprile 2001 (in *Bollettino* n. 19, p. 8 e 10), ha ritenuto di non poter escludere che le comunicazioni inviate fossero riconducibili all'attività di informazione e di comunicazione istituzionale delle pubbliche amministrazioni, pur osservando che, dall'esame della documentazione trasmessa dai due Comuni, potevano ravvisarsi alcuni punti incerti, se rigorosamente confrontati con il paradigma normativo, e tuttavia non tali da configurare un palese contrasto con le norme che regolano la materia.

Un tema ricorrente ha riguardato per altro verso la possibilità per i comuni (ricorrendo alla stipula di convenzioni *ad hoc*), di favorire la trasmissione di dati e documenti anagrafici a soggetti privati avvalendosi della tecnica dell'*outsourcing*, già ampiamente utilizzata nel settore privatistico.

In un caso, il Comune di Roma aveva incaricato una cooperativa di effettuare, mediante convenzione, un servizio di protocollazione di atti di stato civile provenienti dall'estero giacenti presso gli uffici comunali. L'Autorità, pur riconoscendo che nello svolgimento dei propri compiti istituzionali il soggetto pubblico può ricorrere a privati affidando ad essi determinate attività anche attraverso concessioni, appalti o convenzioni (nota prot. 1686/01 del 17 febbraio 2001), ha tuttavia ricordato che, a garanzia della tutela della riservatezza dei dati personali trattati dal soggetto privato, la convenzione deve contenere espresse disposizioni relative alla nomina del responsabile e dei soggetti incaricati del trattamento prevedendo altresì idonee garanzie per la sicurezza dei trattamenti e dei dati ai sensi dell'art. 15 della l. n. 675/1996 e del d.P.R. n. 318/1999.

Analogamente, il Comune di Lamezia Terme, sulla base di una deliberazione di giunta e di una convenzione, aveva affidato ad uno studio associato di liberi professionisti l'incarico per la gestione e la riscossione di alcuni tributi locali, prevedendo per tale finalità la comunicazione allo stesso studio di dati personali, anche

sensibili, dei contribuenti; benché il Comune avesse disposto l'interruzione della comunicazione dei dati personali nei confronti del suddetto studio privato dopo l'audizione delle parti svoltasi nell'ambito del procedimento (art. 29 l. n. 675/1996), il Garante si è riservato comunque di valutare con un autonomo procedimento, le circostanze segnalate riguardo alla designazione dei responsabili del trattamento e degli incaricati (*Provv.* 19 dicembre 2001, in *Bollettino* n. 23, p. 111).

Per quanto attiene agli interventi relativi all'uso di dati per finalità politico-elettorali, si è precisato che il diritto di accesso alle liste elettorali di sezione utilizzate nei singoli seggi in precedenti elezioni, nelle quali sono contenuti dati idonei a rivelare l'effettiva partecipazione dei cittadini alle votazioni, è esercitabile da ogni elettore entro il termine di 15 giorni dal deposito nella cancelleria, al fine dell'eventuale controllo sulla regolarità delle operazioni elettorali. Fuori dal contesto e dai limiti descritti, pertanto, i titolari di cariche elettive che lo richiedano in occasione di successive consultazioni elettorali non possono accedere a dette liste (nota 4 aprile 2001, in *Bollettino* n. 19, p. 5).

Continuando la collaborazione con l'Amministrazione finanziaria, l'Autorità ha reso il proprio parere (*Provv.* 27 giugno 2001, in *Bollettino* n. 21, p. 15) su uno schema di regolamento volto ad istituire un sistema di comunicazione tra regioni ed enti locali per pianificare e gestire la relativa autonomia tributaria e per consentire il decentramento catastale. In tale occasione è stato precisato che l'attivazione dei flussi di dati tra amministrazioni, l'accesso agli archivi, l'apporto al sistema informativo da parte di ciascun ente e le finalità istituzionali perseguibili devono essere regolati sulla base di una più analitica disciplina di riferimento, senza rinvii a fonti ulteriori; è stato altresì suggerito di delineare un nucleo essenziale di misure che i soggetti coinvolti devono osservare per garantire la sicurezza dei dati e il rispetto dei principi di correttezza e di pertinenza delle informazioni trattate (art. 9 l. n. 675/1996).

12 Enti locali

Nel quadro della realizzazione del progetto relativo alla rete unitaria della pubblica amministrazione, la funzione anagrafica riveste un ruolo centrale, in quanto essa è fonte di informazioni di base indispensabili per l'attività di 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 seguito in vista del conseguimento della semplificazione amministrativa e della riduzione dei costi dei servizi pubblici. Nell'ambito del medesimo Sistema, il Ministero dell'interno aveva posto l'esigenza di realizzare 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 innovazione sull'ordinamento anagrafico, e l'ampia individuazione dei soggetti legittimati ad accedere all'Indice, avevano originato fra il 1999 e il 2000 diverse prese di posizione del Garante nei riguardi del Ministro dell'interno nelle quali l'Autorità ha fatto presente che la materia esigeva un intervento a livello legislativo che permettesse anche di definire con chiarezza le finalità di utilizzo, i soggetti aventi accesso e il contenuto stesso di tale Indice. Successivamente a questi interventi, con il d.l. 27 dicembre 2000, n. 392, convertito in legge 28 febbraio 2001, n. 26, è stato appunto previsto da una specifica disposizione, presso il Ministero dell'interno, l'indice nazionale delle anagrafi (INA). Tale disposizione legislativa ha espressamente previsto che ai fini dell'adozione del decreto del Ministro dell'interno per la gestione dell'INA, sia sentito il Garante per la protezione dei dati personali. Su questi temi nel 2001 è quindi proseguito il confronto e la collaborazione con il Ministro.

Un aspetto interessante è stato affrontato in occasione dell'esame di una segnalazione relativa alla prassi, adottata dal comando di polizia municipale di Firenze, di non indicare nei verbali di accertamento delle violazioni al codice della strada (nell'esemplare redatto con strumenti automatizzati e comunicato in copia al proprietario del veicolo) le generalità dei vigili urbani che elevavano contravvenzione; in detto modello era riportata, invece, un'avvertenza che giustificava tale omissione come asserita conseguenza dell'applicazione della legge sulla *privacy*. L'Autorità ha rilevato, da un lato, che nessuna disposizione della legge sul trattamento dei dati personali preclude alla polizia municipale di indicare nei verbali informatizzati le generalità degli agenti e, risultando così del tutto impropria l'avvertenza presente nei verbali, ne ha quindi chiesto l'eliminazione. D'altro lato si è precisato che il principio di pertinenza, in base al quale nei vari atti debbono essere riportati solo i dati indispensabili, opera anche in relazione all'attività di polizia municipale e permette una "calibratura" delle informazioni da indicare, in considerazione della particolare natura dei procedimenti di tipo sanzionatorio e delle esigenze di tutela dei diritti degli automobilisti (*Provv.* 6 febbraio 2001, in *Bollettino* n. 17, p. 9).

Il delicato problema della mancata adozione dei regolamenti previsti dal d.lg. n. 135/1999 in materia di utilizzo di dati sensibili, sul quale il Garante era già intervenuto con specifico riguardo ai comuni italiani nel 2000 (*Provv.* del 23 maggio 2000, in *Bollettino* n. 13, p. 21), è stato affrontato in termini generali in relazione alle pubbliche amministrazioni con provvedimento del 17 gennaio 2002 (in *Bollettino* n. 24, p. 40), sul quale si sofferma il par. 6 della Relazione. Con esso sono stati confermati gli impegni già assunti dall'Autorità con l'ANCI (in forza del protocollo d'intesa firmato il 1° luglio 1998 e rinnovato in data 3 ottobre 2000) per definire un programma di iniziative che favoriscano ulteriormente il processo di recepimento e di adeguamento della normativa in materia di protezione dei dati personali negli enti locali; analoga iniziativa è stata avviata con il CISIS (Centro interregionale sistema informatico e sistema statistico), organo tecnico della Conferenza dei presidenti delle regioni e delle province autonome, al fine di supportare le regioni nella corretta redazione dei regolamenti di competenza.

Tenuto conto che i soggetti pubblici avrebbero dovuto avviare l'adeguamento dei propri ordinamenti entro il 31 dicembre 1999, l'Autorità ha però predisposto un programma di ispezioni, presso enti locali (individuati per sorteggio o sulla base di segnalazioni) per verificare l'attuazione delle disposizioni di cui al d.lg. n. 135/1999 in materia di trattamento di dati sensibili e, in presenza di accertate violazioni di quanto previsto dalle discipline ricordate, adotterà specifici provvedimenti di blocco o di divieto di trattamento.

13 Canone radiotelevisivo

L'Autorità aveva già avuto modo di occuparsi nel 2000 del trattamento dei dati connesso alla gestione e alla riscossione del canone di abbonamento al servizio radiotelevisivo, in particolare in occasione del parere sui due atti aggiuntivi alla convenzione stipulata tra il Ministero delle finanze e la Rai il 23 dicembre 1988 per regolare i rapporti relativi alla gestione del canone.

La materia del canone di abbonamento al servizio radiotelevisivo è disciplinata da un complesso di disposizioni normative, risalenti anche nel tempo, le quali stabiliscono che chiunque detiene "uno o più apparecchi atti o adattabili alla ricezione delle radioaudizioni" deve pagare un canone (in particolare, il r.d.l. 21 febbraio 1938, n. 246, convertito nella l. 4 giugno 1938, n. 880 e la l. 14 aprile 1975, n. 103).

L'amministrazione degli abbonamenti è stata affidata per tutto il territorio nazionale ad un unico ufficio dell'amministrazione finanziaria, ossia all' Urar Tv (ora Agenzia delle entrate, 1° Ufficio entrate Torino – S.a.t. – Sportello abbonamenti tv), il quale si avvale di strutture, mezzi e personale messi a disposizione dalla società concessionaria. Quest'ultima svolge inoltre, per conto di tale ufficio ed in base alla predetta convenzione, diversi compiti relativi alla riscossione degli abbonamenti e al recupero delle somme dovute, a vario titolo, dai detentori degli apparecchi e può inviare ad essi comunicazioni ed avvisi.

La convenzione prevede l'obbligo per la Rai di costituire, sempre per conto dell'Agenzia delle entrate (e in base alla documentazione dalla stessa fornita), un ruolo magnetico degli abbonati residenti nel territorio nazionale, che deve essere periodicamente aggiornato per quanto riguarda i pagamenti, le cancellazioni e le situazioni anagrafiche.

Entrata in vigore la l. n. 675/1996, con un primo atto aggiuntivo alla convenzione (stipulato il 17 giugno 1999 e approvato con decreto del Ministero delle finanze il 23 luglio 1999), erano stati precisati alcuni aspetti relativi al trattamento dei dati. L'amministrazione finanziaria ha designato la Rai – Direzione produzione abbonamenti e attività per le pubbliche amministrazioni, quale responsabile del trattamento dei dati contenuti nell'archivio informatico risultante dal ruolo magnetico degli abbonati (art. 8 l. n. 675/1996), anche per ciò che attiene ai dati anagrafici relativi a cittadini maggiorenni acquisiti dalla Rai per conto dell'Agenzia delle entrate o direttamente da quest'ultima, dati ricavati dagli archivi comunali o dalle banche dati di società che erogano servizi di pubblica utilità.

In qualità di responsabile del trattamento, la società deve attenersi alle istruzioni impartite dall'amministrazione, la quale può effettuare verifiche. Deve inoltre predisporre una relazione periodica sulle attività relative ai dati personali.

Il primo dei due atti aggiuntivi prevede che la Rai riceva periodicamente dall'amministrazione finanziaria i dati dei soggetti che non risultano titolari di abbonamento e (per conto dello stesso Ufficio, ma a proprio nome e spese) debba inviare a tali soggetti "comunicazioni contenenti l'indicazione degli obblighi discendenti dalla detenzione di apparecchi radiotelevisivi e dei vantaggi conseguenti alla regolarizzazione spontanea", comunicando all'amministrazione i risultati della verifica con i dati aggiornati dei soggetti contattati e di coloro che hanno risposto (v. art. 1, commi 6 e 7).

Quale responsabile del trattamento, la Rai collabora con l'amministrazione titolare del trattamento nello svolgimento dei compiti relativi alla gestione e alla riscossione dei canoni. La società non può essere quindi considerata come un soggetto privato che persegue ulteriori finalità e che può decidere autonomamente in ordine al trattamento delle informazioni personali, dovendo la stessa attenersi rigorosamente alle prescrizioni normative e alle istruzioni impartite dall'amministrazione finanziaria.

Limitatamente a questi rapporti, alla società deve ritenersi quindi applicabile il particolare regime previsto per le amministrazioni pubbliche che, a differenza dei privati (i quali possono trattare informazioni personali in presenza del consenso degli interessati o di uno degli altri presupposti equipollenti: artt. 12 e 20 l. n. 675/1996), possono effettuare solo i trattamenti di dati connessi all'esercizio delle proprie funzioni istituzionali, nei limiti stabiliti dalle previsioni di legge o di regolamento (art. 27 l. n. 675/1996).

Il complessivo trattamento da parte della Rai dei dati relativi agli abbonati è risultato quindi lecito in termini generali, ferma restando la necessità di adottare tutti gli accorgimenti richiesti dalla normativa sulla tutela del diritto alla riservatezza (individuazione degli incaricati, informativa, misure di sicurezza, diritti di accesso ai dati personali, ecc.).

È in questo quadro d'insieme, che si è ritenuto utile ricordare benché già richiamato nel corso della precedente Relazione, che si sono innestate alcune ulteriori pronunce dell'Autorità. Il Garante ha ad esempio provveduto su un ricorso presentato da un cittadino, il quale avendo ricevuto dalla Rai comunicazione in diffida per il pagamento del canone, e risultando sprovvisto di apparecchio atto alla ricezione dei segnali radiotelevisivi, aveva richiesto l'immediata cancellazione dei propri dati dagli archivi del titolare (*Provv.* 2 maggio 2001, *Bollettino* n. 20, p. 23).

L'interessato aveva ricevuto l'idoneo riscontro solo in sede di invito ad aderire da parte del Garante, e la società concessionaria si è così vista porre a carico le spese e i diritti del procedimento, riservandosi l'Autorità ulteriori verifiche sul trattamento dei dati svolto dalla Rai in qualità di responsabile designato dall'amministrazione finanziaria.

Il 19 febbraio 2001, in seguito a numerose segnalazioni ricevute da cittadini, il Garante ha altresì avviato, nell'ambito di una complessa istruttoria relativa al trattamento di dati personali svolto dal Ministero delle finanze – Urar tv (ora Agenzia delle entrate, 1° Ufficio entrate Torino – S.a.t. – Sportello abbonamenti tv) e dalla Rai – Radiotelevisione italiana S.p.A., alcuni accertamenti in ordine agli accordi di collaborazione tra la società concessionaria e i rivenditori di apparecchi radiotelevisivi ai fini della segnalazione dei dati dei relativi acquirenti da utilizzare per la formalizzazione di nuovi abbonamenti.

In particolare l'Autorità ha chiesto di fornire informazioni e documenti in ordine ai presupposti ed alle caratteristiche del predetto trattamento di dati da parte sia del Ministero, sia della società, nonché alle specifiche modalità e formule utilizzate per l'informativa agli interessati e per l'eventuale acquisizione di un consenso al trattamento ed alla comunicazione dei dati da parte dei rivenditori. In tale occasione venivano chiesti elementi anche sulle modalità di eventuale raccolta di dati personali presso società di vendita e noleggio di videocassette.

La società concessionaria ha precisato nel procedimento che la stessa, nell'ambito dell'attività di recupero dell'evasione del canone svolta per conto dell'amministrazione finanziaria, aveva formulato una proposta di collaborazione ai rivenditori per la comunicazione dei nominativi degli acquirenti degli apparecchi idonei a ricevere trasmissioni televisive, che a suo avviso rientrava nelle previsioni della convenzione stipulata il 23 dicembre 1988 con il Ministero delle finanze (successivamente integrata dall'atto aggiuntivo approvato con d.m. del 23 luglio 1999), le quali contemplavano, tra l'altro, la possibilità per la società concessionaria di utilizzare i dati acquisiti in esecuzione dei compiti affidati per lo svolgimento di altre iniziative volte a "contribuire al recupero dell'evasione in ottemperanza alle leggi vigenti in materia di tutela dei dati personali".

Nell'ambito di tale iniziativa, come specificava la Rai, i rivenditori che intendevano aderire potevano comunicare solo i dati degli acquirenti che avessero ricevuto le informazioni di cui all'art. 10 della l. n. 675/1996, con particolare riguardo alla comunicazione dei dati alla Rai per gli adempimenti connessi alla detenzione di apparecchi televisivi, e che avessero espresso un consenso (che i rivenditori avrebbero dovuto documentare per scritto sulla base di un modello suggerito dalla Rai). Ai nominativi segnalati relativi a persone che non risultavano abbonate veniva inviata una comunicazione con invito a regolarizzare la propria posizione, contenente anche l'informativa ai sensi della l. n. 675/1996. Non venivano invece conservati, a detta della società, altri dati concernenti, ad esempio, nominativi di persone titolari di abbonamento o appartenenti ad un nucleo familiare in cui vi fosse un altro componente già abbonato.

13

Nel provvedimento del 5 dicembre 2001 (in *Bollettino* n. 23, p. 141), adottato all'esito del procedimento, il Garante ha osservato in primo luogo che le lettere di proposta di collaborazione acquisite agli atti del procedimento contenevano, oltre agli elementi sopra descritti, anche il riferimento ad un "rimborso spese" o "premio" che la società concessionaria si impegnava a corrispondere ai rivenditori di apparecchi televisivi in ragione della loro collaborazione, di entità variabile e collegata all'acquisizione o meno, entro un determinato termine decorrente dalle segnalazioni dei rivenditori, di nuovi abbonamenti al servizio radiotelevisivo.

Il Garante ha invero constatato che il predisposto "fac–simile di modello per la documentazione del consenso (da conservare da parte del rivenditore)", conteneva spazio solo per l'annotazione del nome e cognome, della residenza dell'acquirente e della data dell'acquisto, senza alcuna altra dichiarazione o formula concernente una manifestazione di volontà relativa al trattamento di dati da parte del rivenditore, ivi compresa la comunicazione alla società concessionaria.

L'Autorità ha peraltro sottolineato che l'art. 6, commi 1, lett. *d-bis*), e 2 del d.l. 10 giugno 1994, n. 357, convertito in legge, con modificazioni, dall'art. 1 della l. 8 agosto 1994, n. 489, aveva già soppresso (in base al combinato disposto dell'abrogato art. 2 e degli artt. 5 e 7 della l. 12 novembre 1949, n. 996), in quanto ritenuti adempimenti superflui, gli obblighi a carico dei rivenditori di inviare o segnalare le informazioni sugli acquirenti degli apparecchi radiotelevisivi alla società concessionaria del servizio pubblico radiotelevisivo, facendo venir meno il fondamento normativo che in precedenza obbligava alla raccolta, e al successivo invio, da parte dei rivenditori dei dati riguardanti gli acquirenti.

L'indispensabilità del fondamento in una norma primaria, per le attività di trattamento dati del tutto particolari emerse nella fattispecie, confermato dal fatto che qui ci si trova nella materia tributaria complessivamente interessata anche dalla disciplina costituzionale, era stata del resto confermata dallo stesso legislatore, che aveva ritenuto necessaria una nuova norma per reintrodurre gli obblighi ricordati, come risulta dall'art. 11 del d.l. n. 134/1995, in seguito non convertito per scadenza dei termini.

Sulla scorta di queste considerazioni (e a prescindere dalla carenza dei presupposti relativi all'informativa e al consenso che si è ritenuto di richiedere), il Garante ha pertanto affermato che la rilevata mancanza dei requisiti normativi per la raccolta ed il particolare trattamento dei dati in esame non può essere superata attraverso il consenso degli acquirenti, dal momento che la l. n. 675/1996 esclude che i soggetti pubblici, e con essi i soggetti da questi designati come responsabili del trattamento, possano supplire con una diversa procedura imperniata su un consenso – peraltro invalido – alla mancanza di fondamenti normativi.

Ove si ritenessero necessarie, ai fini di rendere più efficace la lotta all'evasione del canone, forme di collaborazione dei rivenditori, queste dovrebbero essere quindi previste da una specifica normativa conforme all'art. 27 della l. n. 675/1996, con iniziative riservate al Parlamento ed al Governo, e non alla concessionaria.

Accertato che la raccolta ed il trattamento dei dati svolti, con le modalità sopra descritte, dalla Rai per conto dell'amministrazione finanziaria non dovessero ritenersi conformi a quanto disposto dalla l. n. 675/1996 per quanto riguarda il trattamento dei dati da parte dei soggetti pubblici, si è pertanto segnalato alla società e all'amministrazione la necessità di cessare le operazioni in corso di raccolta dei dati relativi ai clienti di imprese e società di rivendita, fabbricazione e importazione di apparecchi televisivi e di vendita o noleggio di videocassette e di astenersi da ogni ulteriore trattamento dei dati in tal modo raccolti.

Constatata, comunque, la mancanza nei modelli utilizzati dai rivenditori di elementi atti a configurare un'idonea informativa, l'autorità ha proseguito gli accertamenti in ordine alle misure attuate dai rivenditori e dagli altri soggetti in tema di notificazione, informativa e consenso.

Nel successivo provvedimento del 30 gennaio 2002, il Garante ha nel frattempo chiarito che con la precedente decisione del 5 dicembre 2001, nel segnalare "la necessità di interrompere la raccolta e il trattamento dei dati personali svolti con le modalità descritte in motivazione e di astenersi dal loro ulteriore trattamento", non si era inteso intimare la cancellazione o la distruzione dei dati, dovendosi piuttosto ritenere il titolare ed il responsabile, in virtù della segnalazione, tenuti a sospendere le operazioni di trattamento tese ad acquisire ulteriori dati con modalità risultate non conformi alla disciplina vigente, nonché a sospendere i trattamenti, diversi e ulteriori rispetto alla "raccolta" che risultassero svolti con le medesime modalità.

In altri termini, l'intimata regolarizzazione riguarda operazioni future di trattamento, nonché la futura utilizzazione, ricondotta a norma, dei dati che risultassero già raccolti, in armonia con quanto disposto dall'art. 31, comma 2, lett. *c)*, della l. n. 675/1996.

Con lo stesso provvedimento, constatata la difficoltà del titolare nell'informare in tempi ravvicinati tutti i rivenditori di apparecchi per la ricezione dei segnali radiotelevisivi, e riservandosi di proseguire le verifiche nei confronti dei rivenditori stessi, il Garante ha differito di 40 gg. l'originario termine previsto per l'attuazione di quanto intimato con la segnalazione del 5 dicembre 2001.

Avverso i due provvedimenti del 5 dicembre 2001 e del 30 gennaio 2002, sia la società concessionaria, sia l'Agenzia hanno instaurato diverse controversie giudiziarie dinanzi al Tribunale di Roma e al Tribunale amministrativo regionale per il Lazio, con connesse istanze cautelari, che sono in corso di svolgimento nelle diverse fasi con la partecipazione, in alcune, di associazioni di utenti e consumatori.

Attività giudiziarie e di polizia

14 Premesse

In attesa del completamento della disciplina sulla protezione dei dati personali applicabile ad alcuni trattamenti di dati svolti in ambito pubblico, la legge n. 675/1996 non trova al momento integrale applicazione per taluni settori caratterizzati dalla particolare delicatezza delle funzioni pubbliche ad essi connesse e, quindi, dalla necessità di individuare gli eventuali, opportuni adattamenti in ragione anche della specifica rilevanza delle informazioni utilizzate.

Il predetto completamento potrebbe intervenire anche attraverso il citato testo unico atteso per la fine del 2002, come ipotizzabile alla luce del recente d.d.l. governativo di ratifica della Convenzione europea di assistenza giudiziaria in materia penale (AC 2372), che all'art. 22 demanda appunto anche al medesimo testo unico la possibilità di introdurre utili disposizioni di tutela.

Il tema interessa, in particolare, i trattamenti effettuati per ragioni di giustizia presso uffici giudiziari, quelli relativi a dati contenuti o destinati a confluire nel centro elaborazione dati del Dipartimento di pubblica sicurezza del Ministero dell'interno o trattati per finalità di prevenzione, accertamento e repressione dei reati, nonché i trattamenti effettuati dai servizi di informazione e di sicurezza o comunque coperti dal segreto di Stato (art. 4, comma 1, l. n. 675/1996).

Per espressa previsione normativa (art. 4, comma 2), non modificata dal d.lg. n. 467/2001, a tali trattamenti sono già applicabili specifiche disposizioni della legge n. 675/1996, concernenti, in particolare, le modalità di raccolta ed i requisiti dei dati, alcuni limiti alle modalità di utilizzazione, la sicurezza del trattamento e l'esercizio dei poteri d'accertamento e di controllo da parte del Garante.

Anche nel corso del 2001, in attesa dell'armonizzazione del quadro normativo sulla *privacy,* il Garante, per i trattamenti in questione, ha perciò nuovamente ribadito e sviluppato in varie occasioni alcuni principi normativi, in parte già applicati in precedenti provvedimenti, tra i quali quello di "pertinenza e non eccedenza" del trattamento rispetto alle finalità istituzionali cui esso è preordinato.

15 Trattamento di dati nell'ambito dell'attività giudiziaria

Per quanto concerne i trattamenti di dati personali effettuati "per ragioni di giustizia" (art. 4, comma 1, lett. *d*), legge n. 675/1996), si è stabilito che tra essi rientrano anche quelli svolti dal collaboratore (nel caso di specie, un professionista sanitario) del consulente tecnico d'ufficio nominato dal giudice: per essi, dunque, non può trovare applicazione il procedimento relativo al ricorso all'Autorità regolato dall'art. 29 della legge n. 675/1996 (*Provv.* 27 marzo 2002, in *Bollettino*, n. 26, p. 3).

Il Garante, chiamato a pronunziarsi su una richiesta di cancellazione o di blocco di dati sensibili proposta dall'interessato nei confronti del presidente di sezione di un tribunale (che avrebbe trasmesso detti dati, peraltro comunicatigli da altro magistrato, alla presidenza del tribunale d'appartenenza ed al Consiglio superiore della magistratura, al fine di fare luce su un esposto e su una denunzia-querela presentati nei confronti di un collega), con provvedimento del 25 ottobre 2001 ha riaffermato che "a tale categoria di trattamenti si applicano al momento solo alcune disposizioni" della legge n. 675/1996 "elencate nel comma 2 dell'art. 4 … fra le quali non sono compresi né l'art. 13 (esercizio del diritto di accesso ai dati), né l'art. 29" (in materia di ricorsi), ferma restando la possibilità di sollecitare, attraverso l'invio al Garante di una segnalazione o di un reclamo, la verifica della rispondenza dei trattamenti di dati ai requisiti stabiliti dalla legge o dai regolamenti (artt. 31, comma 1, lett. *d)* e *p)* e 32, in relazione al citato art. 4, comma 2).

Tale principio, pertanto, come già stabilito dal Garante con pronuncia del 2 dicembre 1997 (in tema di procedimenti disciplinari nei confronti dei magistrati ordinari), deve trovare applicazione anche con riferimento ai profili attinenti all'eventuale responsabilità disciplinare di un magistrato, seppur scaturenti da una vicenda giudiziaria che abbia coinvolto anche lo stesso interessato.

Inoltre, con specifico riferimento al caso oggetto di pronuncia, il Garante ha escluso ragioni per intervenire autonomamente nell'ambito di un separato procedimento, valutando le operazioni di trattamento quali ipotesi di "legittima comunicazione ed utilizzazione di elementi di valutazione in ordine a vicende che afferiscono … al corretto svolgimento dell'attività giudiziaria ed alla liceità e correttezza del comportamento di magistrati".

Il Garante è stato altresì adito, ai sensi dell'art. 29 legge n. 675/1996, da un interessato che, avendo assunto nell'ambito di una controversia civile la qualità di attore, ha contestato la decisione del giudice istruttore di acquisire, presso l'Ufficio del casellario giudiziale, il suo certificato penale e quello relativo ai suoi eventuali carichi pendenti, senza procedere ad una preliminare comparazione tra il rango costituzionale del suo diritto alla riservatezza "e quello del mero diritto patrimoniale" del convenuto (*Provv.* 28 settembre 2001, in *Bollettino* n. 22, p. 7).

Nell'accertare come il trattamento dei dati oggetto di ricorso rientrasse, da un lato, tra quelli svolti "nell'ambito del servizio del casellario giudiziale … o, in base alla legge, nell'ambito del servizio dei carichi pendenti nella materia penale" (art. 4, comma 1, lett. *c)*, l. n. 675/1996) e, dall'altro, con riferimento all'ordinanza di acquisizione dei certificati pronunziata dal giudice istruttore, fra i trattamenti svolti "per ragioni di giustizia nell'ambito di uffici giudiziari …" (art. 4, comma 1, lett. *d)*, l. n. 675/1996), anche in questo caso si è riaffermata l'inapplicabilità delle disposizioni degli artt. 13 e 29 della legge, riconoscendo comunque all'interessato la facoltà di presentare una segnalazione o un reclamo al Garante ai fini della verifica della rispondenza dei trattamenti ai requisiti di legge o di regolamento.

Inoltre, sempre con specifico riferimento al caso in questione, è stata esclusa la necessità di procedere ad autonomi interventi di sorta, avendo constatato che "le operazioni di trattamento svolte dall'autorità giudiziaria e quelle richieste al competente Ufficio del casellario rientrano nell'ambito di un'attività istruttoria volta ad acquisire elementi di prova e di giudizio rispetto ad una controversia in essere", attività che non risultava "svolta in modo illegittimo e in contrasto con la normativa sulla protezione dei dati personali".

15

Deve segnalarsi, infine, un provvedimento riguardante l'utilizzabilità dei risultati di intercettazioni telefoniche, realizzate dall'autorità giudiziaria nell'ambito di un procedimento penale, nel corso di un successivo procedimento disciplinare avviato nei confronti dell'interessato.

L'Autorità, rilevato che la disposizione contenuta nell'art. 270, comma 1, c.p.p. – concernente l'inutilizzabilità dei risultati delle intercettazioni telefoniche in determinati procedimenti penali – prevede una limitazione all'uso di tali elementi di prova solo in altri procedimenti penali disciplinati dal codice di rito, ha riconosciuto che la comunicazione dei dati personali relativi al ricorrente effettuata dall'autorità giudiziaria non viola l'art. 27, comma 2, della legge n. 675/1996, considerato che tale articolo, in virtù dell'art. 4, comma 2, della medesima legge, non trova applicazione al trattamento dei dati svolti da parte degli uffici giudiziari (*Provv.* 27 giugno 2001, in *Bollettino* n. 21, p. 18).

16 Notificazione di atti e comunicazioni

La questione delle modalità relative alla notificazione degli atti giudiziari, siano essi inerenti a un processo civile, penale, amministrativo o contabile, è stata affrontata dal Garante sin dal 1998 (v. *Provv.* 22 ottobre 1998; successivamente *Provv.* 26 ottobre 1999), generando specifiche considerazioni sul tema con particolare riferimento alla materia tributaria e alla circolazione stradale. Su di esse l'Autorità è tornata con nota 2 agosto 2001, con la quale si è nuovamente segnalata "la necessità di applicare le norme vigenti in tema di notificazione di atti giudiziari, di comunicazioni di cancelleria e di atti amministrativi di vario tipo in modo conforme al nuovo quadro di garanzie … introdotto dalla legge del 1996".

Nel provvedimento del 1998, l'Autorità, nel chiarire che la legge n. 675/1996 non aveva abrogato le disposizioni vigenti in materia di notificazioni di atti e, tra esse, quelle che consentono, in caso d'impossibilità di notifica a mani proprie dell'interessato, di rilasciare una copia leggibile di atti – o di un loro estratto – anche a terzi non interessati alla vicenda giudiziaria (portieri di stabili, capi di uffici e di aziende, comandanti di corpo militare, ecc.), evidenziava la necessità di operare un'armonizzazione della complessiva disciplina con la nuova normativa in materia di protezione dei dati personali (art. 1, comma 1, lett. *i)* legge n. 676/1996), al fine di garantire in modo effettivo la dignità e la riservatezza dei cittadini e, al contempo, di prevenire incidenze negative sull'amministrazione della giustizia e sullo svolgimento di altre funzioni pubbliche.

Le specifiche indicazioni rese dal Garante (concernenti soprattutto la modifica di alcune disposizioni dei codici di rito e della normativa sulle notifiche a mezzo posta), non solo furono riprese in occasione del successivo provvedimento pronunziato il 26 ottobre 1999, ma vennero anche portate all'attenzione del Ministero della giustizia, quali suggerimenti per un eventuale progetto di modifica dell'intera disciplina sulle notificazioni; ciò accadde in occasione dell'approvazione, anche se soltanto da un ramo del Parlamento, di un apposito disegno di legge (AC 6735), nel corso della XIII legislatura.

Una versione aggiornata del predetto disegno di legge è stata già presentata in Parlamento (AS 556) nell'attuale legislatura ed è in corso la relativa discussione presso la Commissione giustizia del Senato.

17 Attività di polizia

Nel settore dell'attività di polizia, anche nel 2001 ha assunto un particolare rilievo il profilo dei controlli sui trattamenti effettuati dal centro elaborazione dati del Dipartimento della pubblica sicurezza riconducibili ad attività ricomprese nell'art. 4 della legge n. 675/1996.

Sono state portate a conoscenza del Garante varie istanze di accesso presentate a tale Dipartimento ai sensi della speciale normativa vigente in materia per i dati trattati per finalità di polizia (art. 10, l. n. 121/1981, modificato dall'art. 42 l. n. 675/1996); alcune segnalazioni sono state invece presentate direttamente a questa Autorità.

Per lo più i ricorrenti lamentano la presenza nel c.e.d. di dati inesatti, incompleti ovvero non aggiornati, con grave pregiudizio per la dignità individuale (oltre che per altri versi pregiudizievoli: si pensi al diniego di istanze per il rilascio del passaporto o ad altri provvedimenti sfavorevoli).

In occasione della presentazione di un ricorso avverso il trattamento dei dati personali conservati nella banca dati di una Questura, il Garante ha peraltro dichiarato inammissibile lo stesso, precisando che per i trattamenti riconducibili a "finalità … di prevenzione, accertamento e repressione dei reati" (art. 4, comma 1, lett. *e)*) o effettuati presso il c.e.d. (nel quale eventualmente gli stessi dati avrebbero potuto essere stati riversati), l'interessato può esercitare i diritti di verifica e di rettifica ricorrendo alla procedura prevista dall'art. 10 l. n. 121/1981 o, in alternativa, sollecitare l'instaurazione da parte della medesima Autorità di un autonomo procedimento di verifica ai sensi degli artt. 31, comma 1, lett. *d)* e *p)* e 32 l. n. 675/1996, ma non può presentare ricorso avanti alla stessa *ex* art. 29 della l. n. 675/1996 (*Provv.* 3 ottobre 2001, in *Bollettino* n. 23, p. 82).

Il ricorso è stato dichiarato inammissibile anche sul presupposto dell'ampiezza e genericità delle richieste, tali da riguardare anche eventuali dati relativi a trattamenti previsti dal citato art. 4; si è tuttavia precisato che resta possibile presentare all'ufficio amministrativo competente una più specifica richiesta di accesso ai sensi dell'art. 13 della legge n. 675/1996 quando questa riguardi dati relativi ad attività amministrative (connesse, ad esempio, al rilascio di licenze o autorizzazioni).

A seguito di alcune segnalazioni provenienti da militari e cittadini riguardanti la richiesta di verifica dei trattamenti di dati personali effettuati dall'Arma dei Carabinieri, l'Autorità, dopo averne accertato la legittimità, ha tuttavia sollevato taluni rilievi – dei quali si è già reso conto nella precedente relazione annuale – in relazione alla cornice normativa e regolamentare di riferimento, in ordine alla quale è stato segnalato al Presidente del Consiglio dei ministri e al Ministero della difesa la necessità di un rapido intervento di adeguamento ai principi dettati in materia dalla legge n. 675/1996 (*Provv.* 11 gennaio 2001, in *Bollettino* n. 16, p. 27).

Più precisamente, per i trattamenti perseguenti finalità meramente amministrative, l'integrazione normativa dovrebbe riguardare principalmente le fonti regolamentari e gli atti amministrativi generali che regolano in modo solo parziale le diverse attività amministrative dell'Arma, in quanto antecedenti alla legge n. 675/1996.

Per i trattamenti aventi invece finalità di difesa e di sicurezza dello Stato o di prevenzione, accertamento e repressione dei reati, tenuto conto dell'intento manifestato dal legislatore con la legge n. 675/1996 (art. 4, comma 1, lett. *e)*) di attuare un regime di tutela differenziato, in ragione della loro innegabile incidenza sui diritti fondamentali della persona, se ne è tuttavia ribadito l'assoggettamento ai principi fondamentali della legge n. 675/1996, evidenziando in particolare la necessità che dati e informazioni siano aggiornati .

L'Autorità, adempiendo al disposto di cui all'art. 31, comma 1, lett. *e),* l. n. 675/1996, ha quindi invitato il Comando generale dell'Arma ad avvalersi di una nuova disciplina interna sulla conservazione e distruzione

del cd. carteggio permanente, oltre che sulle modalità di verifica, aggiornamento, conservazione e distruzione del materiale informativo raccolto, in particolare se anteriore all'entrata in vigore della legge n. 675/1996.

Le sopra evidenziate esigenze debbono altresì essere riferite ai dati eventualmente detenuti in sede periferica una volta eseguita la rettifica o la cancellazione presso il c.e.d.

È stata altresì rilevata la necessità della tempestiva comunicazione al c.e.d. delle informazioni detenute a livello periferico, soprattutto al fine di garantire agli interessati l'esercizio del diritto di accesso ai sensi dell'art. 10 della legge n. 121/1981.

Analoghe considerazioni sono state recentemente formulate in una dimensione più specifica con un provvedimento avente ad oggetto trattamenti operati presso l'Arma dei carabinieri, sia a cura della Polizia di Stato, fondati su dati personali risultati inesatti o non aggiornati (*Provv.* 17 gennaio 2002).

Con specifico riguardo a questo profilo, si è in particolare sottolineato che anche i trattamenti effettuati da organi o uffici di polizia concernenti dati memorizzati o destinati a confluire nel centro elaborazione dati del Dipartimento della pubblica sicurezza, ovvero trattati in base ad espresse disposizioni di legge per finalità di prevenzione, accertamento o repressione dei reati devono essere effettuati, secondo quanto previsto dall'art. 4, comma 2, legge n. 675/1996, nel pieno rispetto, in particolare, della disciplina contenuta nell'art. 9 della medesima legge, sotto il profilo della liceità e della correttezza, dell'esattezza e dell'aggiornamento, della pertinenza e della completezza, nonché della non eccedenza rispetto alle finalità istituzionali, e, infine, della conservazione per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono trattati.

Al riguardo, è stata richiamata l'attenzione sulla necessità che gli uffici e i comandi di polizia verifichino periodicamente la rispondenza dei dati trattati ai requisiti menzionati e, ove necessario, modifichino, integrino o cancellino i dati in possesso, tenendo conto anche dei diversi esiti processuali delle vicende eventualmente documentate su iniziativa dell'interessato. Tali attività assumono particolare rilievo al fine di evitare effetti pregiudizievoli per i diritti dei cittadini e per la stessa efficacia dell'azione di polizia.

In effetti, la questione di cui è stata investita l'Autorità ha dato modo di rilevare che il flusso delle informazioni, per esempio dall'ufficio giudiziario all'ufficio di polizia che ha attivato il procedimento e tra uffici di polizia, è ancora strutturato in modo tale da non consentire che i dati possano essere completi in ogni sede interessata, mancando idonei dispositivi che assicurino organicamente e sistematicamente un effettivo aggiornamento, soprattutto quando il procedimento si concluda con un provvedimento favorevole nei confronti del cittadino o sia nuovamente definito a suo favore in altri gradi di giudizio.

In considerazione di tali rilievi, è stata quindi sottolineata la necessità di introdurre opportune modifiche normative e, al riguardo, la stessa adozione del testo unico entro il 31 dicembre 2001 si configura come una possibile via per dare definitiva sistemazione alle disposizioni che applicano i principi in materia di dati personali nel settore della giustizia e dell'attività di polizia.

18 Sistema di informazione Schengen

Nel corso dell'anno sono state presentate al Garante, quale Autorità di controllo sulla sezione nazionale del Sistema Informativo Schengen (N.SIS), numerose richieste di verifica dell'eventuale registrazione, in tali archivi, di dati personali dei soggetti interessati e della liceità dei relativi trattamenti, ai sensi della Convenzione di applicazione dell'Accordo di Schengen e dell'articolo 11 della legge italiana di ratifica (l. 30 settembre 1993, n. 388).

Al riguardo, il Garante ha precisato che gli interessati possono presentare ai suoi uffici una richiesta di verifica dei dati personali che li riguardano inseriti nel S.I.S. e chiederne la rettifica o la cancellazione (accesso indiretto). Al contrario, esso non ha alcun compito istituzionale, diretto o indiretto, in materia di adozione, concessione o revoca dei provvedimenti amministrativi che possono costituire presupposto delle segnalazioni nel S.I.S., ai sensi degli articoli 94-100 della predetta Convenzione (espulsioni, respingimenti alla frontiera, ecc.), né poteri di controllo sulla legittimità degli stessi. Per ogni richiesta avverso tali provvedimenti, quindi, gli interessati sono stati invitati a rivolgersi ai competenti organi o uffici del Ministero dell'interno o ad un organo giurisdizionale.

In numerose ipotesi, le istanze presentate a questa Autorità hanno riguardato provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno nel nostro Paese, quali, ad esempio, casi di diniego del rilascio di visti. Nelle situazioni in cui tale diniego era imputabile a segnalazioni inserite nel S.I.S. dagli organi competenti di altri Stati che aderiscono all'Accordo di Schengen, per procedere all'accertamento richiesto, il Garante – in base alla procedura di consultazione prevista dall'art. 114, comma 2, della Convenzione – ha preventivamente acquisito il parere dell'omologa Autorità di controllo del Paese interessato.

In altri casi, gli interessati hanno invece lamentato di essere vittime di usurpazione d'identità, oppure hanno segnalato casi di omonimia.

L'Autorità ha anche fatto presente al Dipartimento della sicurezza pubblica che, nel caso di richieste di accesso presentate dagli interessati agli organi competenti di altri Paesi, nei quali sia previsto l'accesso diretto in ordine a segnalazioni effettuate dalle autorità italiane, le informazioni richieste dagli uffici S.I.R.E.N.E dei Paesi interessati possono essere rilasciate direttamente dall'ufficio S.I.R.E.N.E. italiano, fatta salva l'informativa al Garante.

L'Autorità, infine, ha sensibilizzato il predetto Dipartimento circa la necessità di assicurare – anche attraverso nuove istruzioni agli uffici periferici competenti – la massima speditezza nelle procedure per il riscontro delle verifiche effettuate dal Garante e un sempre più accurato e tempestivo aggiornamento dei dati.

Da ultimo, il Garante ha avviato le procedure per impostare la realizzazione di una *newsletter* e del nuovo sito *web* dell'Autorità di controllo comune Schengen (Acc) avente sede a Bruxelles, iniziativa intrapresa a seguito della presidenza della medesima Autorità assunta dal Garante, in persona del suo segretario generale.

Sanità

19 Considerazioni generali

Nel corso del 2001, il quadro normativo delineato dal legislatore delegato del 1999 per la disciplina del trattamento dei dati sulla salute in ambito sanitario non ha trovato completa definizione.

La mancata adozione, infatti, del regolamento del Ministro della sanità, con il quale dovranno essere previste modalità semplificate per le informative di cui all'art. 10 della l. n. 675/1996 e per la prestazione del consenso (art. 2, comma 1, d.lg. 30 luglio 1999, n. 282), ha reso finora priva di efficacia la volontà del legislatore delegato di uniformare la disciplina del trattamento dei dati sulla salute da parte dei soggetti pubblici e privati operanti nell'ambito del Servizio sanitario nazionale.

Deve evidenziarsi che tale persistente inadempimento ha comportato rilevanti difficoltà nell'applicazione della normativa – soprattutto da parte degli organismi sanitari pubblici – anche in ragione del fatto che compete al suddetto regolamento il compito di provvedere alla ricognizione di tutti i trattamenti dei dati sulla salute effettuati nell'ambito del Servizio sanitario nazionale e, quindi, alla specificazione dei tipi di dati trattabili e di operazioni eseguibili in relazione alle finalità perseguite (artt. 22, comma 3-*bis* e 23, comma 1-*ter*, l. n. 675/1996).

In diverse occasioni il Garante ha sottolineato l'urgenza di provvedere alla suddetta ricognizione, al fine di ridefinire su basi più rispettose dei diritti della personalità i trattamenti legati alle finalità di rilevante interesse pubblico individuate dall'art. 17 del d.lg. 11 maggio 1999, n. 135, specificamente dedicato alla "tutela della salute".

Si tratta di un provvedimento attraverso il quale devono essere attuati i principi vincolanti del d.lg. 11 maggio 1999, n. 135 (artt. 2-4) e che in primo luogo presuppone una preventiva valutazione della stretta pertinenza e necessità dei dati e delle operazioni rispetto alle finalità in ciascun caso perseguite.

Il richiamo a tali principi è stato ribadito nella nota prot. n. 10243/01 del 30 agosto 2001, con cui l'Autorità si è espressa in ordine alla legittimità della procedura posta in essere da una azienda sanitaria locale allo scopo di effettuare i controlli necessari alla liquidazione delle somme spettanti ai medici di medicina generale partecipanti ad un programma di valutazione-rilevamento della popolazione anziana attraverso la compilazione di schede anonime recanti soltanto un numero progressivo. In particolare, l'azienda chiedeva di verificare la correttezza della trasmissione all'azienda, da parte dei medici, di un elenco nominativo dei soggetti sottoposti a rilevamento. Ciò unitamente alle schede, ma in busta chiusa separata, avendo cura che ai numeri indicati sulle schede corrispondano, progressivamente, i nominativi dei medesimi soggetti.

In tale occasione il Garante, dopo aver chiarito che il trattamento dei dati sensibili finalizzato alla suddetta attività di controllo è espressamente autorizzato dall'art. 17, comma 1, lett. *b)* ed *h)*, del d.lg. n. 135/1999, ha precisato che lo stesso, pur in assenza delle predette disposizioni regolamentari del Ministro della salute, deve essere effettuato nel rispetto dei principi di cui agli artt. 2-5 del medesimo decreto legislativo, verificando che i dati richiesti siano essenziali per svolgere l'anzidetta attività di controllo e che non si possa procedere – anche caso per caso – mediante il trattamento di dati anonimi o di dati non sensibili (art. 3, comma 1, d.lg. n. 135/1999). Ha quindi aggiunto che, una volta verificata l'indispensabilità della richiesta di tali dati, l'apertura delle buste contenenti gli estremi identificativi degli interessati potrà avvenire solo se necessaria al perseguimento della menzionata finalità di controllo (art. 4, comma 1, d.lg. n. 135/1999).

Il Garante ha infine rammentato l'obbligo di conservare i dati sulla salute separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo, nonché quello di ricorrere a tecniche di cifratura o codici identificativi ogniqualvolta i medesimi dati siano contenuti in elenchi, registri o banche dati, ovvero siano tenuti con l'ausilio di mezzi elettronici o comunque automatizzati (art. 3, commi 4 e 5, d.lg. n. 135/1999).

19

Ai medesimi principi generali, l'Autorità ha fatto riferimento nella nota prot. n. 1110/01 del 1° febbraio 2002, relativa al contrassegno per i veicoli destinati al trasporto di persone disabili, osservando che, sebbene il codice della strada e il regolamento di esecuzione autorizzino i comuni a raccogliere, utilizzare e diffondere legittimamente dati personali di natura sensibile, come la condizione di *handicap*, ciò deve pur sempre avvenire nel rispetto dei citati principi di pertinenza e di non eccedenza. Ha quindi invitato il Governo a valutare la possibilità di modificare il modello di contrassegno previsto dal regolamento di attuazione del codice. Ciò potrebbe avvenire omettendo le generalità del beneficiario, ovvero riportandole sul lato posteriore del contrassegno, indicando esclusivamente il comune competente e il numero di autorizzazione: in tal modo, si potrebbe comunque risalire al titolare del permesso per verificarne la validità ed il suo corretto utilizzo. In attesa delle modifiche normative, l'Autorità ha comunque invitato i comuni a consentire agli interessati di evitare di riportare sui contrassegni le proprie generalità ovvero di cancellarle.

Il Garante è poi intervenuto nei confronti di una azienda ospedaliera che, in violazione del divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 23, comma 4, l. n. 675/1996), aveva esposto in una bacheca ubicata nel corridoio di un reparto di chirurgia la lista dei degenti da sottoporre ad intervento chirurgico (nota del 4 giugno 2001).

Con riferimento alle modalità di applicazione dell'art. 23 della legge n. 675/1996, in diverse occasioni l'Autorità ha dovuto segnalare ai titolari del trattamento la necessità di conformare le comunicazioni dei dati personali relativi allo stato di salute degli interessati al principio di cui al comma 2 del medesimo articolo, secondo cui "i dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo per il tramite di un medico designato dall'interessato o dal titolare" (v. da ultimo *Provv.ti* 19 e 27 febbraio 2002, in *Bollettino* n. 25, p. 10 e 12; *Provv.* 20 marzo 2002, in *Bollettino*, n. 26, p. 5 e 7).

Nello svolgimento dei suoi compiti, il Garante ha poi provveduto a rinnovare l'autorizzazione generale al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2002, pubblicata nel supplemento ordinario alla *G.U.* n. 83 del 9 aprile 2002).

Il nuovo testo, che sostanzialmente riproduce la formulazione precedente (la cui efficacia era stata differita al 31 gennaio 2002 con deliberazione del Garante del 31 dicembre 2001), presenta tuttavia alcuni profili di novità anche per quanto attiene il termine di efficacia (fino al 30 giugno 2003) e l'introduzione di un termine transitorio – fissato nel 31 maggio 2002 – entro il quale ciascun titolare dovrà adeguare il trattamento dei dati sulla salute alle prescrizioni non contenute nella precedente autorizzazione n. 2/2000.

Con riguardo all'attività autorizzatoria, l'Autorità ha più volte dovuto precisare che le istanze di autorizzazione ricevute non necessitavano di specifici pronunciamenti. Alcune aziende ospedaliere, ad esempio, hanno chiesto l'autorizzazione a rilasciare copia della cartella clinica relativa al ricovero di pazienti ad avvocati che, nell'esercizio del mandato ricevuto, avevano presentato istanza di accesso ai sensi dell'art. 22 della l. n. 241/1990.

In tali occasioni il Garante, dopo aver chiarito che la questione riguarda più direttamente la normativa sull'accesso ai documenti amministrativi – e che spetta quindi alle aziende stesse verificare in concreto, caso per caso, l'esistenza dei presupposti di applicabilità degli artt. 22 e ss. della l. n. 241/1990 (profili sui quali si sofferma il par. 8) –, ha poi precisato che il d.lg. n. 135/1999, nell'integrare la normativa sul trattamento dei dati sensibili da parte dei soggetti pubblici, ha stabilito che si considerano di rilevante interesse pubblico i trattamenti effettuati per l'applicazione della disciplina sull'accesso ai documenti amministrativi o comunque per permettere a terzi di difendersi in sede giudiziaria (art. 16, comma 1, lett. *c)* e *b),* d.lg. n. 135/1999).

Occorre infine menzionare alcune precisazioni fornite dal Garante nell'ambito dell'esame di alcuni ricorsi presentati ai sensi dell'art. 29 della l. n. 675/1996.

In particolare, esaminando il ricorso con il quale un ricorrente chiedeva ad una azienda ospedaliera di accedere ai risultati di una serie di esami effettuati e di conoscere il significato di alcuni codici utilizzati nella formulazione della diagnosi, è stato precisato che la cartella clinica, ove già consegnata all'interessato, farebbe piena fede dei riscontri clinico-diagnostici effettuati. IL Garante ha accolto il ricorso nella parte in cui si chiedeva di conoscere il significato dei suddetti codici. Ciò tenendo conto che l'art. 13 della l. n. 675/1996 prevede che i dati devono essere comunicati all'interessato "in forma intelligibile" e che l'art. 17, comma 9, del

d.P.R. n. 501/1998 obbliga il titolare ad adottare "le opportune misure volte, in particolare, ad agevolare l'accesso ai dati personali da parte dell'interessato" (nota 26 marzo 2001, n. 4230/14834).

In altra occasione, l'Autorità si è pronunciata in ordine alla richiesta di accedere ai dati personali del ricorrente e a quelli della relativa figlia minore, raccolti da un medico nel corso di visite specialistiche effettuate tramite colloqui e test sulla minore. In proposito il Garante ha riconosciuto il diritto del ricorrente di accedere a tutta la documentazione in possesso del medico (disegno della famiglia, test *Patte Noire*, anamnesi, appunti), muovendo dalla considerazione che la l. n. 675/1996 è applicabile a qualunque informazione di carattere personale relativa a soggetti identificati o identificabili e costituita anche da suoni o da immagini (quale quella che può essere riportata in un disegno), ovvero compresa al loro interno o nell'ambito di dichiarazioni o di altre forme di manifestazione del pensiero (*Provv.* 28 novembre 2001, in *Bollettino* n. 23, p. 57).

L'Autorità ha inoltre esaminato il ricorso con il quale un insegnante aveva chiesto al provveditorato agli studi la cancellazione o la trasformazione in forma anonima della dicitura "portatore di *handicap*" che era riportata accanto al suo nome in un elenco affisso in bacheca di lavoratori trasferiti: riconosciuta l'illiceità del trattamento, il Garante ha vietato al Ministero dell'istruzione, dell'università e della ricerca di diffondere ulteriormente, anche presso altri uffici, il dato sensibile relativo all'*handicap* della ricorrente ed ha invitato l'amministrazione medesima a sostituirlo con diciture generiche o codici numerici (ritenendo peraltro non idonea la soluzione di apporre il riferimento alla l. n. 104/1992). Ottemperando alle indicazioni dell'Autorità, il Ministero dovrà pertanto impartire agli uffici idonee disposizioni in grado di assicurare il rispetto della dignità delle persone. Tale cautela dovrà essere adottata non solo riguardo agli elenchi affissi in locali aperti al pubblico, ma anche nelle graduatorie ad uso interno o nella compilazione di altri atti amministrativi (*Provv.* 27 febbraio 2002, in *Bollettino* n. 25, p. 51).

È noto infine che già la legge finanziaria per il 2001 (l. 23 dicembre 2000, n. 388) ha disposto l'abrogazione delle disposizioni di legge che prevedevano l'introduzione della carta sanitaria elettronica (leggi nn. 449/1999, art. 59, lett. *i*), e n. 39/1999) ed ha al tempo stesso previsto l'inserimento dei dati sanitari nei documenti d'identità elettronici (tema sul quale si rinvia al paragrafo n. 10).

20 Informazioni genetiche

Il legislatore delegato del 1999 aveva previsto che il trattamento dei dati genetici, da chiunque effettuato, dovesse essere oggetto di un' apposita e specifica autorizzazione del Garante (art. 17, comma 5, d.lg. 11 maggio 1999, n. 135, come integrato e modificato dall'art. 16 del d.lg. 30 luglio 1999, n. 281).

In proposito, si deve evidenziare che l'Autorità, benché con deliberazione del 2 maggio 2000, abbia dato avvio alla complessa procedura prevista per l'emanazione della suddetta autorizzazione ("*sentito il Ministro della sanità che acquisisce, a tal fine, il parere del Consiglio superiore di sanità*"), ha successivamente ritenuto – alla luce sia delle difficoltà incontrate nella stesura del testo, sia di indicazioni e suggerimenti ricevuti dagli esperti – di approfondire la materia lasciando nel frattempo inalterata la disciplina già contenuta nell'autorizzazione n. 2/2000 per il trattamento dei dati idonei a rivelare lo stato di salute (punto 2, lett. *b)*), recentemente riprodotta nell'autorizzazione n. 2/2002.

Allo stato, ferme restando alcune esclusioni soggettive e limitazioni nelle finalità, il trattamento dei dati genetici è consentito, sulla base del consenso scritto dell'interessato (ai sensi degli artt. 22 e 23, l. n. 675/1996), "*limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività*". Si rende invece necessaria un'apposita autorizzazione del Garante nel caso in cui manchi il consenso dell'interessato e il trattamento sia finalizzato a tutelare l'incolumità fisica e la salute di un terzo o della collettività. L'inosservanza delle prescrizioni impartite dal Garante attraverso lo strumento autorizzatorio resta punita con sanzione penale (art. 37 l. n. 675/1996).

Come già ricordato nella relazione annuale per l'anno 2000, l'Autorità, a causa di alcune notizie di stampa che annunciavano l'avvio di un importante progetto di ricerca genetica sulle popolazioni sarde della regione dell'Ogliastra, si è avvalsa dei poteri conferitigli dal legislatore (art. 32, comma 1, l. n. 675/1996) ed ha chiesto precise informazioni circa le finalità e le modalità del trattamento. A seguito di tale iniziativa l'Autorità ha avuto diversi contatti con ricercatori coinvolti nel progetto, volti per lo più a accertare come le suddette indagini genetiche possano essere realizzate nel rispetto delle norme che tutelano la riservatezza dei dati personali.

Nel mese di luglio 2001, analoga vicenda ha riguardato le popolazioni del Cilento. Anche in questo caso la stampa ha dato notizia dell'imminente avvio di ricerche genetiche nella zona ed il Garante ha immediatamente inoltrato richieste di informazioni ai sindaci di nove Comuni facenti parte del Parco nazionale del Cilento. Dalle risposte pervenute è emerso che, allo stato, le suddette popolazioni non erano oggetto di alcuna indagine di tipo genetico, bensì di uno studio di fattibilità diretto ad accertare in via preliminare se i suddetti Comuni possano essere considerati quali "isolati genetici" su cui avviare un progetto di ricerca genetica di popolazione.

Nei giorni 21-22 marzo 2002 si è infine tenuta presso la sede dell'Autorità e con il patrocinio della stessa, la Conferenza internazionale sulle "Implicazioni giuridiche e psicosociali della genetica umana".

Tale Conferenza, organizzata dal Consiglio nazionale delle ricerche in collaborazione con l'*Einstein Institute for Science, Health & the Courts* (EINSHAC, istituzione americana che pone al centro della propria attenzione l'impatto delle nuove tecnologie e delle scoperte scientifiche nel contesto giudiziario), si è rivelata un'importante occasione di confronto fra ricercatori, genetisti, medici e psicologi che operano nel campo della consulenza genetica e magistrati impegnati nel settore.

In tale occasione sono state affrontate anche delicate questioni relative all'impatto delle applicazioni genetiche nei procedimenti giudiziari, con riferimento alla possibilità di armonizzare in un'ottica internazionale le norme e le procedure per l'uso di test genetici nei procedimenti civili e penali e nella pratica medica.

21 AIDS

Nel corso di questi anni l'Autorità è stata più volte chiamata a ribadire la specialità delle norme sull'AIDS, disposizioni espressamente fatte salve dall'art. 43, comma 2, della legge n. 675/1996, contenute nella legge 5 giugno 1990, n. 135.

Alcune recenti osservazioni in tema di AIDS sono infatti contenute in un parere, reso dal Garante alla Presidenza del Consiglio dei ministri nell'esercizio della sua funzione consultiva (art. 31, comma 2, l. n. 675/1996), in merito allo schema di regolamento di semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo a militari e a dipendenti delle pubbliche amministrazioni.

In tale occasione l'Autorità, richiamando alcune decisioni del 1998 (riportate nella *Relazione 1999*, p. 53), ha sottolineato la necessità di adeguare lo schema di regolamento alle disposizioni contenute nella legge n. 135/1990 in materia di AIDS, precisando, con riferimento al verbale di accertamento di infermità, che quando il giudizio diagnostico riguarda casi di infezione da HIV/AIDS, esso deve essere consegnato dapprima al solo interessato, per le sue valutazioni. Quindi, ove questi ritenga di chiedere o di non opporsi all'ulteriore prosecuzione del procedimento, gli uffici sono tenuti ad adottare specifiche cautele, in aggiunta a quanto previsto dall'art. 3 del d.lg. n. 135/1999, per l'ulteriore utilizzazione e conservazione dei dati ivi contenuti, in modo da limitarne rigorosamente la conoscibilità (parere del 3 maggio 2001).

Rapporto di lavoro

22 Tutela dei dati personali dei lavoratori e dati valutativi

L'Autorità si è pronunciata in più di un'occasione sul tema della protezione dei dati personali nel settore del diritto del lavoro, con riferimento tanto all'ambito del lavoro pubblico quanto a quello del lavoro privato, con particolare riguardo all'accesso ai dati personali trattati dal datore di lavoro nel corso dello svolgimento del rapporto (*Provv.* 31 gennaio 2002, in *Bollettino* n. 24, p. 9).

Analoga attenzione è stata rivolta agli aspetti inerenti alla liceità e alla correttezza dei trattamenti dei dati personali dei lavoratori dipendenti nel rispetto dei principi di pertinenza, finalità e non eccedenza sanciti all'art. 9 della legge n. 675/1996. Su questo punto, e in riferimento specifico ai fenomeni di ritenuto assenteismo e di eventuale non veritiera certificazione sanitaria, l'Autorità ha affermato che il datore di lavoro può far valere i propri diritti oltre che nei modi consentiti dalla citata legge (e indicati nel menzionato art. 9), anche in conformità a quanto stabilito nell'autorizzazione generale al trattamento di dati sensibili nel rapporto di lavoro. È stato altresì sottolineato che il rispetto dei principi di pertinenza e non eccedenza deve essere perseguito in modo rigoroso anche nell'individuare i competenti destinatari di eventuali comunicazioni e nel redigere note informative dense di elementi conoscitivi (*Provv.ti* 24 e 28 settembre 2001, in *Bollettino* n. 22, pp. 46 e 48).

Il ricorso ai principi di pertinenza e non eccedenza ha poi consentito all'Autorità di ritenere che la dicitura "pignoramento" apposta sulla busta-paga per motivare una ritenuta operata sullo stipendio contrasta con la disciplina sulla protezione dei dati personali, rendendo conoscibili a terzi delicati aspetti della vita privata del lavoratore. Si è inoltre rilevato che le finalità di documentazione e di trasparenza all'interno del rapporto di lavoro possono essere comunque soddisfatte mediante il ricorso a differenti dizioni o a codici identificativi che rendano enucleabile la ritenuta operata senza descriverla specificamente (*Prov.* 19 febbraio 2000, in *Bolllettino* n. 25, p. 34)

Per quel che concerne invece il diritto di accesso del lavoratore ai dati che lo riguardano, il Garante ha più volte precisato che esso non deve essere confuso con il diverso diritto di accesso agli atti e ai documenti amministrativi, e in tal guisa ha affermato che, stante la richiamata distinzione tra tali diritti (ai sensi, rispettivamente, dell'art. 13 della legge n. 675/1996 e dell'art. 22 della legge n. 241/1990), è possibile presentare un'ampia richiesta di accesso al complesso dei dati, ivi compresi quelli valutativi (*Provv.ti* 7 e 14 marzo 2001, in *Bollettino* n. 18, p. 15 e 32; *Provv.ti* 10 gennaio 2002, in *Bollettino* n. 24, p. 6 e 36), mentre non è possibile domandare copia integrale di atti, relazioni, verbali o di altri documenti contenenti dati personali, quando i medesimi siano stati già forniti attraverso la loro estrazione e messa a disposizione, anche se su supporti diversi dagli originali (*Provv.ti* 19 aprile e 30 ottobre 2001, in *Bollettino* n. 19, p. 12 e n. 23, p. 86).

In conformità alle precedenti pronunce, peraltro, l'Autorità ha posto in evidenza il principio in base al quale il diritto tutelato dall'art. 13, comma 1, legge n. 675/1996 permette all'interessato di accedere ai dati personali che lo riguardano comunque trattati dal titolare del trattamento; ai sensi del citato art. 13, infatti, è possibile proporre un'istanza volta ad avere contezza anche del complesso (o, come nel caso di specie, di una particolare tipologia) dei dati personali del richiedente. A fronte di un'istanza di questo tipo, secondo quanto previsto dal combinato disposto di cui agli artt. 13 e 17 del d.P.R. n. 501/1998, il responsabile o gli incaricati del trattamento devono quindi estrarre i dati oggetto di accesso e comunicarli all'interessato senza ritardo (*Provv.* 24 luglio 2001, in *Bollettino* n. 22, p. 32).

Con la medesima pronuncia si è, inoltre, nuovamente sottolineato che le domande di esercizio dei diritti di cui all'art. 13 della legge n. 675/1996 non richiedono alcuna motivazione da parte dell'istante, né tantomeno la dimostrazione della necessità di acquisire i dati per difendere un diritto in giudizio. Con la conseguenza che, anche sotto questo profilo, non ha rilevanza il richiamo a disposizioni regolamentari (attuative della citata l. n. 241/1990) relative ad ipotesi di esclusione dall'accesso di determinati tipi di atti. Parimenti l'Autorità ha rilevato che l'esercizio del menzionato diritto di accesso *ex* art. 13 non è soggetto a limitazione o differimento

secondo i presupposti previsti per il diverso diritto di accesso ai documenti amministrativi, né può essere precluso in ragione della circostanza che i dati oggetto di domanda sono contenuti in documenti in passato esibiti all'autorità giudiziaria su sua richiesta.

Da un punto di vista meramente operativo si è ricordato che tali dati possono "essere comunicati al richiedente anche oralmente, ovvero con prospettazione mediante mezzi elettronici o comunque automatizzati. Se vi è richiesta, si provvede in ogni caso alla trasposizione dei dati su supporto cartaceo o informatico" (*Provv.* 24 luglio 2001, in *Bollettino* n. 22, p. 32). Ove poi l'estrazione di dati personali risulti particolarmente difficoltosa, l'adempimento delle richieste del dipendente può avvenire anche attraverso l'esibizione e/o la consegna in copia della relativa documentazione (*Provv.ti* 19 luglio e 27 dicembre 2001, in *Bollettino* n. 22, p. 38 e n. 23, p. 72).

L'importanza di questa modalità alternativa si evidenzia nei casi in cui, accanto a tipologie di dati di più facile reperimento o estrazione, ne possono essere richiesti dal dipendente altri dei quali occorre accertare in via preliminare l'effettiva esistenza e la cosiddetta "afferenza" alla persona interessata, oltre che dati il cui medesimo reperimento può esigere indagini e approfondimenti particolari nell'ambito di una struttura aziendale articolata, specie con riguardo a documenti risalenti nel tempo.

Rispetto al complesso di dati personali detenuti in modalità cifrata o comunque in forma non immediatamente leggibile a ciascun incaricato del trattamento, l'Autorità ha precisato che gli stessi conservano la natura di dato personale qualora siano ricollegabili ad una determinata persona identificata o identificabile. In tali casi il titolare del trattamento, a fronte di una richiesta di accesso, deve comunque provvedere, ai sensi dell'art. 17, comma 6, d.P.R. n. 501/1998, alla "messa in chiaro" dei dati medesimi in modo che la loro comprensione risulti agevole (*Provv.* 21 novembre 2001, in *Bollettino* n. 23, n. 69).

In ordine al trattamento dei dati personali effettuato nell'ambito di un rapporto di pubblico impiego, è stato affermato che il consenso degli interessati non deve essere chiesto (*Provv.* 30 ottobre 2001, in *Bollettino* n. 23, p. 35), stante l'applicazione in tali ipotesi delle disposizioni di cui agli artt. 22, commi 3 e 3-*bis* e 27 della l. n. 675/1996, disciplinanti il trattamento dei dati personali da parte dei soggetti pubblici. Inoltre, per quanto riguarda più specificatamente il trattamento dei dati sensibili da parte dei datori di lavoro pubblici, l'art. 3 del d.lg. n. 135/1999 ha introdotto a carico dei soggetti pubblici una serie di obblighi e cautele da rispettare relativamente alle finalità e alle modalità di trattamento dei dati personali, senza porre peraltro un obbligo di assoluta e integrale "segretazione" dei dati personali sensibili da parte dell'ente pubblico datore di lavoro. L'ente, tuttavia, è tenuto a impiegare tecniche, codici o altri sistemi che permettano di identificare gli interessati solo in caso di necessità e unicamente per lo svolgimento delle rilevanti finalità di interesse pubblico per le quali il trattamento è effettuato (art. 3, commi 4 e 5, d.lg. n. 135/1999).

A questo proposito, peraltro, l'Autorità ha affermato 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".

Il principio della conservazione separata rileva, tuttavia, in modo parzialmente diverso a seconda delle modalità di raccolta di atti e documenti del dipendente, come nel caso di fascicolo personale cartaceo, il quale presenta caratteristiche di unitarietà e, per le finalità di cui all'art. 9 del d.lg. n. 135/1999, può richiedere il periodico utilizzo anche di dati riguardanti lo stato di salute o relativi a varie vicende del dipendente medesimo.

Questa particolarità non elimina la necessità di dare congrua applicazione al principio della conservazione separata anche in riferimento ai fascicoli personali cartacei, i quali, pur dovendo mantenere la loro unitarietà in relazione a singoli dipendenti interessati, richiedono l'adozione di cautele per assicurare, con opportuni accorgimenti, l'osservanza del richiamato principio di separazione (ad esempio, utilizzando sezioni o sottofascicoli dedicati alla custodia di eventuali dati sensibili, da conservare chiusi o comunque con modalità che circoscrivano la possibilità di una loro indistinta consultazione nel corso di ordinarie attività amministrative).

Infine, con riferimento alle procedure di valutazione poste in essere dai datori di lavoro nei riguardi dei loro dipendenti, l'Autorità ha affermato che devono essere considerate come dati personali ai sensi della definizione

22

di cui all'art. 1, comma 2, lett. *c*), della legge n. 675/1996 tutte le informazioni, anche se comprese in atti recanti giudizi e valutazioni, che contengano alcuni elementi distintivi del soggetto al quale si riferiscono, benché annotati in schede, note di qualifica o documenti dello stesso genere. Ciò comporta il diritto, per ciascun lavoratore interessato, di accedere a dati personali contenuti anche all'interno di note di qualifica e giudizi che lo riguardano e non anche, in mancanza di delega o procura, a quelli relativi ad altri colleghi (*Provv.* 6 febbraio 2001, in *Bollettino* n. 17, p. 24).

Tali elementi distintivi vanno a comporre il quadro dei "dati" dell'interessato relativi alle attitudini, alle capacità, al rendimento e alle prospettive di impiego e carriera, e possono confluire in un fascicolo personale contribuendo così a definire un quadro di riferimento per il datore di lavoro avente precisi effetti sulla persona.

Ad ogni modo, occorre tenere presente che tali informazioni personali provengono anche da valutazioni che restano espressione del libero e soggettivo convincimento del "valutatore" benché, per effetto degli specifici diritti riconosciuti dalla l. n. 675/1996, non possano essere sottratti al diritto di accesso dell'interessato. Questo ultimo gode, infatti, in conformità alla normativa comunitaria contenuta nella direttiva n. 95/46/CE – e già ampiamente attuata dalla l. n. 675/1996 –, di un diritto soggettivo a conoscere le informazioni di carattere personale che lo riguardano, anche nei casi in cui tali dati personali non siano eventualmente suscettibili di correzione in quanto contenuti nell'ambito di un giudizio o di una valutazione.

In conclusione, l'Autorità ha rilevato che il diritto di accesso non limita in alcun modo l'invocato "diritto alla libertà di pensiero" del datore di lavoro, poiché il diritto dell'interessato a conoscere dati che lo riguardano non comporta di per sé il diritto ad ottenere una rettifica di dati personali riportati all'interno di valutazioni rimesse al discrezionale apprezzamento del datore di lavoro (*Provv.ti* 10 ottobre e 5 dicembre 2001, in *Bollettino* n. 23, p. 88 e 96).

La complessa problematica – che in altri Paesi europei appare già pacifica – è venuta al pettine in senso più ampio, anche in riferimento ai dati personali contenuti nell'ambito di altri tipi di giudizi e valutazioni, ad esempio nei settori medico-assicurativi. Essa richiederà indubbiamente ulteriori approfondimenti, alcuni dei quali già maturi (come quello relativo all'esclusione dell'accesso delle coordinate identificative della persona fisica che cura le valutazioni all'interno dell'azienda o ufficio), altri meritevoli di riflessione (si pensi al profilo concernente il momento temporale in cui i giudizi e le valutazioni vengono a giuridica esistenza).

23 Informative e controllo a distanza del personale

L'impiego di sistemi informativi nel rapporto di lavoro e le forme del controllo a distanza del personale, con riguardo specifico alla videosorveglianza, sono temi di crescente attualità.

Sull'argomento si è richiamata più volte l'attenzione, in particolare, sul principio contenuto nell'art. 4 della legge n. 300/1970 che sancisce il divieto del "controllo a distanza dell'attività dei lavoratori".

Tale norma distingue l'ipotesi dell'utilizzo di impianti audiovisivi e di altre apparecchiature avente mera finalità di controllo dell'attività dei lavoratori (comma 1) dall'ipotesi in cui l'uso dei medesimi impianti e apparecchiature risponda ad esigenze di tipo organizzativo e produttivo (comma 2). In questo secondo caso è consentito il controllo a distanza dei lavoratori solo se l'installazione dei predetti mezzi viene concordata previamente con le rappresentanze sindacali aziendali.

Sul punto, l'Autorità ha poi ricordato che la direttiva comunitaria n. 95/46/CE e la Convenzione n. 108/1981 del Consiglio d'Europa comportano l'applicazione della disciplina sul trattamento dei dati personali anche ai suoni e alle immagini (quali quelle registrate nei controlli video), qualora permettano di identificare un soggetto anche in via indiretta, e ha evidenziato che la legge n. 675/1996, attuativa della citata Convenzione, ha considerato quale "dato personale" qualunque informazione che permetta l'identificazione, anche in via indiretta, dei soggetti interessati, ivi compresi i suoni e le immagini (art. 1, comma 1, lett. *c)*).

Un'altra questione nella quale è intervenuto il Garante, sempre in tema di controllo a distanza dei lavoratori, ha riguardato le modalità di controllo da parte del datore di lavoro degli accessi alle reti telematiche ad opera del personale e l'uso della posta elettronica.

In proposito è in preparazione un provvedimento generale, in particolare per quel che concerne il controllo delle *e-mail* dei lavoratori dipendenti (v. anche *Comunicato stampa* 7 luglio 2001, in *Bollettino* n. 22, p. 94); sono stati per contro posti in essere alcuni specifici accertamenti di carattere preliminare in riferimento ai profili dell'informativa ai lavoratori interessati, del principio di proporzionalità nel trattamento dei dati, della trasparenza dei controlli e dei limiti entro i quali gli stessi sono consentiti *ex* art. 4 della legge n. 300/1970, disciplina espressamente fatta salva dall'art. 43, comma 2, l. n. 675/1996.

In materia di videosorveglianza, sono stati altresì compiuti accertamenti ispettivi nei luoghi di lavoro a seguito di segnalazioni e reclami pervenuti in riferimento a realtà commerciali (cfr. atto di contestazione di violazione amministrativa del 3 settembre 2001) e ricreative (scuole e locali per lo svolgimento di attività sportive) nelle quali il sistema non era finalizzato ad effettuare un controllo diretto sul lavoratore, essendo orientato a perseguire diversi e altri profili di sicurezza.

Su tale aspetto, inoltre, e in generale sul problema delle procedure di informazione e di controllo a distanza del personale, l'Autorità è impegnata attivamente in un dibattito in corso in ambito comunitario tra i rappresentanti delle autorità garanti dei Paesi membri dell'Unione europea, costituito ai sensi dell'art. 29 della direttiva 95/46/CE, che dovrebbe concludersi con l'approvazione di una decisione comune entro il mese di maggio del 2002.

24 Annunci di lavoro

Con riguardo alla fase dell'instaurazione del rapporto di lavoro, il Garante ha effettuato ulteriori verifiche rispetto a quelle già avviate (e in parte concluse) nel 2000 (e sulle quali si rinvia alla precedente relazione annuale) su un campione significativo di annunci di lavoro pubblicati su alcuni quotidiani curati da soggetti operanti nel settore dell'intermediazione di lavoro (società di selezione o di ricerca del personale, società di lavoro temporaneo).

Dette verifiche hanno evidenziato un'alta percentuale di violazioni delle disposizioni poste dalla legge n. 675/1996, con particolare riguardo ai profili dell'informativa e dell'acquisizione del consenso. In conseguenza di ciò si sono avviati alcuni procedimenti per l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 39, comma 2, legge n. 675/1996.

Gli annunci con riferimento ai quali sono state contestate le violazioni indicate contengono, infatti, soltanto una sintetica richiesta ai candidati interessati di inviare il *curriculum*, priva delle informazioni che, in virtù dell'art. 10 della legge n. 675/1996, devono essere rese all'interessato previamente rispetto alla raccolta dei dati personali, nonché l'invito a rilasciare un consenso al trattamento, peraltro impropriamente definito "autorizzazione ai sensi della l. n. 675/1996".

In questo modo gli interessati non possono acquisire, neanche indirettamente, indicazioni relative alle caratteristiche del trattamento dei dati che i destinatari dei *curricula* così sollecitati si accingono ad effettuare (in relazione, per esempio, alle modalità, alle eventuali finalità ulteriori, all'ambito di comunicazione o diffusione dei dati conferiti, con particolare riguardo alle categorie dei destinatari, all'esercizio dei diritti di cui all'art. 13 della legge).

In relazione alla diversa ipotesi in cui gli autori dell'annuncio si avvalgano di caselle postali cui inviare i *curricula*, o di altre modalità atte a preservarne l'anonimato (impedendo così all'interessato l'individuazione del titolare del trattamento), è stata ravvisata la necessità di ulteriori accertamenti, specie di carattere ispettivo, al fine di risalire alla loro identità, dovendosi verificare anche, in tali casi, l'eventuale violazione di disposizioni rilevanti sul piano penale.

Alla luce di queste considerazioni il Garante, con un provvedimento a carattere generale, ha segnalato alle società rispetto alle quali sono state accertate le violazioni menzionate ed agli organismi pubblici e privati rappresentativi dei settori interessati la necessità di conformare la raccolta ed il successivo trattamento dei dati personali alle disposizioni contenute nella l. 675/1996, indicando contestualmente anche soluzioni operative volte a favorire l'attuazione in concreto dei principi di lealtà e correttezza nel trattamento dei dati personali, sin dal momento di pubblicazione degli annunci di lavoro (*Provv.* 10 gennaio 2002, in *Bollettino* n. 24, p. 22 e vedi anche il *Provv.* 13 gennaio 2000).

Nel dettaglio, si è specificato che gli annunci di lavoro richiedono una chiara informativa tale da evidenziare l'insieme degli elementi indispensabili per un conferimento consapevole dei dati e, ove necessario, per l'acquisizione di un consenso informato e specifico. È stato così sottolineato che l'informativa può essere effettuata anche ricorrendo a messaggi brevi e in stile colloquiale (omettendo superflue "assicurazioni" circa il rispetto della normativa sulla *privacy*), che permettano ai candidati interessati di comprendere i seguenti aspetti:

- l'identità del/i titolare/i del trattamento dei dati riportati nei *curricula* e le finalità e modalità del medesimo trattamento, specificando se vi siano ulteriori finalità oltre quelle connesse alla specifica ricerca di personale, o particolari modalità di organizzazione, di raffronto o di elaborazione dei dati. Devono essere indicati altresì i tempi della conservazione (anche per permettere agli interessati di poter eventualmente aggiornare ed integrare i dati), i quali devono risultare brevi e proporzionati rispetto alle finalità e modalità del trattamento;

- l'eventualità che i dati siano divulgati a terzi, individuati almeno per categorie;

- la circostanza che il conferimento dei dati è facoltativo e che la mancata indicazione di alcuni di essi può avere determinate conseguenze, invitando ad omettere dati non pertinenti in relazione all'offerta di lavoro e a manifestare per scritto il consenso al trattamento di dati sensibili (ad esempio, per quanto riguarda l'appartenenza a particolari categorie protette);

- una descrizione dei diritti riconosciuti al candidato interessato ai sensi dell'art. 13 della legge n. 675;

- i dati identificativi di almeno un responsabile del trattamento, ove questi sia designato (preferibilmente indicato nel soggetto preposto ai rapporti con gli interessati ai sensi dell'art. 13 della legge n. 675).

Al fine di agevolare le società interessate a rendere l'informativa in conformità alle indicazioni menzionate, l'Autorità ha ritenuto utile suggerire altresì, a titolo esemplificativo, un possibile schema di informativa – riproducibile anche in parte nell'annuncio, a seconda dello spazio disponibile e della complessa utilizzazione dei dati – nonché altre formule-tipo utilizzabili anche in relazione alla richiesta di consenso, ove necessario.

Peraltro, si è pure prospettata la possibilità di evitare l'inserimento dell'intera informativa nell'annuncio, quando esigenze di spazio lo richiedano, purché siano rese agevolmente disponibili agli interessati, prima del conferimento dei dati, informazioni più dettagliate su un indirizzo *web* indicato nell'annuncio o mediante altre idonee modalità alternative (quale ad esempio un messaggio telefonico pre-registrato).

Con riferimento, invece, alla diversa ipotesi in cui i *curricula* sono inviati spontaneamente dagli interessati, i destinatari degli stessi, trovandosi di regola nell'impossibilità di fornire in via preventiva l'informativa, sono chiamati ad adempiere comunque, senza ritardo, tale obbligo in caso di successivo trattamento dei dati (sul punto meritano di essere tenute presenti anche le osservazioni già formulate nel *Provv.* 28 dicembre 1998, in *Bollettino* n. 6, p. 119).

Per quanto attiene, poi, alla richiesta del consenso al trattamento (negli annunci, come già ricordato, impropriamente definito autorizzazione), si è sottolineato che detto consenso è necessario esclusivamente per il trattamento delle informazioni di natura sensibile che siano eventualmente fornite dai candidati (come, ad esempio, l'appartenenza a particolari categorie protette), secondo il disposto dell'art. 22 della l. n. 675/1996.

Al riguardo, si è precisato che l'acquisizione preventiva del consenso legittima il trattamento dei dati e la loro comunicazione ad aziende clienti per le sole finalità riguardanti la possibile instaurazione di un rapporto di lavoro o di collaborazione professionale e che lo stesso, se slegato da un'idonea informativa, risulta comunque invalido.

Con riguardo, invece, al trattamento di dati personali comuni, e con specifico riferimento anche alla loro comunicazione, il titolare del trattamento (qui le società di selezione) può, comunque, far ricorso alle disposizioni contenute negli artt. 12, comma 1, lett. *b*), e 20, comma 1, lett. *a-bis*), che gli consentono di prescindere dal consenso.

Il Garante ha sottolineato, infine, l'opportunità di attivare forme di collaborazione, peraltro già avviate in precedenza, con gli enti, gli organismi e le associazioni del settore, per assicurare un più ampio rispetto della legge n. 675/1996 e un'omogeneità dei comportamenti degli operatori coinvolti, anche in vista dell'adozione del codice di deontologia e di buona condotta per i trattamenti di dati personali per finalità previdenziali o per la gestione del rapporto di lavoro che, secondo quanto previsto dall'art. 20, comma 2 del d.lg. n. 467/2001, prevederà anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di *curricula* contenenti dati personali anche sensibili.

25 Sistemi informativi in materia di lavoro

In materia di incontro tra domanda e offerta di lavoro, già in passato l'Autorità è stata chiamata ad esprimersi sulle modalità di realizzazione delle procedure di informazione, con riferimento sia ad uno schema di regolamento riguardante il riordino del collocamento pubblico e istitutivo del Sistema informativo lavoro (SIL), sia alla previsione di una "scheda professionale" del lavoratore (cfr. *Relazioni 1999* e *2000*, rispettivamente pp. 34 e 37).

Nel corso del 2001, in particolare, è stato formulato un parere (*Provv.* 24 aprile 2001, in *Bollettino* n. 19, p. 30) relativamente a due schemi di decreti ministeriali attuativi del regolamento di semplificazione della disciplina per il collocamento ordinario dei lavoratori adottato con d.P.R. 7 luglio 2000, n. 442. Tali schemi riguardano il contenuto e le modalità di trattamento dei dati personali attinenti, rispettivamente, all'elenco anagrafico delle persone in cerca di lavoro e alla connessa scheda professionale (artt. 4, comma 3, e 5, comma 1, d.P.R. n. 442/2000).

Come riferito nella precedente relazione annuale, l'Autorità ha rilevato il mancato recepimento, con il d.P.R. n. 442/2000, di diversi profili considerati nel provvedimento del 30 novembre 1999 (in *Bollettino* n. 10, p. 27) circa il rapporto tra i flussi di dati personali previsti, la peculiare organizzazione del SIL e la delimitazione degli obblighi di verifica dell'esattezza e della pertinenza delle informazioni, anche in termini di uniformità di disciplina sulle modalità di accesso da parte di regioni ed enti locali. A questo riguardo, ulteriori osservazioni hanno avuto ad oggetto la titolarità del trattamento dei dati relativi all'elenco anagrafico delle persone in cerca di lavoro e, sotto diverso profilo, alcuni aspetti dello schema di decreto concernente la scheda professionale del lavoratore.

La confusa e carente tutela dei dati personali nei sistemi informativi in materia di lavoro, stratificata in più provvedimenti non sempre armonici tra loro, induce ad auspicare che una visione più organica possa essere introdotta già a partire dall'approvazione del decreto legislativo recante "*Disposizioni integrative e modifiche del decreto legislativo 21 aprile 2000, n. 181, recante norme per agevolare l'incontro tra domanda e offerta di lavoro*" approvato in via preliminare dal Consiglio dei ministri lo scorso 11 aprile 2002. Si impone, infatti, una valutazione più uniforme dei vari aspetti riguardanti la costituzione del Sistema informativo lavoro e le modalità di redazione della scheda professionale del lavoratore che dovrebbe sostituire il vecchio libretto di lavoro.

Statistica, ricerca scientifica e ricerca storica

26 Statistica e ricerca scientifica

In materia di trattamento dei dati personali per finalità di statistica e di ricerca scientifica, il Garante ha seguito, conformemente alle previsioni contenute nella legge n. 675/1996 e nel d.lg. n. 281/1999, i lavori preparatori del codice di deontologia e buona condotta per il trattamento dei dati personali effettuati a fini statistici in ambito Sistan e quello relativo alla statistica privata, proseguendo così l'attività che ha già condotto all'adozione dei codici deontologici dei giornalisti e degli storici; questa attività ha visto impegnati gruppi di lavoro costituiti da enti, associazioni, fondazioni ed istituzioni rappresentative della variegata realtà della statistica pubblica e privata, che si sono ispirati alla disciplina comunitaria ed a documenti internazionali quali le Raccomandazioni del Consiglio d'Europa.

La prossima emanazione dei nuovi codici, oltre a contribuire alla creazione della disciplina di settore prevista dalla normativa a protezione dei dati personali, individuerà le regole atte a calibrare l'attività statistica con il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

Lo strumento dei codici permette, inoltre, di disciplinare, con una fonte normativa flessibile e più facilmente emendabile, un settore quale quello della statistica che ha una forte connotazione tecnica. Tale strumento, infatti, essendo fondato sulla spontanea e sentita adozione da parte delle stesse categorie interessate, favorisce una più attenta osservanza delle nuove regole, il cui rispetto è comunque, grazie all'apposita previsione normativa, una "*condizione essenziale*" per la liceità del trattamento dei dati.

Il Garante ha altresì fornito diversi pareri all'Istituto centrale di statistica: in merito a quello relativo al questionario da adottare per la rilevazione delle convivenze nell'ambito del 14° censimento generale della popolazione e delle abitazioni (v. parere 30 luglio 2001), sono state espresse le medesime preoccupazioni precedentemente manifestate (cfr. pareri 14 marzo e 27 giugno 2001, rispettivamente in *Bollettino* n. 18, p. 37 e n. 22, p. 16), in relazione a quesiti – pur formulati con alcune precauzioni e nell'ottica del perseguimento di una rilevante finalità di interesse pubblico – idonei a rivelare informazioni, fra le più intime, delle persone interessate. Il peculiare ambito di indagine del questionario esaminato ha infatti coinvolto, inevitabilmente, dati sensibili degli interessati in relazione a particolari situazioni di coabitazione (presenza in ospedali, case di cura, istituti penitenziari, religiosi, ecc.).

È stato così ribadito l'invito a valutare nuovamente, alla luce dei principi di pertinenza e di non eccedenza enunciati dall'art. 9 della legge n. 675/1996 e dal d.lg. n. 135/1999, il carattere indispensabile delle domande inerenti alle condizioni di salute (ad es. quelle relative alle ore non lavorate in una certa settimana), o alle condizioni etnico-razziali (nazionalità, condizione di profugo/rifugiato, ecc.), e si è sottolineata altresì l'esigenza di verificare con particolare attenzione la reale necessità di disporre in dettaglio di alcune informazioni relative a comunità terapeutiche e di recupero per tossicodipendenti. Il fatto di dimorare in tali strutture, infatti, a differenza di quanto può avvenire per la presenza in altri luoghi di cura, è indice non solo di generici problemi di salute, ma consente anche di risalire alla circostanza che ha originato il "ricovero". Il Garante ha così rilevato che tale informazione poteva essere resa meno evidente, ad esempio, incorporando le notizie relative alla presenza in detti luoghi nell'ambito di quelle più generiche degli istituti assistenziali o di cura. In questo stesso senso, inoltre, è apparso più opportuno, in riferimento ai casi di "*Assistito in un centro di accoglienza per immigrati*", eliminare la specificazione "*per immigrati*".

Con il medesimo parere si sono espresse anche valutazioni sulla circolare inerente la costituzione degli uffici di censimento comunali e provinciali, richiamando l'attenzione, in analogia a quanto già indicato nei pareri del 14 marzo e del 27 giugno 2001, sull'importanza di procedere ad un'attenta valutazione dei requisiti di esperienza, capacità ed affidabilità delle persone da designare quali responsabili o incaricati nelle attività di censimento. L'Autorità ha evidenziato inoltre che, per l'espletamento delle relative mansioni, tali figure necessitano di precise istruzioni, affinché le informazioni ricevute siano trattate e custodite con la massima diligenza e nel rispetto del segreto, evitando rigorosamente accessi di terzi non autorizzati ai dati ed usi degli stessi diversi da quelli previsti dal censimento.

27 Ricerca storica

Il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici (pubblicato in *G.U.* n. 80 del 5 aprile 2001), il cui rispetto costituisce condizione essenziale per la liceità del trattamento dei dati personali in tale ambito, è stato elaborato da un gruppo di lavoro costituito da associazioni, fondazioni ed istituzioni rappresentative della multiforme realtà della ricerca storica e del mondo archivistico.

Il Garante è intervenuto in varie fasi della redazione del codice: promuovendone dapprima l'adozione e la sottoscrizione, così come prevede anche l'art. 6, comma 1, del d.lg. n. 281/1999, prestando successivamente la propria assistenza al gruppo di lavoro e, infine, constatando la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, in particolare all'art. 31, comma 1, lett. *h*), della legge n. 675/1996, nonché agli artt. 6 e 7 del d. lg. n. 281/1999.

Tale documento completa l'impianto normativo introdotto dal decreto legislativo del 1999 e stabilisce principi di comportamento per i soggetti che trattano, per scopi storici, i dati personali conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico, mirando a favorire l'attività di ricerca storica e archivistica e individuando nel contempo adeguate modalità per garantire i diritti della personalità degli interessati.

Per quanto riguarda gli archivisti, il codice definisce regole di correttezza e di non discriminazione nei confronti di coloro che richiedano la consultazione di fonti storiche, mentre con riferimento agli "*utenti*", cioè a chiunque faccia ricerca storica, il codice individua cautele per la raccolta, l'utilizzazione e la diffusione dei dati contenuti nei documenti.

Il codice prevede diversi obblighi per gli archivisti: tutelare l'integrità degli archivi e l'autenticità dei documenti, compresi quelli elettronici e multimediali, anche attraverso l'adozione di idonee misure di sicurezza; non utilizzare per uso personale le informazioni non disponibili agli utenti, di cui essi dispongano in ragione della propria attività; favorire l'esercizio del diritto degli interessati all'aggiornamento, alla rettifica o alla integrazione dei dati, garantendone la conservazione secondo modalità che assicurino la distinzione delle fonti originarie dalla documentazione successivamente acquisita.

Il codice di deontologia e buona condotta, inoltre, non tralascia di affrontare l'aspetto delle fonti orali, prevedendo la necessità che gli intervistati esprimano il proprio consenso in modo esplicito, anche in forma verbale, e stabilendo, altresì, che gli archivi richiedano all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti nell'intervista stessa e del relativo consenso manifestato dagli interessati.

Per quanto riguarda la categoria degli utenti degli archivi, il codice stabilisce che chiunque ha libero accesso agli archivi pubblici e che i documenti devono essere utilizzati, sotto responsabilità, attenendosi agli scopi perseguiti e delineati nel progetto di ricerca, nel rispetto dei principi di pertinenza ed indispensabilità. Le eccezioni al libero accesso agli archivi pubblici riguardano i documenti di carattere riservato relativi alla politica interna ed estera dello Stato (consultabili dopo cinquant'anni dalla loro data) e quelli che contengono dati sensibili e giudiziari (che divengono consultabili dopo quarant'anni). Il termine è di settant'anni se i dati sono relativi allo stato di salute o alla vita sessuale, oppure a rapporti riservati di tipo familiare.

Per i documenti contenenti questo tipo di dati resta prevista la possibilità di un'autorizzazione alla consultazione prima della scadenza dei termini, rilasciata dal Ministero dell'interno, udita un'apposita commissione nella quale siedono rappresentanti della ricerca storica, degli archivi di Stato e del Garante. L'autorizzazione è rilasciata a parità di condizioni ad ogni altro richiedente.

Il codice stabilisce che, nel far riferimento allo stato di salute delle persone, chi fa ricerca debba astenersi dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad un determinato soggetto identificato o identificabile.

Inoltre, la sfera privata delle persone note o che abbiano esercitato funzioni pubbliche deve essere rispettata nel caso in cui le notizie o i dati non abbiano alcun rilievo sul ruolo svolto o sulla loro vita pubblica.

Nonostante alcuni timori manifestati prima dell'entrata in vigore del codice circa le conseguenze sull'attività degli storici e più, in generale, sulle funzionalità degli archivi, ad un anno dalla sua pubblicazione non è emerso alcun contenzioso sull'argomento, confermandosi così l'opportunità e la correttezza operata dal legislatore con tale scelta.

Associazioni, movimenti politici e partiti

28 Trattamento dei dati e realtà associative

La materia associativa, interessata da significative modifiche normative introdotte dall'art. 8 del d.lg. n. 467/2001 – che ha novellato, in relazione al trattamento dei dati sensibili, l'art. 22 della legge n. 675/1996, da un lato introducendovi, *ex novo*, il comma 1-*ter* e, dall'altro, modificandone il comma 4 – è stata altresì oggetto di attenzione da parte del Garante in alcune delle autorizzazioni generali per il trattamento dei dati sensibili recentemente rinnovate, ed in particolare nell'autorizzazione n. 3/2002.

Per quanto riguarda l'attività svolta nel corso del 2001, si è intervenuti sia a tutela del diritto all'informativa ai sensi dell'art. 10 della l. n. 675/1996, sia al fine di garantire il rispetto dei diritti dell'interessato sanciti dall'art. 13 della medesima legge.

Per ciò che concerne il diritto dell'interessato all'informativa di cui al citato art. 10, l'Autorità – in virtù dell'art. 39, comma 2, della legge n. 675/1996 – ha applicato una sanzione amministrativa nei confronti di circoli privati e associazioni che, come riscontrato a seguito di controlli effettuati dalle forze di polizia, non fornivano la suddetta informativa agli aspiranti soci, in occasione della raccolta di loro dati personali (*Provv.ti* 28 settembre 2001).

Un altro provvedimento è intervenuto nel caso di un tesserato della Federazione italiana giuoco calcio (F.I.G.C.) che, inizialmente, aveva fornito solo parzialmente riscontro alle richieste da questi presentate ai sensi dell'art. 13 della l. n. 675/1996. A seguito dell'intervento, la Federazione ha provveduto ad informare l'interessato delle finalità e delle modalità del trattamento dei dati personali e ha dato comunicazione, anche in senso negativo, relativamente all'esistenza di altri dati personali, del loro contenuto e della loro origine (*Provv.* 28 novembre 2001, in *Bollettino* n. 23, p. 55).

In altra occasione, infine, a fronte di analoghe richieste rivolte nei confronti dell'Associazione italiana per la ricerca sul cancro da una persona destinataria di una pubblicazione promozionale relativa ad una manifestazione promossa dall'Associazione medesima, l'Autorità, preso atto delle attestazioni dell'associazione di non detenere dati relativi alla persona interessata nell'archivio soci, ha dichiarato il non luogo a provvedere ai sensi dell'art. 20, comma 2, del d.P.R. n. 501/1998 (*Provv.* 24 gennaio 2002, in *Bollettino* n. 24, p. 31).

29 L'uso di dati per finalità politico-elettorali

Lo svolgimento delle consultazioni elettorali nel corso del 2001 ha determinato numerosi interventi dell'Autorità in materia di trattamento di dati personali, su parte dei quali si è già ampiamente soffermata la precedente relazione annuale (v. *Relazione 2000*, p. 42). Basti richiamare, in particolare, i provvedimenti aventi carattere generale del 7 febbraio 2001 (*G.U.* 13 febbraio 2001, n. 36 e *Bollettino* n. 17, p. 7) – con il quale si sono esonerati fino al 30 giugno 2001 partiti, movimenti politici, comitati promotori, sostenitori di liste e di candidati dall'obbligo di rendere l'informativa prevista dall'art. 10, comma 3, della legge n. 675/1996 – e del 7 marzo 2001 (in *Bollettino* n. 18, p. 24) – con il quale il Garante ha segnalato a partiti e movimenti politici i principi ai quali ispirare i trattamenti dei dati personali nel corso della campagna elettorale, al fine di renderli armonici con la disciplina introdotta dalla legge n. 675/1996.

Entrambi i menzionati provvedimenti, il 9 maggio 2001, sono stati altresì comunicati all'Adusbef che aveva previamente interpellato il Garante in ragione delle numerose segnalazioni di cittadini indirizzate all'associazione, riguardanti il trattamento dei loro dati personali per finalità di propaganda elettorale.

Per altro verso, numerosi cittadini hanno fatto ricorso al Garante lamentando le diverse modalità utilizzate per l'invio di messaggi di propaganda elettorale: oltre alle tradizionali comunicazioni cartacee, infatti, si è avuto un ampio impiego di messaggi inviati sulle utenze telefoniche mobili degli abbonati *(sms)* e di messaggi inviati tramite internet (v. *Relazione 2000*, p. 43, relativamente al *Provv.* 11 gennaio 2001, in *Bollettino* n. 16, p. 39).

In particolare, rispetto all'invio di una missiva avente contenuto propagandistico il Garante, considerando l'attestazione fornita dal titolare del trattamento, secondo il quale i dati personali erano stati ricavati da elenchi ufficiali, tra i quali la guida telefonica, e prendendo atto dell'adesione dello stesso alla richiesta dell'interessato di non vedere comunque più utilizzati i propri dati, ha dichiarato – ai sensi dell'art. 20, comma 2, del d.P.R. n. 501/1998 – non luogo a provvedere sul ricorso (*Provv.* 10 ottobre 2001, in *Bollettino* n. 22, p. 54).

Ad identica conclusione si è giunti in altra circostanza, nella quale il messaggio propagandistico era pervenuto tramite *sms* sull'utenza telefonica mobile dell'interessato, muovendo dalla considerazione che il beneficiario dei messaggi promozionali si era rivolto ad una società che aveva previamente raccolto il consenso dei destinatari rispetto a questa tipologia di comunicazione promozionale (*Provv.* 20 giugno 2001, in *Bollettino* n. 21, p. 39). Alla società è stata peraltro applicata, con distinto provvedimento, una sanzione amministrativa pecuniaria per mancata risposta al Garante alla richiesta di informazioni *ex* art. 32, comma 1, della legge n. 675/1996, formulata nel quadro di un procedimento successivo alla decisione adottata sul predetto ricorso.

30 Condomini

Per quanto attiene al trattamento dei dati personali nel contesto condominiale, il Garante ha riconosciuto che l'affissione dell'ordine del giorno di un'assemblea condominiale nella bacheca posta nello spazio di accesso comune ad uno stabile integra una modalità di trattamento dei dati personali che, in linea di massima, è lecita; tuttavia, in un caso di specie, un avviso così pubblicato conteneva anche un riferimento specifico ad un'asserita morosità dell'interessato (conoscibile, in tal modo, anche da terzi estranei al condominio), mentre sarebbe stato più appropriato inserire, in tale avviso, le sole informazioni necessarie per un'efficace comunicazione dell'evento (la convocazione dell'assemblea condominiale). Un approfondimento nel merito delle singole questioni, con eventuale indicazione delle informazioni relative allo stato di morosità, sarebbe stato possibile, infatti, anche attraverso l'invio di documenti ai singoli aventi diritto, oppure differendone la trattazione alla discussione comune (*Provv.* 12 dicembre 2001, in *Bollettino* n. 23, p. 7).

In altro caso, preso atto dell'adesione dell'amministratore del condominio alle richieste dell'interessato, volte a far venir meno la divulgazione dell'identità dei presunti condomini morosi, il cui elenco era depositato in un cassetto della portineria, è stato disposto non luogo a provvedere sul ricorso a seguito del ritiro del menzionato elenco (*Provv.* 17 maggio 2001, in *Bollettino* n. 20, p. 11).

In altre fattispecie, attraverso il ricorso all'Autorità il condomino ha ottenuto soddisfazione rispetto alle richieste precedentemente avanzate e inizialmente disattese dal titolare del trattamento: in un caso, esse miravano a conoscere l'origine – poi individuata nel presidente della cooperativa costruttrice dello stabile – dei dati personali contenuti in una convocazione di assemblea di condominio (*Provv.* 20 giugno 2001, in *Bollettino* n. 21, p. 25); in altro caso, invece, esse miravano a conoscere quali dati fossero detenuti dal titolare (*Provv.* 10 ottobre 2001, in *Bollettino* n. 23, p. 132).

Attività forense, investigazione privata e liberi professionisti

31 Liberi professionisti e albi professionali

L'Autorità è stata sollecitata nuovamente ad esprimersi su questioni afferenti il regime di pubblicità degli albi professionali e degli atti connessi allo *status* di iscritto all'albo e, in un provvedimento emesso in relazione all'albo degli avvocati (*Provv.* 29 marzo 2001, in *Bollettino* n. 18, p. 20), ha confermato la linea interpretativa espressa in termini generali in precedenza (*Pareri* 30 giugno, 22 luglio e 4 agosto 1997, in *Bollettino* n. 1, p. 33, 40 e 46, emessi rispettivamente in relazione agli albi dei medici ed odontoiatri, degli ingegneri ed architetti e dei dottori commercialisti).

Si è ricordato, infatti, che la legge n. 675/1996 non ha modificato la disciplina legislativa relativa al regime di pubblicità degli albi professionali ed alla conoscibilità degli atti ad essi connessi e che gli albi professionali sono destinati per la loro natura e funzione ad un regime di piena conoscibilità da parte di chiunque, anche in funzione della tutela dei diritti di coloro che a vario titolo hanno rapporti con gli iscritti.

Analoga indicazione è stata formulata con riguardo all'albo dei medici chirurghi (*Parere* del 24 luglio 2001), richiamando le norme che ne prevedono l'indifferenziata conoscibilità attraverso la stampa, la pubblicazione a cura di ciascun Ordine, nonché la trasmissione di una copia ad alcune amministrazioni pubbliche, anche al fine della affissione nelle prefetture (d.lg. C.p.S. n. 233/1946; d.P.R. n. 221/1950).

Con riguardo al profilo attinente al regime di pubblicità dei provvedimenti disciplinari adottati nei confronti degli iscritti all'albo degli avvocati, il Garante ha inoltre rilevato che, in considerazione delle disposizioni sulle forme di pubblicità previste dalla normativa in materia (r.d.l. n. 1578/1933; r.d. n. 37/1934), i provvedimenti disciplinari menzionati si configurano quali atti pubblici soggetti ad un regime di conoscibilità anche da parte di altri professionisti e di terzi. In riferimento a tale regime, che si fonda su rilevanti motivi di interesse pubblico connessi anche a ragioni di giustizia ed al regolare svolgimento dei procedimenti in ambito giudiziario, non si è ritenuto prevalente, nel caso esaminato, l'interesse alla riservatezza del singolo professionista destinatario di una misura disciplinare. L'Autorità ha comunque precisato che la menzione del provvedimento che applica la misura deve essere pur sempre effettuata nel rispetto del principio di correttezza, esattezza e completezza dei dati fissato dall'art. 9 della legge n. 675/1996.

In considerazione, dunque, del regime di conoscibilità dei provvedimenti disciplinari in esame deve ritenersi lecita la loro divulgazione tramite riviste, notiziari o altre pubblicazioni curate dai Consigli dell'ordine, ricadendo del resto la stessa nell'ampia nozione di trattamento di dati personali finalizzato alla pubblicazione o diffusione occasionale di articoli, saggi o altre manifestazioni di pensiero, comunque soggetta alla disciplina dettata dall'art. 25 della legge n. 675/1996.

Merita infine di essere ricordato, con particolare riferimento ai cd. "dati sensibili", che il Garante ha reiterato le autorizzazioni n. 4 e n. 6 in tema di trattamento di tali categorie di dati da parte dei liberi professionisti e degli investigatori privati, attesi i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti. Tali provvedimenti, che tengono conto delle modifiche alla legge n. 675/1996 nel frattempo intervenute ad opera del d.lg. n. 467/2001, nonché, in materia di esercizio della professione di avvocato, da parte del d.lg. n. 96/2001 e, infine, in materia di investigazioni difensive, dalla legge n. 397/2000, hanno efficacia fino al 30 giugno 2003.

32 La raccolta di dati per finalità di difesa e di indagine difensiva

Le questioni connesse alla raccolta dei dati per l'esercizio del diritto di difesa, la cui liceità, con una rigorosa applicazione del principio di finalità, è riconosciuta e puntualmente regolamentata in più luoghi della disciplina vigente (artt. 10, comma 4; 12, comma 1, lett. *h)*; 14, comma 1, lett. *e*); 20, comma 1, lett. *g)*), sono state ripetutamente affrontate – soprattutto in sede di risoluzione di ricorsi proposti ai sensi dell'art. 29 della legge n. 675/1996 – specie in relazione a fattispecie afferenti l'attività svolta da agenzie investigative private.

In uno di questi casi il Garante ha rilevato la liceità del trattamento operato dal titolare per acquisire materiale probatorio utile al fine di contestare ad alcuni dipendenti eventuali infrazioni disciplinari, rilevando che, in ragione della particolarità delle mansioni svolte (nel caso di specie, trattavasi di addetti al servizio di esazione autostradale), era giustificato ricorrere ad investigatori privati.

Il trattamento posto in essere da questi ultimi, sia in relazione alle modalità utilizzate, sia in riferimento alla durata delle operazioni svolte, è stato del pari valutato come non eccedente rispetto allo scopo perseguito (*Provv.* 21 novembre 2001, in *Bollettino* n. 23, p. 98, nel quale si è richiamato il precedente *Provv.* 9 novembre 2000); analoghe considerazioni sono state svolte nell'ambito di altra vicenda, relativa ad un procedimento di separazione personale (*Provv.* 28 febbraio 2002).

In un altro caso (*Provv.* 19 febbraio 2002, in *Bollettino* n. 25, p. 17), concernente l'asserita violazione di un patto di non concorrenza, il Garante, riconosciuto che il riferimento normativo (art. 10, comma 4, l. 675/1996) alla "sede giudiziaria" presso la quale far valere un diritto è tale da ricomprendere anche il procedimento arbitrale rituale (instaurato dalla società titolare nei confronti dell'interessato e nell'ambito del quale i dati raccolti erano stati depositati), ha rilevato che alcuni dati personali erano stati acquisiti direttamente presso l'interessato, mediante ascolto, registrazione o intercettazione effettuati a cura di un istituto investigativo, sancendo che tali modalità di raccolta si pongono in violazione con l'obbligo di informare l'interessato. Obbligo, quest'ultimo, che opera quando i dati sono acquisiti direttamente dalla persona fisica che li fornisce, come prescritto dall'art. 10, comma 1, legge n. 675/1996. Ciò in armonia con le disposizioni della successiva legge n. 397/2000 sulle indagini difensive, la quale, in riferimento all'investigazione privata collegata alla difesa penale, prevede l'obbligo dell'investigatore di avvertire le persone con cui si instaura il colloquio (art. 391-*bis* c.p.p., introdotto dall'art. 11 della legge n. 397/2000).

In considerazione della rilevata illiceità, il Garante ha quindi disposto sia nei confronti della agenzia investigativa, sia della società committente il divieto di ogni ulteriore trattamento dei dati raccolti.

Infine, rispondendo ad un quesito formulato da una società (*Parere* 15 gennaio 2001), è stato precisato che la comunicazione a studi legali esterni alla struttura aziendale di dati relativi a terzi (clienti, fornitori, dipendenti ed altri) è consentita, anche senza il consenso degli interessati, ai sensi dei già citati artt. 12 e 20 della legge n. 675/1996, se finalizzata alla tutela di un diritto in sede giudiziaria, anche nella fase prodromica all'eventuale inizio di un procedimento, per il periodo strettamente necessario al perseguimento di tale finalità.

33 I codici deontologici

I codici di deontologia e di buona condotta per il trattamento dei dati da parte dei difensori e degli investigatori privati, la cui adozione è stata promossa dal Garante in data 10 febbraio 2000, sono in avanzata fase di redazione e dovrebbero trovare compiuta realizzazione nell'arco del 2002, in coincidenza con la emanazione da parte del Governo del testo unico.

La predisposizione di detti codici è destinata ad inserirsi nel più vasto ambito di attività del Garante delineato dal recente d.lg. n. 467/2001, con il quale (art. 20, comma 1) è stato attribuito al Garante il compito di promuovere, entro il 30 giugno 2002, la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali nei settori indicati nell'art. 20, comma 2, del citato decreto.

Merita di essere nuovamente segnalato che il rispetto delle disposizioni contenute nei codici di deontologia e di buona condotta costituisce condizione essenziale per la liceità del trattamento dei dati (previsione che induce a qualificare tali atti quali fonti normative atipiche, di rango secondario) e che, sempre secondo l'art. 20 del d.lg. n. 467/2001, tali codici saranno pubblicati, a cura del Garante, nella Gazzetta Ufficiale della Repubblica Italiana e andranno riportati in allegato al testo unico.

Settore del credito, finanziario ed assicurativo

34 Profili generali

Cresce l'attenzione rivolta dai cittadini nei confronti della raccolta, dell'utilizzazione e della circolazione dei dati in ambito bancario, finanziario ed assicurativo. Nonostante i rilevanti sforzi organizzativi ed economici compiuti in questi settori per l'attuazione delle complesse regole poste a tutela delle informazioni di carattere personale, esistono ancora diversi, delicati aspetti che necessitano di essere "messi a fuoco" e che, anche per l'assenza di specifiche disposizioni, determinano la diffusione di prassi non corrette o disomogenee tra i singoli operatori, da un lato, e un largo contenzioso con la clientela, dall'altro.

È infatti in aumento il numero di istanze, segnalazioni, reclami, ricorsi e quesiti rispetto ad alcune particolari attività creditizie ed assicurative che, nella relazione dello scorso anno, sono state definite come filoni "patologici" per i loro riflessi in materia di *privacy* e per la loro incidenza nella vita quotidiana di qualsiasi individuo (v. la *Relazione 2000*, p. 48).

Con riferimento al settore delle assicurazioni, rimangono anzitutto sul tappeto alcuni problemi interpretativi legati all'accesso, da parte di clienti o di terzi danneggiati, a perizie medico-legali predisposte dai medici di fiducia delle compagnie assicurative, in relazione a richieste di risarcimento dei danni ed alla liquidazione dei sinistri (sia per le assicurazioni auto, sia per le polizze sanitarie). Nel paragrafo successivo verranno descritte le pronunce più significative dell'Autorità su tale argomento. In proposito, occorre però rilevare sin d'ora che alcuni giudici di merito, a differenza del Garante, sono a volte propensi a non considerare come dati personali degli assicurati le informazioni riportate nell'ambito delle valutazioni sanitarie espresse su questi ultimi da consulenti delle società di assicurazioni (sulla questione si attende un primo pronunciamento della Corte di cassazione).

Sempre in rapporto al settore assicurativo, vanno segnalate le questioni applicative connesse all'ormai prossima entrata in funzione della banca dati dei sinistri automobilistici gestita dall'Isvap per la lotta contro le frodi assicurative (anche questo argomento sarà oggetto di approfondimento in un ulteriore paragrafo).

L'altro fronte "patologico" riguarda poi le attività di acquisizione, trattamento e messa a disposizione nei circuiti bancari e finanziari delle informazioni sui finanziamenti erogati ai cittadini. Come si vedrà in seguito, si tratta di attività svolte, oltre che dalla Banca d'Italia, da società private che gestiscono sistemi informativi centralizzati di rilevazione dei rischi creditizi, le cd. "centrali rischi", strumenti di tutela preventiva del credito ritenuti essenziali per lo sviluppo delle forme di credito al consumo. Su questo fronte, il recente decreto legislativo 467/2001 ha previsto di rinviare direttamente all'autoregolamentazione degli operatori del settore e delle associazioni dei consumatori, seppur con il vaglio del Garante, la definizione di puntuali ed omogenee disposizioni per il rispetto dei principi sulla protezione dei dati relativi ai rapporti di finanziamento, alla puntualità nei pagamenti ed all'affidabilità dei clienti interessati.

Risulta, poi, confermato il dato, già indicato nella relazione 2000, del tendenziale, progressivo aumento delle segnalazioni e delle istanze presentate dai clienti degli istituti di credito contro le violazioni delle norme poste a tutela della riservatezza nei rapporti bancari, relativamente alla divulgazione a persone estranee di informazioni su proprie operazioni, conti od investimenti. In proposito, sono stati assunti alcuni provvedimenti che forniscono chiarimenti in materia di segreto bancario, individuando criteri utili per la determinazione dei comportamenti leciti nell'uso e nella divulgazione dei dati da parte dei dipendenti delle banche che garantiscano sia il cittadino, sia l'impresa bancaria. Tali principi potrebbero essere ripresi nell'ambito del rafforzamento del dovere di riserbo degli impiegati bancari o della predisposizione di apposite regole di condotta sulla protezione dei dati personali da parte degli istituti di credito e finanziari, alla luce del provvedimento del 10 febbraio 2000 per la promozione della sottoscrizione di codici di buona condotta in diversi settori (v. rispettivamente *Relazione 2000*, p. 49 e *Relazione 1999*, p. 223).

In particolare (*Provv.* 23 maggio 2001, richiamato nella *Relazione 2000* e pubblicato in *Bollettino* n. 20, p.

30), è stata ritenuta fondata la segnalazione del cliente di una banca il cui dipendente aveva divulgato dati su rapporti di conto corrente e di deposito titoli ad un legale esterno il quale, a sua volta, li aveva utilizzati in una controversia tra il cliente ed un terzo (si trattava, in concreto, di una causa tra ex coniugi relativa all'aumento dell'assegno di divorzio). In tale provvedimento, è stato evidenziato che la disposizione della legge 675/1996 la quale permette di comunicare dati personali senza il consenso dell'interessato, qualora ciò sia necessario per la difesa di un diritto in sede giudiziaria (nel rispetto della normativa vigente in materia di segreto aziendale ed industriale: art. 20, comma 1, lett. *g)*), attribuisce al titolare del trattamento solo una facoltà di divulgare i dati all'esterno.

Per gli istituti di credito esiste tuttavia l'obbligo del cd. segreto bancario che è presupposto, o richiamato, da diverse normative in materia fiscale o tributaria e che viene comunemente configurato come connaturato al rapporto banca-cliente in applicazione dei principi di correttezza e buona fede nell'esecuzione del contratto, trovando riscontro anche negli usi e nelle consuetudini bancarie (nonché negli impegni che gli istituti di credito assumono nei confronti della clientela allorché dichiarano di rispettare le regole di comportamento indicate dalla relativa associazione di categoria, anche per ciò che attiene alla riservatezza nella raccolta e nel trattamento delle informazioni sui clienti).

Al di fuori di operazioni di comunicazione dei dati strumentali alle prestazioni richieste e ai servizi erogati, gli istituti di credito ed il relativo personale sono di regola tenuti a mantenere la riservatezza sulle informazioni relative ai propri clienti e a non divulgarle a soggetti esterni, a meno che tali soggetti abbiano il diritto di ottenerle o, comunque, il potere di conoscerle in base a specifiche disposizioni normative o contrattuali. Ne deriva che una comunicazione di informazioni sui conti dei clienti effettuata in violazione del descritto impegno al riserbo nello svolgimento del rapporto bancario risulta contraria ai principi di liceità e correttezza sanciti dall'articolo 9 della legge n. 675/1996.

Con una successiva deliberazione (adottata il 27 giugno 2001), è stata invece dichiarata l'infondatezza di un'altra segnalazione presentata da un cliente di un istituto bancario che aveva divulgato dati relativi ai rapporti di conto corrente di quest'ultimo nell'ambito della controversia giudiziaria concernente l'attività professionale dallo stesso precedentemente svolta per il medesimo istituto. In questo caso è stato ribadito che l'istituto di credito può comunicare informazioni relative ai rapporti di conto corrente quando tale comunicazione sia effettuata in sede giudiziaria per tutelare i propri diritti nelle controversie con i clienti interessati, non assumendo valore ostativo, in questa ipotesi, l'impegno di riservatezza assunto nei confronti della clientela in relazione ai servizi prestati, che non può tradursi in un vincolo tale da produrre effetti lesivi nella sfera giuridica della stessa banca e in un limite all'esigenza di difesa giudiziaria dei propri diritti. Il cliente non può difatti pretendere dalla banca un comportamento che si risolva in una lesione dei propri interessi giuridicamente rilevanti e del proprio diritto di difesa, in contrasto con lo stesso principio di solidarietà che impronta i richiamati doveri di correttezza nei rapporti obbligatori.

Ulteriore fonte di intensa attività, come già accennato nella scorsa relazione annuale, è risultato l'esame delle istanze presentate da diverse società in relazione alle modalità alternative di informativa ai clienti interessati, utilizzabili in relazione a complesse operazioni di cartolarizzazione dei crediti.

A seguito del provvedimento di carattere generale adottato il 4 aprile 2001 (pubblicato in *Bollettino* n. 19, p. 20), le società cessionarie di crediti sono state autorizzate a fornire l'informativa agli interessati mediante pubblicazione nella Gazzetta Ufficiale, attraverso modalità sostanzialmente analoghe a quelle previste dal testo unico in materia bancaria e finanziaria (che appunto prevede tale forma di pubblicazione per rendere note le cessioni in blocco di rapporti giuridici: v. la *Relazione 2000*, p. 48), mediante la messa a disposizione dell'informativa nelle filiali e negli uffici delle società cessionarie, nonché con la sua pubblicazione su almeno due quotidiani nazionali ed uno locale (nel luogo in cui sono insediate le filiali che hanno intrattenuto il maggior numero di rapporti con i clienti interessati).

In tale provvedimento, si è altresì precisato che l'autorizzazione si intende automaticamente concessa anche per le altre società che ne abbiano fatto richiesta, trovandosi nelle medesime condizioni, decorsi trenta giorni dal ricevimento delle istanze senza che il Garante abbia chiesto chiarimenti o comunicato il rigetto. E, in verità, anche nei primi mesi del 2002, è stata effettuata un'attività di monitoraggio delle frequenti richieste presentate da società che pur rientrano nell'ambito di applicazione del citato provvedimento e che sono tenute ad inviare i modelli informativi predisposti. In diversi casi, però, alcuni operatori hanno avanzato quesiti ed istanze per otte-

nere un'ulteriore semplificazione degli adempimenti o hanno sottoposto al vaglio dell'Ufficio operazioni di cartolarizzazione o di cessione in blocco di crediti che si svolgono secondo norme e con formalità differenti da quelle individuate dal testo unico bancario.

Per queste ipotesi, il Garante dovrà a breve pronunciarsi per fornire ulteriori, opportune indicazioni di carattere generale, in modo anche da far diminuire o cessare l'afflusso di tale tipologia di richieste.

In relazione alla semplificazione degli adempimenti per la tutela della *privacy* nel settore bancario e finanziario, va da ultimo sottolineata anche in questa sede l'importanza delle recenti modifiche introdotte dal decreto legislativo n. 467/2001, soprattutto per ciò che attiene alla previsione di nuovi casi di esclusione del consenso anche per operazioni di comunicazione di dati personali strumentali all'esecuzione di obblighi contrattuali. Ciò dovrebbe comportare una definitiva risoluzione dell'annoso problema della mancata restituzione da parte di diversi clienti dei moduli che gli istituti di credito avevano inviato anche alla clientela acquisita prima dell'entrata in vigore della legge n. 675/1996, allo scopo di legittimare ordinarie attività connesse all'esecuzione di servizi bancari o comunque di prestazioni contrattuali, per le quali risulti indispensabile comunicare i dati ad altre banche, istituti finanziari o società che collaborano con i medesimi istituti.

I rilevanti riflessi delle recenti modifiche sui settori in esame, anche per quanto riguarda la modulistica distribuita dagli operatori, potranno essere meglio valutati anche sulla base della complessiva attività cui dovrà attendere il Garante nei prossimi mesi, con riferimento non solo ai nuovi presupposti equipollenti al consenso ed all'attuazione del principio del cd. bilanciamento di interessi, ma anche all'individuazione di accorgimenti specifici per i trattamenti di dati particolari e all'esercizio dei poteri di verifica preliminare di determinate utilizzazioni delle informazioni.

35 Perizie medico-legali

Nel corso del 2001, gli approfondimenti dell'Autorità sulla definizione di dato personale e la Raccomandazione sui dati valutativi dei dipendenti del Gruppo dei Garanti europei (v. *Relazione 2000*, p. 49), hanno contribuito ad un diverso atteggiamento delle compagnie di assicurazione, con riguardo alle istanze avanzate dall'interessato ai sensi dell'art. 13 l. n. 675/1996, volte a conoscere le informazioni a carattere personale contenute nei documenti redatti dal medico fiduciario delle società assicurative a seguito di un sinistro (cd. perizie medico-legali).

In considerazione di ciò, nel documento predisposto dal medico fiduciario delle diverse compagnie di assicurazioni, compaiono accanto ai dati personali dell'interessato, quali ad esempio i dati anagrafici o le lesioni riportate, anche valutazioni che sono frutto di un giudizio del professionista che ha visitato l'interessato o ha esaminato la relativa documentazione. La posizione espressa ha come finalità principale quella di riconoscere all'interessato il diritto di accedere anche a questo genere di dati personali che lo riguardano, benché contenuti anche all'interno di valutazioni espresse dal medico autore della perizia o dalla società di assicurazione (*Provv.* 3 maggio 2001, in *Bollettino* n. 20, p. 17).

La visita eseguita dal medico delle società ha fra i propri scopi anche quello di verificare l'effettivo nesso di causalità fra il sinistro e le conseguenze riportate, specie a fini risarcitori. Nel documento è a volte indicata anche la "strategia" che la società dovrebbe seguire per contrastare un eventuale intento fraudolento dell'interessato, evidenziandosi anche eventuali suggerimenti sulla condotta processuale da privilegiare, che quest'ultimo non ha il diritto di conoscere ai sensi della legge n. 675/1996, fatto salvo quanto previsto dalla legge 5 marzo 2001, n. 57 sull'accesso agli atti a conclusione dei procedimenti di valutazione, constatazione e liquidazione dei danni.

Questo quadro complessivo è supportato dalla *Raccomandazione sui dati valutativi dei dipendenti*, approvata il 22 marzo 2001 dal Gruppo dei Garanti europei, dalla quale emerge conferma che devono essere considerati dati personali anche quelli presenti in giudizi o valutazioni sintetizzate attraverso un punteggio o una classifica, ovvero espressi attraverso criteri valutativi.

Sembra in ogni caso consolidato, al contempo, l'orientamento fondato sull'art. 14, comma 1, lett. *e)*, della legge 675/1996 che consente ai titolari di trattamento di poter differire temporaneamente l'accesso ai dati contenuti nelle perizie, limitatamente al periodo in cui potrebbe derivare, negli stessi, un effettivo pregiudizio per lo svolgimento delle indagini difensive o per far valere o difendere un diritto in sede giudiziaria; l'Autorità si è nuovamente espressa sull'argomento chiarendo che è, tuttavia, necessario dimostrare l'effettiva esistenza del pregiudizio, con una valutazione da condurre caso per caso (*Provv.* 4 aprile 2001, in *Bollettino* n. 19, p. 15; *Provv.ti* 3 e 8 maggio 2001, in *Bollettino* n. 20, p. 13 e 17).

In alcune occasioni, è stata infatti riscontrata la sola deduzione da parte delle società di assicurazioni dell'esistenza di una possibile, futura controversia, senza che fosse prospettato alcun elemento o circostanza che permettesse di ravvisare un concreto pregiudizio al diritto di difesa. In tali casi, quindi, è stato riconosciuto il diritto dell'interessato di accedere a tutti i dati personali che lo riguardano contenuti nella perizia.

È infine opportuno segnalare che, modificando alcune disposizioni della legge n. 990/1969 sull'assicurazione obbligatoria della responsabilità civile derivante dalla circolazione dei veicoli a motore e dei natanti, il legislatore ha previsto l'introduzione di tempi certi per la consegna all'interessato di tutta la documentazione relativa al sinistro (art 12-*ter* della legge citata come modificato dall'art. 5, l. n. 57/2001), comprese le eventuali perizie redatte dal medico di fiducia della società di assicurazione.

36 Raccolte di dati in ambito assicurativo e banca dati Isvap

Come già accennato, oltre alle descritte questioni legate al tema dell'accesso alle perizie medico-legali, va segnalato, come tema rilevante per i riflessi nella sfera personale e privata di ogni cittadino, il problema dell'applicazione delle disposizioni sulla tutela dei dati personali nei confronti della banca dati dei sinistri relativi all'assicurazione obbligatoria per i veicoli a motore immatricolati in Italia, recentemente istituita presso l'Isvap per rendere più efficace la prevenzione ed il contrasto di comportamenti fraudolenti in tale settore (ai sensi dell'art. 2, commi 5-*quater* e 5-*quinquies*, l. 26 maggio 2000, n. 137, di conversione, con modificazioni, del d.l. 28 marzo 2000, n. 70, recante disposizioni urgenti per il contenimento delle spinte inflazionistiche).

In tale banca dati, come già evidenziato nella scorsa relazione annuale (v. *Relazione 2000*, p. 52), andrà infatti a confluire un'ingente mole di informazioni sui sinistri stradali per i quali pervenga denuncia o richiesta di risarcimento alle società assicurative. Queste ultime potranno avere accesso alla banca dati, come altri soggetti, per effettuare le necessarie verifiche volte a prevenire comportamenti illeciti, come truffe o frodi.

Nel corso di questi ultimi mesi, è stata avviata una positiva attività di collaborazione istituzionale con il predetto Istituto che è in procinto di adottare un provvedimento attuativo per la definizione delle procedure e delle modalità di funzionamento della predetta banca dati. In questa sede potranno essere quindi valutati alcuni delicati profili concernenti la raccolta, il trattamento e la circolazione delle informazioni a carattere personale, con l'indicazione di specifiche misure ed accorgimenti a garanzia degli interessati. In primo luogo, è in corso un attento esame della pertinenza e dell'essenzialità dei dati che dovranno essere registrati nella banca dati e dei tempi relativi alla loro conservazione. In secondo luogo, occorre delimitare puntualmente l'ambito dei soggetti pubblici (organi ed uffici giudiziari) e privati (compagnie di assicurazione) che potranno avervi accesso, con l'individuazione dei limiti e delle forme di consultazione e successiva utilizzazione delle informazioni, con la predisposizione di idonee misure di sicurezza e la previsione di agevoli modalità di esercizio dei diritti di accesso da parte delle persone interessate.

Continua poi l'attività di collaborazione con la competente associazione di categoria per lo studio e l'adozione di modelli semplificati per l'informativa ed il consenso, che tengano conto della particolarità e della complessità dei trattamenti di dati personali, anche sanitari, svolti in ambito assicurativo (dalle medesime compagnie di assicurazioni, dagli agenti o dalla variegata rete di intermediari assicurativi, dai periti, dai legali, dalle autofficine, ecc.). Come già accennato con riferimento alle banche, è evidente che tale modulistica potrà essere ora rivista alla luce delle rilevanti modifiche introdotte dal d.lg. n. 467/2001, soprattutto per ciò che attiene ai casi di esclusione del consenso per il trattamento di dati personali "comuni".

Minori, invece, sono state le novità previste per la raccolta e l'utilizzazione di dati relativi alla salute di clienti o terzi, proprie di alcune attività assicurative (in caso, ad esempio, di polizze infortuni o sanitarie oppure di procedimenti di risarcimento dei danni a persone fisiche). Per i trattamenti di tali dati sensibili, le compagnie continuano a far riferimento alle prescrizioni contenute nelle autorizzazioni generali che sono state recentemente rinnovate con alcune modifiche (cfr. le autorizzazioni nn. 2 e 5 del 2002, in allegato).

37 Centrali rischi

Anche quest'anno sono pervenuti numerosi ricorsi, reclami ed istanze riguardanti il trattamento di dati personali svolto da società che gestiscono sistemi di rilevazione dei rischi creditizi per finalità di tutela nell'erogazione dei finanziamenti da parte di istituti di credito e finanziari, confermando così il fenomeno, già rilevato negli anni scorsi, del progressivo aumento del contenzioso relativo alle attività delle cd. centrali rischi.

In queste banche dati, messe a disposizione di circuiti bancari o finanziari, sono registrate informazioni analitiche sui finanziamenti rilasciati a cittadini ed imprese, in modo da permettere agli operatori del settore di valutare la posizione complessiva ed il pregresso comportamento (il cd. merito creditizio) di coloro che richiedono un prestito o un mutuo.

Nelle centrali rischi possono essere riportate informazioni di tipo positivo e negativo con la segnalazione, ad esempio, sia del regolare svolgimento di un rapporto di finanziamento o della sua anticipata estinzione, sia della morosità nella restituzione dei ratei in scadenza, degli altri inadempimenti contrattuali e delle sofferenze.

La rilevazione preventiva del rischio creditizio è collegata ai sistemi di credito al consumo, e in particolare ai finanziamenti connessi all'acquisto di beni, servizi e prestazioni presso società, banche ed esercizi commerciali.

È evidente, quindi, l'impatto dei trattamenti di dati svolti nell'ambito dei predetti sistemi informativi nei riguardi della sfera privata di consumatori che, spesso, lamentano un ingiustificato inserimento o mantenimento del loro nominativo nelle banche dati delle centrali rischi o un'erronea indicazione di informazioni che li riguardano, con conseguente difficoltà ad accedere ad altre forme di finanziamento ed altri effetti negativi riflessi nella vita sociale e professionale.

Come è noto, in Italia esistono diverse centrali rischi gestite da soggetti privati e, in ambito pubblico, dalla Banca d'Italia. In quest'ultima sono censiti tutti i finanziamenti di importo minimo già pari al valore di L. 150.000.000 e i crediti in sofferenza, che devono essere segnalati a prescindere dall'importo (sono escluse le sofferenze fino a L. 500.000).

Nel corso del 2001, pur essendo pervenute diverse segnalazioni, non sono stati molti i casi affrontati in relazione a tale centrale rischi, in considerazione della specifica disciplina di settore (in base alle disposizioni del t.u. bancario, è previsto l'obbligo, per gli intermediari, della tempestiva segnalazione dei finanziamenti oltre la soglia prevista e delle posizioni di indebitamento) e del particolare assetto previsto dalla legge n. 675/1996 per i soggetti pubblici il quale esclude, come confermato da pronunce di questa Autorità, la necessità di acquisire il consenso degli interessati per il trattamento di dati (v. anche *Provv.* 10 aprile 2001, in *Bollettino* n. 19, p. 26) e prevede una preclusione a proposito della centrale rischi di Banca d'Italia all'esercizio dei diritti di accesso ai dati da parte degli interessati (v. *Relazione 1999*, p. 51).

Al riguardo, si è ribadito in un recente provvedimento che la segnalazione della sofferenza di un cliente deve essere trasmessa alla centrale rischi a prescindere dall'ammontare del debito e che, nel caso specifico, essendo in corso un contenzioso dinanzi all'autorità giudiziaria ordinaria, la segnalazione era stata effettuata in conformità alla specifica normativa di riferimento che obbliga gli istituti di credito alla comunicazione dei dati dei soggetti con i quali è in atto un procedimento giudiziario relativo a finanziamenti ottenuti (*Provv.* 17 ottobre 2001, in *Bollettino* n. 23, p. 29).

Va poi ricordato che, accanto alla centrale rischi gestita dalla Banca d'Italia, è stato istituito di recente un archivio per la rilevazione dei rischi di importo contenuto, ovvero inferiore a L. 150.000.000 e superiore a L. 60.000.000, con esclusione dei crediti in sofferenza. Come già evidenziato lo scorso anno (v.

37

Relazione 2000, par. 41, p. 52), la gestione di questo sistema di rilevazione del rischio creditizio, pur essendo emanazione del sistema pubblico, è stata affidata ad una società privata, la Società interbancaria per l'automazione "S.I.A. S.p.a.", ed è soggetta solo in parte alla disciplina prevista per la Banca d'Italia (le banche e gli intermediari finanziari hanno, infatti, l'obbligo di comunicare i dati relativi alle esposizioni creditizie, non dovendo richiedere il consenso dei clienti interessati, ma questi ultimi possono esercitare pienamente i diritti previsti dalla legge n. 675/1996).

Vi sono poi diversi sistemi di rilevazione del rischio creditizio gestiti da società o enti privati, cui banche ed istituti finanziari aderiscono volontariamente fornendo, a loro volta, informazioni sui rapporti di finanziamento intrattenuti con la clientela. La maggior parte delle contestazioni riguarda tali sistemi, nei cui confronti i cittadini fanno, ormai, uso frequente degli strumenti di difesa indicati dalla legge sulla *privacy*, avanzando spesso richieste di accesso, rettifica o cancellazione dei dati.

Vari sono i profili messi in luce dalle numerose istanze e segnalazioni pervenute: dalle formule di informativa e consenso inserite nella modulistica utilizzata per la richiesta di finanziamento alla tempestività dei riscontri forniti alle richieste degli interessati, alle modalità di registrazione dei dati, ai tempi della loro conservazione.

Soprattutto in seguito a ricorsi, sono stati adottati diversi provvedimenti nei quali è stato ribadito l'obbligo per le centrali rischi private di dare immediato riscontro alle istanze formulate dagli interessati ai sensi dell'art. 13 della legge n. 675/1996 (*Provv.* 29 marzo 2001) e di rispettare i principi di correttezza nel trattamento dei dati dei clienti, soprattutto riguardo alla tempestività nella rettifica e nell'aggiornamento dei dati comunicati. In un caso particolare, poiché la centrale rischi aveva provveduto a rettificare i dati inesatti solo a seguito dell'intervento del Garante (essendo rimasta inevasa la richiesta di accesso ai dati avanzata dall'interessato direttamente alla società), l'Autorità, pur ritenendo di non dare ulteriore corso al procedimento, ha tuttavia disposto a carico della società la rifusione delle spese e dei diritti del procedimento a causa della tardiva correzione di dati (*Provv.* 28 novembre 2001).

In un altro provvedimento, è stato evidenziato che il periodo di conservazione dei dati nella centrale rischi stabilito da alcune società (cinque anni dalla data di estinzione del contratto di finanziamento) può risultare, in alcuni casi, eccedente rispetto alle finalità per le quali i dati sono stati raccolti e successivamente trattati, in quanto, ad esempio, il finanziamento è stato estinto anticipatamente senza alcuna pendenza o debito residuo.

La prolungata utilizzazione dei dati anche dopo l'estinzione del contratto è da ritenersi in questi casi eccessiva anche in considerazione del fatto che i dati sono inseriti in banche dati consultabili da terzi per finalità di erogazione di altri crediti e che tutto ciò può comportare un grave pregiudizio per l'interessato e le sue attività economico-professionali (*Provv.* 27 dicembre 2001, in *Bollettino* n. 23, p. 77).

Il Garante ha altresì avuto modo di precisare, in un recente provvedimento (*Provv.* 7 febbraio 2002, in *Bollettino* n. 25, p. 14), che i dati relativi ai protesti cambiari contenuti in banche dati private devono essere trattati conformemente alle nuove disposizioni dettate dalla legge 18 agosto 2000, n. 235 e dal regolamento approvato con d.m. 9 agosto 2000, n. 316 in materia di cancellazione dal registro informatico dei protesti. La nuova normativa, infatti, incide sulla disciplina relativa alla conservazione nel tempo dei dati, prevedendo che nei casi accertati di pagamento successivo al protesto o di illegittima o erronea levata del protesto stesso, nonché nella ipotesi di riabilitazione e pagamento non tempestivo, si debba procedere alla cancellazione dal registro dei protesti il quale deve essere a sua volta tenuto osservando modalità idonee ad assicurare "completezza, organicità e tempestività dell'informazione su tutto il territorio nazionale".

Le finalità della nuova disciplina non possono essere quindi eluse dai soggetti che gestiscono "banche dati o archivi paralleli di analogo contenuto, nei quali siano riportate informazioni anche esatte, ma risalenti nel tempo e di cui, in rapporto alle finalità perseguite, non sia giustificato l'ulteriore trattamento, anche in caso di eventuale prestazione del consenso da parte dell'interessato (art. 9, comma 1, lett. *e*), legge n. 675/96)". Nel caso che ha provocato la pronuncia del Garante la centrale rischi aveva invece conservato i dati relativi ad un protesto elevato nel 1997, nonostante l'avvenuta cancellazione effettuata dalla camera di commercio a seguito dell'intervenuta riabilitazione.

I problemi in esame hanno assunto proporzioni a tal punto rilevanti, che si è ritenuto necessario avviare

un'indagine approfondita sul tema delle centrali rischi private, in modo da individuare criteri e procedure omogenee tra gli operatori del settore in relazione al trattamento dei dati relativi ai rapporti di finanziamento. A tal fine, l'Ufficio ha tenuto recentemente anche alcuni incontri con esponenti di centrali rischi private e di associazioni di categoria in ambito finanziario così da poter valutare meglio le possibili indicazioni da fornire per la corretta attuazione delle norme sulla tutela dei dati personali da parte degli operatori del settore e per l'eliminazione di larga parte del contenzioso esistente con gli interessati.

Va, infine, evidenziata l'importanza che le modifiche apportate dal d.lg. n. 467/2001 avranno anche per le attività delle centrali rischi, in considerazione dei nuovi casi di esclusione del consenso, dei maggiori poteri riconosciuti all'Autorità e soprattutto riguardo alla promozione (entro il 30 giugno 2002) di un codice deontologico relativo al trattamento di dati personali effettuato nell'ambito di sistemi informativi gestiti dalle centrali rischi private, ai fini di concessione di crediti al consumo o relativi alla valutazione dell'affidabilità e della puntualità nei pagamenti da parte degli interessati (art. 20, comma 2, lett. *e*), d. lg. n. 467/2001).

38 Anagrafe degli assegni bancari e postali

Nel novembre 2001 è entrato in vigore il regolamento sul funzionamento dell'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (adottato dal Ministro della giustizia con decreto 7 novembre 2001, n. 458), istituito presso la Banca d'Italia nel quadro degli interventi di depenalizzazione dei reati minori previsti dal d.lg. n. 507/1999 (che ha modificato diverse disposizioni della disciplina sanzionatoria in materia di assegni bancari, *ex* l. 15 dicembre 1990, n. 386).

Tale archivio, che risponde alla finalità di interesse generale di assicurare il regolare funzionamento del sistema dei pagamenti, viene alimentato da soggetti pubblici (autorità giudiziaria e prefetti) e privati (banche, uffici postali, società emittenti carte di credito) tenuti a trasmettere i provvedimenti adottati o le segnalazioni rilevanti ai fini dell'archivio (riguardanti, ad esempio, sanzioni amministrative o penali irrogate, revoche dell'autorizzazione ad emettere assegni, moduli di assegni sottratti, smarriti, non restituiti o bloccati, carte di pagamento revocate, smarrite o sottratte); questi stessi soggetti sono abilitati alla consultazione della banca dati così costituita ed interessati all'individuazione di situazioni anomale od irregolari, anche rispetto alla propria clientela.

Come ricordato nella relazione dello scorso anno (cfr. *Relazione 2000*, p. 53), nel predetto regolamento sono state recepite diverse osservazioni formulate dall'Autorità, consultata preventivamente nell'ambito dei rapporti di proficua collaborazione istituzionale con la Banca d'Italia ed il Ministero della giustizia, con particolare riguardo alla durata delle iscrizioni dei dati in archivio ed alle modalità di esercizio dei diritti di accesso ai dati da parte delle persone interessate.

Tale attività di collaborazione è continuata, più recentemente, con la Banca d'Italia in relazione alla predisposizione da parte di quest'ultima del distinto regolamento per disciplinare le modalità e le procedure relative alle attività previste dal richiamato regolamento ministeriale con particolare riguardo alla trasmissione, rettifica ed aggiornamento dei dati da inserire nell'archivio (nonché alla determinazione dei criteri generali per la quantificazione dei costi per l'accesso e la consultazione dell'archivio da parte dei soggetti privati abilitati).

Anche nel regolamento emanato dal Governatore della Banca d'Italia il 29 gennaio 2002, sono state recepite varie indicazioni fornite dall'Autorità, soprattutto per ciò che attiene all'eliminazione, alle scadenze prestabilite dal citato regolamento ministeriale (art. 10), dei dati sia identificativi personali, sia non nominativi (ma che potrebbero permettere di risalire all'identità delle persone interessate, come, ad esempio, le coordinate di un assegno o di un modulo di assegni) iscritti nell'archivio.

Attività giornalistiche e mezzi di informazione

39 Attività giornalistica e rispetto dei principi della legge n. 675/1996

La definizione dei rapporti tra tutela della riservatezza e diritto di cronaca costituisce un tema particolarmente delicato e complesso, in relazione al quale è possibile riscontrare una sempre maggiore attenzione da parte dei cittadini ed una richiesta sempre più frequente di tutela, confermata dal numero crescente di istanze pervenute all'Autorità.

Quest'ultima è chiamata sempre più spesso ad esaminare i casi alla luce della specifica disciplina dettata in materia dalla legge n. 675/1996 (artt. 12, 20 e 25) e dal codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*Provv.* 29 luglio 1998, in *G.U.* n. 179 del 3 agosto 1998), con l'obiettivo di garantire, di volta in volta, un giusto bilanciamento tra il diritto-dovere dei mezzi di informazione di rendere edotta la collettività su fatti di rilievo pubblico e il diritto delle persone coinvolte in fatti di cronaca di non subire dannose ed ingiustificate intrusioni nella propria vita privata.

La legge n. 675/1996 e il codice deontologico forniscono alcuni parametri attraverso cui operare detto bilanciamento: primo fra tutti quello di trattare i dati personali nel rispetto del principio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. A tale principio generale si affiancano specifiche garanzie poste a tutela di soggetti "deboli" (come i minori) o facenti riferimento a trattamenti idonei a rivelare informazioni particolarmente delicate (si pensi ai dati sulla salute).

Il principio e le garanzie ora richiamati – estesi dall'art. 25, comma 4-*bis*, l. 675/1996 ai trattamenti temporanei finalizzati esclusivamente alla pubblicazione occasionale di articoli, saggi e altre forme di manifestazione del pensiero (*Provv.* 28 settembre 2001, in *Bollettino* n. 22, p. 13) – hanno trovato applicazione e specificazione in numerosi casi esaminati dall'Autorità nel corso del 2001.

Esercizio dei diritti ex art. 13 nei confronti di giornalisti ed editori

Confermando un orientamento già espresso in precedenza, l'Autorità si è trovata a ricordare, nel corso del 2001, che i diritti di cui all'art. 13 della legge n. 675/1996, riconosciuti a ciascun interessato in relazione al trattamento dei dati personali che lo riguardano, possono essere esercitati anche nei confronti dei giornalisti e degli editori. Alla luce di ciò, il Garante ha, in parte, accolto due ricorsi con i quali gli interessati lamentavano di non aver ottenuto riscontro ad una richiesta di accesso a dati personali formulata nei confronti di un quotidiano locale. L'unico limite alla comunicazione all'interessato di tali informazioni – ha ricordato il Garante – poteva eventualmente fondarsi nel caso di specie su quanto espressamente previsto dall'ordinamento a tutela del segreto professionale sulla fonte della notizia (*Provv.* 3 settembre 2001, in *Bollettino* n. 22, p. 9).

Pubblicazione a mezzo stampa dei dati relativi ai redditi dichiarati

La liceità della pubblicazione, da parte degli organi di informazione, dei dati relativi al reddito delle persone fisiche è stata riconosciuta sulla base del regime di pubblicità di tali informazioni, espressamente previsto dalla disciplina vigente (cfr. art. 69 del d.P.R. n. 600/1973 come modificato, in particolare, dall'art. 19 della legge n. 413/1991). Pertanto, la diffusione di dati estratti lecitamente da elenchi accessibili a chiunque è da ritenersi lecita, anche senza il consenso degli interessati e senza che sia necessario, per la testata che li riproduce, dimostrare la sussistenza del requisito dell'essenzialità dell'informazione (*Provv.* 17 gennaio 2001, in *Bollettino* n.16, p. 5).

Riprese televisive delle sedute consiliari

L'Autorità si è pronunciata altresì sul tema della pubblicità di atti e sedute consiliari, del quale si è già riferito al paragrafo 7.

39

Pubblicazione delle targhe in divieto di sosta

Sulla base di alcune segnalazioni, l'Autorità ha avviato alcuni accertamenti in merito alla prassi, adottata da un quotidiano, di pubblicare – all'interno di una sezione dedicata alle informazioni sul traffico cittadino e sul sistema dei trasporti pubblici – i numeri delle targhe ed altre informazioni relative alle automobili parcheggiate irregolarmente. Ad esito di tali verifiche, dirette essenzialmente a valutare se tale prassi comportasse ingiustificate ingerenze nella sfera privata degli interessati – che agevolmente potevano essere identificati – l'Autorità ha rilevato che la finalità di informare il pubblico sulle possibili cause di disfunzione del servizio di trasporto pubblico poteva essere ugualmente perseguita limitandosi ad indicare, per esempio, il tipo di autovetture che ostacolavano il traffico (nota dell'11 marzo 2002, n. 2958/17051).

40 Tutela dei minori

Uno dei settori nel quale è fortemente sentita l'esigenza di limitare indebite intrusioni nella vita privata è quello concernente i minori: questi ultimi risultano, infatti, particolarmente esposti ai rischi legati alla diffusione non controllata dei dati personali che li riguardano. Diffusione che, in molti casi, può segnare profondamente il loro sviluppo, provocando danni ben più ingenti di quelli che possono essere prodotti in riferimento ad adulti.

Molteplici sono state le domande di tutela rivolte al Garante con riferimento a diversi trattamenti concernenti tali soggetti.

Al riguardo, come è noto, il codice di deontologia sopra richiamato detta una speciale disciplina. In particolare, è utile ricordare che il relativo art. 7 – nel ritenere primario il diritto del minore alla riservatezza rispetto al diritto di critica e di cronaca – vieta ai giornalisti di pubblicare i nomi dei minori coinvolti in fatti di cronaca, ovvero di diffondere altri particolari che ne consentano l'identificazione. Ciò, facendo espresso richiamo anche ai principi dettati dalla Carta di Treviso.

In varie occasioni, pertanto, l'Autorità ha ritenuto non conformi alla normativa ora richiamata le condotte di quotidiani ed emittenti televisive che riportano notizie relative a delicate vicende familiari, pubblicando fotografie o dati identificativi relativi a minori. In queste circostanze il Garante ha sottolineato la necessità di evitare spettacolarizzazioni eccessive o tali, comunque, da ingenerare turbamenti e pregiudicare il normale sviluppo dei minori coinvolti in tali accadimenti (*Provv.* 15 novembre 2001, in *Bollettino* n. 23, p. 9). Ciò, a maggior ragione, nei casi in cui le notizie riportate dai mezzi di informazione riguardino presunte molestie sessuali commesse ai danni di tali soggetti: in tali ipotesi, invero, il giornalista è chiamato ad individuare la misura più idonea a salvaguardare gli interessi del minore, eventualmente limitando la diffusione di informazioni che lo riguardano anche nel caso in cui i genitori abbiano manifestato il loro consenso a tale forma di pubblicità (*Provv.* 15 novembre 2001, in *Bollettino* n. 23, p. 11 e 13).

Sviluppando alcuni principi già presenti nella richiamata Carta di Treviso, l'Autorità ha contribuito altresì ad ampliare gli ambiti di tutela di tali soggetti, assicurando l'anonimato previsto dal citato art. 7 del codice deontologico anche con riguardo alla pubblicazione di notizie contenenti informazioni relative a determinate situazioni familiari quali, ad esempio, l'affidamento e l'adozione. Tale linea interpretativa è suggerita anche dalla considerazione che, al momento della divulgazione dei dati, il minore potrebbe non essere ancora stato informato della sua condizione dai genitori adottivi, ai quali è affidata in via esclusiva la scelta su modi e termini per procedervi, secondo quanto previsto da un recente intervento di modifica della legge sull'adozione (l. n. 184/1983 e l. n. 149/2001). Rilevano anche, al riguardo, ragioni di opportunità nel senso di escludere che la condizione di figlio adottivo venga resa nota nell'ambito dei luoghi e delle persone da lui frequentate (*Comunicato stampa* 28 novembre 2001, in *Bollettino* n. 23, p. 202).

In altri casi, si è richiamata l'attenzione dei mezzi di informazione sulla necessità di operare un vaglio particolarmente rigoroso del criterio dell'essenzialità riguardo alla diffusione di alcune notizie e fotografie relative a personaggi pubblici e ai loro figli. Il Garante – oltre a ribadire la natura di dato personale delle informazioni contenute in fotografie (cfr. anche *Provv.* 4 gennaio 2001, in *Bollettino* n. 16, p. 23) – ha ritenuto che la più attenuata tutela accordata dalla legge (art. 25) e dal codice di deontologia (art. 6) alla riservatezza dei personaggi noti – in considerazione del possibile rilievo pubblico di taluni aspetti della loro vita privata – non deve in alcun modo comportare un'indebita interferenza nella sfera privata dei minori ed un pregiudizio al loro armonioso sviluppo. Ciò, anche quando i minori stessi assumono – seppur indirettamente – una certa notorietà (si veda, fra gli altri, *Provv.* 28 maggio 2001, in *Bollettino* n. 20, p. 7).

A proposito del delicato tema della diffusione dei dati di minori coinvolti in procedimenti penali – pro-

40

blematica emersa in relazione all'avvenuta pubblicazione, da parte di un quotidiano, di ampi stralci di una perizia psichiatrica disposta dal giudice nei riguardi un giovane imputato di un delitto – l'Autorità, oltre a ricordare gli specifici divieti posti dall'art. 13 del d.P.R. n. 448/1988 (*Approvazione delle disposizioni sul processo penale a carico di imputati minorenni*), ha sottolineato anche che la speciale tutela riservata ai minori trova applicazione, a maggior ragione, quando si pubblicano dati relativi allo stato di salute dei medesimi (art. 7 e 10 del codice deontologico citato: cfr. *Provv.* 15 novembre 2001, in *Bollettino* n. 23, p. 15).

Le norme a tutela dei minori sono state richiamate anche con riferimento ad un complesso e delicato episodio di cronaca in cui ha trovato la morte un bimbo di tre anni, e che ha visto coinvolti i suoi familiari, ivi compreso il fratellino di sette anni. A tale vicenda e alla famiglia gli organi di informazione hanno dedicato particolare attenzione. Il Garante, ha ritenuto pertanto necessario un suo intervento, invitando gli organi di stampa ad astenersi dal divulgare ulteriori dettagli e informazioni relative al fratellino della vittima in ragione della primaria esigenza di tutelarne la personalità (*Provv.* 10 aprile 2002).

41 Cronache giudiziarie

Un numero rilevante di segnalazioni pervenute al Garante si riferisce a presunte violazioni della normativa in materia di protezione dei dati con riguardo ai trattamenti effettuati nell'ambito delle cosiddette "cronache giudiziarie". I problemi emersi attengono a diversi profili della vigente normativa in materia di protezione dei dati personali.

In primo luogo, occorre evidenziare l'aspetto relativo all'acquisizione delle informazioni da parte degli organi di informazione e al fenomeno cosiddetto delle "fughe di notizie". In relazione a tale profilo, va ricordato che assurgono a parametro di valutazione di liceità del trattamento, oltre ai principi dettati dalla legge n. 675/1996, anche le specifiche norme di carattere sostanziale e procedurale: si pensi alla disciplina sul segreto sugli atti d'ufficio e sull'attività di indagine e al diverso regime riservato agli atti processuali, alle udienze e ai provvedimenti del giudice, generalmente improntato al principio di pubblicità.

L'Autorità, nell'esaminare alcuni casi di diffusione, da parte degli organi di stampa, dei dati relativi a persone vittime di reati (furti, aggressioni, rapine), ha ribadito il necessario rispetto del principio di essenzialità dell'informazione riguardo a fatti di interesse pubblico (artt. 12, 20 e 25 della legge n. 675/1996 e artt. 5 e 6 codice deontologico), nonché dei principi di liceità e correttezza del trattamento dei dati (art. 9, l. n. 675/1996). D'altra parte il Garante ha richiamato anche il divieto, per gli organi di polizia e per gli uffici giudiziari, di comunicare o diffondere i dati acquisiti nel corso dello svolgimento delle proprie funzioni istituzionali, fuori dei casi consentiti.

In altra occasione l'Autorità ha ricordato come il segreto professionale sulla fonte della notizia non faccia venire meno il dovere del giornalista di acquisire lecitamente le trascrizioni di intercettazioni telefoniche disposte dall'autorità giudiziaria. Inoltre ha precisato che l'eventuale pubblicazione del loro contenuto deve avvenire, non solo nel rispetto delle norme vigenti, ma anche in modo da non ledere i diritti degli interessati, soprattutto se le informazioni acquisite riguardano la vita privata dei medesimi (*Provv.* 11 aprile 2002).

Altre volte il Garante non ha riscontrato una specifica violazione delle norme in materia di protezione dei dati personali da parte degli organi di informazione, in quanto questi si erano limitati a riportare dati resi noti in occasione di pubbliche udienze o desunti da documenti (sentenze) legittimamente conoscibili e acquisibili anche da parte di persone diverse dalle parti e dai loro difensori (*Provv.ti* 30 ottobre e 21 novembre 2001, in *Bollettino* n. 23, p. 22 e 108; si vedano, inoltre, con specifico riferimento alla divulgazione dei dati concernenti persone rinviate a giudizio, le decisioni del 25 ottobre 2001 e del 19 dicembre 2001, in *Bollettino* n. 23, p. 19 e 17).

Quanto ora evidenziato in tema di diffusione di informazioni acquisite da fonti accessibili al pubblico ha trovato specifica attuazione anche con riferimento a fatti accaduti e provvedimenti adottati nell'ambito di procedimenti di diversa natura (non giurisdizionali): ci si riferisce, in particolare, ad un caso in cui il Garante ha ritenuto lecita la pubblicazione del provvedimento di sospensione di un avvocato, all'interno della rivista dell'ordine di appartenenza di quest'ultimo, in considerazione del regime di pubblicità degli albi professionali e alla conoscibilità degli atti connessi (*Provv.* 29 marzo 2001, in *Bollettino* n. 18, p. 20). L'Autorità ha assunto una posizione analoga in merito alla pubblicazione di un articolo che riferiva della transazione di un comune con un cittadino, relativamente al versamento di una penale contrattuale. La vicenda, oggetto di interrogazione parlamentare e segnalata alla Corte dei conti, era infatti documentata da atti e documenti accessibili al pubblico e quindi lecitamente divulgabili dalla stampa (*Provv.* 22 gennaio 2001, in *Bollettino* n. 16, p. 8).

Sempre nell'ambito degli interventi realizzati in materia di cronache giudiziarie, il Garante è stato investito della richiesta di fornire chiarimenti in ordine all'applicazione e all'interpretazione del già richiamato limite dell'essenzialità dell'informazione con riferimento a fatti di interesse pubblico. Alcune segnalazioni hanno posto

41

il problema – in fase di approfondimento – relativo alla necessità o meno per il giornalista, di adottare, di volta in volta, cautele differenziate a garanzia della riservatezza dei vari soggetti coinvolti nei fatti riportati, tenendo conto delle diverse circostanze in cui tali fatti avvengono (ad esempio, prevedendo modalità di trattamento dei dati differenziate a seconda del ruolo svolto dalla persona implicata nella vicenda giudiziaria riportata – vittima o autore del reato, testimone o collaboratore, ecc. – ovvero, a seconda del tipo di reato, della fase processuale, del tipo di procedimento in corso, del genere di pronuncia emessa dall'autorità giudiziaria, e così via).

Un primo caso sottoposto con formale ricorso è stato risolto senza una valutazione nel merito, avendo l'editore del quotidiano aderito spontaneamente alla richiesta di cancellare alcuni dati personali di una ricorrente che aveva lamentato – rivolgendosi poi al giudice per il merito della questione – l'indicazione di alcuni elementi idonei ad identificarla nell'ambito di un articolo che aveva reso nota un'aggressione perpetrata nei suoi confronti (*Provv.* 3 maggio 2001, in *Bollettino* n. 20, p. 5).

42 Dignità della persona e dati idonei a rivelare lo stato di salute

Pur essendo prevista la possibilità che anche i dati idonei a rivelare lo stato di salute vengano trattati a fini giornalistici, prescindendo dal consenso dell'interessato, il codice di deontologia ha previsto specifiche garanzie affinché il trattamento di tali delicatissime informazioni avvenga nel rispetto della dignità e del diritto alla riservatezza dell'interessato (artt. 5 e 10).

Ciò è avvenuto in relazione ad un'inchiesta giornalistica sull'anoressia, pubblicata su un settimanale, nella quale l'Autorità ha riscontrato che il trattamento è avvenuto in base ad una preventiva e adeguata informazione alle degenti e nel rispetto della loro dignità, evitando, comunque, che fossero in alcun modo identificabili persone di minore età (*Provv.* 20 giugno 2001, in *Bollettino* n. 21, p. 4).

Alla luce delle norme da ultimo citate, invece, è stata ritenuta illecita la condotta tenuta da taluni organi di informazione, attraverso la quale è stata resa identificabile una ragazza sospettata di aver contratto la variante umana della malattia di Creutzfeldt-Jakob (encefalopatia spongiforme bovina – BSE) in ragione della dovizia di particolari forniti da giornali e *mass-media*, contrariamente al principio di essenzialità dell'informazione.

L'indubbio interesse generale della vicenda (la presenza della malattia nel nostro Paese), non rendeva necessario né il riferimento alla specifica persona, né la pubblicazione di informazioni dettagliate relative ai congiunti dell'interessata e ad altre persone estranee ai fatti. Per tali ragioni, l'Autorità ha ravvisato in tale condotta una grave violazione della dignità delle persona e degli altri principi dettati dal codice deontologico dei giornalisti (*Provv.* 7 febbraio 2002, in *Bollettino* n. 25, p. 8).

I medesimi principi relativi all'essenzialità dell'informazione ed al rispetto della dignità della persona sono stati richiamati in un provvedimento relativo all'avvenuta pubblicazione, su un quotidiano, di una condanna per ingiuria nei confronti di un uomo. In particolare, il giornale aveva riportato il nome della donna vittima dell'ingiuria e il contenuto della frase ingiuriosa (nella quale si faceva riferimento ad una grave malattia della quale sarebbe stata affetta la donna e ad un presunto contagio dell'uomo). Il contenuto della frase avrebbe dovuto indurre l'autore dell'articolo e il direttore responsabile del quotidiano ad operare un vaglio rigoroso dei limiti posti al diritto di cronaca, in ragione della necessità di salvaguardare la dignità della donna (*Provv.* 14 febbraio 2002, in *Bollettino* n. 25, p. 6).

Analoghe cautele sono state indicate dal Garante anche in relazione ad una vicenda che ha riguardato un docente universitario con riferimento ad alcuni incontri di carattere sessuale avuti con talune studentesse. Gli organi di informazione, anche in questo caso, hanno dato ampio risalto a tali accadimenti, giungendo a pubblicare, insieme ad altre informazioni, anche alcuni fotogrammi delle videoregistrazioni dei predetti incontri.

Fermo restando il rilievo pubblico assunto dalla vicenda – connesso, peraltro, al fatto che sull'accaduto sono state avviate diverse indagini da parte dell'autorità giudiziaria – l'Autorità ha segnalato agli organi di informazione che il rispetto della riservatezza e della dignità delle studentesse potenzialmente identificabili, e i profili controversi della vicenda, avrebbero dovuto indurre a non pubblicare le foto in questione. L'Autorità ha quindi sottolineato, anche in questo caso, la necessità che il trattamento dei dati personali a fini giornalistici avvenga nei limiti dell'essenzialità dell'informazione e, soprattutto, nel rigoroso rispetto della dignità e del decoro delle persone (*Provv.* 19 febbraio 2002, in *Bollettino* n. 25, p. 3).

Sorveglianza e sistemi biometrici

43 Videosorveglianza

Il tema della videosorveglianza è da annoverare tra i temi più significativi della recente attività del Garante: una conferma viene anche dalle risultanze delle attività, specie di tipo ispettivo, realizzate nel corso del 2001, che hanno confermato l'ampia diffusione del fenomeno e una costante crescita di attenzione al problema da parte di moltissimi cittadini.

Dal punto di vista del diritto positivo, il persistere della carenza di una specifica normativa in materia di utilizzo dei sistemi di videosorveglianza ha trovato un efficace elemento di contrasto nella messa a punto, prima, e nella diffusione poi, di un cd. decalogo, attraverso il quale il Garante ha enucleato dalla disciplina nazionale e comunitaria in materia di trattamento dei dati personali talune regole di fondo la cui osservanza consente di effettuare lecitamente il trattamento di immagini e suoni, nei casi in cui le apparecchiature che li rilevano permettano di identificare, in modo diretto o indiretto, un determinato soggetto.

Alla luce di tali indicazioni, è proseguita anche nel corso del 2001 la prassi di fattiva collaborazione tra l'Autorità e le amministrazioni pubbliche, specie locali, in particolare attraverso la tecnica dell'interpello preventivo con riferimento a programmate iniziative di controllo del territorio da realizzare attraverso l'impiego di dispositivi elettronici.

Peraltro, in un caso un cittadino ha promosso un ricorso concernente l'accesso a dati personali che lo riguardano dalla stessa trattati da una università statale, con specifico riferimento ad immagini riprese e temporaneamente registrate da una telecamera posizionata all'ingresso di un'aula collegata ad un sistema di allarme audio che si attiva al passaggio di un soggetto sensibile alla rilevazione. Con dichiarazione di non luogo a provvedere il Garante – nel ribadire che i dati raccolti mediante strumenti di videosorveglianza sono di carattere personale ai sensi dell'art. 1, comma 2, lettera *c)*, della legge n. 675/1996, sicché nei confronti del relativo titolare si può proporre un'istanza ai sensi dell'art. 13 della medesima legge – ha rilevato che l'università ha dichiarato di non conservare dati dell'interessato, stante l'asserita, rapida cancellazione delle immagini quotidianamente eseguite dall'impianto, e che la condotta posta in essere non contrasterebbe, secondo l'ente, con le prescrizioni della legge n. 675/1996 dal punto di vista della logica e delle modalità del trattamento, non essendosi indicato nella notificazione il trattamento di dati mediante impianti di videosorveglianza, ma essendosi menzionate la "*raccolta di dati mediante impianti di videoregistrazione*" e "*l'impiego di supporti audiovisivi*".

L'Autorità ha però avviato un autonomo procedimento in relazione a tali circostanze e agli aspetti relativi agli obblighi di informativa e agli incaricati del trattamento. (*Provv.* 19 dicembre 2001, in *Bollettino* n. 23, p. 40).

Da ultimo l'Autorità ha evidenziato, in risposta ad un esposto presentato da un'associazione per la tutela dei diritti dei consumatori, che dagli accertamenti effettuati in relazione alla presenza e all'utilizzo di impianti di videosorveglianza sul litorale di Ostia, non sono emerse specifiche violazioni dei principi in materia di trattamento di dati personali (*Provv.* 14 giugno 2001, *Bollettino* n. 21, p. 43).

Nonostante la presenza diffusa di telecamere riprendenti alcuni tratti di spiaggia installate sia da privati, a fini promozionali e pubblicitari o di informazione sulle condizioni meteorologiche, sull'affollamento delle spiagge o sulla disponibilità di impianti, sia dall'autorità regionale, per controllare il fenomeno dell'erosione delle spiagge, gli accertamenti svolti e le informazioni raccolte presso i gestori degli stabilimenti hanno consentito di stabilire che, in conformità al già citato decalogo redatto dal Garante, le stesse non consentivano l'individuazione dei soggetti ripresi: gli impianti sui quali sono stati condotti gli accertamenti risultavano invero privi della possibilità di utilizzare la funzione *zoom*, non consentivano il brandeggio ed erano in alcuni casi a bassa risoluzione o dislocate a lunga distanza dalla zona ripresa (20-25 mt.); analoga verifica, sempre con esito positivo, è stata effettuata sui siti *web* che riproducono le immagini in diretta o sulla base di periodici aggiornamenti.

A fronte di ciò, l'Autorità si è però riservata di disporre ulteriori accertamenti in presenza di circostanziate segnalazioni, e nell'ottica di piena collaborazione e di stimolo sopra menzionata, ha inviato copia del provvedimento anche alle autorità amministrative competenti in materia di occupazione di zone demaniali marittime, affinché valutassero la possibilità di indicare – nell'ambito del disciplinare di concessione – l'obbligo del gestore dello stabilimento di rispettare i vigenti principi in materia di trattamento di dati personali, anche per quanto riguarda l'installazione di telecamere.

44 Rilevazioni biometriche

Il tema delle tecniche biometriche ha occupato anch'esso un posto prioritario nell'agenda di lavoro del Garante anche per la continua evoluzione tecnologica che caratterizza tale problematica.

Come noto, l'analisi delle caratteristiche biometriche (geometria del volto, della mano, dell'iride, etc.), consente di porre a confronto le informazioni rilevate con quelle preventivamente memorizzate e viene di recente indicata come asserito fattore risolutivo di problemi di sicurezza, non sempre, peraltro, in termini rispettosi del principio di proporzionalità rispetto alle finalità perseguite. Al riguardo, l'Autorità, dopo accurate indagini è intervenuta disponendo la disattivazione dei sistemi di rilevazione delle impronte biometriche in precedenza installati – senza informativa – presso alcuni istituti bancari oggetto di segnalazioni (*Provv.* 28 settembre 2001, in *Bollettino* n. 22, p. 82). Nel provvedimento si è escluso che l'utilizzazione dei sistemi di rilevazione cifrata delle impronte digitali possa farsi in forma generalizzata, dovendo viceversa riferirsi a situazioni di concreto rischio riconducibili a circostanze obiettive, rimesse alla valutazione del singolo istituto bancario: quest'ultimo deve quindi procedere con particolare cautela, tenendo conto anche di precedenti eventi e di concordanti valutazioni da parte degli organi locali competenti in materia di tutela dell'ordine e della sicurezza pubblica, ai quali occorre comunque dare comunicazione dei sistemi installati.

Il divieto di utilizzo generalizzato ed indiscriminato di tali sistemi non è invece consentito per una pluralità di ragioni: da un lato in quanto si pone in contrasto con il principio di proporzionalità tra strumenti impiegati e finalità perseguite, dovendosi ricorrere a mezzi che comportano minori problemi per la tutela dei diritti e della dignità delle persone interessate; d'altro canto perché un'attività indifferenziata (clienti e non) di raccolta di dati, quali quelli relativi alle impronte biometriche, non può ritenersi legittimata da una generica esigenza di sicurezza, richiedendo invece l'allegazione di specifici elementi che evidenzino una concreta situazione di rischio. In difetto, tale rilevazione finisce con il comportare un sacrificio sproporzionato della sfera di libertà e della dignità delle persone interessate.

Nell'ambito delle tecniche di rilevazione biometriche, infatti, quelle concernenti le impronte digitali richiedono per la loro stessa natura una protezione più elevata, di fronte al rischio di ipotetiche utilizzazioni abusive, tanto che persino quando la raccolta di questo genere di informazioni viene realizzata da parte di soggetti pubblici è circondata da particolari cautele, come dimostra il fatto che la raccolta delle impronte digitali da parte di organi di polizia o giudiziari si fonda su specifiche previsioni normative che ne circoscrivono la rilevazione alle sole persone qualificabili come "pericolose o sospette", o a coloro che non sono in grado o si rifiutano di provare la propria identità, oppure, ancora, in caso di identificazione di un indagato o di detenuti ed internati all'ingresso di un istituto penitenziario (art. 7 r.d. n. 635/1940; art. 349, comma 2, c.p.p.; ex artt. 23 e 26 d.P.R. n. 230/2000). Scelta, questa, che può risultare coerente con la Raccomandazione del Comitato dei Ministri del Consiglio d'Europa RN (87) 15 in materia di dati utilizzati a fini di pubblica sicurezza – che l'Italia si è impegnata ad attuare integralmente – la quale consente la raccolta di dati mediante dispositivi tecnici di sorveglianza o altri mezzi automatizzati solo se prevista da disposizioni specifiche (punto 2.3).

Ma anche al di fuori dell'ambito della pubblica sicurezza, con riguardo alle recenti disposizioni normative in materia di carta di identità elettronica, a fronte della possibilità di inserirvi dati biometrici è stata prevista una specifica base normativa, ancorché in termini insufficienti, allo scopo di tener conto dei diritti fondamentali delle persone interessate.

Il problema posto dall'uso delle tecniche biometriche di rilevazione delle impronte digitali assume, d'altra parte, speciale delicatezza in tutti i casi in cui, come accade per gli sportelli bancari, acconsentire o meno alla rilevazione dell'impronta può tradursi nell'alternativa tra fruizione o non fruizione dei servizi offerti nei locali cui si accede previa rilevazione. In gioco sono evidentemente, da un lato, il pericolo di "schedatura" da parte

degli istituti di credito; da un altro lato, il rischio di privazione della libertà degli utenti degli sportelli bancari.

In proposito, con il già citato provvedimento il Garante, oltre a raccomandare l'osservanza degli obblighi di legge in materia di informativa e misure di sicurezza, ha non soltanto evidenziato che l'accesso agli sportelli bancari tramite i sistemi di rilevazione installati deve comunque avvenire su base volontaria e consensuale (cfr. artt. 11 e 12 l. n. 675/1996), evitando l'uso di meccanismi complicati ed ulteriori rispetto a quelli già ordinariamente adoperati, ma ha altresì puntualizzato che, a salvaguardia della libertà degli utenti, deve essere in ogni caso predisposto un meccanismo che, in caso di volontà contraria dell'utente, permetta a quest'ultimo di accedere egualmente all'istituto bancario, salva l'eventuale adozione – nei soli casi necessari – di misure non vessatorie di cautela, quale può essere la richiesta di esibizione di un documento di identità, rimesse alla ragionevole valutazione dei responsabili della filiale.

Inoltre, ove la rilevazione abbia avuto effettivamente luogo, soltanto l'autorità giudiziaria o di polizia, e con riferimento a specifiche attività investigative connesse alla commissione di reati, potrà decifrare ed avere accesso alle informazioni non nominative raccolte con i sistemi di rilevazione, con esclusione – in via assoluta – del personale di banca, fermo restando che i dati cifrati relativi alle impronte e alle eventuali immagini potranno essere conservati in *file* giornalieri per un periodo non superiore a una settimana, alla cui scadenza dovranno operare sistemi di integrale cancellazione automatica delle informazioni.

In conclusione l'Autorità, nel confermare l'orientamento manifestato in precedenza, ne ha sviluppato in senso propositivo alcuni principi che tengono conto della specifica situazione che la realtà bancaria poneva rispetto ad altri soggetti privati, ed ha prospettato alcune soluzioni che, temporanee e prodromiche rispetto ad un futuro intervento legislativo, hanno permesso di affrontare in un quadro di garanzie le particolari esigenze legate alla disponibilità presso gli istituti bancari di ingenti quantitativi di danaro contante per effetto dell'introduzione dell'euro.

45 Braccialetto elettronico

È proseguita l'attività di monitoraggio del Garante sul processo di introduzione e diffusione di forme di controllo a distanza – nella misura in cui implicano raccolta e trattamento di dati personali – dei soggetti sottoposti alla misura cautelare degli arresti domiciliari o alla detenzione domiciliare, in attuazione del d.m. del 2 febbraio 2001 recante "modalità di installazione ed uso e descrizione dei tipi e delle caratteristiche dei mezzi elettronici e degli altri strumenti tecnici destinati al controllo delle persone sottoposte alla misura cautelare degli arresti domiciliari nei casi previsti dall'art. 275-*bis* del codice di procedura penale e dei condannati nel caso previsto dall'art. 47-*ter*, comma 4-*bis*, della l. 26 luglio 1975, n. 354".

In particolare, si è seguita con attenzione la vicenda del cd. braccialetto elettronico, cioè dello strumento destinato al controllo delle persone sottoposte agli arresti o alla detenzione domiciliare che viene applicato all'interessato al fine di consentire all'autorità giudiziaria di localizzarlo. In questa prospettiva è proseguito il rapporto di collaborazione tra l'Autorità e i competenti uffici coinvolti nella vicenda normativa, allo scopo di conciliare le esigenze di sicurezza sempre più irrinunciabili con le forme elementari di rispetto della persona, ancorché responsabile di fatti di reato.

Nonostante il d.m. abbia recepito varie osservazioni dell'Autorità, restano da monitorare i rischi di possibile inosservanza nei casi concreti dei principi sanciti nell'art. 9 della l. n. 675/1996, specie per quanto concerne le finalità e la durata della conservazione dei dati raccolti, nonché i problemi relativi alla sicurezza delle informazioni personali (art. 15 l. n. 675/1996 e d.P.R. n. 318/1999).

46 *Marketing* e diritti dell'interessato

Le strategie di comunicazione adottate dalle società di *marketing* diretto, quando non siano condotte attraverso metodologie adeguate a garantirne un impatto limitato e tendenzialmente "condiviso" dal consumatore, si trovano a fronteggiare, sempre più frequentemente, la reazione di numerosi cittadini.

Si tratta di una crescente sensibilizzazione di consumatori ed utenti che si evince anche dal progressivo aumento del contenzioso relativo a episodi di "contatto" indesiderato da parte di operatori di *direct marketing* con gli interessati, eventuali futuri clienti.

Una parte di tale contenzioso è definibile a volte senza un integrale esame nel merito da parte del Garante in quanto il titolare del trattamento finisce per aderire spontaneamente alle richieste dell'interessato, nel corso del procedimento instaurato dinanzi all'Autorità.

In un caso specifico il Garante si è trovato di fronte alla richiesta dell'interessato volta ad ottenere la cancellazione di alcuni dati personali detenuti da una società ed impiegati da altra società ad essa collegata per fini di *marketing* diretto (*Provv.* 10 aprile 2001). Chiamata ad aderire all'istanza dell'interessato, la società titolare del trattamento ha disposto la cancellazione dei dati dagli archivi della sua controllata e ha comunicato che gli stessi sarebbero stati conservati al solo fine della pubblicazione dell'elenco degli abbonati al servizio telefonico. Il Garante ha così pronunciato non luogo a provvedere sul ricorso, ponendo a carico della società le spese e i diritti inerenti al procedimento.

Esito analogo ha avuto la richiesta presentata da un cittadino, in seguito alla ricezione di una telefonata a contenuto pubblicitario da parte di una società che gestisce corsi di formazione in lingue straniere, intesa a conoscere, nel dettaglio, gli estremi identificativi del titolare, le finalità del trattamento, nonché i dati personali relativi all'interessato detenuti dalla società e la loro origine. Dopo aver ignorato, in un primo momento, la richiesta presentata dall'interessato ex art. 13, la società ha fornito riscontro a tale istanza in seguito all'invito formale formulato dal Garante che, in sede di decisione di non luogo a provvedere, ha quindi posto a suo carico spese e diritti del procedimento (*Provv.* 31 dicembre 2001, in *Bollettino* n. 23, p 126).

Non diversamente si è ritenuta fondata la richiesta (v. *Provv.* 20 marzo 2002, in *Bollettino* n. 26, p. 37), proveniente dal destinatario di comunicazioni promozionali via Internet, di vedere interrotta l'utilizzazione di dati che lo riguardano (nel caso di specie, l'indirizzo di posta elettronica) muovendo sia dall'art. 10, comma 2, d.lg. n. 171/1998, sia dall'art. 10, comma 2, d.lg. n. 185/1999 (in materia di protezione dei consumatori con riguardo alla contrattazione a distanza).

L'auspicio per il futuro è naturalmente che, in casi analoghi, stante l'oggettiva fondatezza dell'istanza dell'interessato (quando non addirittura la mancanza di "controindicazioni" per il titolare nel fornire riscontro alle richieste inoltrate), i rispettivi titolari non frappongano inutili ostacoli all'esercizio dei diritti salvo poi "ritirarli" allorché viene attivata la competenza del Garante (andando però incontro alle inevitabili conseguenze del proprio originario inadempimento).

Telefonia e reti di comunicazione

47 Profili generali

Il progressivo sviluppo del settore della comunicazione telematica determina continuamente la nascita e la crescita di nuovi servizi e tecnologie, con il conseguente incremento del numero degli utenti dei servizi di comunicazione accessibili al pubblico, sia con riferimento al settore della telefonia – con un'incidenza particolare su quella mobile – sia con riguardo al mondo della rete *Internet*.

Di qui è derivato un crescente impegno dell'Autorità in ragione delle innumerevoli segnalazioni pervenute da parte di cittadini e da operatori del settore, dirette ad ottenere chiarimenti sulla disciplina applicabile o a denunciare lesioni della sfera di riservatezza propria o altrui. Ciò testimonia l'accresciuta sensibilità degli utenti di fronte ai rischi ed alle possibili lesioni derivanti dai trattamenti svolti sulle reti telematiche ed il peso sempre maggiore attribuito alle politiche a tutela della riservatezza, adottate dai diversi fornitori di servizi, nella scelta dell'operatore cui rivolgersi o del servizio da utilizzare.

Sempre più frequentemente, insomma, il raggiungimento di livelli adeguati di tutela rappresenta, almeno per gli operatori più avvertiti, non solamente la conseguenza dell'obbligo di adeguarsi a precisi vincoli di legge, ma anche e soprattutto, un mezzo strategico fondamentale per conquistare e conservare nel tempo la fiducia dei propri clienti e utenti.

Anche muovendo da tali considerazioni, il codice deontologico sui trattamenti di dati personali effettuati dai fornitori di servizi di comunicazione e informazione, che dovrebbe essere emanato nel corso del 2002, pur ponendosi come disposizione generale dell'ordinamento, il cui rispetto costituisce una condizione essenziale per la liceità del trattamento medesimo, cercherà di valorizzare ed incoraggiare anche tutte le pratiche poste in essere dagli operatori, con l'intento di raggiungere il maggior soddisfacimento di clienti e utenti attraverso un aumento della tutela della riservatezza anche oltre i requisiti minimi di legge.

48 Accesso ai dati di traffico telefonico

Le diverse problematiche sottese alla tutela della riservatezza per quanto attiene alle fatture contenenti il dettaglio degli addebiti relativi alle telefonate effettuate dagli abbonati sono già state analizzate nelle relazioni annuali successive all'emanazione del d.lg. 13 maggio 1998, n. 171, soprattutto con riferimento all'oscuramento delle ultime tre cifre dei numeri telefonici chiamati. Per tale ragione, si omette qui di richiamare i contenuti di tale normativa e le relative implicazioni, rinviando, per essi, alle relazioni precedenti.

In più casi il Garante è stato chiamato a pronunciarsi su ricorsi presentati da intestatari di utenze telefoniche al fine di ottenere dai fornitori dei servizi la comunicazione dei dati personali relativi al traffico in entrata e in uscita: in aderenza con quanto precedentemente affermato (v. *Relazione 2000*, p. 76) si è precisato che i dati relativi ad entrambi i tipi di chiamate sono da considerarsi dati personali ai sensi dell'art. 1, comma 1, lett. *c*), della legge 675/1996. Per tale ragione, è stato riconosciuto il diritto degli interessati di ottenere, ai sensi dell'art. 13 della citata legge, l'accesso ai dati personali che li riguardano concernenti il traffico in uscita (*Provv.* 4 aprile 2001; *Provv.* 30 ottobre 2001, in *Bollettino* n. 23, p. 84).

Per quanto riguarda il traffico in entrata, è stato anche chiarito che i diritti di cui all'art. 13 sopra citato possono essere esercitati altresì per ottenere l'accesso ai dati personali non ancora registrati, oltre che ai dati disseminati in più luoghi o archivi, ovvero conservati in modo disorganico. Tale previsione normativa non può, invece, essere estesa all'accesso ai dati personali non raccolti o che divengono materialmente esistenti solo a seguito di una attività creativa notevolmente complessa e che potrebbe essere realizzata solo con la collaborazione di altri soggetti (*Provv.* 3 maggio 2001, in *Bollettino* n. 22, p. 37; *Provv.* 17 ottobre 2001, in *Bollettino* n. 23, p. 93; *Provv.* 5 dicembre 2001, in *Bollettino* n. 23, p. 48; *Provv.* 12 dicembre 2001, in *Bollettino* n. 23, p. 44; *Provv.* 10 gennaio 2002, in *Bollettino* n. 24, p. 19).

A questo riguardo, il decreto legislativo 28 dicembre 2001, n. 467, recante disposizioni correttive e integrative della normativa in materia di protezione dei dati personali, ha introdotto alcune novità particolarmente rilevanti: fra i casi in cui non possono essere esercitati i diritti di cui al citato art. 13, è stato infatti inserito anche quello riguardante l'ipotesi in cui i dati identificativi delle chiamate telefoniche in entrata siano stati raccolti da fornitori di servizi di telecomunicazioni accessibili al pubblico. Ciò salvo il caso in cui dal mancato accesso possa derivare un pregiudizio per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 (cfr. art. 14, comma 1, lett. *e-bis*), l. n. 675/1996, come inserita dall'art. 6, d.lg. n. 467/2001).

Con riferimento a tali problematiche, occorre altresì ricordare che l'art. 21 del decreto delegato appena menzionato ha inserito un comma all'art. 5 del decreto legislativo n. 171 del 1998, con il quale è stato previsto che, entro il 30 giugno 2002, i fornitori di servizi di telecomunicazione dovranno documentare al Garante le misure predisposte per consentire modalità alternative di pagamento che mantengano l'anonimato. In mancanza di idonee misure, questa Autorità potrà provvedere segnalando le modificazioni necessarie o opportune per adeguarsi alla normativa vigente, eventualmente vietando, in tutto o in parte, i trattamenti realizzati dalle società telefoniche o disponendone il blocco, anche nell'ipotesi in cui le società medesime non abbiano provveduto ad adeguarsi alle modificazioni richieste (art. 31, comma 1, lett. *c)* ed *l)*, legge n. 675/1996).

Anche in vista dell'applicazione di tale nuova disposizione, l'Autorità si è attivata per la predisposizione di un provvedimento sui diritti coinvolti e per garantire l'equo contemperamento tra i legittimi interessi coinvolti. A tal fine è stata realizzata, anche a completamento di un'attività che era stata intrapresa tempo addietro, un'indagine conoscitiva presso i fornitori di servizi di telefonia, volta ad ottenere informazioni sull'effettiva attivazione e funzionamento di modalità alternative di pagamento del traffico telefonico, quali schede anonime e prepagate. L'effettiva fruibilità di tali servizi è particolarmente importante in quanto consentirà all'utente di addebitare su tali schede il costo delle chiamate effettuate e, in tal modo, di non farle comparire nella documentazione inviata agli abbonati.

49 Attivazione di nuovi servizi e consenso dell'interessato

Sono state ricevute numerose segnalazioni sull'utilizzo dei dati personali per l'attivazione di contratti e servizi di telefonia senza che gli interessati avessero preventivamente manifestato il proprio consenso. In particolare, con riferimento alla telefonia mobile, è stata denunciata l'intestazione di più schede telefoniche, in qualche caso centinaia, a nome dello stesso utente (*Provv.* 10 gennaio 2002, in *Bollettino* n. 24, p. 3). Per la telefonia fissa, invece, era stato lamentato che alcuni fornitori di servizi avevano attivato contratti nei confronti di abbonati ad altro gestore (preselezione automatica dell'operatore) e che altri avevano attivato nuovi servizi di telefonia fissa nei confronti dei propri abbonati.

Al fine di raccogliere maggiori informazioni sull'accaduto, l'Autorità ha avviato un procedimento presso gli operatori del settore, provvedendo a predisporre – ai sensi dell'art. 32, comma 1, l. n. 675/1996 – diverse richieste di informazioni indirizzate alle diverse società telefoniche, nonché ad alcuni esercizi commerciali abilitati all'attivazione dei contratti di telefonia mobile.

50 Elenchi abbonati e diritto alla riservatezza

Hanno formato oggetto di esame anche le problematiche legate alla compilazione, alla diffusione e all'utilizzo degli elenchi telefonici. Tale tematica presenta diversi aspetti di particolare complessità in ordine alla protezione dei dati personali, anche con riferimento alla fase transitoria che porterà all'applicazione di quanto previsto dal d.P.R. 11 gennaio 2001, n. 77.

Al riguardo, occorre dapprima ricordare che, nonostante i ripetuti richiami in ordine alla necessità che siano sempre rispettate le disposizioni secondo cui il Presidente del Consiglio dei ministri e ciascun ministro sono tenuti a consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 31, comma 2, l. n. 675/1996), la stessa Autorità non è stata consultata durante la predisposizione del d.P.R. appena citato, con conseguente vizio dell'atto.

L'art. 20 dello stesso d.P.R., benché di imprecisa formulazione, subordina la disciplina relativa ai servizi elenchi abbonati alla normativa generale sulla riservatezza ed a quella dettata con specifico riguardo ai trattamenti realizzati nell'ambito delle telecomunicazioni (in particolare, al d.lg. 13 maggio 1998, n. 171). Tale disposizione (benché presenti alcuni aspetti problematici anche sul piano transitorio) ha dunque inteso salvaguardare le garanzie contenute nell'art. 9 del d.lg. n. 171/1998 che prevede, in particolare: la possibilità di limitare i dati inseriti negli elenchi a quelli necessari per identificare l'abbonato, salvo consenso espresso di quest'ultimo alla diffusione di dati ulteriori; la possibilità di chiedere gratuitamente che il proprio indirizzo sia in parte omesso nonché, qualora ciò sia fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso.

Queste garanzie sono del resto in fase di possibile rafforzamento da parte degli artt. 12 e 16 della proposta di modifica della direttiva 97/66/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM (2000)385 - COD 2000/0189), in cui – secondo la posizione comune definita dal Consiglio il 28 gennaio 2002 – si prevede, tra l'altro, il previo consenso dell'interessato per l'inserimento dei dati personali in elenchi telefonici (v. par. 126).

Con riguardo a tale problematica, inoltre, l'Autorità per le garanzie nelle comunicazioni ha richiesto al Garante un parere su un provvedimento predisposto in materia; in tale occasione, sono state già fornite alcune prime indicazioni al fine di assicurare che i trattamenti di tali dati, effettuati attraverso la predisposizione e la pubblicazione di elenchi, siano conformi a quanto previsto dalla vigente normativa in materia di *privacy*.

La decisione dell'Autorità per le garanzie nelle comunicazioni appena richiamata prevede l'emanazione di un ulteriore provvedimento, specificatamente dedicato alla tutela dei dati personali utilizzati nella predisposizione degli elenchi, che dovrebbe essere adottato in breve tempo in cooperazione tra le Autorità.

51 Comunicazioni indesiderate su utenze telefoniche mobili

Con specifico riguardo al settore della telefonia mobile, l'Autorità si è anche occupata a più riprese dell'utilizzo del sistema di messaggeria (*sms*) dei telefoni cellulari.

La questione è stata inizialmente esaminata nell'ambito di un ricorso presentato al Garante con riguardo alla ricezione di alcuni *sms* su utenze telefoniche mobili contenenti indicazioni di voto a favore di un parlamentare (*Provv.* 20 giugno 2001, in *Bollettino* n. 21, p. 39).

Un successivo intervento, invece, ha preso le mosse da notizie apparse sugli organi di stampa riguardanti l'iniziativa di alcuni enti pubblici di inviare messaggi di pubblica utilità o di emergenza avvalendosi di alcuni fornitori di servizi di telefonia mobile. Sulla base di esse, sono state assunte informazioni presso enti e fornitori al fine di verificare la rispondenza di tali trattamenti alle vigenti norme in materia di protezione dei dati personali; dalle informazioni acquisite è emerso che l'utilizzo di tale sistema di comunicazione era stato predisposto per consentire alle persone che in un dato momento si trovavano in una determinata area geografica di venire tempestivamente a conoscenza dei provvedimenti adottati in via d'urgenza dalle autorità locali.

Oltre a questa iniziativa, si è venuti a conoscenza di altre, in fase di progettazione o di sperimentazione, riguardanti la possibilità, per taluni enti locali, di fornire ai cittadini – sempre attraverso *sms* – informazioni concernenti i servizi di pubblica utilità resi dagli stessi enti (es. informazioni sulla viabilità, sugli avvenimenti culturali in corso, sugli scioperi, sul pagamento delle imposte, sui termini di validità dei documenti).

A tutto ciò, si aggiunge, altresì, l'ormai noto sistema di utilizzo di tali mezzi di comunicazione, soprattutto da parte di soggetti privati, per l'invio di messaggi a fini di commercializzazione diretta. È infine in fase di definizione il profilo concernente i messaggi promozionali inviati, rispetto a propri servizi, dagli stessi fornitori di servizi di telecomunicazione.

Pur riconoscendo la possibile utilità di tali nuovi servizi, non si può sottovalutare la particolare forza invasiva che caratterizza le comunicazioni realizzate attraverso l'invio di *sms*, avvalendosi peraltro del numero del telefono cellulare, generalmente considerato come personale e riservato. Pertanto, si è ritenuto necessario offrire alcune indicazioni in materia e l'Autorità è in procinto di definire alcuni provvedimenti volti a segnalare misure ed accorgimenti idonei ad evitare che il trattamento di dati personali, effettuato con servizi *sms*, determini un'ingiustificata lesione della riservatezza dei soggetti cui i dati stessi si riferiscono.

Trattamento di dati personali in *Internet*

52 Profili generali

Con riguardo ai trattamenti realizzati sulle reti telematiche, la continua evoluzione tecnologica che ha interessato il settore ha determinato il sorgere di nuove problematiche con riguardo alla protezione degli utenti rispetto al trattamento e alla circolazione dei loro dati personali.

Ciò è testimoniato anche dagli innumerevoli quesiti, segnalazioni, richieste di chiarimenti pervenuti sia da parte dei singoli utenti (in particolare in relazione alle modalità con cui gli stessi possono ottenere la cancellazione dei propri dati raccolti per il tramite dei siti Internet), sia da parte degli stessi gestori dei siti *web*.

È stato avviato un nuovo monitoraggio sulle modalità utilizzate da siti *web* italiani per fornire l'informativa e richiedere il consenso, ove necessario, nonché per ottemperare agli obblighi in materia di protezione dei dati.

L'Autorità ha già fornito alcuni primi chiarimenti circa le modalità con cui è possibile esercitare i diritti riconosciuti dall'articolo 13 della legge n. 675/1996 sulla rete *Internet*, fornendo di volta in volta indicazioni agli utenti al fine di ottenere la cancellazione dei propri dati personali o indicando ai gestori dei siti gli accorgimenti necessari per conformarsi alla disciplina sulla tutela dei dati personali e, quindi, le misure da adottare al fine di favorire l'esercizio dei diritti medesimi.

Con riguardo al diritto di accesso in questione, si segnala un intervento dell'Autorità, a seguito di un ricorso, in cui è stata riconosciuta la legittimità della richiesta dell'interessato di conoscere, ai sensi dell'art. 13, i propri dati personali contenuti nei messaggi di posta elettronica (*Provv.* 30 ottobre 2001, in *Bollettino* n. 23, p. 86).

Sono state altresì affrontate le problematiche legate all'utilizzo, da parte dei gestori di siti *web*, di particolari dispositivi e/o programmi (*software* spia, *cookies*) che, specie ove introdotti nel terminale dell'utente a sua insaputa, magari all'atto del suo collegamento ad un determinato sito, permettono di seguirne la navigazione, consentendo finanche l'accesso a informazioni archiviate dallo stesso.

Per tali ragioni, il Garante, anche a seguito di numerose segnalazioni prevenute in tal senso, ha provveduto a richiedere puntuali informazioni sui trattamenti realizzati a diversi gestori di siti *Internet*. Sulla base delle risultanze di tali controlli, nonché di quelli effettuati in via autonoma su altri siti, l'Autorità provvederà fra breve ad offrire alcune indicazioni con un provvedimento anche di carattere generale, al fine di invitare i gestori dei siti a conformarsi alle garanzie previste dal nostro ordinamento a tutela della riservatezza, tenendo conto anche dei principi della Raccomandazione adottata dal Gruppo dei garanti europei lo scorso 17 maggio 2001.

53 Comunicazioni indesiderate ed utilizzo dei nomi di dominio *Internet*

Il Garante si era occupato del problema dell'invio di messaggi di posta elettronica contenenti comunicazioni pubblicitarie indesiderate – il cosiddetto *spamming* – anche in passato (v. *Relazione 2000*, p. 68) ed aveva già avuto modo di confrontarsi, fra l'altro, con le differenti discipline previste in materia, in Europa e negli USA, a seconda dell'adozione di regimi fondati sul consenso positivo – ossia, sulla possibilità per l'utente di scegliere se accettare o meno tali comunicazioni pubblicitarie (cd. *opt-in*) – oppure sul consenso negativo (cd. *opt-out*).

L'occasione per un nuovo esame della questione da parte dell'Autorità, è stata offerta dall'intenso contributo fornito nel quadro dei lavori di modifica della direttiva 97/66/CE del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM (2000)385 – COD 2000/0189; v. anche par. 77). Dopo un lungo dibattito in sede comunitaria, il 28 gennaio 2002, il Consiglio dell'Unione europea ha definito la cd. posizione comune in vista dell'adozione della direttiva, con la quale, seguendo l'orientamento innovativo proposto dalla Commissione rispetto alla direttiva del 1997, si prevede che la disciplina relativa all'invio di chiamate con sistemi automatizzati debba riferirsi anche ai messaggi di posta elettronica, applicando obbligatoriamente anche ad essi la regola del consenso positivo (*opt-in*) già osservata in alcuni Paesi europei.

In particolare, per quanto attiene specificamente all'invio di chiamate indesiderate, nella posizione comune si rinviene l'impostazione originaria, distinguendo anche l'ipotesi in cui le chiamate vengano effettuate con o senza l'intervento di un operatore (in quest'ultimo caso, che fa riferimento all'uso di strumenti automatizzati di chiamata, è stato previsto che per autorizzare l'invio sia necessario, in ogni caso, ottenere il consenso preventivo ed esplicito del ricevente). Tutto ciò in considerazione delle più ampie possibilità di invio anche durante orari notturni, nonché del fatto che, al di là della valenza intrusiva propria di tali forme di comunicazione, esse comportano spesso costi legati alla ricezione del messaggio (es. la carta del fax su cui viene stampato il messaggio o – ed è l'ipotesi che qui maggiormente ci interessa – i costi necessari a collegarsi alla rete telefonica per scaricare i messaggi di posta elettronica).

Va anche ricordata una pronuncia – alla quale si è fatto cenno al par. 29 – relativa all'invio non consensuale e generalizzato di *e-mail* con finalità di comunicazione politica (*Provv.* 11 gennaio 2001, in *Bollettino* n. 16, p. 39): nell'accogliere il ricorso, si è ribadita la nozione di pubblici registri, contenuta nella legge 675/1996, al fine di evidenziare il fatto che la rinvenibilità di indirizzi di posta elettronica in spazi pubblici di *Internet* non ne comporta un uso libero per l'ulteriore invio di posta elettronica.

In occasione di altri ricorsi, sono state esaminate questioni relative alla protezione dei domini *Internet* con specifico riguardo alla rettifica dei dati relativi al "*registrant*" (*Provv.* 7 marzo 2001, in *Bollettino* n. 18, p. 5) e alla pubblicazione di alcuni dati personali sulle pagine *web* lesive dell'onore e della reputazione (*Provv.* 16 gennaio 2001, in *Bollettino* n. 16, p. 36; v. anche *Relazione 2000*, p. 72).

54 Il codice deontologico

Come accennato, al fine di garantire la piena attuazione dei principi previsti dalla disciplina in materia di trattamento dei dati personali, il Garante, sulla base di quanto stabilito dal decreto legislativo 28 dicembre 2001, n. 467, ha promosso la sottoscrizione di un codice di deontologia e di buona condotta riguardante il trattamento dei dati personali effettuato nell'ambito dei servizi di comunicazione e informazione offerti per via telematica e in particolare nella rete *web*. Il codice avrà, fra l'altro, l'obiettivo di assicurare una più adeguata informazione e consapevolezza degli utenti delle reti di telecomunicazione gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole ed interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti.

Con l'intento di garantirne un'adeguata pubblicità, si è previsto che il codice venga pubblicato sulla Gazzetta Ufficiale e che il suo testo sia allegato al testo unico sulla protezione dei dati personali che dovrà essere emanato entro la fine del 2002.

È necessario infine sottolineare che, al pari di quanto previsto per i codici sui trattamenti realizzati a fini storici o statistici, e nonostante la sua denominazione, tale codice non avrà il valore di una qualunque altra disposizione di carattere deontologico, ma assumerà la veste di una vera e propria fonte dell'ordinamento generale, come si evince dal fatto che il rispetto delle disposizioni in esso contenute costituirà condizione essenziale per la liceità del trattamento dei dati (art. 20 d.lg. n. 467/2001).

Sicurezza dei dati e dei sistemi

55 Le misure di sicurezza: casi applicativi

Il titolare e, se designato, il responsabile del trattamento dei dati personali, hanno l'obbligo di custodire e controllare i dati trattati mediante l'adozione di idonee e preventive misure di sicurezza – individuate alla luce delle conoscenze acquisite in base al progresso tecnico, in relazione alla natura dei dati e alle specifiche caratteristiche del trattamento – tali da ridurre al minimo i rischi di distruzione, perdita accidentale, accesso non autorizzato, trattamento non consentito o, comunque, non conforme alle finalità della raccolta (art. 15, comma 1, l. n. 675/1996).

Le "*misure minime di sicurezza*" – definite con il d.P.R. 28 luglio 1999 n. 318 e la cui mancata osservanza comporta sanzioni di carattere penale (art. 36 l. n. 675/1996) e civile (art. 18 l. n. 675/1996) – in virtù dell'art. 15, comma 3, sono soggette ad adeguamento, con cadenza almeno biennale, in relazione all'evoluzione tecnica e all'esperienza maturata. Il Garante fornirà un contributo per il loro aggiornamento rendendo noti i risultati di un gruppo di lavoro, la cui attività potrebbe risultare utile nel quadro di un'autonoma revisione del d.P.R. o della sua integrazione all'interno dell'atteso testo unico.

Dal punto di vista applicativo, la questione delle misure di sicurezza ha formato oggetto di vari provvedimenti: in data 23 febbraio 2001, è stata ad esempio valutata la conformità al d.P.R. n. 318/1999 della richiesta, avanzata da un'azienda ai propri dipendenti – che utilizzano strumenti informatici – di servirsi di *password* loro singolarmente assegnate, con il contestuale divieto di autonoma modifica della stessa (v. nota prot. 2074/01, in *Bollettino* n. 17, p. 32); in merito, l'Autorità ha ricordato che gli incaricati, ove tecnicamente possibile, devono poter procedere autonomamente alla sostituzione della *password*, previa comunicazione, però, ai soggetti preposti alla loro custodia (es. comunicazione effettuata tramite busta chiusa) per consentire al titolare del trattamento eventuali interventi nel caso di assenza o di impedimento dell'incaricato; inoltre, in caso di "elaboratori accessibili in rete", oltre la parola chiave, è necessario utilizzare i codici identificativi.

Anche nel fornire, poi, il cd. "decalogo" per l'utilizzazione di dati da parte di partiti e movimenti politici durante il periodo di propaganda elettorale ovvero per la presentazione di liste e candidature o per la sottoscrizione di referendum (per il quale v. par. 29), è stata ribadita la necessità di rispettare alcuni principi sulla raccolta dei dati, sottolineando altresì l'obbligo di adottare le misure di sicurezza, ed in particolare quelle minime di cui al d.P.R. n. 318/1999, con riferimento ai trattamenti di dati cartacei e automatizzati. Analoga indicazione è stata fornita in un parere relativo ad uno schema di regolamento volto ad istituire un sistema di comunicazione tra regioni ed enti locali per pianificare e gestire la relativa autonomia tributaria e per consentire il decentramento catastale, evidenziando che la complessa articolazione dei flussi di dati che saranno trattati in base alle citate disposizioni presuppone la doverosa adozione di idonee misure di sicurezza "*a prescindere da eventuali regole tecniche indicate per i sistemi utilizzati*" (*Provv.* 27 giugno 2001, in *Bollettino* n. 21, p. 15).

In alcuni casi, l'Autorità ha esaminato segnalazioni riguardanti l'utilizzazione di dati estratti dall'anagrafe della popolazione per l'invio di lettere ai cittadini da parte del Sindaco e ha avviato accertamenti presso i comuni interessati su alcuni aspetti, tra cui le misure di sicurezza adottate, anche sotto il profilo inerente all'eventuale collaborazione di terzi all'inoltro delle lettere.

Non diversamente è accaduto in relazione alle questioni dei trattamenti di dati in sede di svolgimento del censimento nella provincia di Bolzano (*Provv.* 6 febbraio 2001, in *Bollettino* 17, p. 11) e dell'installazione all'entrata degli istituti bancari di sistemi di rilevazione delle impronte digitali degli utenti – eventualmente associate ad immagini – per i quali occorre adottare parimenti misure di sicurezza che osservino i parametri fissati dalla l. 675/1996 e dal d.P.R. 318/1999, in particolare per quanto riguarda la custodia delle chiavi di accesso. Inoltre, si è stabilito che detti sistemi di rilevazione devono offrire una "*rigorosa garanzia di affidabilità ed integrità dei dati*", anche sulla base di eventuali certificazioni od omologazioni dei dispositivi, e che le informazioni relative a immagini e impronte devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della loro rilevazione (*Provv.* 28 settembre 2001, in *Bollettino* n. 22, p. 82).

I trasferimenti all'estero di dati

56 Paesi che offrono una protezione adeguata

Il crescente rilievo delle questioni riguardanti il trasferimento all'estero di dati personali è segnalato anche dalla recente modifica, ad opera del decreto legislativo n. 467/2001, dell'articolo 28 della legge 675/1996, in base alla quale è demandato al Garante il compito di autorizzare il trasferimento dei dati verso Paesi terzi sulla base di adeguate garanzie per l'interessato, prestate anche con un contratto, ovvero individuate dalla Commissione europea (al cui sito *http://europa.eu.int/comm/internal-market* è opportuno fare riferimento per una completa ricognizione dei materiali pertinenti, i più rilevanti dei quali sono richiamati in allegato alla presente relazione).

Viene così esplicitamente individuato lo strumento di attuazione delle decisioni comunitarie previste dagli articoli 25, par. 6, e 26, par. 4, della direttiva 95/46/CE, rispettivamente riguardanti l'adeguatezza della protezione dei dati personali offerta dall'ordinamento di un Paese terzo e le garanzie risultanti da clausole contrattuali, reputate idonee a tal fine dalla Commissione.

Con il medesimo decreto legislativo, semplificando gli adempimenti per i destinatari del citato art. 28, si è stabilito che il trasferimento di dati personali all'estero deve essere notificato al Garante solo qualora sia diretto verso un Paese non appartenente all'Unione europea e ricorra uno dei casi individuati ai sensi dell'articolo 7, comma 1, della legge, disposizione anch'essa oggetto di rivisitazione.

In alcune circostanze, tuttavia, anche il trasferimento a Paesi membri può porre questioni di natura particolare. Rispondendo ad una richiesta di parere del Ministro delle comunicazioni, il 3 settembre 2001, l'Autorità, in sede di primo riscontro e rimanendo a disposizione per ogni approfondimento, ha richiamato la necessità della massima cautela relativamente al trasferimento di dati di traffico ad una società spagnola *partner*, prospettato – per esigenze gestionali – da un gestore italiano di servizio di telefonia mobile secondo lo standard Umts. La competente Direzione generale del Ministero aveva peraltro già fornito al gestore risposta negativa, evidenziando che esigenze giudiziarie richiedono che i dati siano conservati nella loro integrità originaria in Italia.

Il Garante – che ha poi riferito sul caso al Gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE – nel sottolineare che si tratta di dati tutelati anche costituzionalmente, ha invitato a considerare, inoltre, le problematiche relative alla sicurezza dei dati ed al loro possibile incrocio con i dati detenuti dalla società spagnola. La questione sembra aver successivamente perso di attualità per il sostanziale venir meno delle prospettate esigenze gestionali.

Delle decisioni comunitarie in materia di adeguatezza degli ordinamenti stranieri, riguardanti l'Ungheria e la Svizzera, si è dato conto nella relazione annuale dello scorso anno (v. *Relazione 2000*, p. 85).

Esse sono state attuate con deliberazioni dell'ottobre 2001 (pubblicate sulla *Gazzetta Ufficiale* e consultabili sul sito *web* dell'Autorità anche ai fini dell'invio di osservazioni, volte ad evidenziarne eventuali problemi applicativi), nelle quali il Garante si è comunque riservato di procedere ai necessari controlli sulla legittimità dei trasferimenti.

Passando ora al piano internazionale, va tenuto presente che la disciplina comunitaria si applica anche ai Paesi che, con quelli dell'Unione, costituiscono lo Spazio economico europeo – cioè Norvegia, Lichtenstein ed Islanda – e che negli Usa sono in vigore i principi cd. del *Safe Harbor* (v. paragrafo successivo).

Con decisione del 20 dicembre 2001 (2002/2/CE, in *G.U.C.E.* L 002, 4 gennaio 2002), la Commissione europea ha riconosciuto che la legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (*Canadian Personal Information Protection and Electronic Documents Act*) assicura una protezione adeguata per il trasferimento di alcuni dati personali dall'Unione europea al Canada. Viene così facilitato il flusso di dati

56

dall'Europa verso un Paese terzo in cui, come previsto dall'art. 25, par. 6, della direttiva sulla protezione dei dati (95/46/CE), si riconosce l'esistenza di un livello adeguato di protezione.

Il gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE si era espresso sul grado di protezione offerta dall'ordinamento canadese, con un parere del 26 gennaio 2001 (parere n. 2/2001) sostanzialmente interlocutorio e che, tra l'altro, sottolineava le questioni relative all'ambito di applicazione della legge canadese ed alla problematica del rapporto tra norme federali e norme delle diverse province (v. anche *Relazione 2000*, p. 85).

La decisione della Commissione, in qualche misura, ha tenuto conto di tale parere, commisurando il proprio ambito di applicazione a quello della legge canadese che, in prima approssimazione, è applicabile (dal 1° gennaio 2002) ai soggetti disciplinati da norme di livello federale, e (dal 1° gennaio 2004) a tutte le organizzazioni federali o non federali, che rilevano, utilizzano o comunicano dati personali nell'ambito di attività commerciali, con eccezione dei soggetti ai quali sia applicabile la legislazione provinciale, considerata sostanzialmente simile a quella federale.

Nella decisione comunitaria viene sottolineato che l'applicazione delle norme canadesi di protezione è garantita da ricorsi giurisdizionali nonché dal controllo indipendente esercitato da Autorità quali il Commissario federale per la *privacy* (*Federal Privacy Commissioner*), che ha poteri di investigazione ed intervento ed al quale ci si può rivolgere anche nei casi in cui non sia chiaro l'ambito di applicazione della citata legge; nel caso di conseguenze pregiudizievoli per la persona si applicano inoltre le norme canadesi sulla responsabilità civile.

Le autorità degli Stati membri hanno facoltà di sospendere flussi di dati verso i destinatari in Canada nei casi in cui sia stato accertato dalle competenti autorità canadesi che il destinatario dei dati stessi non rispetta le norme sulla loro protezione, ovvero in altre complesse ipotesi, sostanzialmente corrispondenti a quelle previste nelle decisioni relative ad Ungheria e Svizzera.

Gli Stati membri devono adottare tutte le misure necessarie per conformarsi alla decisione – modificabile in qualsiasi momento alla luce delle esperienze relative al suo funzionamento o a modifiche dell'ordinamento canadese – entro 90 giorni dalla sua notifica, il che avverrà, per l'Italia, nel breve periodo.

La deliberazione del Garante attuativa della decisione, al momento in cui il presente testo viene redatto, è in fase di predisposizione.

57 "*Safe Harbor*"

Il 10 Ottobre 2001 l'Autorità ha adottato un'autorizzazione (pubblicata in *G.U.* 26 novembre 2001) che attua la decisione n. 2000/520/CE, in base alla quale la Commissione europea ha riconosciuto che i principi internazionali di riservatezza del *Safe Harbor* (letteralmente, "approdo sicuro"), pubblicati dal Dipartimento del commercio degli Stati Uniti, costituiscono un'adeguata protezione ai fini del trasferimento di dati personali dall'Unione europea verso tale Paese. Dei principi e della complessa negoziazione che ha portato alla loro determinazione si è detto nella precedente relazione (v. *Relazione 2000*, p. 86).

Anche in questa autorizzazione il Garante si riserva di controllare la legittimità dei trasferimenti e di adottare i provvedimenti ad essa eventualmente conseguenti.

Sull'applicazione della decisione 2000/520/CE, la Commissione europea ha adottato un primo documento il 13 febbraio 2002, corrispondendo a quanto auspicato dal Parlamento europeo che, con risoluzione del 5 luglio 2000, aveva invitato la Commissione ad assicurare uno stretto monitoraggio del funzionamento del sistema dell'approdo sicuro.

Il documento si basa su informazioni raccolte in Europa presso le autorità di garanzia dei Paesi membri e negli Stati Uniti, presso il sito *Internet* del Dipartimento del commercio, autorità pubbliche e private in vario modo interessate all'esecuzione dei principi, nonché presso i siti delle organizzazioni aderenti all'accordo alla data del 4 giugno 2001.

Si tratta di un rapporto provvisorio che offre, comunque, significativi spunti di riflessione ed evidenzia alcuni punti critici sulle carenze che si registrano in termini di effettiva applicazione dell'Accordo e di trasparenza in relazione alle prassi applicative ed alle decisioni adottate sulle dispute. In sintesi, viene anzitutto rilevata l'importanza, in termini di semplificazione e riduzione delle incertezze, di aver identificato uno *standard* che corrisponde all'adeguata protezione richiesta dalla direttiva, e viene altresì osservato, in linea generale, che i principi, tanto negli Usa quanto nell'Ue, sono in atto.

In proposito, per quanto riguarda gli Stati uniti, il Dipartimento del commercio cura l'elenco pubblico delle organizzazioni insediate negli Usa che hanno autocertificato la propria adesione ai principi (183 al 19 aprile 2002) ed ha assunto iniziative opportune per far conoscere agli operatori il contenuto dell'Accordo. Per quanto concerne invece l'Unione europea, i Paesi membri hanno adottato, ove richieste dai loro ordinamenti interni, le misure necessarie per consentire il flusso dei dati verso gli aderenti all'Accordo, ed è stato reso operativo l'elenco di autorità garanti cui possono rivolgersi gli aderenti per la soluzione delle dispute negli Usa.

Dei pochi interpelli negli Usa provenienti da cittadini, a conoscenza della Commissione, nessuno è rimasto in sospeso.

Sono stati segnalati alcuni problemi invece, per quanto riguarda, in sintesi, il grado di trasparenza richiesto agli aderenti all'Accordo: sia perché dai loro siti *Internet* non sempre risulta dichiarata o agevolmente visibile la dichiarazione di adesione ai principi; sia perché le politiche sulla *privacy* adottate non riflettono sistematicamente i principi stessi; sia perché i cittadini che vogliono esercitare i loro diritti sui dati che li riguardano sono spesso tenuti all'oscuro dei modi per farlo.

Inoltre, gli enti di risoluzione delle controversie possono operare senza dover pubblicamente dichiarare l'intenzione di applicare i principi, ovvero senza dover seguire pratiche di tutela della *privacy* ad essi conformi, ancorché solo 2 enti sui 6 operanti non abbiano né autocertificato la loro adesione ai principi, né dichiarato pubblicamente di agire quali enti di risoluzione di controversie per gli aderenti all'approdo sicuro.

57

Almeno una parte di tali problemi è stata imputata a "difetti di avviamento", ed i servizi della Commissione hanno positivamente accolto la disponibilità espressa dal Dipartimento statunitense del commercio al miglioramento del sistema.

In questo quadro, il Garante continua a partecipare all'attività di monitoraggio, in vista ormai della valutazione d'insieme sul funzionamento del *Safe Harbor*, prevista per il 2003 da parte della Commissione europea, ed è attivamente impegnato nel favorire la cooperazione tra Usa ed Ue. In tal senso, va ricordata da ultimo la visita negli Usa nel marzo 2002 di una delegazione di rappresentanti delle autorità di protezione dati europee, guidata dal Prof. Rodotà – quale Presidente del Gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE – che ha consentito incontri con rappresentanti del Congresso, dell'amministrazione Usa, con imprese multinazionali aderenti al meccanismo del *Safe Harbor* e con numerose organizzazioni non governative da anni impegnate nella tutela della *privacy*.

Dai risultati assai proficui di tale visita deriverà probabilmente un nuovo pronunciamento a breve del Gruppo europeo.

58 Clausole contrattuali standard

Come riferito nella scorsa relazione, il 27 marzo 2001 il Comitato previsto dall'art. 31 della direttiva 95/46/CE ha espresso parere favorevole allo schema di decisione della Commissione europea sulle clausole contrattuali standard relative al trasferimento di dati personali ad un titolare autonomo di trattamento in un Paese terzo (v. *Relazione 2000*, p. 87).

La Commissione, con decisione del 15 giugno 2001 (2001/497/CE, in *G.U.C.E.* L 181 del 4 luglio 2001), ha approvato le clausole con le quali l'importatore di dati del Paese terzo si impegna nei confronti dell'esportatore comunitario dei dati, ma anche a beneficio dei soggetti cui i dati si riferiscono, ad adottare un certo livello di protezione dei dati medesimi.

Nel dare attuazione alla decisione comunitaria – con deliberazione del 10 ottobre 2001 (riportata negli allegati) – l'Autorità, riservandosi di procedere ai necessari controlli sulla legittimità dei trasferimenti, ha altresì escluso la necessità di ottenere, se non su sua richiesta, copia del contratto relativo al trasferimento dei dati; deve comunque essere comunicata all'Autorità la scelta, effettuata in caso di controversia non risolta in via amichevole, di sottoporre la risoluzione della stessa a soggetto diverso dal Garante o dall'autorità giudiziaria (clausola 7, par. 2 e par. 1, lett. *a)*; art. 31 l. n. 675/1996).

Su un altro schema di decisione, relativo alle clausole contrattuali sul trasferimento di dati personali a responsabili del trattamento residenti in Paesi terzi, il Gruppo di lavoro previsto dall'art. 29 della direttiva 95/46/CE ha espresso parere favorevole il 13 settembre 2001; il testo, ottenuto il parere favorevole da parte del Comitato previsto dall'art. 31 della medesima direttiva, è stato poi adottato con decisione della Commissione del 27 dicembre 2001 (2002/16/CE in *G.U.C.E.* L 6 del 10 gennaio 2002).

Tali clausole, che anche nel nostro Paese sono applicabili dal 3 aprile 2002 (deliberazione del Garante n. 3 del 10 aprile 2002), riguardano il trasferimento dei dati a soggetti insediati in Paesi terzi che si impegnano a riceverli dall'esportatore per trattarli per suo conto e secondo le sue istruzioni. Esse riprendono la terminologia adoperata nella direttiva – che distingue tra responsabile e incaricato del trattamento – e a cui corrispondono, nel diritto nazionale, rispettivamente le figure del titolare e del responsabile del trattamento.

Anche queste clausole, come quelle riguardanti il trasferimento ad un titolare autonomo di trattamento, non sono "obbligatorie", ma il loro utilizzo comporta che gli ordinamenti dei Paesi membri debbano riconoscere come adeguata la protezione offerta da contratti che le contengono.

Ciò non toglie da un lato che tale protezione possa essere riscontrata anche in clausole di diverso contenuto, dall'altro che permangano in capo alle autorità garanti poteri di vigilanza e di adozione dei provvedimenti conseguenti.

Una valutazione complessiva della Commissione sul funzionamento delle clausole è prevista dopo tre anni di applicazione della decisione comunitaria.

Le clausole prevedono l'applicabilità della legge del Paese membro in cui ha sede l'esportatore. Per quanto riguarda la giurisdizione, l'importatore si obbliga ad accettare la decisione dell'interessato, che agisca nei suoi confronti per il risarcimento del danno, di deferire la controversia al giudice dello Stato membro in cui ha sede l'esportatore, oppure alla mediazione di un terzo indipendente o di un'autorità di controllo, ovvero, in ordinamenti che presentino determinate garanzie di esecuzione, ad organi arbitrali.

Nella sostanza l'importatore e l'esportatore convengono l'attuazione di determinate misure, e rispondono dei rispettivi obblighi, ma i soggetti cui i dati si riferiscono possono far valere, anche verso l'importatore, la responsabilità dell'esportatore nei cui confronti non sia più possibile agire perché di fatto scomparso, non

più esistente giuridicamente, ovvero insolvente.

Da questo complesso intreccio tra i diversi piani, interno, estero e sopranazionale da un lato, e gli strumenti di diritto privato e pubblico dall'altro, con i quali si disciplina la materia del trasferimento di dati verso i Paesi terzi, si evidenzia il rilievo che decisioni e determinazioni relative al singolo caso sono destinate ad assumere e si conferma la delicatezza, prima ancora che la centralità, delle funzioni demandate alla nostra Autorità garante.

Da qui anche l'esigenza sostanziale di un continuo raffronto con l'esperienza degli altri Stati membri e, più in generale, con gli altri ordinamenti in cui si dia adeguato rilievo alla protezione dei dati personali. In tal senso assume un significato più ampio di quello che la sua formulazione palesa, la decisione con cui, il 13 dicembre 2001, il Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46/CE ha previsto la possibilità di invitare alle proprie riunioni, quali osservatori, i rappresentanti delle autorità di protezione dei dati personali dei Paesi che abbiano richiesto l'adesione alla Ue.

Il Garante

La nuova composizione del Collegio

59 La continuità nell'attività dell'Autorità

Il 28 febbraio 2001 la Camera dei deputati e il Senato della Repubblica hanno eletto i quattro componenti del collegio del Garante, in vista del completamento del primo mandato quadriennale che aveva avuto inizio il 17 marzo 1997, subito dopo l'approvazione della legge n. 675/1996, con l'accettazione della nomina da parte dei componenti.

Il nuovo collegio si è insediato il 19 marzo 2001, alla presenza dei professori Stefano Rodotà e Giuseppe Santaniello (già componenti del collegio nel precedente quadriennio) e degli onorevoli Mauro Paissan e Gaetano Rasi, eletti nuovi componenti il 28 febbraio 2001.

Il 19 marzo 2001 il collegio del Garante ha eletto all'unanimità il prof. Stefano Rodotà e il prof. Giuseppe Santaniello, rispettivamente come Presidente e Vice presidente dell'Autorità, ed ha dato inizio al nuovo mandato ribadendo anche il carattere collegiale dell'organo nel lavoro interno ed esterno dell'istituzione, secondo le linee già affermatesi nel corso della precedente composizione della stessa Autorità.

La trattazione dei ricorsi

60 Principali problemi esaminati

I ricorsi al Garante ai sensi dell'art. 29 della legge n. 675/1996 sono divenuti ormai, a solo tre anni dall'entrata in vigore delle norme regolamentari relative alla loro trattazione (contenute nel d.P.R. n. 501 del 1998), uno strumento di tutela utilizzato sempre più frequentemente dagli interessati (direttamente o ricorrendo al patrocinio di un legale). Molti titolari di trattamento (soprattutto enti di livello nazionale o grandi società di servizi) hanno anzi predisposto apposite unità organizzative per rispondere alle richieste provenienti dagli interessati.

Negli ultimi mesi, invero, si è registrato un flusso crescente di ricorsi: a fronte dei 381 pervenuti complessivamente al 1° giugno 2001, al 1° aprile 2002 il loro totale era già salito a 540.

Se il dato numerico è di per sé significativo, un esame del contenuto dei ricorsi medesimi sollecita ulteriori considerazioni.

Va anzitutto rilevato che si è arricchito il panorama delle posizioni giuridiche, comunque specificatamente tutelate dall'art. 13, comma 1, della legge n. 675 (le sole per le quali sia attivabile, in caso di mancato o inidoneo riscontro, il meccanismo di tutela di cui all'art. 29 della medesima legge), in concreto fatte valere. Mentre in una prima fase la quasi totalità dei ricorsi era incentrata su problematiche attinenti all'accesso ai dati, negli ultimi tempi lo spettro dei diritti di cui al medesimo art. 13, comma 1, concretamente esercitati è cresciuto e si è diversificato.

Sono infatti sempre più frequenti le richieste di integrazione, di correzione o anche di cancellazione dei dati, o le richieste di opposizione al trattamento per motivi legittimi. Conseguentemente, anche la struttura delle decisioni è divenuta più complessa. Ne sono prova molti dei dispositivi adottati nel periodo più recente che racchiudono una variegata articolazione di decisioni (accoglimenti parziali, profili di infondatezza, non luogo a provvedere).

È altresì interessante notare come sia migliorata, in generale, la qualità redazionale degli atti introduttivi, con la proposizione di domande sempre più specifiche e pertinenti: il (particolare) campo di applicazione della legge – la tutela dei dati personali – viene sempre meglio evidenziato dagli interessati, diradandosi i riferimenti ad altri plessi normativi non sempre strettamente pertinenti (come, ad esempio, le norme sull'accesso agli atti e documenti amministrativi).

Per quanto attiene infine, alle macro-aree nelle quali i ricorsi sono stati presentati, se pure si conferma la rilevanza di alcuni "filoni" emersi con forza fin dalla prima fase applicativa del nuovo strumento, nuovi settori sono stati portati all'attenzione dell'Autorità nel corso di quest'ultimo anno, i quali senza pretesa di esaustività, sono qui tratteggiati rinviando per una loro più approfondita trattazione alle singole parti della Relazione.

Accesso ai dati personali dei lavoratori. È una delle ipotesi più ricorrenti che, verosimilmente, corrisponde alla tendenza, sempre più diffusa, di chiedere al proprio datore di lavoro l'accesso al complesso dei dati personali dallo stesso detenuti, comprendendo (specie per funzionari, quadri e dirigenti) le (eventuali) valutazioni espresse in giudizi o rapporti annuali. Dopo le inevitabili difficoltà del primo momento è però possibile constatare come, nella maggior parte dei casi, le risposte dei titolari siano ora più pronte e complete e, attraverso strumenti sia cartacei, sia automatizzati, consentano ormai un'ampia possibilità di acquisizione dei dati da parte degli interessati.

Dati sanitari e dati contenuti in perizie medico legali. Si sono presentati diversi casi volti ad ottenere pieno accesso a questa particolare e delicata categoria di dati personali a seguito di richieste destinate sia ad a.s.l. o

ad aziende ospedaliere, in riferimento a insiemi di dati di notevole corposità (riferiti ad una pluralità di interventi delle strutture sanitarie stesse o a patologie di particolare complessità), sia a liberi professionisti operanti nel settore sanitario.

Il Garante si è poi ripetutamente soffermato anche sul tema dei dati riguardanti lo stato di salute contenuti nelle perizie medico-legali redatte in ambito assicurativo, rispetto al quale (come sottolineato nel paragrafo n. 35) è peraltro in corso un dibattito anche in sede giurisprudenziale.

Dati relativi a minori. Diversi ricorsi hanno riguardato richieste di accesso ai dati personali trattati da psicologi o da strutture di assistenza sociale e sanitaria nell'ambito di complesse vicende legate a controversie in tema di separazione dei genitori e di affidamento dei figli. Nei casi trattati le richieste provenienti da uno dei genitori erano preordinate a conoscere informazioni personali sia relative al minore, sia riferite al trattamento di delicati dati personali dei genitori stessi.

Il Garante ha peraltro esaminato con attenzione la posizione rivestita, specie dai professionisti autori delle relazioni richieste, nell'ambito dei giudizi in corso. In caso di accertata posizione di ausiliarietà del giudice nelle predette vicende si è ritenuto inammissibile il ricorso che non opera per i trattamenti in materia di giustizia.

Dati trattati da investigatori privati. Il corretto uso delle informazioni da parte degli investigatori privati (la cui attività è oggetto di specifiche disposizioni della legge n. 675/1996 e di un'apposita autorizzazione generale riferita al trattamento dei dati sensibili) è stato al centro di alcuni provvedimenti significativi (come tre decisioni del 19 febbraio 2002) che hanno messo a fuoco ambiti e limiti dell'attività investigativa stessa, fissando i punti di equilibrio fra esercizio di un'attività fondamentale per il pieno esercizio del diritto di difesa e le esigenze ineludibili del diritto alla riservatezza.

Dati trattati dalle cd. centrali rischi private. Fra gli ambiti più strettamente legati alla realtà economica, quello delle cd. centrali rischi continua a rappresentare il settore verso il quale si appunta il maggior numero di istanze da parte degli interessati, incentrate sui profili dell'accesso, della correzione e (spesso) cancellazione dei dati. In particolare il Garante ha avuto modo di pronunciarsi su delicati profili relativi al tempo di conservazione dei dati di alcuni soggetti (vedi decisione del 27 dicembre 2001), con ciò in qualche misura promuovendo un più generale ripensamento sulle concrete modalità di raccolta, trattamento e conservazione di questi dati (la cui incidenza sulla libera esplicazione delle attività economiche dei singoli è rilevantissimo) che sarà presumibilmente oggetto nei prossimi mesi di interventi e provvedimenti di carattere generale.

Dati relativi al traffico telefonico. È un altro settore sul quale si sono registrate sia richieste di accesso e di correzione di dati relativi ad intestatari di schede telefoniche, sia istanze volte ad ottenere la conoscenza delle utenze telefoniche non solo "in uscita", ma anche "in entrata" rispetto allo stesso terminale di telecomunicazione. Significative, a questo proposito, le decisioni del 17 ottobre e del 5 dicembre 2001 nelle quali è stato ribadito il diritto degli interessati ad avere accesso (in modo completo, senza oscuramento delle ultime tre cifre), ai sensi dell'art. 13 della legge n. 675, ai dati personali contenuti nei tabulati relativi alle chiamate "in uscita".

In tali occasioni il Garante ha avuto modo di soffermarsi anche sulla natura dei dati relativi al traffico "in entrata", svolgendo considerazioni problematiche che hanno trovato poi riscontro, in chiave normativa, nell'art. 6 del d.lg. n. 467/2001: con esso è stata introdotta la nuova lettera *e-bis*) nell'art. 14, comma 1, della legge n. 675, escludendo l'esercizio dei diritti di accesso ai dati raccolti "da fornitori di servizi di telecomunicazioni accessibili al pubblico, limitatamente ai dati personali identificativi di chiamate telefoniche entranti, salvo che da tale esclusione possa derivarne pregiudizio per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397".

61 Profili procedurali e procedimenti instaurati autonomamente

Il crescente numero di ricorsi correttamente formulati, posti in istruttoria e decisi, ha evidenziato profili procedurali nuovi, quali gli interventi in caso di mancato o incompleto adempimento delle decisioni, l'instaurazione di autonomi procedimenti di segnalazione, ecc. Si evidenziano, di seguito, alcuni profili meritevoli di attenzione.

Requisiti formali per la proposizione del ricorso al Garante. I requisiti formali richiesti dal d.P.R. n. 501/1998 per la presentazione del ricorso ex art. 29, comunque estremamente ridotti (autenticazione della firma del ricorrente, pagamento dei diritti di segreteria, previa formulazione di un'istanza ai sensi dell'art. 13), sono ormai correttamente posti in essere dagli interessati grazie anche alla diffusione data alle istruzioni, da tempo divulgate anche attraverso il sito *web* del Garante nell'apposita sezione (Faq) riservata ai quesiti più frequenti. In proposito, qualche perplessità è emersa da parte di alcuni comuni (in verità pochi) rispetto alla richiesta di autenticazione della sottoscrizione da parte dei cittadini che intendevano presentare personalmente il ricorso. Secondo la testi – non condivisa dall'Autorità – di tali comuni, non più sarebbe dovuta la medesima autenticazione (ai sensi del recente d.P.R. 28 dicembre 2000, n. 445), obbligo che sarebbe stato sostituito dalla autocertificazione da parte del soggetto interessato.

L'Autorità ha più volte ribadito (v. *Relazione 2000*, p. 92) la persistente necessità di tale adempimento, in virtù della peculiarità del procedimento attivato dal ricorso medesimo (che, come noto, è alternativo rispetto ad un'azione dinanzi all'autorità giudiziaria), trovando pacifico accoglimento da parte di moltissimi comuni e riservandosi, peraltro, di intervenire nuovamente sul punto con un provvedimento di carattere generale destinato alla più ampia diffusione.

Il d.P.R. n. 501/1998. Le norme procedurali concernenti specificamente i ricorsi sono, come noto, contenute nel predetto d.P.R., specificamente negli artt. 18, 19 e 20. Tale regolamento, principalmente dedicato alla disamina dell'organizzazione e del funzionamento del Garante, è stato però in larga parte abrogato dalle nuove disposizioni emanate internamente dal Garante medesimo con i regolamenti nn. 1, 2 e 3 del 28 giugno 2000 (pubblicati sulla *G.U.* del 13 luglio 2000). Appare ora opportuna, pertanto, una rivisitazione di tali norme per inserirle in un più organico contesto e soprattutto per integrarle e modificarle alla luce dell'esperienza di questi primi anni di applicazione.

Decisioni sui ricorsi: inadempimenti. In riferimento ad alcune proprie decisioni, l'Autorità è intervenuta a seguito della segnalazione di alcuni ricorrenti che hanno lamentato o un mancato riscontro alle decisioni dell'Autorità o un inesatto adempimento delle stesse, provvedendo a definire la vicenda, precisando altresì, ove necessario, gli specifici termini dell'adempimento e ricordando che l'inosservanza dei provvedimenti dell'autorità è penalmente sanzionata (art. 37 l. n. 675/1996); in caso di prolungato silenzio o inadempimento da parte del titolare del trattamento ha proceduto invece alla trasmissione degli atti alla procura della Repubblica competente.

Altri procedimenti attivati a seguito delle decisioni emesse in riferimento ai ricorsi ex art. 29. Spesso la decisione emessa in ordine al ricorso consente all'Autorità, al di là della valutazione delle pretese fatte valere ai sensi dell'art. 13, di venire a conoscenza (attraverso l'esame di atti e documenti) della complessiva attività di trattamento svolta dal titolare, determinando così l'instaurazione, dopo la decisione del ricorso, di autonomi procedimenti di segnalazione ai sensi dell'art. 31 della legge n. 675/1996, miranti a valutare il corretto adempimento di tutte le prescrizioni previste dalla legge n. 675/1996. Si tratta di procedimenti che, pur richiedendo tempi più lunghi rispetto a quelli prescritti per la decisione sui ricorsi, spesso hanno consentito all'Autorità di mettere a fuoco, ben al di là del caso di specie, le problematiche relative alla protezione dei dati riferite ad interi settori.

Trattamenti di cui all'art. 4. Seppur più raramente, pervengono ancora ricorsi relativi ai particolari tipi di trattamento enumerati nell'art. 4, comma 1, della legge n. 675/1996, nei cui confronti non sono invero direttamente proponibili al titolare del trattamento né le istanze ex art. 13, né i ricorsi ai sensi dell'art. 29 (trattamenti svolti presso uffici giudiziari, forze di polizia, organi preposti alla sicurezza dello Stato). In questi casi è risultata quindi inevitabile la dichiarazione di inammissibilità del ricorso stesso, anche se il Garante, sulla base del comma 2 del medesimo art. 4, si è sempre riservato la possibilità di verificare, con riguardo ai principi di cui all'art. 9 della legge, la correttezza dei trattamenti svolti.

Riesame delle decisioni del Garante. È stata posta da alcuni ricorrenti la questione del riesame o della modifica delle decisioni dell'Autorità, specie con riguardo alla determinazione delle spese e dei diritti allo stesso inerenti. In proposito, questa Autorità ha rilevato che non è possibile dare corso a tali istanze e che le stesse devono essere considerate improponibili. Una volta adottata la decisione di cui all'art. 29, comma 4, della legge n. 675/1996, il riesame compete unicamente al tribunale ordinario eventualmente investito con l'opposizione ai sensi del comma 6 del medesimo articolo.

62 Impugnazione dei provvedimenti dell'Autorità

Come già rilevato nelle precedenti relazioni, si conferma che il numero di provvedimenti dell'Autorità oggetto di impugnazione (e specificamente di decisioni relative a ricorsi ex art. 29) è molto limitato. Peraltro, il monitoraggio al riguardo non può essere del tutto preciso in quanto non di tutte le impugnazioni proposte nei confronti dei predetti provvedimenti è giunta necessariamente notizia all'Autorità. Va ancora una volta rimarcato (come già rilevato nella *Relazione 2000*) che l'atipicità del procedimento di cui all'art. 29 della legge n. 675/1996, la peculiarità del Garante e del suo ruolo di autorità amministrativa indipendente pongono, dal punto di vista processuale, questioni nuove e controverse come quella, già segnalata l'anno scorso, della legittimazione passiva del Garante, cioè la possibilità per lo stesso di costituirsi innanzi ai tribunali o alla Corte di cassazione per difendere le ragioni giuridiche dei provvedimenti opposti (secondo la particolare procedura di cui al medesimo art. 29, comma 6).

Tale tema, peraltro, è già stato posto all'attenzione della Corte di cassazione in relazione allo sviluppo di due ricorsi, già decisi dal Garante, opposti successivamente in tribunale e infine oggetto, appunto, di ricorso per cassazione.

Alla luce di questa situazione, ancora in attesa di un assestamento definitivo, il Garante, nell'adunanza del 17 gennaio 2002, ha convenuto di proseguire nella linea fin qui seguita di costituirsi in giudizio solo per quanto riguarda questioni di diritto legate alla generale e corretta applicazione della legge n. 675/1996 e dei principi di garanzia da questa affermati, tralasciando di regola di entrare nel merito di profili puramente di fatto o relativi unicamente a determinati rapporti fra le parti.

Nei casi in cui non si pongano, invece, le predette questioni di diritto, l'Autorità si è riservata di inviare una memoria in merito all'Avvocatura dello Stato per richiamare l'illustrata posizione dell'Autorità e per rimettere alla stessa, nei casi dubbi, una prima valutazione sull'opportunità di una costituzione.

Va peraltro richiamata in questa sede l'importante sentenza della Corte di cassazione (sez. I civ. 30 giugno 2001, n. 8889), che, pur dichiarando inammissibile il ricorso incidentale del Garante (senza peraltro affermare principi contrastanti con la sopra prospettata legittimazione passiva di quest'ultimo), ha accolto il ricorso proposto dall'interessata, rigettando definitivamente l'opposizione proposta da un editore contro il provvedimento del Garante del 19 aprile 1999. La decisione della Suprema Corte ha confermato, nella sostanza, l'impostazione seguita dall'Autorità, ribadendo la piena applicazione delle disposizioni della legge n. 675/1996 anche agli archivi ed ai trattamenti svolti in ambito giornalistico, riconoscendo così la possibilità di esercitare gli specifici diritti tutelati dall'art. 13 della legge n. 675 anche nei confronti di dati personali trattati a tale fine (con particolare riguardo al diritto di accesso, integrazione ed eventuale correzione di dati inesatti).

Attività ispettive e applicazione di sanzioni amministrative

63 La programmazione delle ispezioni e i risultati

L'attività ispettiva del Garante è stata influenzata, nell'anno 2001, dalle norme organizzative che hanno definito la struttura dell'Ufficio, le competenze delle articolazioni interne e le modalità della gestione. In particolare, la delibera n. 5 del 2001 ha determinato i rapporti tra i dipartimenti giuridici dell'Autorità e il dipartimento vigilanza e controllo, attribuendo ai primi la competenza a provvedere alle attività preliminari e istruttorie, con particolare riferimento alla figura del "responsabile del procedimento", e al secondo la responsabilità della fase dell'intervento.

Per *attività ispettive* si intendono, come noto, gli interventi esterni effettuati dal Garante nei luoghi dove si svolgono i trattamenti, classificabili in cinque principali tipologie, la cui scelta è determinata in ragione del fine istituzionale da raggiungere ed è informata a principi di *proporzionalità*, *adeguatezza* e *gradualità*. In particolare, si distinguono sopralluoghi (con o senza preavviso), accessi alle banche di dati, collaborazioni, investigazioni e indagini conoscitive.

I *sopralluoghi con preavviso*, effettuati sulla base del disposto dell'art. 32, comma 1, della legge, hanno natura collaborativa e consistono nell'invio di funzionari del Garante nei luoghi dove si svolge il trattamento per procedere, di concerto con il titolare o il responsabile, all'acquisizione diretta di informazioni e di documenti. Si tratta di una procedura utilizzata quando sono necessarie descrizioni analitiche alle quali titolare e responsabile potrebbero avere difficoltà a rispondere in modo esaustivo.

Nel 2002, sopralluoghi con preavviso sono stati effettuati nei confronti di sei comuni – individuati con metodo casuale, attraverso un sorteggio che ha tenuto conto della collocazione geografica (comuni del centro-nord e comuni del centro-sud) e del numero di abitanti (fino a 20.000 abitanti, fino a 200.000, sopra i 200.000) – in occasione del 14° Censimento generale della popolazione e dell'8° Censimento dell'industria e dei servizi, per controllare le modalità concrete con cui i rilevatori hanno acquisito i dati dalle famiglie e dalle aziende, l'adeguatezza delle istruzioni impartite dall'Istat agli uffici di censimento e le misure di sicurezza adottate effettivamente dai comuni.

I *sopralluoghi senza preavviso* sono disposti con i poteri dell'art. 13, comma 1, della legge 24 novembre 1981, n. 689, e sono finalizzati anche al controllo dell'osservanza delle disposizioni per la cui violazione l'art. 39 della legge n. 675 prevede la sanzione amministrativa del pagamento di una somma di denaro.

Si fa riferimento, quindi, alle ipotesi di mancata o infedele risposta alle richieste di informazioni e di esibizione di documenti (art. 32, comma 1), di mancata o irregolare informativa (art. 10), di rivelazione dello stato di salute da parte di medico diverso da quello designato dall'interessato o dal titolare (art. 23, comma 2) e di cessione di dati ad altro titolare a seguito di cessazione del trattamento senza la prescritta notifica al Garante (art. 16, comma 3). A tali fattispecie si sono aggiunti, a decorrere dal 1° febbraio 2002, i casi di omessa o incompleta notificazione a seguito dell'emanazione del d.lg. n. 467/2001. Il decreto, infatti, ha modificato l'originaria formulazione dell'art. 34 della legge, prevedendo la sanzione amministrativa del pagamento di una somma da dieci a sessanta milioni di lire per chi non provveda con tempestività e completezza a comunicare al Garante l'inizio del trattamento, il trasferimento di dati all'estero ovvero la loro destinazione in caso di cessazione.

Nel corso dei sopralluoghi, i dirigenti ed i funzionari del Garante possono effettuare diversi tipi di operazioni tecniche, tra cui assumere informazioni e procedere a ricognizioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici.

63

Tali modalità sono state utilizzate per il ciclo di ispezioni, peraltro non ancora concluso, in materia di videosorveglianza. Si è trattato di accertamenti senza preavviso eseguiti nei confronti di aziende, enti e associazioni che hanno installato telecamere in luoghi pubblici o aperti al pubblico in mancanza dell'informativa prevista dall'art. 10 della legge oppure rendendo un'informativa incompleta.

Le violazioni constatate riguardano, in particolare, due società e un ente pubblico operanti nel settore del grande trasporto, due supermercati appartenenti a catene di distribuzione presenti su tutto il territorio nazionale, due banche e una associazione che gestisce un impianto sportivo di proprietà pubblica.

Gli *accessi alle banche dati* sono effettuati in base ai poteri dell'art. 32, comma 2, della legge. La norma fa riferimento anche ad "altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo". In tali casi l'intervento può essere eseguito anche contro la volontà degli interessati, previa autorizzazione del presidente del tribunale territorialmente competente (art. 32, comma 3, della legge), oppure dotandosi dell'assenso scritto e informato del titolare o del responsabile del trattamento (art. 15, comma 1, d.P.R. n. 501/1998).

A differenza dell'anno precedente, nel 2001 non è emersa la necessità di effettuare accertamenti con decreto giudiziario, procedura che del resto non sempre risponde ai requisiti di speditezza di cui normalmente necessitano gli interventi del Garante e che si intende riservare ai casi di maggiore complessità.

Ulteriori tipologie ispettive sono rappresentate dalle richieste di *collaborazioni* che pervengono da autorità giudiziarie o di polizia e dalle *investigazioni di polizia giudiziaria*.

Con riferimento a queste ultime, sono state inviate due informative per i reati di trattamento illecito di dati personali (art. 35 della legge) e di inosservanza dei provvedimenti del Garante (art. 37).

Va evidenziato, peraltro, che il personale addetto agli accertamenti dell'art. 32 riveste, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria (art. 33, comma 6-*bis*) e che tali qualifiche sono attualmente rivestite da tre unità.

Le *indagini conoscitive*, infine, sono interventi esterni a carattere collaborativo disposti per verificare lo stato di attuazione della legge in determinati settori che possono concludersi anche con delibere di portata applicativa generale nei confronti di tutti i soggetti che svolgono trattamenti della specie considerata.

Tutte le ispezioni del Garante vengono effettuate sulla base di programmi che determinano, per ciascuna tipologia, le priorità e i criteri informatori ai quali l'Ufficio deve attenersi. Così, i sopralluoghi collaborativi vengono di regola disposti quando, per acquisire gli elementi necessari, non sia ritenuto utile rivolgere una richiesta di informazioni o di esibizione di documenti, mentre si procede ai sopralluoghi senza preavviso ed agli accessi alle banche dati quando non sia ritenuto opportuno procedere alla richiesta di informazioni o di esibizione di documenti, o quando le informazioni o i documenti richiesti o pervenuti siano ritenuti incompleti e non veritieri. Le collaborazioni su richiesta della magistratura e delle forze di polizia vengono eseguite dando priorità ai contesti dai quali emergono notizie di reato.

L'Ufficio si avvale anche della collaborazione di altri organi dello Stato quando ciò sia necessario per assicurare la speditezza e la completezza dei controlli. In tale ambito, si colloca il protocollo d'intesa che l'Autorità è in procinto di sottoscrivere con la Guardia di finanza che, su richiesta del Garante, collaborerà per l'accertamento delle violazioni amministrative e penali, per lo sviluppo delle attività delegate dall'autorità giudiziaria e nell'esecuzione delle indagini conoscitive sullo stato di attuazione della legge in determinati settori.

64 L'attività sanzionatoria del Garante

Nel rendere conto dei poteri sanzionatori del Garante, occorre preliminarmente evidenziare un momento di importante intervento sul piano normativo con la pubblicazione in Gazzetta Ufficiale del decreto legislativo del 28 dicembre 2001, n. 467, che ne ha in parte modificato l'impianto incidendo su due profili (con effetti a decorrere dal 1° febbraio 2002): la natura della sanzione (penale o amministrativa) e il *quantum* della sanzione amministrativa applicabile.

Per quanto concerne il primo, con l'art. 12 del decreto, è stato depenalizzato il reato previsto all'art. 34 della legge n. 675/1996 prevedendo che in caso di omessa o incompleta notificazione venga irrogata una "sanzione amministrativa del pagamento di una somma da lire dieci milioni a sessanta milioni e la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione", mentre si è mantenuta la sanzione penale nel caso di "falsità nelle dichiarazioni e notificazioni al Garante" (art. 37-*bis* della legge, introdotto dall'art. 16 del d.lg.).

La novella ha riguardato anche la materia del reato derivante da omessa adozione di misure necessarie alla sicurezza dei dati (art. 36). L'art. 14 del decreto legislativo, pur mantenendo la previsione della sanzione penale (arresto sino a due anni), ha trasformato il delitto in contravvenzione punita con la pena alternativa (ammenda da lire dieci milioni a lire ottanta milioni). Ma l'elemento di novità forse più rilevante che si rinviene nel nuovo testo dell'art. 36 della legge, è nel fatto che con esso si è introdotto una sorta di "ravvedimento operoso", all'esito del quale si può pervenire all'estinzione del reato.

Il nuovo sistema prevede che all'autore del reato, all'atto dell'accertamento o in casi di maggiore complessità anche con successivo atto del Garante, venga impartita una prescrizione che fissa un termine (non eccedente il tempo tecnicamente necessario, prorogabile in caso di oggettiva complessità e comunque non superiore a sei mesi) per la regolarizzazione di quanto omesso. Nei sessanta giorni successivi alla scadenza di detto termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari ad un quarto del massimo dell'ammenda. L'adempimento e il pagamento estinguono il reato.

Circa il secondo aspetto sopra segnalato, l'art. 17 del decreto legislativo ha modificato i commi 1 e 2 dell'art. 39 della legge, per quanto riguarda l'ammontare delle sanzioni amministrative ivi previste. Si è infatti preso atto che le somme contemplate nell'impianto originario della legge del 1996 erano a volte inadeguate rispetto alle realtà economiche a cui erano rivolte e, dunque, rischiavano di risultare totalmente inefficaci a fini di prevenzione delle violazioni in materia di trattamento di dati personali.

Allo stato, pertanto, in caso di violazione delle norme sull'informativa (artt. 10 e 39, comma 2), la sanzione prevista è da lire sei milioni a lire diciotto milioni, mentre nel caso in cui chiunque vi sia tenuto ometta di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi dell'art. 29, comma 4 (cioè a seguito della presentazione di un ricorso), ovvero ai sensi dell'art. 32, comma 1 (perché occorre ai fini dell'espletamento dei compiti del Garante) la sanzione introdotta varia da lire sei milioni a diciotto milioni.

Le somme dovute in caso di violazione dell'art. 23, comma 2, della legge (dati inerenti alla salute), non hanno invece subito modifiche nel loro ammontare.

Per quanto riguarda l'*iter* del procedimento amministrativo per l'applicazione delle sanzioni amministrative si continuano ad osservare, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni.

Venendo ora a descrivere l'attività operativa effettuata in materia di sanzioni amministrative nel corso del 2001, l'Autorità, a seguito di accertamenti, segnalazioni e non ultimo all'esito di indagini conoscitive compiute d'ufficio, ha provveduto a far notificare una serie di "contestazioni di violazioni amministrative", contestando,

64

nei casi di volta in volta oggetto del procedimento in questione, atti quali l'aver omesso di fornire le necessarie ed idonee informazioni agli interessati circa il trattamento dei loro dati personali (art. 10 l. n. 675/1996), ovvero l'inadempimento a fronte di richieste di informazioni formulate dall'Ufficio così come previsto dall'art. 32, comma 1, della legge medesima.

Sono stati inoltre adottati, con deliberazione dell'Autorità, alcuni provvedimenti ai sensi dell'art. 18 della legge n. 689/1981 (ordinanza-ingiunzione di pagamento) in relazione ai quali la preliminare attività di accertamento e contestazione era stata effettuata da altri organi dello Stato (Carabinieri, Polizia di Stato e Guardia di finanza) che, in occasione di controlli amministrativi effettuati nell'ambito di attività istituzionali, avevano tra l'altro rilevato e provveduto a contestare ai trasgressori violazioni della normativa sulla protezione dei dati personali.

Con riguardo alle risultanze di detta attività, a prescindere dai procedimenti che sono ancora in corso ed a quelli attivati nei primi mesi del 2002, in alcuni casi i trasgressori fatti oggetto delle contestazioni si sono avvalsi della facoltà di effettuare il pagamento in misura ridotta (art. 16 l. n. 689/1981), mentre in altri hanno inviato memorie e scritti difensivi esaminati i quali l'Ufficio ha ritenuto di dover accogliere le motivazioni addotte e concludere il procedimento amministrativo con l'archiviazione dello stesso.

Per quanto attiene alle ordinanze-ingiunzione, non avendo esse formato oggetto di impugnazione (ai sensi dell'art. 22-*bis* della legge n. 689/1981), si sta predisponendo quanto necessario per il recupero forzato delle somme ai sensi dell'art. 27 della legge n. 689/1981.

La prevista destinazione dei proventi delle sanzioni, nella vigenza della formulazione originaria dell'art. 39, comma 3, della legge n. 675/1996, risultava espressamente limitata agli illeciti di cui ai commi 1 e 2 dell'art. 39 medesimo.

Con l'entrata in vigore del decreto legislativo n. 467/2001, la competenza del Garante ad applicare le sanzioni e a ricevere il rapporto ai sensi dell'art. 17 della legge n. 689/1981, è stata estesa all'intero Capo VII della legge sulla protezione dei dati personali, derivandone anche per tali somme l'estensione del vincolo di destinazione anzidetto.

L'attività di informazione e comunicazione

65 Profili generali

L'impegno del Garante per una comunicazione efficace e capillare ha risposto, anche nel corso del 2001, da una parte all'esigenza di adempiere ai compiti attribuiti all'Autorità, in linea anche con i principi fissati dalla legge n. 150 del 2000 sulla comunicazione pubblica, e dall'altra alla primaria necessità di assicurare ai cittadini, ai consumatori, al mondo imprenditoriale, alla pubblica amministrazione un puntuale lavoro di chiarificazione sulle modalità di applicazione della legge, sulle problematiche collegate all'uso indiscriminato delle nuove tecnologie, sul rispetto dei diritti introdotti dalla normativa sulla tutela dei dati personali. Gli obiettivi rimangono sempre quelli che hanno caratterizzato l'attività di informazione del Garante dalla sua nascita: salvaguardia della libertà e della dignità della persona, gestione trasparente delle banche dati, uso non discriminatorio delle informazioni personali, specie di quelle più delicate.

Le grandi questioni internazionali e i tragici avvenimenti occorsi nel settembre 2001 hanno caratterizzato parte dell'impegno comunicativo dell'Autorità, in particolare per mettere in luce alcuni delicati aspetti sollevati dal dibattito sul rapporto tra sicurezza e *privacy*. Ma costante è stata anche l'azione di intervento sul difficile bilanciamento tra diritto di cronaca e rispetto della *privacy* e tra mondo produttivo e rispetto dei cittadini e dei lavoratori.

Sono state utilizzate diverse forme di comunicazione: da quelle tradizionali (comunicati stampa, *newsletter*, conferenze stampa) a quelle multimediali ed interattive, diffondendo e rendendo consultabili *on line* sul proprio sito *web* documentazione e pubblicazioni.

L'attività di informazione ha mantenuto la scelta di un linguaggio rigoroso e insieme attento ad una funzione divulgativa, dei principi sanciti dall'Autorità e dei processi e delle ragioni alla base delle sue decisioni e iniziative, così come delle innovazioni, in termini di procedure e prassi, che la legge sulla protezione dei dati ha introdotto.

La comunicazione ha dunque puntato a stimolare l'applicazione della legge n. 675/1996 da parte di pubbliche amministrazioni e mondo dell'impresa, con il rigoroso rispetto degli obblighi previsti ai fini di un'effettiva tutela della protezione dei dati personali, esigenza irrinunciabile per avviare processi di trasformazione e per la definizione di un nuovo sistema di relazioni tra istituzioni e cittadini.

Le tematiche che più hanno sollecitato il mondo dell'informazione hanno riguardato il settore delle telecomunicazioni, i rischi della raccolta di dati su *Internet* e i cosiddetti "tracciamenti invisibili", i rapporti tra informazione, riservatezza e dignità delle persone, la tutela dei soggetti deboli, la tutela dei consumatori, l'uso delle nuove tecnologie di raccolta dei dati (biometria), i dati genetici, il *direct marketing* e l'informazione commerciale in generale, la *privacy* nel rapporto di lavoro e il controllo sui lavoratori, la videosorveglianza, l'attività sanzionatoria del Garante rispetto alle violazioni delle norme sulla *privacy,* le grandi reti della pubblica amministrazione, le schedature di massa.

Nel periodo dal gennaio 2000 ad aprile 2001, le pagine dedicate alla *privacy* dai maggiori quotidiani e periodici nazionali sono state circa 5000, delle quali oltre 1800 dedicate specificamente all'attività del Garante. Le prime pagine dedicate ai temi della *privacy* sono state circa 700.

La tipologia dei prodotti informativi è stata, come si è detto, ampia e differenziata.

La *Newsletter* settimanale è al suo terzo anno di pubblicazione. Illustrando gli interventi del Garante in chiave divulgativa, essa ha consentito di raggiungere un pubblico sempre più ampio, composto non soltanto, come in un primo tempo, di giornalisti, amministratori pubblici e professionisti, ma anche di operatori del settore creditizio, industriale, di rappresentanti delle associazioni di categoria e di semplici cittadini.

65

Affiancando la comunicazione tradizionale, realizzata attraverso comunicati stampa, con una di tipo più ampio e approfondito, la *Newsletter* si è rivelata oltre che uno strumento di comunicazione, anche una sorta di "archivio" di consultazione relativamente ai diversi ambiti di applicazione della legge n. 675 e ai variegati aspetti connessi con la tutela della riservatezza sui quali l'Autorità è intervenuta. La possibilità di consultare la *Newsletter on-line* ha facilitato la diffusione delle informazioni.

Le *Newsletter* diffuse tra il 1° gennaio 2001 e il 30 marzo 2002 sono state 54, mentre i comunicati stampa 39.

Nel 2001, è giunto alla sua quinta edizione l'archivio digitale "*Cittadini e Società dell'informazione*", che contiene la documentazione integrale relativa all'attività del Garante, alla normativa nazionale ed internazionale di riferimento e alle pubblicazioni fin qui realizzate. L'archivio digitale ipertestuale è distribuito su *CD-Rom* multipiattaforma ed è 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. 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. Un lavoro di catalogazione dei documenti consente infine, grazie agli strumenti messi a disposizione da *Acrobat*, di effettuare ricerche *full text* all'interno del *CD-Rom*.

Il successo del *CD-Rom*, che viene inviato gratuitamente a chiunque ne faccia richiesta, è testimoniato dall'alto numero di copie distribuite (nel 2001, oltre 9.000) ad amministrazioni pubbliche, al settore privato, a liberi professionisti e a semplici cittadini.

Tra le attività di comunicazione va ricordata inoltre la pubblicazione del Bollettino "*Cittadini e Società dell'Informazione*" che ha raggiunto il numero 26 e raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa ed altra documentazione.

Allo scopo di far conoscere in maniera approfondita e sistematica l'attività svolta sia nell'interpretazione dei principi posti in materia di *privacy* dalla normativa nazionale e comunitaria, sia negli indirizzi per la loro concreta applicazione alle specifiche fattispecie, è stata recentemente avviata un'attività di massimazione, esplicata in chiave tecnico-giuridica, dei provvedimenti emessi nel corso degli anni.

Questa attività, per la cui realizzazione ci si avvale dell'opera di specifiche professionalità, è preordinata alla formazione di una rassegna di giurisprudenza che, attraverso un'articolazione in voci e sottovoci, permetta la rapida e corretta individuazione degli argomenti trattati e delle decisioni assunte.

L'opera, che arricchisce il panorama delle pubblicazioni curate dal Garante, e la cui edizione, anche su supporto informatico, è imminente, si indirizza in particolar modo ad una platea di utenti costituita da giuristi, ordini professionali, operatori del diritto, imprese, istituzioni pubbliche e private.

L'attenzione ad un rapporto diretto con la società riveste, inoltre, un'importanza fondamentale inserendosi in quel modello di istituzione aperta, vicina ai cittadini, attenta ai processi in atto e alle nuove prospettive, perseguito dall'Autorità fin dall'inizio della sua attività. La messa a disposizione sul sito di una notevole quantità di documentazione, con continui aggiornamenti in tempo reale, ha avuto, comunque, un parziale effetto deflativo sul numero dei contatti telefonici giornalieri. In questo senso, il servizio di *help-desk* ha fornito in passato un contributo fondamentale, mentre risulta ora necessario attivare forme di contatto più efficaci.

È infatti imminente l'operatività di un ufficio per le relazioni con il pubblico collegato con un *call-center*, avente il compito di favorire ulteriormente modalità di interazione ancora più funzionali e dirette con tutti i cittadini che avranno bisogno di informazioni, strumenti illustrativi e divulgativi, così sviluppando un flusso costante di informazione verso l'esterno e consentendo, nello stesso tempo, l'acquisizione di problematiche ed esigenze provenienti dalla società civile, dal mondo delle imprese, dalla ricerca, dalle pubbliche amministrazioni.

66 Seminari, convegni ed altre iniziative

L'attività dell'Autorità collegata ai seminari, convegni e altre iniziative ha visto, nel corso del 2001 e nei primi mesi del 2002, una serie di importanti occasioni di confronto e approfondimento sui temi di maggiore impatto.

In linea con l'obiettivo di promuovere la conoscenza della legge e di diffonderla presso cittadini ed operatori pubblici e privati, il Garante ha confermato la sua presenza in importanti manifestazioni.

Il Forum P.A. edizione 2001, svoltosi a Roma dall'8 al 12 maggio, ha visto una significativa presenza dell'Autorità. Il Forum ha infatti dedicato uno specifico convegno al tema "*I nuovi diritti nella Società dell'informazione: rispetto, qualità, trasparenza nel rapporto tra cittadini e pubblica amministrazione dopo la legge sulla privacy*", svoltosi l'8 maggio, cui hanno partecipato oltre 300 congressisti. Anche il Master, curato dal Servizio e tenuto dal Segretario generale e da due dirigenti dell'Ufficio, ha registrato la nutrita partecipazione di amministratori locali e rappresentanti della p.a.

L'Autorità è stata anche presente al COM-P.A., Salone della comunicazione pubblica, svoltosi a Bologna dal 19 al 21 settembre, e allo Smau di Milano, svoltosi dal 19 al 23 ottobre, nell'ambito del quale il prof. Gaetano Rasi ha tenuto una relazione sulla carta elettronica e la firma digitale.

Va ricordato, inoltre, che anche il 2001 ha registrato la costante presenza di rappresentanti del Garante e di funzionari dell'Ufficio in innumerevoli convegni, seminari ed incontri organizzati da università, associazioni di categoria o organismi allo scopo di approfondire e discutere i diversi aspetti attuativi ed interpretativi della legge n. 675/1996.

Dal 24 al 26 settembre del 2001, l'Autorità ha partecipato alla XXIII Conferenza internazionale delle Autorità Garanti, svoltasi a Parigi e dedicata al tema "Dati personali – Diritti umani". La Conferenza si è articolata in varie sessioni dedicate, tra l'altro, alle biometrie, alle tecniche di localizzazione, al *cybercrime*, alla videosorveglianza, alla protezione dei dati sanitari, alle nuove tecnologie, alla democrazia elettronica; nell'ambito della Conferenza, il Prof. Stefano Rodotà ha presieduto la sessione *"One world, One Privacy"* – ideale continuazione del tema della Conferenza di Venezia – dedicata alla necessità di perseguire regole comuni universalmente condivise per la salvaguardia della *privacy;* il Segretario generale, Giovanni Buttarelli, ha tenuto invece una relazione sulla democrazia elettronica.

Nella Conferenza di primavera delle Autorità europee per la *privacy*, svoltasi ad Atene il 10 e 11 maggio 2001, i Garanti hanno ribadito le proprie preoccupazioni in relazione ai tempi di conservazione dei dati di traffico su Internet ribadendo la validità del "modello europeo" di protezione dei dati personali, accolto anche nella Carta europea dei diritti fondamentali

Tra i diversi convegni ai quali l'Autorità ha preso parte vanno poi citati, tra gli altri, il convegno su la "E-society una rivoluzione da governare" presso il Ministero delle comunicazioni, nell'aprile 2001; il convegno organizzato dall'Associazione industriali di Genova su "Internet e controllo del personale", dell'aprile 2001, che ha visto come relatore il Prof. Gaetano Rasi; il convegno della Confindustria del luglio 2001 dedicato a "Lo Statuto dei lavoratori alla prova della net economy"; il Forum sull'informazione, organizzato a Gubbio, dalla Federazione Nazionale della stampa nell'ottobre 2001, su "Crisi internazionale e ruolo dell'informazione"; il convegno organizzato il 5 ottobre dalla provincia di Treviso e dall'Unione stampa cattolica italiana su "Minori e informazione", e l'incontro nazionale dei fotografi italiani su "Fotogiornalismo e privacy", ai quali ha partecipato il dott. Mauro Paissan; il seminario organizzato nel gennaio 2002 da Mediaset su "Il ruolo delle Autorità indipendenti nell'ordinamento italiano e nella prospettiva europea", che ha visto la presenza del Prof. Stefano Rodotà e del Prof. Giuseppe Santaniello; il convegno dedicato a privacy, salute e assicurazioni svoltosi a Napoli nel febbraio 2002.

66

Grande rilevanza per la complessità e la delicatezza della materia in discussione, ha assunto il convegno organizzato dal Consiglio nazionale delle ricerche, in collaborazione con l'*Einstein Institute for Science, Health & the Courts* (EINSHAC), con il patrocinio del Garante, intitolato "Implicazioni giuridiche e psicosociali della Genetica Umana". La Conferenza, svoltasi il 21-22 marzo 2002 presso la sede del Garante, alla quale hanno partecipato ricercatori, genetisti, medici, psicologi e magistrati di varie nazionalità, oltre ai membri dell'Autorità, ha affrontato le questioni legate all'uso sempre più frequente dei test genetici, anche a scopi non esclusivamente medici: la tutela dei dati genetici; la creazione di banche dati per la lotta anticrimine; le indagini su intere popolazioni; la cosiddetta medicina predittiva.

Un'importante occasione per approfondire le novità, in termini di semplificazioni per le imprese e di maggiori garanzie per i cittadini, introdotte dal recente d. lg. n. 467/2001, che integra e modifica la disciplina sulla *privacy* in Italia, è stata la conferenza stampa tenutasi il 30 gennaio 2002.

L'impegno per una comunicazione efficace e quanto più capillare deve, comunque, tener conto della ancora non completa penetrazione, in alcuni strati della società, della legge e degli strumenti di tutela da essa offerti. Un'indagine commissionata dal Garante sull'impatto determinato dalla legge sui cittadini italiani ha mostrato un buon livello di conoscenza della rete (67% degli intervistati) e ha indicato la televisione come canale preferenziale di acquisizione di notizie.

Si è posta, quindi, l'esigenza di un'azione di comunicazione sui *media* che utilizzi in maniera ancora più efficace questa fonte di conoscenza. In questo senso la collaborazione avviata con la Presidenza del Consiglio per una campagna di comunicazione istituzionale ha proprio l'intento di rispondere a questa esigenza strategica, per la quale è stata prevista anche la realizzazione di *depliant* divulgativi da distribuire al pubblico.

67 Il sito *Internet* dell'Autorità

Il 2001 è stato l'anno di pieno funzionamento del sito *web* del Garante, consultabile all'indirizzo *www.garanteprivacy.it* o *www.dataprotection.org*.

Internet si è dimostrato uno strumento insostituibile di comunicazione e diffusione su larga scala, nazionale ed internazionale, delle informazioni e della cultura della *privacy*, in grado spesso di generare il primo contatto tra il cittadino e l'Autorità.

L'anno che è trascorso ha visto aumentare i visitatori, pari a 4.500/5.000 al giorno, il 10% dei quali stranieri, che consultano una banca dati di provvedimenti e documenti anche multimediali ricca, aggiornata e coordinata.

La redazione, osservando le dinamiche di utilizzo del sito e le crescenti esigenze di diffusione delle informazioni, ha prodotto alla fine del 2001 un progetto per un nuovo *web* che terrà conto non solo della politica di sviluppo dell'*e-government*, ma anche dei criteri di usabilità ed accessibilità alle informazioni per tutti i portatori di *handicap*, come peraltro indicato in una serie di circolari della Presidenza del Consiglio dei ministri.

Nel progetto è stato dato particolare rilievo alla modularità grafica del nuovo sito, alla struttura gerarchica delle informazioni ed alla loro fruibilità, pensando un nuovo motore di ricerca che – basandosi sui principi dell'*information retrieval* – consenta il sicuro reperimento dei documenti non solo per parole del testo, ma anche per riferimenti normativi e schema di classificazione in combinazione fra loro attraverso gli operatori logici booleani con l'ausilio di un *thesaurus* giuridico costruito *ad hoc*.

Particolare spazio è stato poi dedicato alle funzionalità multimediali, come la predisposizione di un *video server* per la trasmissione in diretta *Internet* di eventi/seminari/convegni o "schede didattico-divulgative" sugli argomenti di maggior interesse od anche di "contributi monografici tecnico-giuridici".

Il progetto, qui sinteticamente descritto, esteso anche ad una nuova struttura della *Intranet* – già ricca di contenuti ed utilizzata abitualmente da tutto il personale – e del *workflow* documentale interno, fonte di produzione dei testi e dei contenuti del sito web, è stato aggiudicato alla fine del mese di marzo di quest'anno per essere *on-line* nel prossimo mese di ottobre.

Compito della redazione, una volta predisposta l'infrastruttura informatica del nuovo *web* (prima fase della realizzazione) e adeguatamente potenziata nelle risorse, sarà quella di "popolare" un nuovo database multilingua, classificando ogni documento e costruendo il *thesaurus* e le sinapsi di relazione tra le informazioni.

La redazione *web* ha poi approfondito l'uso dei sofisticati applicativi *software* per l'impaginazione tipografica, diventando un vero e proprio "centro stampa" interno. Tutti i bollettini "*Cittadini e Società dell'Informazione*" dall'anno 2001 sino ad oggi, il volume "*Privacy e nuove tecnologie*" distribuito in occasione dell'edizione 2001 dello S.M.A.U., la "*Relazione 2000*" come il presente testo, sono stati realizzati dalla redazione: impaginazione, collazione delle bozze, pre-stampa, sino alla produzione dell'impaginato con il "visto si stampi" da inviare allo stampatore. Il risparmio si concretizza non solo in termini economici, ma soprattutto in termini di rapidità, conoscenza della materia per la correzione delle bozze e correttezza formale del prodotto.

La gestione amministrativa dell'ufficio

68 I regolamenti del Garante e la nuova organizzazione dell'Ufficio

L'organizzazione e il funzionamento dell'Ufficio del Garante, il trattamento giuridico ed economico del personale e la gestione amministrativa e contabile sono stati definiti con tre complessi regolamenti approvati il 28 giugno 2000 (reg. nn. 1/2000, 2/2000 e 3/2000, pubblicati nella *G.U.* n. 162 del 13 luglio 2000).

Nel delineare il proprio modello organizzativo e nel definire la disciplina dei rapporti di lavoro, il Garante era consapevole dell'esigenza di sottoporre a successive verifiche e ad eventuali modifiche, per così dire *in progress*, l'assetto ordinamentale ed organizzativo dell'Ufficio, avvalendosi dell'esperienza maturata in sede di prima applicazione dei regolamenti.

In linea con tale indirizzo, nel corso del 2001 è emersa l'esigenza di ridefinire alcuni limitati aspetti dell'organizzazione e dell'ordinamento professionale del personale dipendente, tenendo anche conto della indubbia rilevanza dell'evoluzione normativa che ha interessato e continua ad interessare le pubbliche amministrazioni e dell'elaborazione dottrinale e giurisprudenziale cui essa si accompagna.

Alcune modifiche apportate ai regolamenti nn. 1/2000 e 2/2000 (pubblicate nella *G.U.* n. 185 del 10 agosto 2001) mirano infatti a completare la disciplina relativa all'affidamento di mansioni superiori e di funzioni dirigenziali, regolando gli effetti economici da ciò derivanti, sulla base del principio previsto dall'art. 52 del d.lg. n. 165/2001 ("*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*").

Nel colmare tale lacuna normativa, a conclusione di una lunga riflessione sono state delineate le procedure selettive interne per gli avanzamenti di carriera del personale in servizio presso l'Ufficio, sulla base delle analoghe previsioni contenute nei regolamenti di altre autorità indipendenti. Tali modifiche regolamentari prevedono la possibilità per il personale che non abbia demeritato e che abbia maturato severi requisiti di anzianità e di professionalità di partecipare alla selezione per l'accesso all'area e qualifica immediatamente superiori. Tale possibilità non è però automatica, ma è rimessa alle autonome valutazioni dell'Autorità, la quale può decidere di bandire con cadenza annuale procedure selettive nel limite del 40% dei posti disponibili nelle varie qualifiche.

Altre modifiche rafforzano le tutele a favore delle lavoratrici madri, nello spirito delle disposizioni contenute nel testo unico delle disposizioni a tutela e sostegno della maternità e paternità (d.lg. 26 marzo 2001, n. 151), ovvero prevedono, mediante l'attribuzione di alcuni scatti stipendiali, un più ampio riconoscimento economico dell'esperienza maturata presso le amministrazioni di provenienza dal personale appartenente al contingente utilizzato dal Garante in sede di prima applicazione della legge n. 675/1996, inquadrato nel ruolo organico con effetto dal 1° settembre 2000.

Un'ulteriore conferma del peculiare approccio ai problemi organizzativi prima richiamato, è possibile trarla da altre due modifiche regolamentari volte al miglioramento della capacità di risposta dell'Ufficio e alla razionalizzazione dell'organizzazione interna. Tali modifiche, oltre ad alcuni interventi di carattere prevalentemente terminologico (concernenti la denominazione dei tre dipartimenti giuridici in relazione alla competenza per materia ad essi assegnata), hanno riguardato la separazione in due distinte unità organizzative del dipartimento vigilanza, controllo e registro generale dei trattamenti e la precisazione dei compiti del servizio "segreteria del collegio", quest'ultima deliberata in data 19 luglio 2001 e pubblicata nella *G.U.* del 14 novembre 2001.

Il regolamento n. 1/2000 del Garante, concernente l'organizzazione e il funzionamento dell'Ufficio, ha delineato un assetto organizzativo dell'Ufficio caratterizzato dalla presenza di 14 unità di primo livello (dipartimenti e servizi) e dalla possibilità di istituire unità temporanee di primo livello per lo svolgimento di specifici compiti e per il raggiungimento di obiettivi nel breve periodo.

Nella *Relazione 2000* è stata sottolineata la peculiarità di tale modulo organizzativo che tenta di conciliare

esigenze di certezza e continuità istituzionale con la necessaria flessibilità organizzativa. In sede di prima applicazione del regolamento, le scelte organizzative si sono orientate, per un verso, all'attuazione dell'assetto organizzativo e, per un altro verso, alla individuazione di soluzioni in grado di assicurare, nella fase di transizione, la realizzazione della missione istituzionale e il buon andamento dell'Autorità.

Sono state così individuate alcune unità temporanee di primo livello in relazione ad impegni anche internazionali dell'Autorità (partecipazioni a gruppi di lavoro in sedi internazionali o attività di natura regolamentare), ovvero all'imprescindibile esigenza di assicurare lo svolgimento di funzioni essenziali che attengono al rapporto con il cittadino, quali la decisione dei ricorsi ex art. 29 della legge n. 675/1996 e l'osservanza della legislazione in materia di tutela dei dati personali, rendendo disponibile, anche ad utenti esterni, la vasta produzione documentale e di materiale bibliografico, italiana e straniera, reperibile in materia di *privacy* (Progetto biblioteca).

Questi ultimi incarichi di funzioni dirigenziali, di durata annuale, sono cessati alla scadenza.

Sono stati presentati al T.a.r. del Lazio due ricorsi nei quali vengono dedotte censure nei confronti degli incarichi di direzione delle unità di primo livello e dell'affidamento degli incarichi di funzioni dirigenziali. Per quanto riguarda quest'ultimo ricorso, il T.a.r. del Lazio nell'udienza del 13 marzo 2002 ha preso atto della rinuncia dei ricorrenti all'istanza cautelare prodotta con il ricorso.

Da tempo è in atto una più ampia riflessione finalizzata al potenziamento della struttura organizzativa dell'Ufficio, anche alla luce dell'esperienza maturata in sede di prima applicazione del regolamento n.1/2000, ricorrendo altresì all'ausilio di due società di consulenza che hanno offerto un valido contributo conoscitivo che è stato oggetto di attenta analisi con la collaborazione delle stesse società che lo hanno curato. Su questa base, l'Autorità ha ultimato il lavoro preparatorio che porterà a completare entro poche settimane un meditato disegno di riorganizzazione e potenziamento dell'Ufficio che, traendo spunto dalla prima esperienza applicativa dei citati regolamenti, e in vista dei nuovi compiti derivanti dal d.lg. n. 467/2001 e dal più volte menzionato testo unico, permetterà di innovare nella gestione, valorizzando al tempo stesso l'autonomia e la responsabilità dei dirigenti, e di raggiungere ulteriori obiettivi.

69 Il bilancio, gli impegni di spesa e l'attività contrattuale

Il bilancio di previsione del 2001 è il primo elaborato secondo le direttive del regolamento 3/2000 – concernente la gestione amministrativa e la contabilità dell'Ufficio – con il quale si sono recepite le norme di principio contenute nel d.lg. n. 29/1993 (e successive modificazioni ed integrazioni), in materia di riforma della contabilità pubblica.

Detto regolamento attribuisce ai dirigenti un ruolo fondamentale sia nel processo di formazione del bilancio, considerato che tale documento è predisposto sulla base delle esigenze funzionali rappresentate dai dipartimenti e dai servizi, sia con riguardo all'acquisizione di beni e servizi.

Inoltre con deliberazioni del 14 marzo 2001 il Garante ha completato l'assetto organizzativo dell'Ufficio attribuendo al personale dirigenziale la titolarità dei dipartimenti e dei servizi di primo livello (così come individuati dal regolamento n. 2/2000).

Il bilancio 2001 è stato quindi predisposto tenendo conto di questo assetto organizzativo, delle diverse esigenze dei dipartimenti e dei servizi e, altresì, del completamento della presa di possesso dei locali dell'Autorità, adibendo gli stessi a sala-conferenze, biblioteca e ufficio per le relazioni con il pubblico. Il personale è stato incrementato di diciannove unità tra cui sette con contratto a tempo determinato, di cui due a livello dirigenziale, e dodici provenienti da amministrazioni pubbliche con provvedimenti per fuori ruolo o per comando, tra cui un magistrato, otto funzionari, tre operativi.

Risultato di questo maggior dinamismo nell'attività amministrativa del Garante è rappresentato dalle spese erogate, che sono passate dai 14 miliardi di lire (euro 7.230.500,00 circa) del 2000 ai 20 miliardi di lire (euro 10.330.000,00 circa) del 2001, con un incremento pari quasi al trenta per cento. Le spese per il personale, comprese le indennità spettanti ai componenti il Collegio, hanno superato i 9 miliardi di lire (euro 4.650.000,00 circa).

Per il 2001 le risorse a disposizione del Garante sono state pari a lire 24.069.705.190 (euro 12.430.965,30). Di tale somma, il contributo dello Stato, pari a lire 22.000.000.000 (euro 11.362.051,78), è stato trasferito dal capitolo dello stato di previsione della spesa del Ministero del tesoro sul conto della banca cassiera dell'Autorità in quattro rate trimestrali di lire 5.500.000.000 (euro 2.840.512,94).

Per il 2001 le altre risorse finanziarie di cui ha potuto disporre il Garante si riferiscono agli interessi maturati sui fondi relativi agli avanzi pregressi (oltre un miliardo di lire, pari a euro 516.500,00 circa), ai fondi rappresentati dalle quote di iscrizione dei partecipanti alla XXII Conferenza internazionale delle autorità di protezione dei dati personali svoltasi a Venezia dal 28 al 30 settembre 2000 (circa lire 200.000.000, pari a euro 103.291,38), dalle entrate derivanti dalla sublocazione di parte dei locali di piazza di Monte Citorio (circa lire 300.000.000, pari a euro 154.937,07), dal trasferimento di lire 550.000.000 (euro 284.051,29) dal conto corrente postale in cui affluiscono i diritti di segreteria per le notificazioni e per i ricorsi e le autorizzazioni. Le rimanenti entrate riguardano i rimborsi spese provenienti dalle istituzioni comunitarie e dal Consiglio d'Europa per la partecipazione di rappresentati del Garante alle previste riunioni.

Nel documento programmatico del 2001 sono stati individuati come progetti prioritari la ristrutturazione e l'arredo dei nuovi locali, la dotazione della biblioteca di un patrimonio bibliografico di settore e di idonei strumenti, anche multimediali, per la ricerca e la consultazione, l'allestimento della sala convegni con tecnologie moderne e sofisticate, nonché dell'ufficio relazioni con il pubblico.

Tra le priorità deve essere altresì menzionato il potenziamento delle strutture informatiche e telematiche (soprattutto per l'operatività della rete interna) descritti con maggior dettaglio in altro paragrafo.

Per la realizzazione di questi progetti l'impegno del Garante è stato di notevoli proporzioni considerato che per i capitoli di spesa interessati sono state erogati nell'anno 2001 oltre 2.200 milioni di lire (euro 1.136.205,18).

A tale proposito si ritiene utile evidenziare anche alcuni dati relativi all'attività contrattuale del dipartimento contratti e risorse finanziarie, alla quale sono seguiti gli impegni della prevedibile spesa da parte del settore contabile: per la realizzazione della sala conferenze, biblioteca e sala consultazione sono state avviate cinque diverse procedure (arredi speciali, sedute, scaffalature, tende) per l'importo complessivo di lire 335.000.000 (euro 173.013,06). A queste va aggiunto il contratto per gli impianti elettrici, la cui gara è stata espletata dal Provveditorato alle opere pubbliche del Lazio e il cui onere a carico del Garante è stato di oltre 383 milioni di lire (euro 197.803,00).

Per l'Ufficio relazioni con il pubblico si sono curate cinque procedure per un costo totale di oltre lire 130.000.000 (euro 67.139,40), mentre il dipartimento risorse tecnologiche ha attivato sei procedimenti tesi all'acquisizione di beni e servizi per un totale di lire 841.000.000 (euro 434.340,25).

Il servizio relazioni con i mezzi di informazione ha attivato cinque procedimenti negoziali per l'importo di lire 330.000.000 (euro 170.430,78), compresa la fornitura di *Cd rom* per le nuove edizioni di *Cittadini e società dell'informazione*, la realizzazione dello *stand* fieristico e la sua installazione per le tre manifestazioni nazionali annuali, alle quali il Garante partecipa ormai stabilmente: il *Forum della P.A.* di Roma, il *Com.pa* di Bologna e lo *Smau* di Milano. Si è curato anche il *software* per la rassegna stampa in corso di acquisizione.

L'unità temporanea flussi informativi e analisi delle procedure ha richiesto l'attivazione di due procedure per un totale di lire 213.000.000 (euro 110.005,32) con cui tra l'altro è stata attivata la nuova fase di preparazione delle notificazioni, di immissione dei dati e archiviazione nel registro generale dei trattamenti.

Il dipartimento risorse umane ha attivato il dipartimento per i contratti per la fornitura dei buoni pasto e per i corsi di lingua straniera ai dipendenti (per i buoni pasto si è proceduto utilizzando la convenzione Consip che garantisce all'Autorità un costo unitario di lire 13.669,50 pari a euro 7,06 a fronte di lire 15.000 pari a euro 7.75, nominali).

Sono stati inoltre conclusi ulteriori procedimenti relativi alla vigilanza della sede, anche con passaggi notturni; alla realizzazione degli archivi con impianti compattati a volantino; alla sistemazione dei locali situati al primo piano della scala A e del terzo piano della scala B con interventi edili atti a consentire una migliore sistemazione per il nuovo personale assegnato all'Autorità.

Il dipartimento contratti e risorse finanziarie ha infine attivato alcune volte il meccanismo dell'aumento del quinto delle forniture di cui all'art. 11 della vigente legge per l'amministrazione del patrimonio e per la contabilità generale dello Stato, che obbliga il fornitore ad assoggettarvisi (qualora nel corso di esecuzione del contratto occorra un aumento o una diminuzione della fornitura fino alla concorrenza del quinto del prezzo della provvista).

70 Lo sviluppo del sistema informativo

L'attività di sviluppo dei sistemi informativi ha attraversato nello scorso anno una fase di forte espansione, caratterizzata dalla messa a punto dell'ambiente tecnologico informatico del Garante, nelle sue componenti infrastrutturale e di servizi.

Sono stati introdotti e messi in produzione i seguenti componenti s*oftware* o infrastrutturali del sistema informativo:

- rete locale a larga banda che, sfruttando l'impianto di cablaggio strutturato già realizzato nella sede dell'Ufficio, ha consentito di pervenire a prestazioni ed efficienza enormemente superiori rispetto alla rete locale precedentemente utilizzata; l'infrastruttura, basata sullo standard *Gigabit Ethernet*, consente velocità di trasmissione dei dati fino a 1 *Gigabit*/secondo sulle tratte in fibra ottica, permettendo un efficiente utilizzo delle risorse di rete condivise; gli apparati utilizzati supportano i più avanzati sistemi di sicurezza e protezione del traffico, consentendo tra l'altro la suddivisione della rete in *LAN* virtuali;

- nuovi server a tecnologia *Unix* (sistemi operativi *Solaris* e *Linux*), per ospitare i sistemi di gestione di basi di dati relazionali e le applicazioni connesse, i servizi di rete *Internet*, i sistemi di cifratura e sicurezza;

- nuovi server a tecnologia *Windows* che consentono l'erogazione dei servizi di autenticazione del dominio, di file *sharing,* di *database* oltre che il supporto di applicazioni di produttività individuale;

- nuovo sistema di gestione delle rassegne stampa, dotato di interfaccia *web* e con avanzate funzioni di indicizzazione e di ricerca, che consente una più efficiente selezione delle notizie e degli articoli e la produzione dei ritagli elettronici;

- sistema *software* per la gestione bibliotecaria, che consente la pubblicazione sul *web* dell'*OPAC* e l'eventuale futura integrazione della biblioteca nella rete del servizio bibliotecario nazionale.

È stato installato e messo in produzione il nuovo collegamento numerico dedicato a 2 *megabit*/secondo che collega la rete dell'Ufficio a *Internet* garantendo un'ampiezza di banda sedici volte maggiore di quella precedentemente utilizzata, e consentendo così di ospitare presso la sede nella rete locale dell'Ufficio i servizi accessibili al pubblico.

La disponibilità del nuovo collegamento e la presenza di un'infrastruttura di rete interna altamente affidabile hanno consentito di trasferire presso la sede del Garante, facendo cessare il ricorso all'*outsourcing*, i servizi *Internet* fondamentali, quali la posta elettronica, il servizio *web* e il *DNS*. La disponibilità in sede dei sistemi ha consentito di implementare nuovi servizi quali il *Network Time Protocol* per la sincronizzazione del clock di sistema e la certificazione dei log, il servizio di directory *LDAP*, il servizio di autenticazione Radius.

Accanto alla tradizionale rete cablata è stata sviluppata una rete a standard *IEEE* 802.11 (*Wireless Ethernet*) che offre servizi di connettività *wireless* con protocolli *IP* in alcune aree dell'Ufficio e nella sala convegni del Garante.

È stato predisposto un servizio di accesso remoto con otto linee telefoniche a ricerca automatica che consente al personale autorizzato il collegamento con protocolli *TCP/IP* alla rete *Internet* e alla rete interna dell'Ufficio, tramite la rete telefonica, permettendo l'accesso autenticato ai documenti di pertinenza di ciascun utente anche in occasione di missioni o di servizio fuori sede, prestando particolare cura agli aspetti di sicurezza.

In collaborazione con il responsabile del Progetto Biblioteca, è stata progettata e realizzata una sala di consultazione dotata di postazioni *SunRay,* caratterizzate dal collegamento diretto alla rete e dall'uso della tecnologia *smart card* per l'autenticazione e per la gestione della mobilità delle sessioni di lavoro tra le postazioni.

In collaborazione con il responsabile del Progetto contenzioso è stato definito e implementato un *database* a interfaccia *web* che consente di inserire, aggiornare e consultare le pratiche relative.

Di particolare rilievo per l'organizzazione interna dei servizi informatici è stata l'implementazione di un servizio di *system and network management*, basato su uno dei più affermati *framework* gestionali, che consente al personale tecnico del dipartimento risorse tecnologiche di effettuare il monitoraggio degli apparati di rete, dei *server* e dei *personal computer*, di intervenire a distanza sui sistemi assumendone il controllo, di gestire la distribuzione automatica degli aggiornamenti e l'installazione delle applicazioni su tutti i personal computer in rete, di gestire gli *asset* informatici dell'Ufficio.

È stato poi progettato l'allestimento audiovisivo della sala convegni del Garante, parzialmente realizzato con la predisposizione dell'amplificazione di sala e delle apparecchiature di regia che consentono già l'uso della sala per convegni e seminari.

È stato progettato, con la collaborazione di grafici esterni all'Autorità e del responsabile della redazione *web*, il nuovo sito ufficiale del Garante, la cui implementazione è stata successivamente avviata, con una previsione di completamento nell'arco dei prossimi sei mesi. Il progetto prevede la revisione della linea grafica comunicativa, la ristrutturazione della base di dati documentali e del sistema di redazione, con particolare attenzione alla gestione dei contenuti, alla fruibilità delle informazioni, alla compatibilità con gli standard di usabilità del *World Wide Web Consortium*.

È stato predisposto, in collaborazione con il dipartimento amministrazione e contabilità, il progetto per l'implementazione del sistema amministrativo contabile, che costituirà l'ossatura del sistema di controllo di gestione e che si avvarrà di tecnologia *software ERP* d'avanguardia, e che prevede anche la gestione dei cespiti con funzionalità avanzate di inventariazione dei beni mobili.

È stato predisposto il progetto per l'automazione con tecnologia *web-oriented* delle procedure di calcolo delle missioni e del rilevamento e controllo delle presenze del personale.

Per quanto attiene alla sicurezza informatica, sono stati predisposti sistemi *firewall* basati su ambienti operativi "*open source*" a protezione della rete interna e dei computer in zona franca, e sistemi di rilevamento intrusioni e di verifica dell'integrità dei dati (per i *server Unix*); per quanto riguarda la protezione *antivirus* si è implementato un sistema centralizzato di gestione e allarme, con aggiornamento automatico delle firme virali, e il filtraggio automatico della posta in ingresso e in uscita.

L'attività del dipartimento è stata rivolta infine anche alle tecnologie non prettamente informatiche, curando l'ammodernamento del centralino telefonico, il progetto di un sistema di *unified messaging* e di un sistema di videoconferenza con gestione integrata delle risorse (allocazione di canali, regia multipunto, codifiche e *streaming*), l'integrazione dei sistemi di allarme e controllo degli impianti tecnologici.

71 Biblioteca e centro di documentazione

L'organizzazione e la strutturazione delle attività del Garante, seguita al trasferimento nella nuova sede di Piazza di Monte Citorio, ha consentito di rideterminare gli scopi del progetto di costituzione della biblioteca, non più vincolato alla sola funzione di raccolta del vasto materiale di documentazione utile allo svolgimento delle attività dell'Ufficio. Il progetto di creazione di una biblioteca dell'Autorità è stato infatti ricollegato anche alla previsione normativa di cui all'art. 31, comma 1, lett. h) della Legge n. 675, che indica, tra i compiti del Garante, quello di "curare la conoscenza tra il pubblico delle norme che regolano la materia e delle relative finalità".

La biblioteca dell'Autorità è stata pertanto pianificata come una biblioteca di ampie dimensioni con accesso all'utenza pubblica, dove le tematiche della *privacy* si collocano all'interno di una dimensione culturale incentrata sulla difesa dell'individuo e sulla tutela della persona.

Ciò va visto come una diretta conseguenza della dimensione culturale insita nella realtà operativa del Garante. L'approfondimento delle matrici giuridiche, storiche, filosofiche e religiose che sono all'origine della "tutela dei dati personali" fa sì che la difesa della riservatezza, nella moderna democrazia tecnologica, arrivi a ridefinire l'idea di "persona" e della "libertà della persona" come espressione anche del diritto fondamentale alla *dignità*. Sotto questo aspetto la biblioteca, nella stessa caratterizzazione delle sue collezioni, diventa così il luogo di registrazione, sul piano culturale generale, del fenomeno quotidianamente rilevato dall'Ufficio nell'ambito, più ristretto e focalizzato, della sfera del diritto: l'estendersi della "tutela dei dati personali" ad ogni aspetto della società, in termini tali da stimolare una riflessione sulla necessità di restituire all'individuo la capacità autonoma di formulazione della realtà, una "consistenza" che nasca appunto dalla *dignità* di poter elaborare un'autonoma visione dei progetti di vita.

In questa prospettiva, la creazione della biblioteca dell'Autorità presuppone una selezione bibliografica strutturata. Il sapere disponibile in materia di *privacy* viene organizzato e razionalizzato secondo una mappa di percorsi, collegamenti e ramificazioni in cui gli elementi gnoseologici sono sistematicamente coordinati e in correlazione.

Un primo nucleo è rappresentato da un "fondo" giuridico di contenuto specialistico multisettoriale. Tale fondo prevede, tra l'altro, la raccolta sistematica di tutte le monografie, italiane e straniere, che abbiano per oggetto la *privacy*. La raccolta è stata estesa retrospettivamente anche a titoli fuori commercio. Attualmente sono già disponibili, inventariati e catalogati, oltre 2000 titoli. Ad integrazione di questa prima collezione, sono in programma rapporti di collaborazione con organismi istituzionali italiani e stranieri e con fondazioni culturali pubbliche e private. Una ulteriore articolazione prevede scambi e contati con università ed istituti di ricerca italiani e stranieri. Una stretta cooperazione verrà stabilita con le altre autorità europee di protezione dei dati: a questo riguardo, la biblioteca ha già avviato la raccolta sistematica del materiale bibliografico prodotto e pubblicato dalle autorità straniere omologhe.

Un secondo nucleo, di proporzioni maggiori, prevede la formazione di un fondo multidisciplinare a vasto raggio su quattro temi primari: la comunicazione e i suoi strumenti, le tecnologie di massa invasive, le matrici culturali e ideologiche dell'attuale evoluzione tecnologica, il pensiero religioso e laico sulla sacralità della persona e sull'autonomia sovrana dell'individuo, il tutto in termini collegati e giustificati con le attribuzioni che la legge demanda all'Autorità.

La fisionomia complessiva della biblioteca, grazie alla combinatoria strutturata delle diverse aree di approfondimento, presenterà un taglio originale per la qualità delle collezioni e per i rapporti che nasceranno tra campi di conoscenze altrimenti destinati a rimanere separati.

In margine a questa specificità, sul piano catalografico la caratteristica della biblioteca permetterà di creare un elenco completo o *Thesaurus* uniforme di concetti e di parole-chiave che non risultano ancora altrimenti disponibili.

Un primo esempio della capacità innovativa di questa visione dei legami tra la *privacy* e la cultura della persona si è concretizzato nella decisione dell'Autorità di pubblicare la traduzione italiana del saggio *On Privacy* di William Faulkner. La scelta di stampare letteratura di alto livello nel quadro dell'attività istituzionale di informazione va nella direzione di questo lavoro di riflessione e di approfondimento. Si deve osservare, al riguardo, che il saggio costituisce un vero "incunabolo" poiché non risulta mai citato nei lavori giuridici sulla protezione della vita privata, pur rappresentando un ambizioso tentativo di porre in rapporto l'idea di *privacy* con le radici puritane del "sogno americano".

A completamento del progetto della biblioteca resta prevista, come già menzionato lo scorso anno, la creazione di un comitato scientifico composto da eminenti personalità soprattutto del mondo accademico che, sulla scorta dell'esempio di altre autorità, sappia individuare temi e problemi con i quali l'Ufficio sarà chiamato negli anni a venire a confrontarsi, segnatamente in ragione dei veloci cambiamenti della società dell'informazione.

Nell'ambito della prevista apertura della biblioteca al pubblico, una particolare cura è stata già dedicata ai supporti tecnologici. E' stata progettata e realizzata una sala di consultazione dotata di postazioni multimediali *SunRay*, caratterizzate dal collegamento diretto alla rete e dall'uso della tecnologia *Smart card* per l'autenticazione e per la gestione della mobilità delle sessioni di lavoro tra le postazioni. Tale sistema, di elevato impatto innovativo, consentirà agli utenti di consultare i cataloghi *online* accessibili sulla rete *Internet* e le risorse bibliografiche dell'Ufficio, come le banche dati su *Cd-Rom* e gli abbonamenti *online*. La peculiarità dell'architettura realizzata, basata su un sistema *server* ad alte prestazioni di tipo *Sun Solaris*, consiste nello svincolare la sessione di lavoro dalla particolare postazione fisica: associandola al *token* identificativo trasportato dalla *Smart card*, l'utente ha la possibilità di abbandonare la postazione per effettuare consultazioni dirette di libri e riviste o per usufruire di altri servizi disponibili nell'area bibliotecaria, senza doversi prendere cura della prenotazione del posto e senza perdere traccia del lavoro svolto fino a quel momento. Questa impostazione tecnologica della sala evita la prolungata occupazione del posto di consultazione informatizzato che si verifica in tutte le grandi biblioteche e consente invece una ampia fruibilità delle risorse.

L'organizzazione e la gestione della biblioteca e delle sue infrastrutture disporrà inoltre di un sistema *software* per la pubblicazione sul *web* dell'*Opac* – consultabile anche dalla utenza "remota" - e di un sito *web* per l'accesso ai servizi interni secondo percorsi guidati e personalizzabili.

72 Il personale e i collaboratori esterni

Come già evidenziato nella Relazione per il 2000, l'Autorità ha attuato l'assetto organizzativo previsto dal proprio regolamento di organizzazione e ha completato la disciplina dei rapporti di lavoro, definendo anche il protocollo per le relazioni collettive in ottemperanza all'art. 66 del regolamento n. 2/2000.

L'anno 2001 si è contraddistinto come un anno di intensa attività per il consolidamento organizzativo dell'Ufficio.

Ciò ha comportato l'adozione di un insieme di atti di organizzazione – dalla definizione dei principali obiettivi dell'attività istituzionale alla delimitazione dei compiti delle unità di primo livello (dipartimenti e servizi) – propedeutici all'affidamento degli incarichi di direzione e all'assegnazione delle limitate risorse umane a disposizione. Nel corso del periodo considerato i dipartimenti e i servizi hanno iniziato ad organizzare la propria attività sulla base delle risorse umane disponibili, nelle more dell'espletamento delle procedure selettive e concorsuali bandite dal Garante nel giugno del 2001 che, una volta terminate, dovrebbero permettere un rafforzamento dell'organico dell'Ufficio.

Il Garante ha infatti bandito concorsi pubblici (pubblicati nella *G.U.*, 4ª serie speciale, n. 47 del 15 giugno 2001) per la copertura di complessivi 21 posti di varie posizioni (di cui n. 3 dirigenziali, n. 10 direttive e n. 8 operative). Contestualmente l'Autorità ha promosso alcune opportunità professionali e di lavoro rivolte a giovani laureati, indicendo due selezioni pubbliche: la prima per il reclutamento fino a sei giovani laureati, di età inferiore a 35 anni, da assumere con contratto di specializzazione a tempo determinato, e la seconda per la frequenza di periodi di tirocinio presso l'Ufficio rivolta a giovani laureati di età non superiore a 28 anni.

La procedura selettiva per l'individuazione dei giovani da assumere con contratto di specializzazione è stata affidata ad una commissione presieduta dal segretario generale dell'Autorità e composta da un dirigente dell'Ufficio e da un docente universitario e si è svolta in due fasi: nella prima, sono stati valutati i titoli prodotti dai circa 450 aspiranti sulla base di rigorosi ed oggettivi criteri di massima preventivamente elaborati dalla commissione e resi noti in termini di trasparenza; nella seconda, come previsto dall'avviso di selezione, sono stati convocati per un colloquio i candidati risultati più meritevoli e all'interno di questa rosa sono stati selezionati i sei giovani da assumere. Ad aprile di quest'anno sono stati sottoscritti i relativi contratti di specializzazione per un primo gruppo di 4 giovani, mentre, per almeno altri due, i rapporti di lavoro sono in corso di perfezionamento.

Esaurita tale procedura selettiva, la medesima commissione è in procinto di completare la valutazione delle domande per gli *stages,* che dovrebbe concludersi in tempi ragionevolmente brevi.

Le procedure per i concorsi pubblici sono anch'essi in procinto di iniziare, avendo il Consiglio di presidenza del Consiglio di Stato designato di recente, su precedente richiesta del Garante, i presidenti delle commissioni esaminatrici.

L'organico dell'Autorità si avvia così ad essere coperto al 90%. Attualmente l'Ufficio dispone complessivamente di sole 69 unità, di cui 11 assunte con contratto a tempo determinato (ivi compresi i giovani con contratto di specializzazione), come da prospetto allegato:

SITUAZIONE DEL PERSONALE PER AREA E TIPOLOGIA CONTRATTUALE

		PERSONALE IN SERVIZIO			
Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	Personale a contratto	TOTALE
Dirigenti	26	15	4		19
Funzionari	40	18	7		25
Operativi	25	9	5		14
Esecutivi	9				0
Personale a contratto	20			11	11
TOTALE	120	42	16	11	69

L'Autorità attualmente si avvale, inoltre, della collaborazione di n. 6 consulenti per i necessari approfondimenti nelle tematiche giuridiche e della comunicazione istituzionale, nonché per le problematiche del bilancio di previsione e consuntivo e per l'attuazione del regolamento sull'amministrazione e la contabilità. Si è altresì reso necessario acquisire, nel corso dell'anno, occasionali consulenze qualificate in materia informatica per le problematiche concernenti il sistema informativo interno, il sito *web* del Garante e la sicurezza dei dati.

Come detto, la commissione di selezione per il reclutamento di sei giovani con contratto di specializzazione e per gli *stages* si avvale di un componente esterno individuato in un docente universitario.

Il registro dei trattamenti

73 Organizzazione e futuri sviluppi

L'istituto della notificazione del trattamento dei dati personali, previsto dagli artt. 7, 16 e 28 della legge n. 675/1996 subirà una profonda rivisitazione in attuazione dell'emanazione del d.lg. 28 dicembre 2001, n. 467. Le novità introdotte sono diverse e riguardano:

- l'obbligo di designazione del rappresentante nel territorio dello Stato da parte del titolare stabilito in un paese extraeuropeo in caso di trattamento mediante mezzi situati nel territorio dello Stato (art. 2, comma 2);

- l'indicazione nella notificazione (oltre all'eventuale rappresentante del titolare nel territorio dello Stato) di almeno un responsabile (art. 3, comma 3);

- la sostituzione delle sanzioni penali con sanzioni amministrative in caso di omessa o incompleta notificazione (art. 12, comma 1);

- la definizione dei casi e dei contenuti della notificazione - che attualmente sono stabiliti direttamente dalla legge n. 675/1996 - mediante un emanando regolamento.

Su tale ultimo aspetto va evidenziato che il regolamento disciplinerà l'istituto dando concreta efficacia all'obbligo di notificare i soli trattamenti che, in ragione delle relative modalità o della natura dei dati personali, siano suscettibili di arrecare pregiudizio ai diritti e alle libertà dell'interessato. La disposizione trae origine da un generale ripensamento dell'istituto con il chiaro intento di procedere ad un approfondito monitoraggio dei casi di trattamento maggiormente a rischio, esonerando i restanti dall'obbligo di notificazione. Si limita così l'obbligo ad una platea di titolari più ridotta.

C'è da considerare, infatti, che attualmente nel registro generale dei trattamenti sono presenti anche numerose notifiche da parte di soggetti non tenuti alla notificazione – in quanto esonerati – e che ad esse si aggiunge un numero considerevole di ulteriori notificazioni di trattamenti che non sembrano presentare rischi per l'interessato.

Un apposito gruppo di lavoro interno al Garante ha già ultimato un primo contributo per definire i casi di notificazione, ed è tutt'ora impegnato nel fornire analogo supporto per stabilire i contenuti da trasfondere nel relativo modello, in maniera da rendere l'adempimento pienamente rispondente alle esigenze di garanzia.
In attesa dell'emanazione del regolamento, previsto per fine anno, la disciplina della notificazione al Garante, salvo quanto già detto circa le nomine del responsabile e del rappresentante nello Stato, rimane sostanzialmente immutata.

Le notificazioni confluiscono nel registro generale dei trattamenti previsto dall'art. 31, comma 1, lett. *a*), legge n. 675/1996, che ne contiene circa 310.000. Esse vengono redatte su un modello standard o, in alternativa su *floppy disk*. Il modello e il programma, in attuazione dell'art. 12, comma 2, del d.P.R. n. 501/1998, oltre ad essere reperibili sul mercato, sono altresì distribuiti gratuitamente da circa 14.000 uffici postali e comunque scaricabili dal sito *Internet* del Garante.

Il servizio di distribuzione si è rivelato funzionale e capillare, seppure in qualche misura economicamente oneroso. Un progetto in corso prevede la possibilità di ridurre i costi, migliorando ulteriormente il servizio mediante utilizzo di altre modalità in particolare via Internet e tramite gli uffici relazioni per il pubblico di organismi pubblici, con l'effettuazione degli adempimenti in via telematica.

Il progetto di consultazione diretta in remoto del registro da parte dell'interessato e di trasmissione telematica delle notificazioni tramite terminali ubicati nell'ambito degli uffici per le relazioni con il pubblico

presso le amministrazioni provinciali e di eventuali altre amministrazioni pubbliche (art. 13, comma 2, del d.P.R. n. 501/98 e comma 3, dell'art. 31 della legge) ha subito necessariamente una lieve battuta d'arresto a seguito dell'emanazione della nuova disciplina prevista dal d.lg. n. 467/2001 e anche a causa di difficoltà nello sviluppo *software* da parte dell'impresa già affidataria.

Sono stati però facilmente colmati alcuni ritardi nella registrazione di precedenti notifiche, mentre sono state prontamente esaudite tutte le richieste di accesso al registro.

Gli importi dei diritti di segreteria sono rimasti invariati, anche se hanno subito la trasformazione da lire in euro: euro 7,75 per le notificazioni su *floppy disk* e euro 12,91 per quelle su modello cartaceo.

È stata incrementata l'attività di assistenza, anche telefonica, agli utenti che si rivolgono all'Ufficio per fornire chiarimenti sull'interpretazione della legge ed aiuto nella compilazione della modulistica, oltre che per soddisfare le richieste d'accesso al registro. Le risposte ai quesiti più frequenti (Faq) sono consultabili direttamente dall'utente sul sito.

Le richieste d'accesso al registro sono state circa un centinaio nel corso dell'anno, effettuate direttamente da parte dell'interessato, in prevalenza per la richiesta di copie, da studi legali a fini di tutela degli interessati e dal Dipartimento vigilanza e controllo dell'Ufficio.

Sono inoltre proseguite le attività di routine consistenti, essenzialmente, nella memorizzazione delle notificazioni pervenute (circa 17.000) e nella regolarizzazione delle notificazioni irregolari o incomplete. L'Ufficio ha elaborato procedure automatizzate tese al recupero dei diritti di segreteria non versati.

Sempre a seguito delle innovazioni da introdurre, è in corso la revisione dell'attuale struttura del registro per renderlo conforme alle novità apportate e da apportare all'istituto della notificazione, adottando gli opportuni accorgimenti in maniera da poter interrogare contemporaneamente l'attuale e il futuro registro, privilegiando al massimo sistemi di memorizzazione automatizzata e trasmissione della notificazione telematica. Nel frattempo è stata affidata ad una nuova impresa l'attività di "normalizzazione" di quello attuale, per renderlo più funzionale anche in ragione delle inadempienze contrattuali della precedente impresa che ha indotto il Garante a risolvere il contratto.

Per quanto attiene all'organizzazione, il dipartimento registro generale dei trattamenti ne cura la tenuta avvalendosi, oltre che del dirigente, di due dipendenti e di un numero variabile di collaboratori (attualmente tre) fornito dalla stessa impresa che cura la normalizzazione del *database*, a fini di verifica e memorizzazione degli atti pervenuti. Assestatosi il flusso di atti che pervengono all'Ufficio (circa 17.550 all'anno), l'intero ciclo avviene all'interno dell'Autorità, essendo ormai esaurita la fase iniziale caratterizzatasi per l'abnorme afflusso di notificazioni in un breve periodo di tempo.

Costante è la revisione delle notificazioni irregolari, pervenute in gran numero, destinate ad assottigliarsi drasticamente con l'introduzione del nuovo modello di notificazione, più "leggero" e comprensibile rispetto alla attuale edizione.

Nel prossimo futuro l'Ufficio sarà pertanto impegnato nella predisposizione dei nuovi modelli (ridisegno, stampa, distribuzione), sviluppo *software* e stipula di convenzioni per effettuare la notificazione per via telematica. In tal senso sono state anche positivamente concluse alcune sperimentazioni con un comune del centro Italia per l'effettuazione della notificazione telematica con l'utilizzo della firma digitale.

Dati statistici

74 Prospetto analitico

ATTI E PROVVEDIMENTI / ATTIVITA' GARANTE

Richieste di informazione e quesiti telefonici	7.000	
Segnalazioni e reclami pervenuti	4.295	
Quesiti pervenuti	1.755	
Richieste di parere pervenute (parere ex. art. 31, comma 2)	81	
Richieste di autorizzazione pervenute	98	
Assistenza telefonica relativa alle notificazioni	10.000	
Nuove notificazioni dei trattamenti (artt.7, 16 e 28) (***)	17500 (310.000)	
Comunicazioni previste dall'art. 27, comma 2	22	
Comunicazioni in tema di dati sensibili e giudiziari previste dall'art. 41, comma 5	23	
Autorizzazioni generali 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	2	
Risposte a richieste di autorizzazione (art. 22)	19	
Atti e provvedimenti a seguito di segnalazioni e reclami	2.327	
Risposte a quesiti	898	
Risposte a richieste di parere (esclusi art. 31 comma 2)	3	
Pareri rilasciati in base all'art. 31, comma 2	27	
Altri provvedimenti di segnalazione del Garante	15	
Provvedimenti istruttori ai sensi dell'art. 32, comma 1	242	
Procedimenti contenziosi definiti sulla base di ricorsi (art. 29)	211	
Elementi forniti per la risposta del Governo a interrogazioni parlamentari	1	
Note e comunicazioni in materia di misure minime di sicurezza	170	
Note e comunicazioni in materia di data certa ai fini dell'applicazione delle misure minime di sicurezza	309	
Comunicati stampa e dichiarazioni alla stampa	38	
Notiziari settimanali pubblicati a cura del Servizio relazioni con i mezzi di informazione	54	
Richieste di accesso e/o di verifica di dati esistenti nel Sistema d'informazione Schengen (**)	219	
Procedimenti relativi alle richieste di accesso e/o di verifica di dati esistenti nel Sistema d'informazione Schengen definiti (**)	122	
Seminari e conferenze internazionali	5	
Procedimenti ispettivi	18	
Segnalazioni all'autorità giudiziaria	7	
Ordinanze di ingiunzione	6	
Verbali di contestazione	5	

(**) periodo di riferimento della statistica: 1 gennaio 2002-31 marzo 2002

(***) la prima cifra è riferita alle notificazioni pervenute nell'anno, la seconda al n. complessivo di notificazioni pervenute

SERVIZI ISPETTIVI

Ispezioni effettuate:		
Sopralluoghi ex art. 32, comma 1		18
Sopralluoghi ex art. 13 l. n. 689/1981		
Accessi alle banche dati con decreto dell'a.g.		
Accessi alle banche dati con assenso		
Collaborazioni con autorità giudiziarie		

Ispezioni effettuate nei confronti di:		
Soggetti privati	12	
Soggetti pubblici	6	
		18

Risultati ottenuti:		
Provvedimenti di divieto di trattamento ex art. 31, comma 1, lettera l)	3	
Provvedimenti di blocco di trattamento ex art. 31, comma 1, lettera l)	1	
		4

SANZIONI AMMINISTRATIVE E DENUNCE ALL'A.G.

Contestazione della sanzione amministrativa o ingiunzione di pagamento (art. 39):	11	
Per violazione dell'art. 10	10	
Per violazione dell'art. 32, comma 1	1	
Pagamenti in misura ridotta della sanzione	(2)	

Persone segnalate all'autorità giudiziaria:	7	
Per omessa notificazione al Garante		
Per trattamento illecito (art. 35)		
Per omessa adozione misure minime di sicurezza (art. 36)		

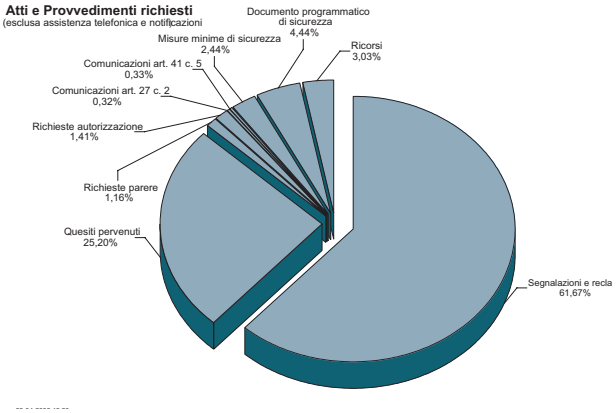
RICORSI

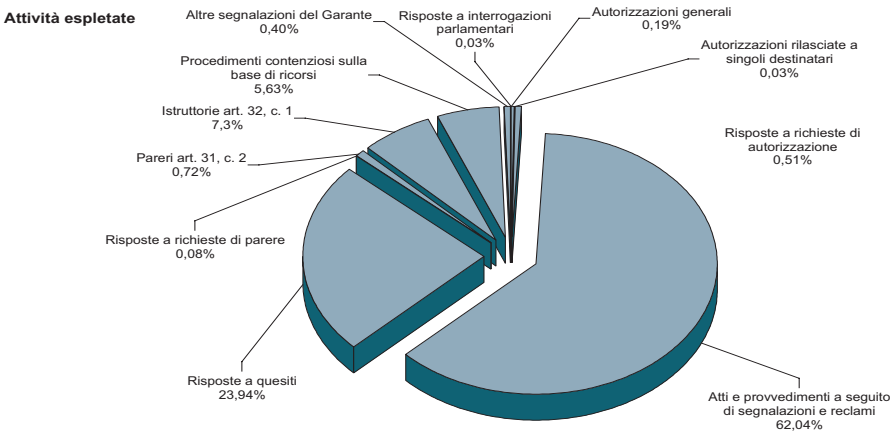
Pervenuti		
		211

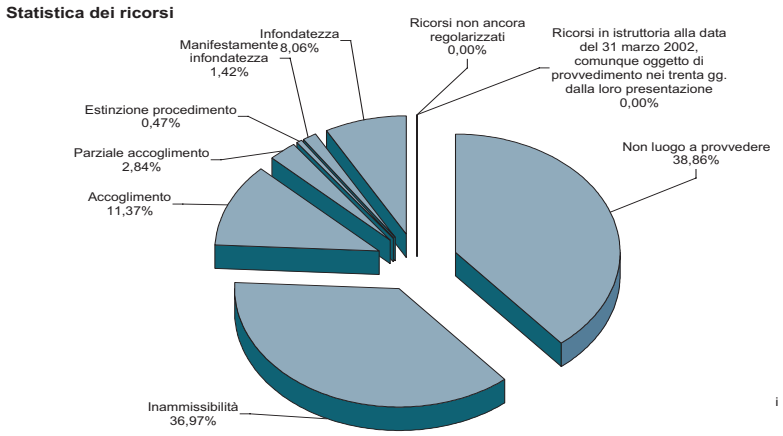
Tipo di decisioni adottate:		
Non luogo a provvedere	82	
Inammissibilità	78	
Accoglimento	24	
Parziale accoglimento	6	
Estinzione procedimento	1	
Manifestamente infondatezza	3	
Infondatezza	17	
Ricorsi non ancora regolarizzati	0	
Ricorsi in istruttoria alla data del 31 marzo 2002, comunque oggetto di provvedimento nei trenta gg. dalla loro presentazione	0	

Statistica di quelli pervenuti dal 1 gennaio 2002 al 31 marzo 2002

74


Atti e Provvedimenti richiesti
(esclusa assistenza telefonica e notificazioni
Documento programmatico di sicurezza 4,44%
Misure minime di sicurezza 2,44%
Ricorsi 3,03%
Comunicazioni art. 41 c. 5 0,33%
Comunicazioni art. 27 c. 2 0,32%
Richieste autorizzazione 1,41%
Richieste parere 1,16%
Quesiti pervenuti 25,20%
Segnalazioni e recla 61,67%


Attività espletate
Altre segnalazioni del Garante 0,40%
Risposte a interrogazioni parlamentari 0,03%
Autorizzazioni generali 0,19%
Autorizzazioni rilasciate a singoli destinatari 0,03%
Procedimenti contenziosi sulla base di ricorsi 5,63%
Istruttorie art. 32, c. 1 7,3%
Risposte a richieste di autorizzazione 0,51%
Pareri art. 31, c. 2 0,72%
Risposte a richieste di parere 0,08%
Risposte a quesiti 23,94%
Atti e provvedimenti a seguito di segnalazioni e reclami 62,04%


Statistica dei ricorsi
Infondatezza 8,06%
Ricorsi non ancora regolarizzati 0,00%
Manifestamente infondatezza 1,42%
Ricorsi in istruttoria alla data del 31 marzo 2002, comunque oggetto di provvedimento nei trenta gg. dalla loro presentazione 0,00%
Estinzione procedimento 0,47%
Non luogo a provvedere 38,86%
Parziale accoglimento 2,84%
Accoglimento 11,37%
Inammissibilità 36,97%

Attività comunitarie e internazionali

Il recepimento delle direttive comunitarie

75 Le direttive sulla protezione dei dati

Il processo di recepimento della direttiva generale in materia di protezione dei dati personali, intrapreso con la legge n. 675/1996 (e proseguito con ulteriori successive modifiche ed integrazioni della stessa, delle quali si è reso conto nelle precedenti relazioni annuali), ha registrato un ulteriore passo in avanti con il d.lg. 28 dicembre 2001, n. 467: in particolare, come si è già accennato, con esso sono stati disciplinati gli aspetti relativi al bilanciamento degli interessi (art. 7, lett. *f)* della direttiva) ed è stato attribuito al Garante il compito di individuare ulteriori casi nei quali il titolare potrà effettuare il trattamento dei dati personali in mancanza del consenso dell'interessato. Il decreto ha inoltre introdotto nell'ordinamento italiano l'istituto del controllo preliminare (*prior checking*) sui trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone, attribuendone al Garante la competenza. In altra sede si sono precisate le condizioni alle quali la disciplina nazionale può trovare applicazione nel caso di trattamenti svolti da soggetti stabiliti al di fuori dell'Unione europea, derivandone in tal caso l'obbligo in capo al titolare di nominare un suo rappresentante in Italia.

La direttiva sulla protezione dei dati nelle telecomunicazioni (97/66/CE) è stata già sostanzialmente trasposta con il d.lg. 13 maggio 1998, n. 171, recante disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni.

Come già menzionato, con il d.lg. n. 467/2001 sono state altresì apportate le modifiche al d.lg. n. 171/1998 resesi necessarie alla luce dei rilievi mossi dalla Commissione europea, in particolare con riguardo all'articolo 5 del medesimo decreto, anche per adeguare la normativa vigente agli sviluppi intervenuti nel settore delle comunicazioni elettroniche. Esse attengono alle modalità di pagamento alternative alla fatturazione, all'informazione al pubblico sull'identificazione della linea chiamante e collegata e alle chiamate di emergenza.

76 Stato di recepimento delle direttive 95/46/CE e 97/66/CE negli Stati membri

La principale novità relativa al recepimento della direttiva 95/46/CE sulla protezione dei dati nel corso del 2001 riguarda l'approvazione della legge federale tedesca (*Bundesdatenschutzgesetz* del 23 maggio 2001), cui peraltro si è fatto cenno nella precedente relazione annuale. Dei quindici Paesi dell'Unione europea, pertanto, soltanto Francia, Irlanda e Lussemburgo devono ancora provvedere al recepimento. Rinviando al sito *web* della Commissione europea (http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm) per l'aggiornamento in relazione allo stato del recepimento delle direttive in materia, si riassumono di seguito le novità intervenute nel corso del 2001 e dei primi mesi del 2002 nei Paesi da ultimo menzionati.

In Francia è stato approvato dall'Assemblea Nazionale, il 30 gennaio 2002, il progetto di legge, presentato dal Ministro della giustizia il 18 luglio 2001, relativo alla protezione delle persone fisiche rispetto al trattamento di dati personali, che modifica la legge "informatica e libertà" del 6 gennaio 1978 e sul quale l'Autorità francese per la protezione dei dati (CNIL) si era pronunciata in modo sostanzialmente favorevole nel settembre del 2001. Senza entrare nel merito del testo, va sottolineato che il progetto di legge conferisce alla Commissione poteri sanzionatori diretti dei quali la stessa era finora sprovvista.

In Irlanda è stato approvato il "Regolamento 2001 sulla protezione dei dati", firmato dal Ministro della giustizia il 19 dicembre 2001, entrato in vigore il 1° aprile 2002, con il quale sono state recepite alcune disposizioni della direttiva relative, in particolare, al diritto applicabile (art. 4), alle misure di sicurezza che i titolari sono tenuti ad adottare (art. 17), ai trasferimenti di dati all'estero (artt. 25 e 26). In sostanza, le disposizioni della legge sulla protezione dei dati (che risale al 1988) si applicheranno a tutti i titolari stabiliti in Irlanda anche attraverso un intermediario; dovranno essere adottate le misure di sicurezza necessarie alla luce delle attuali conoscenze tecnologiche, indicando per iscritto i compiti affidati all'eventuale responsabile del trattamento (cosa che finora non era prevista); i trasferimenti di dati personali dal territorio irlandese verso Paesi terzi potranno avvenire in presenza di un livello adeguato di protezione dei dati (o ricorrendo ad altri strumenti, quali il *Safe Harbor* e le clausole contrattuali standard).

Recentemente (25 febbraio 2002), il Ministro della giustizia irlandese ha annunciato la presentazione al Parlamento del progetto di legge per il recepimento integrale della direttiva, che potrebbe essere approvato definitivamente entro la metà del corrente anno.

Per quanto riguarda il Lussemburgo, il progetto di legge presentato dal Governo nel mese di ottobre 2000 è tuttora all'esame del Parlamento.

- Direttiva 97/66/CE

Non vi sono rilevanti novità rispetto al quadro tracciato nella precedente relazione annuale.

77 *Privacy* nelle telecomunicazioni

Nel corso del 2000 il settore delle comunicazioni elettroniche è stato oggetto, a livello comunitario, di proposte di direttive volte a modificare il precedente quadro normativo. Tali proposte, che originariamente facevano parte del cd. "*pacchetto Telecom*" (direttiva quadro, direttive su interconnessione, accesso, servizio universale), sono state definitivamente approvate e sono state di recente pubblicate sulla *G.U.* delle Comunità europee. Non è stata ancora adottata, invece, la proposta di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, che maggiormente interessa questa Autorità.

Sulla base di un accordo politico raggiunto nella riunione del 6 dicembre 2001 in seno al Consiglio dei ministri telecomunicazioni, il 28 gennaio 2002 il Consiglio affari generali dell'Unione europea ha adottato a maggioranza qualificata (con il voto contrario della delegazione lussemburghese) la posizione comune sulla proposta di direttiva. In particolare, il Consiglio, non accogliendo alcuni emendamenti del Parlamento, ha confermato la scelta del consenso preliminare dell'interessato ai fini dell'inserimento dei dati personali in elenchi telefonici (art. 12) e per l'invio di comunicazioni commerciali non sollecitate (art. 13), anche a mezzo della posta elettronica e di *sms*.

Su tali aspetti il Parlamento europeo aveva già espresso un diverso avviso, impedendo l'adozione del testo in prima lettura. Allo stato, il testo è nuovamente al vaglio del Parlamento che appare fermo nelle richieste emendative precedentemente presentate.

Altre novità nel diritto comunitario e nel settore giustizia-affari interni

78 Profili generali

In ambito europeo, nel corso del 2001, si è assistito ad un progressivo diradamento delle occasioni di dibattito e discussione istituzionale nel settore della protezione dei dati personali.

I tragici eventi legati all'attentato dell'11 settembre hanno richiamato con forza l'attenzione di tutte le istituzioni comunitarie sul tema del terrorismo e, quindi, della lotta alla criminalità ed alla *cybercriminalità*, privando l'aspetto della tutela dei dati personali dell'attenzione che esso merita nella realizzazione e nello sviluppo dell'integrazione europea.

Questo atteggiamento sembra, tuttavia, in controtendenza rispetto all'importante affermazione contenuta nell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea proclamata a Nizza, contestualmente alla firma dell'omonimo Trattato, nel dicembre del 2001 e alla cui redazione ha lavorato anche il prof. Stefano Rodotà.

La Carta contribuisce a fissare e definire il nucleo di diritti, libertà e principi che potranno essere posti alla base del futuro trattato costituzionale europeo.

Nel testo approvato a Nizza, il diritto alla tutela dei dati personali si afferma in via autonoma, affiancandosi al diritto alla tutela della vita privata e familiare (previsto all'art. 7 della Carta), precedentemente enunciato dall'art. 8 della Convenzione europea dei diritti dell'uomo del 1950. L'art. 8 della Carta dei diritti fondamentali, infatti, non solo ne specifica il contenuto, ma affida anche ad una autorità indipendente la verifica del rispetto delle regole da esso fissate.

Tuttavia, a fronte del grande impegno per l'affermazione del principio, non vi è stata alcuna attività concreta nel settore, non essendo state convocate né riunioni del gruppo di lavoro protezione dati del Consiglio dell'Unione, né del gruppo cd. di "terzo pilastro", denominato "Sistemi di informazione e protezione dei dati".

A seguito di segnali di una possibile volontà di soppressione di quest'ultimo, il Garante è intervenuto, rivolgendosi al Rappresentante permanente d'Italia presso l'Unione europea per manifestare le proprie preoccupazioni rispetto ad una tale eventualità. L'Autorità ha auspicato che l'eventuale revisione dei gruppi di lavoro, operanti in seno al Consiglio dell'Unione, tenga doverosamente conto dell'importanza e della specificità della protezione dei dati personali – anche alla luce del riconoscimento operato nella Carta dei diritti fondamentali dell'Unione – ed assicuri alla stessa una adeguata visibilità all'interno delle strutture di lavoro del Consiglio.

Infatti, il Gruppo sistemi di informazione e protezione dei dati, nato nel 1998 su iniziativa italiana, ha ricevuto un ampio mandato dai Ministri ed ha operato – anche con la partecipazione di rappresentanti del Garante e di altre autorità di protezione dei dati personali dei Paesi dell'Unione – al fine di coordinare e razionalizzare, in considerazione della particolare delicatezza della materia, l'approccio seguito nelle diverse convenzioni, elaborate nel settore della giustizia ed affari interni, che prevedono lo scambio di dati personali e la creazione di sistemi informatizzati.

Va osservato infine che le varie istanze competenti per la protezione dei dati non risultano coinvolte nei processi che hanno portato le autorità comunitarie ad adottare importanti atti in materia di antiterrorismo (posizioni comuni nn. 2001/930/Pesc e 2001/931/Pesc del 27 dicembre 2001; regolamento n. 2580/2001 in pari data).

Vanno però segnalati importanti aspetti che interessano anche indirettamente la protezione dei dati personali posti in luce dal Parlamento europeo in una risoluzione adottata il 5 settembre 2001 a proposito del sistema Echelon, nonché in una raccomandazione sulla lotta al crimine informatico (n. 2001/1970).

La cooperazione tra autorità garanti in Europa

79 Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

Considerevole è stata l'attività svolta dal Gruppo istituito in base all'art. 29 della direttiva 95/46/CE, di cui il Presidente del Garante è stato recentemente riconfermato presidente per un secondo mandato.

In particolare, il Gruppo ha continuato a seguire le delicate problematiche legate all'applicazione dell'Accordo con gli Stati Uniti, relativo alle condizioni che consentono il trasferimento dei dati verso quel Paese. Come segnalato dalla Commissione europea in un recente documento di sintesi basato su uno studio realizzato per suo conto (SEC 2002/196 del 13 febbraio 2002), sono emersi diversi elementi di insoddisfazione relativi alle modalità di effettivo funzionamento e applicazione dell'Accordo, che saranno approfonditi dal Gruppo nelle prossime settimane tenedo conto dei risultati di un'apposita visita ufficiale che il Gruppo ha curato a Washington nel marzo del 2002, partecipando a incontri con qualificati esponenti delle amministrazioni interessate, del Congresso e degli organismi privati di risoluzione delle controversie.

Il Gruppo ha inoltre espresso pareri in ordine all'adeguatezza della legge canadese sui dati personali e i documenti elettronici (parere 2/2001 WP 39) e della modifica alla legge australiana sulla tutela della vita privata (parere 3/2001 WP40), ed in merito a due progetti di decisione della Commissione europea relativi alle clausole contrattuali tipo per il trasferimento dei dati personali verso Paesi terzi (parere 1/2001 WP38, concernente i trasferimenti a titolari situati in paesi terzi, e parere 7/2001 WP 47, relativo ai trasferimenti di dati da titolari situati nell'Unione europea a responsabili del trattamento situati in Paesi terzi), progetti adottati in via definitiva dalla Commissione, rispettivamente, il 15 giugno ed il 17 dicembre 2001.

Il Gruppo di lavoro ha anche approvato un documento relativo alle disposizioni impartite dalla IATA in materia di protezione della riservatezza e flussi transfrontalieri di dati personali utilizzati per il trasporto aereo internazionale (WP 49).

In materia di sfide poste dalle nuove tecnologie, il parere 9/2001 WP 51 offre la valutazione del Gruppo in relazione alla comunicazione della Commissione europea intitolata "Creare una società dell'informazione più sicura rafforzando la sicurezza delle infrastrutture, dell'informazione e lottando contro la criminalità informatica".

Il Gruppo si è soffermato anche sul tema del trattamento dei dati nel contesto lavorativo (v. parere 8/2001 WP 48) e, in tale ambito, in modo particolare sulle problematiche relative alla sorveglianza delle comunicazioni elettroniche sui luoghi di lavoro. Un apposito gruppo di lavoro, infatti, è stato costituito per approfondire i vari aspetti del tema nella prospettiva di pervenire nel maggio del 2002, all'adozione di una raccomandazione in materia che dovrebbe essere approvata contestualmente ad una importante presa di posizione del Gruppo sul diritto applicabile in relazione ai flussi di dati personali gestiti da titolari di siti *web*, che ha impegnato i componenti riuniti in un apposito sottogruppo.

A seguito degli attentati dell'11 settembre, il Gruppo ha espresso il parere 10/2001 WP 53, con cui ha sottolineato la necessità di garantire nella lotta contro il terrorismo, un approccio equilibrato, che rispetti i diritti umani e le libertà fondamentali, di cui la protezione dei dati personali è parte integrante.

Le attività del Gruppo sono esaustivamente menzionate nel rapporto annuale richiamato negli allegati alla presente Relazione.

80 La partecipazione ad altri comitati e gruppi di lavoro

Nel quadro delle forme di collaborazione e scambio tra le autorità di protezione dei dati, va ricordato anche l'*International Working group on data protection in telecommunications* (cd. Gruppo di Berlino) – luogo di discussione ed approfondimento, non solo a livello europeo, tra esperti in materia di tecnologie ed informazione – che si occupa di temi quali Internet, crittografia, comunicazioni elettroniche.

Tale gruppo ha tenuto due riunioni, la prima a Bangalore (India) e la seconda a Berlino: nel corso di questi incontri, oltre ai consueti aggiornamenti sullo stato di attuazione e sul completamento delle normative inerenti alla tutela dei dati personali, si è proseguito nell'analisi delle problematiche connesse all'uso di Internet – e, in particolare, della posta elettronica – sul posto di lavoro. Tutti i delegati, consapevoli della delicatezza del tema, hanno convenuto sulla necessità di trovare un giusto compromesso tra le esigenze di controllo nell'uso degli strumenti telematici da parte dei datori di lavoro e il diritto alla protezione dei dati personali dei lavoratori. Trasparenza e proporzionalità delle misure adottate sono stati i concetti che hanno caratterizzato il dialogo.

Altro tema di grande interesse è stato quello relativo al bilanciamento tra sicurezza e *privacy* in merito allo sviluppo dei sistemi di votazione elettronica, di imminente adozione in diversi Paesi. In particolare, è stata rilevata la necessità di effettuare alcuni *test* sul campo prima di adottare in via definitiva tali sistemi.

Va infine ricordato l'avvio di uno studio sulle implicazioni relative alla protezione dei dati personali derivanti dall'adozione dell'*Internet Protocol* versione 6-IPV6, atteso che, nel prossimo futuro, alla luce della crescita esponenziale dei terminali d'utente e della progressiva integrazione nella rete di apparati terminali, in passato autonomi o comunque funzionanti su reti differenziate, sarà necessario l'ampliamento considerevole della disponibilità di indirizzi Internet.

Una ulteriore occasione per favorire ed ampliare la cooperazione tra le autorità nazionali per la protezione dei dati, secondo quanto previsto dall'art. 28, punto 6, par. 2 della direttiva 95/46/CE, è stata rappresentata dai seminari internazionali sulla trattazione dei ricorsi e delle segnalazioni (*Complaints Handling Workshops*).

Essi sono stati avviati nel febbraio 2000, a Manchester – facendo seguito ad un'esigenza manifestata nel corso della *Spring Conference of European Data Protection Commissioners* di Helsinki (aprile 1999) – con il primo di una serie di seminari dedicati allo scambio di informazioni e alla definizione di un *modus operandi* comune per quanto concerne la trattazione dei ricorsi e delle segnalazioni presentati alle autorità nazionali per la protezione dei dati, con particolare riguardo a quei casi che, per la loro rilevanza o per la natura delle parti interessate, travalichino l'ambito nazionale.

Ad oggi, si sono tenuti cinque incontri su questo tema, con cadenza semestrale (primavera-autunno), secondo le indicazioni emerse nella Conferenza di Stoccolma (aprile 2000). Rappresentanti di tutte le autorità garanti degli Stati membri dell'Ue, oltre alla Norvegia e, a partire dal secondo seminario, anche dell'autorità svizzera e di quella ungherese, hanno partecipato ai singoli incontri, unitamente ad un rappresentante della Commissione europea.

Nel corso dei seminari sono stati sviluppati alcuni temi fondamentali. Dopo una prima individuazione delle linee-guida comuni che devono ispirare la trattazione di questi ricorsi e/o segnalazioni, si è deciso di costituire un gruppo di discussione, all'interno del sito *web* europeo CIRCA, per facilitare lo scambio di informazioni e documenti su casi specifici. Le modalità operative di tale gruppo di discussione, protetto da *UserID* e *password* e da appositi protocolli crittografici, sono state concordate in sede di seminario. L'utilizzo del forum CIRCA si è dimostrato particolarmente proficuo, costituendo un canale privilegiato che mette direttamente in comunicazione funzionari delle singole autorità, operanti su casi concreti, e favorisce l'elaborazione di prassi comuni.

È emersa, in questo contesto, l'esigenza di confrontarsi su alcune tematiche (sorveglianza sul luogo di lavoro, flussi transfrontalieri, trattamento dei dati relativi a minori, attività ispettive) che presentano particolare rilevanza per i risvolti transnazionali che le caratterizzano e per l'impatto che hanno sulla percezione pubblica dei poteri e dell'azione delle autorità di protezione dati. In particolare, attraverso questionari elaborati congiuntamente, si è pervenuti a chiarire le modalità procedurali utilizzate nei singoli Paesi in rapporto alle tematiche indicate. Una sintesi delle informazioni raccolte rispetto al tema della sorveglianza sul luogo di lavoro ed a quello dei poteri di ispezione e controllo delle autorità nazionali di protezione dati, con le rispettive incongruenze e/o difficoltà, è stata presentata alla *Spring Conference* delle autorità di protezione dati, tenutasi a Bonn il 24/26 aprile 2002.

L'analisi dei casi presentati di volta in volta nei singoli incontri ha permesso inoltre di verificare l'effettiva esigenza, al di là dell'armonizzazione legislativa offerta dallo spazio comune europeo, di elaborare e sviluppare un approccio comune alla gestione di questioni che tendono a travalicare, in misura crescente, l'ambito nazionale – soprattutto per quanto concerne il tema dei flussi transfrontalieri di dati, che appare destinato ad assumere sempre maggiore importanza nel contesto della circolazione internazionale di merci e servizi. Le recenti decisioni della Commissione europea, relative all'adeguatezza di sistemi quali il *Safe Harbor* o l'impiego di clausole contrattuali standard, hanno invitato a riflettere sull'opportunità di definire strategie comuni per evitare che le singole autorità nazionali si presentino, di fatto, in ordine sparso rispetto all'applicazione delle lineeguida generali definite in sede comunitaria.

L'Autorità di controllo comune Schengen

81 Il rapporto per il 2000-2001

L'Autorità comune di controllo prevista dall'art. 115 della Convenzione di applicazione dell'Accordo di Schengen, che dalla fine del 2001 è presieduta dal Segretario generale del Garante, ha proseguito l'attività di verifica e controllo del funzionamento della parte centrale del Sistema di informazione Schengen.

Nel periodo considerato è inoltre proseguita l'analoga attività svolta dal Garante sul funzionamento dell'archivio della sezione nazionale del Sistema d'informazione, anche in ragione delle numerose segnalazioni pervenute (v. par. 19).

A seguito dell'entrata in vigore del Trattato di Amsterdam, l'attività di cooperazione svolta in ambito Schengen è stata ricollocata nel Consiglio e con una decisione del maggio 1999 lo stesso Consiglio ha ritenuto di disporre analoga collocazione anche per l'Autorità di controllo comune. Questo ha comportato alcune difficoltà di azione per l'Acc, come documentato nell'allegata relazione relativa al periodo 2000-2001, e solo l'entrata in funzione del segretariato unico delle autorità comuni di controllo, avvenuta nell'autunno del 2001, ha consentito un lieve miglioramento del relativo funzionamento, dotandola di una struttura amministrativa stabile, ancorché di esile spessore (solo due unità di personale per tre Acc) e non supportata dalla pur richiesta autonomia di bilancio.

L'Autorità continua a lamentare la scarsa attenzione riservata da parte degli organi competenti del Consiglio ai pareri e alle raccomandazioni da essa emesse, alle richieste di maggiore e diretto coinvolgimento, ad esempio, nei lavori relativi alla valutazione delle legislazioni dei Paesi nordici, che recentemente sono entrati a pieno titolo a far parte dell'Accordo, ed in prospettiva, dei Paesi candidati all'adesione.

Elemento sicuramente positivo rimane, comunque, il dialogo aperto con il Parlamento europeo (in particolare con la Commissione diritti e libertà pubbliche) e, da ultimo, con la presidenza di turno del Consiglio.

Particolare attenzione è stata e verrà prestata nei prossimi mesi, nel quadro delle inziative per il rilancio dell'attività dell'Acc, ai diversi problemi nascenti dal previsto passaggio al nuovo Sistema d'informazione Schengen "Sis II", che sarà probabilmente basato su nuove piattaforme informatiche, ulteriori categorie di informazioni e di organismi aventi accesso ai dati anche nei nuovi Paesi via via aderenti all'Accordo, con conseguente necessità di una simmetrica estensione delle garanzie previste dall'originaria Convenzione.

È altresì in programma nelle prossime settimane l'avvio dell'istituzione di una *newsletter* dell'Acc, da inviare a diversi organismi e organi di stampa, e del rinnovamento del sito *web* su impulso della presidenza italiana.

Un ulteriore tema che ha continuato ad impegnare l'Autorità riguarda le segnalazioni nel Sis delle persone la cui identità è stata usurpata ed il modo per evitare che le stesse subiscano pregiudizi dall'abuso perpetrato a loro danno.

Europol

82 L'attività dell'Autorità di controllo comune e i primi casi di contenzioso

L'Autorità di controllo comune, composta da due rappresentanti (di regola appartenenti alle autorità nazionali di protezione dei dati) di ogni Paese parte della Convenzione, è prevista dall'art. 24 della stessa ed ha continuato la sua attività esercitando un'incisiva azione di verifica e controllo sulla gestione degli archivi Europol, comprendenti in particolare gli archivi di lavoro per fini di analisi previsti dall'art. 10.

L'Autorità ha proseguito la valutazione dei progetti di negoziato che il Direttore dell'Europol è abilitato a svolgere in relazione allo scambio di dati con Paesi terzi e, in particolare nell'ultimo periodo dell'anno, ha affrontato il problema della trasmissione di dati da Europol agli Stati Uniti; in questa occasione l'Acc, sottolineando la necessità di pervenire ad un accordo formale che definisca le garanzie necessarie per operare in piena legittimità, ha richiesto un proprio coinvolgimento nel negoziato in corso.

La menzionata Conferenza di Bonn dell'aprile 2002 ha permesso alle autorità interessate di sviluppare un bilancio dei contatti e dei negoziati con le autorità americane.

Nell'ambito dell'attività svolta, sono stati espressi pareri in relazione all'apertura di *files* di analisi ed è stata effettuata, presso la sede dell'Europol, un'ispezione incentratasi sugli archivi in funzione, in occasione della quale sono state presentate le iniziative in corso sugli sviluppi tecnologici del sistema.

È attualmente in corso la predisposizione della prima relazione di attività e l'individuazione delle categorie di documenti che possono essere resi accessibili al pubblico e, tra le attività informative, è altresì in programma l'apertura di una pagina *web* e la pubblicazione di un opuscolo divulgativo.

Sono, infine, ancora in trattazione i primi due ricorsi ricevuti dal comitato di appello.

Il controllo sul Sistema informativo doganale

83 La creazione dell'Autorità di controllo

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'art. K3 del Trattato sull'Unione europea del 26 luglio 1995 – con la quale si mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'Unione europea, in particolare 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 un'autorità comune di controllo, composta da due rappresentanti delle autorità nazionali di protezione dei dati per ciascun Paese.

L'Autorità ha tenuto la sua prima riunione nel mese di marzo, nel corso della quale, dopo aver provveduto alla nomina del Presidente e del vice presidente (quest'ultimo nella persona del dr. Giuseppe Busia, dirigente dell'Ufficio del Garante), è stato discusso il regolamento interno senza, tuttavia, giungere alla sua approvazione definitiva.

Eurodac

84 Collaborazione tra Stati membri e garanzie per gli interessati

A seguito dell'adozione del regolamento che istituisce l'Eurodac per il confronto delle impronte digitali dei richiedenti asilo – al fine di rendere efficace l'applicazione della Convenzione per la determinazione dello Stato competente per l'esame delle domande di asilo, firmata a Dublino il 15 giugno 1995 – i compiti di supervisione e controllo spettano provvisoriamente all'autorità comune di controllo individuata all'articolo 20 del regolamento stesso. Il regolamento prevede infatti la soppressione dell'autorità di controllo "all'atto dell'istituzione dell'organo di controllo indipendente di cui all'articolo 286, paragrafo 2 del Trattato. L'organo di controllo indipendente sostituisce l'autorità comune di controllo ed esercita tutti i poteri ad essa attribuiti nell'atto istitutivo".

Tale organo di controllo indipendente è il Garante europeo istituito dal regolamento n. 45/2001 su cui ci si è soffermati largamente nella precedente relazione annuale.

Poiché, tuttavia, l'individuazione del suddetto Garante e l'effettiva applicazione del regolamento, prevista per il 1° febbraio 2002, non è stata ancora realizzata, la Commissione ha richiesto alle autorità garanti degli Stati membri di procedere all'individuazione di due rappresentanti per Paese, al fine di favorire la funzionalità provvisoria del sistema di controllo previsto dal regolamento Eurodac, che costituisce elemento imprescindibile ai fini della messa in funzione del sistema.

L'avvio imminente del sistema è confermato dall'avvenuta pubblicazione sulla Gazzetta ufficiale delle Comunità europea di un ulteriore regolamento che definisce alcune modalità di applicazione del regolamento Eurodac.

Consiglio d'Europa

85 La convenzione sul *cybercrime*

Il 23 novembre 2001, nel corso di una solenne cerimonia svoltasi a Budapest, è stata firmata da 30 Paesi la convenzione sul c*ybercrime*, predisposta nell'ambito del Consiglio d'Europa.

Si tratta del primo strumento internazionale a carattere cogente che disciplina i crimini commessi contro o con l'ausilio di reti telematiche, che segue una Raccomandazione del 1989 del Consiglio d'Europa già attuata dall'Italia con la legge n. 547/1993 sui reati informatici. La convenzione, adottata dal Comitato dei Ministri del Consiglio d'Europa l'8 novembre 2001, entrerà in vigore tre mesi dopo il deposito di cinque ratifiche, di cui almeno tre di Paesi aderenti al Consiglio d'Europa.

Il testo attuale tiene conto in parte delle forti preoccupazioni espresse dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali nel parere 4/2001, di cui dovrà tenersi conto in sede di eventuale ratifica da parte dell'Italia.

86 L'attività dei gruppi di esperti

Il Consiglio d'Europa ha svolto e svolge tuttora un importante ruolo in materia di protezione dei dati personali. Il primo strumento internazionale cogente in materia è infatti la Convenzione del 28 gennaio 1981, n. 108, frutto dei lavori svoltisi per lunghi anni in quel consesso. La Convenzione trae diretta ispirazione dall'articolo 8 della Convenzione europea dei diritti umani del 1950 ed ha carattere tendenzialmente universale: l'articolo 23 della stessa prevede infatti che possano essere invitati ad aderire anche Stati non membri del Consiglio d'Europa.

Un protocollo addizionale alla Convenzione, facoltativo per i Paesi che intendano accedere ad essa, è stato aperto alla firma l'8 novembre 2001 (l'Italia è tra i Paesi firmatari). Esso integra e specifica le disposizioni della Convenzione n. 108, da un lato, recependo le soluzioni introdotte a livello comunitario con la direttiva 95/46/CE, relativamente all'attribuzione dei compiti di verifica e controllo dei trattamenti in ciascun Paese ad autorità di controllo indipendenti e, dall'altro, in materia di disciplina dei flussi transfrontalieri di dati.

Inoltre, nel corso della Conferenza di Varsavia sulla protezione dei dati – promossa dal Consiglio d'Europa e dall'autorità garante polacca, il 19/20 novembre 2001 – che ha celebrato il ventesimo anniversario della Convenzione, è stata riaffermata la permanente centralità dei principi dalla stessa sanciti. Le conclusioni della Conferenza, cui ha preso parte il Segretario generale del Garante, hanno confermato la scelta di lasciare immutato il testo della Convenzione e di operare invece, laddove necessario, per adeguare – attraverso strumenti vincolanti o meno, a seconda delle materie trattate – i principi sanciti alle "nuove emergenze", quali quelle legate agli sviluppi tecnologici ed all'uso crescente delle tecnologie elettroniche (ad esempio videosorveglianza, digitalizzazione, *smart card*, Internet, comunicazioni elettroniche).

Proseguirà in tal modo l'attività dei due comitati (o gruppi di lavoro a carattere permanente) che si occupano della protezione dei dati: il T-PD, comitato detto "convenzionale" in quanto previsto dall'articolo 18 della stessa Convenzione, ed il CJ-PD, costituito nell'ambito del comitato cui fa capo la cooperazione giudiziaria (CD-CJ), anche se, in considerazione delle recenti ristrettezze di bilancio, essi hanno avviato lo studio di modalità per la razionalizzazione dei lavori, incaricando a tal fine un sotto gruppo *ad hoc*, a composizione mista. Le proposte, che potrebbero includere anche la fusione degli stessi comitati in un'unica struttura, saranno poi vagliate in seduta plenaria dal T-PD e dal CJ-PD e, se approvate, dovranno essere sottoposte ai competenti organi decisionali del Consiglio d'Europa.

Il T-PD, formato da rappresentanti dei 27 Paesi aderenti alla Convenzione n. 108 (gli Stati membri dell'Unione europea, oltre Islanda, Lettonia, Lituania, Norvegia, Slovacchia, Slovenia, Ungheria, Svizzera, Cipro, Romania, Estonia e Repubblica Ceca), ha il compito di interpretare le disposizioni della Convenzione e di assicurarne l'effettiva applicazione. L'art. 19 conferisce al comitato ampie possibilità di intervento, che comprendono la formulazione di proposte per facilitare o migliorare l'applicazione della disciplina, anche emendandone il testo, e l'emissione di pareri sia in ordine ad ipotesi emendative sottoposte da uno Stato parte o dal Comitato dei Ministri, sia su ogni questione comunque relativa all'applicazione della convenzione.

Gli altri Stati membri del Consiglio d'Europa – che sono attualmente 45 – e la Comunità europea, attraverso la Commissione, possono prendere parte alle riunioni in qualità di osservatori, senza tuttavia diritto di voto, non essendo state ancora approvate le necessarie modifiche alla convenzione. Inoltre, la composizione attuale è mista in quanto alcuni Paesi, come l'Italia, hanno rappresentanti provenienti dalle Autorità nazionali di protezione dei dati, altri, inclusi alcuni Paesi dell'Unione europea, sono presenti con funzionari designati dai ministeri della giustizia o dell'interno.

Il T-PD sta elaborando il testo di clausole contrattuali standard miranti a facilitare il trasferimento di dati verso Paesi che non hanno proceduto alla ratifica della convenzione e che non dispongono di una legislazione

86

che garantisca il richiesto livello di protezione ("equivalente" nel testo originario, "adeguato" nella dizione usata dal protocollo aggiuntivo).

Il CJ-PD è il comitato che ha lavorato alla predisposizione della convenzione n. 108 e, successivamente, all'elaborazione delle Raccomandazioni volte a disciplinare i singoli settori in modo da garantire l'applicazione della normativa in materia di tutela dei dati.

L'attività più recente del comitato è stata, in particolare, rivolta allo studio ed alla predisposizione della Raccomandazione sulla protezione della vita privata su Internet (Racc. 99/5) e della proposta di Raccomandazione sul trattamento dei dati personali raccolti e trattati a fini assicurativi, il cui testo è stato recentemente approvato dal Comitato dei Ministri.

Altri argomenti all'esame del Comitato, sviluppati anche attraverso la costituzione di specifici gruppi di lavoro ristretti, riguardano l'applicazione dei principi della protezione dei dati in materia di videosorveglianza ed in relazione all'uso delle *smart card.*

È stato inoltre costituito un qualificato gruppo di lavoro – di cui fa parte anche il Segretario generale del Garante – per approfondire, anche alla luce dei risultati del "Progetto Falcone" (v. *Relazione 2000*, par. 97, p. 131), gli aspetti relativi all'applicazione dei principi di protezione dei dati all'attività di polizia (e giudiziaria) e per una valutazione della Raccomandazione 87/15 del Consiglio d'Europa.

87 Linee-guida in materia di sorveglianza

Con riguardo alle attività di videosorveglianza, che presentano specifiche problematiche per la protezione dati, il Consiglio d'Europa, sulla base del rapporto commissionato al Segretario generale del Garante italiano, sta definendo un intervento in materia.

Per il momento è stata esclusa l'ipotesi di adottare una raccomandazione, orientandosi piuttosto il CJ-PD verso la predisposizione di uno strumento di indirizzo più flessibile per i destinatari, in modo che le esigenze di sicurezza e di controllo anticrimine tengano in debito conto il diritto dei cittadini di difendere la propria sfera privata e la propria libertà ed in modo da assicurare che le attività di videosorveglianza si svolgano nel pieno rispetto dei principi della convenzione n. 108 e delle specifiche raccomandazioni.

Il documento, presentato sotto forma di linee-guida, individua le regole di base che chiunque intenda porre in essere tale attività è tenuto a rispettare, di tal che:

- l'attività di sorveglianza si esplichi su base legale per fini leciti, espliciti e legittimi;

- "siano adottate tutte le misure volte ad assicurare che questa attività sia conforme alla normativa in materia di protezione dei dati personali";

- il ricorso alla videosorveglianza possa darsi solo quando non sia possibile utilizzare sistemi meno invasivi ed intrusivi della *privacy*;

- si rispetti il principio di selettività e di proporzionalità in rapporto agli scopi perseguiti nei singoli casi, in modo da prevenire conseguenze irragionevoli sulle libertà e sui comportamenti degli interessati;

- si rispetti il principio di pertinenza e di non eccedenza rispetto a immagini, suoni e dati biometrici raccolti, con particolare attenzione alle modalità di raccolta, onde evitare che le informazioni raccolte siano registrate, indicizzate o conservate per lunghi periodi;

- si eviti che l'attività di videosorveglianza possa determinare discriminazioni o possa essere disposta nei confronti di soggetti per il solo fatto di avere determinate opinioni, convinzioni o comportamenti di tipo sessuale;

- l'attività si svolga nel rispetto del principio di trasparenza e di pubblicità;

- si escluda, in linea di principio, la diffusione e la comunicazione dei dati personali a soggetti non interessati all'attività di sorveglianza;

- si regolamenti il diritto di accesso, nonché gli altri diritti delle persone interessate;

- si assicuri un'adeguata informativa ai lavoratori interessati e una possibile intesa con le organizzazioni sindacali per esigenze organizzative e/o produttive o per ragioni di sicurezza del lavoro che possano comportare un controllo a distanza.

O.C.S.E.

88 I risultati conseguiti nel 2001

Nel corso del 2001, il Garante ha partecipato ai lavori del *Working Party on Information Security and Privacy* (WPISP) all'interno del *Committee for Information, Computer and Communication Policy* (ICCP).

A seguito della Dichiarazione di Ottawa del 1998, relativa alla protezione della vita privata sulle reti, l'O.C.S.E. ha concentrato molte energie su tutti gli aspetti della *privacy* maggiormente collegati all'innovazione tecnologica. In quella sede, infatti, era emerso con molta chiarezza che il commercio elettronico avrebbe potuto sviluppare tutte le sue potenzialità solo se fossero state fornite, agli utilizzatori delle reti e ai consumatori, adeguate garanzie in materia di trattamento di dati personali. Oltre a riaffermare la validità e l'attualità delle linee-guida dell'O.C.S.E. sulla protezione della vita privata del 1980, sono stati invitati i Paesi membri a incoraggiare l'adozione di specifiche politiche in tema di riservatezza – attuabili con strumenti giuridici, amministrativi, tecnologici e di autoregolamentazione – e si è posto l'accento sulla necessità di prevedere, in caso di mancato rispetto di tali principi, meccanismi efficaci e supportati da idonee garanzie con riferimento ai mezzi di tutela. In quella occasione, si era auspicata, inoltre, una campagna di sensibilizzazione degli utilizzatori delle reti in merito ai problemi del rispetto della riservatezza e ai possibili mezzi di protezione *on-line*, soprattutto attraverso l'utilizzo di tecnologie che permettessero di migliorare la protezione della vita privata.

All'interno di questa cornice si devono collocare gli studi portati avanti in sede O.C.S.E. in relazione alla protezione dei dati personali.

Va innanzitutto ricordato che, in materia di risoluzione alternativa delle controversie (ADR), il segretariato ha sottoposto ai delegati un questionario relativo al ricorso a queste ultime nei singoli ordinamenti, al fine di avere un quadro complessivo della situazione esistente e di trovare spunti per incoraggiare gli operatori a ricorrere a tale tipo di risoluzione. Le ADR risultano, infatti, particolarmente vantaggiose sia in termini di costi, sia in termini di tempo, oltre ad essere un elemento decisivo per invogliare i cittadini a ricorrere al commercio elettronico. Il documento di sintesi sarà reso pubblico nei prossimi mesi.

Il tema delle tecnologie volte ad aumentare la *privacy* ("*Privacy Enhancing Technologies*") è stato oggetto di numerosi incontri, cui hanno partecipato anche consulenti esterni. Oltre alla volontà di aumentarne la diffusione tra le imprese e i consumatori, è emersa anche la necessità di rendere tali tecnologie più efficaci e più trasparenti.

L'aggiornamento e l'approvazione delle nuove linee-guida per la sicurezza dei sistemi informativi e delle reti è stato il tema centrale del lavoro del WPISP a partire dal mese di settembre del 2001. Tale documento ha assunto un valore simbolico dell'impegno dell'O.C.S.E. nella lotta al terrorismo, ed è proprio in quest'ottica che si è deciso di approvare il nuovo testo entro il settembre 2002, primo anniversario degli attentati a New York. Il contenuto non ha subito sostanziali modifiche rispetto alle linee-guida del 1992, salvo un profondo riorientamento alla luce delle nuove tecnologie emerse nel frattempo, soprattutto con riferimento alle reti. La filosofia che sottende questi nuovi principi è volta a sensibilizzare tutti gli utenti delle reti ad una nuova "cultura della sicurezza" che diventi in qualche modo "istintiva" per ogni utilizzatore di computer. I principi enunciati, che prenderanno la forma di una raccomandazione del Consiglio dell'O.C.S.E. ai Paesi membri, riguardano la consapevolezza dei rischi, la responsabilità, il rispetto dei legittimi interessi dei terzi, la compatibilità con i valori democratici, la capacità di reazione agli incidenti relativi alla sicurezza, la valutazione dei rischi, la salvaguardia e la gestione della sicurezza e l'aggiornamento costante dei sistemi di sicurezza.

Il segretariato, infine, nell'ambito di uno studio sugli strumenti giuridici e tecnici di regolamentazione e autoregolamentazione volti a garantire la *privacy* in rete, ha diffuso un questionario da sottoporre ai delegati, al fine di individuare tutti gli strumenti esistenti nel campo dell'autodisciplina. La finalità è quella di fare un inventario sia per il settore pubblico, sia per il settore privato, con particolare riferimento al grado di rispetto di queste norme oltre che alla reale possibilità di applicazione *on-line*.

89 Ulteriori iniziative

Il Garante ha inoltre partecipato con assiduità a numerose conferenze europee e di rilevanza mondiale che, per la loro importanza e la natura dei temi trattati, hanno rappresentato un significativo foro di discussione e hanno consentito un puntuale aggiornamento.

Sono state, in particolare, seguite le Conferenze internazionali ed europee delle Autorità garanti (a partire da quella di Parigi del settembre del 2001 che ha fatto seguito a quella di Venezia del precedente anno), le quali sono organizzate con criteri di periodicità, nella primavera e nell'autunno di ciascun anno.

Oltre alla Conferenza europea dell'aprile del 2001, tenutasi ad Atene, va tra l'altro ricordata la Conferenza di Varsavia del 19/20 novembre 2001 organizzata dal Consiglio d'Europa, cui ha partecipato il segretario generale dell'Autorità, nonché quella di rilevanza mondiale tenutasi di recente a San Francisco, cui hanno preso parte il prof. Gaetano Rasi e alcuni collaboratori del Garante (CFP2002, 12^ *Conference on Computers, Freedom and Privacy*, 16/19 aprile 2002).

Da segnalare infine la particolare attenzione rivolta in più circostanze dalle autorità europee al tema della conservazione dei dati di traffico ed in genere delle "tracce" di comunicazioni elettroniche ed alle esigenze in materia delle forze di polizia e della magistratura.

Documentazione

TESTI

90 Legge 31 dicembre 1996, n. 675
Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
(testo aggiornato con le modifiche del d.lg. 28 dicembre 2001, n. 467)

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.

1-bis. [1] *La presente legge si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, mezzi situati nel territorio dello Stato anche diversi da quelli elettronici o comunque automatizzati, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea.*

1-ter.[1] *Nei casi di cui al comma 1-bis il titolare stabilito nel territorio di un Paese non appartenente all'Unione europea deve designare ai fini dell'applicazione della presente legge un proprio rappresentante stabilito nel territorio dello Stato.*

(1) Commi aggiunti dall'art. 1, comma 2, d.lg. 28 dicembre 2001, n. 467.

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.[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 *l'articolo 18*.

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 confluirvi 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) [3]

1. [4] 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 *se il trattamento, in ragione delle relative modalità*

(2) Comma così modificato dall'art. 2, d.lg. 28 dicembre 2001, n. 467.

(3) Per quanto concerne il presente articolo, si rammenta che l'art. 3, comma 4, d.lg. 28 dicembre 2001, n. 467, prevede quanto segue: "Le disposizioni di cui all'articolo 7, commi 3, 4, 5, 5-bis, 5-ter, 5-quater e 5-quinquies, 13, comma 1, lett. b) e 28, comma 7, della legge 31 dicembre 1996, n. 675 sono abrogate a decorrere dalla data di entrata in vigore delle modifiche apportate al regolamento di cui all'articolo 33, comma 3, della medesima legge in applicazione del comma 1 del presente articolo."

(4) Comma così modificato dall'art. 3, comma 1, d.lg. 28 dicembre 2001, n. 467.

o della natura dei dati personali, sia suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato, e nei soli casi e con le modalità individuati con il regolamento di cui all'articolo 33, comma 3.

2.[5] 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 che *devono essere indicati* 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) [6] il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede *del rappresentante del titolare nel territorio dello Stato e di almeno un responsabile, da indicare nel soggetto eventualmente designato ai fini di cui all'articolo 13*; in mancanza di tale indicazione si considera responsabile il notificante;
i) la qualità e la legittimazione del notificante.

5. I soggetti tenuti ad iscriversi o che devono essere annotati nel registro delle imprese di cui all'articolo 2188 del codice civile, nonché coloro che devono fornire le informazioni di cui all'articolo 8, comma 8, lettera d), della legge 29 dicembre 1993, n. 580, alle camere di commercio, industria, artigianato e agricoltura, possono effettuare la notificazione per il tramite di queste ultime, secondo le modalità stabilite con il regolamento di cui all'articolo 33, comma 3. I piccoli imprenditori e gli artigiani possono effettuare la notificazione anche per il tramite delle rispettive rappresentanze di categoria; gli iscritti agli albi professionali anche per il tramite dei rispettivi ordini professionali. Resta in ogni caso ferma la disposizione di cui al comma 3.

5-bis [7]. 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;
c-bis) [8] 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-ter [7]. 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;

(5) Comma così modificato dall'art. 3, comma 2, d.lg 28 dicembre 2001, n. 467.
(6) Lettera così modificata dall'art. 3, comma 3, d.lg. 28 dicembre 2001, n. 467. In base all'art. 24, comma 1, di quest'ultimo d.lg., la disposizione in oggetto si applica a decorrere dal 1 marzo 2002.
(7) Commi aggiunti dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.
(8) Lettera inserita dall'art. 2, comma 1, lett. a), d.lg. 30 luglio 1999, n. 281.

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) [9] *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.*

5-quater. [10] *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.

(9) Lettera inserita dall'art. 2, comma 1, lett. b), d.lg. 30 luglio 1999, n. 281.
(10) Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

5-quinquies[11]*. 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-bis.[12] *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. 10. (Informazioni rese al momento della raccolta)

1.[13] 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;

---

(11) Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

(12) Comma aggiunto dall'art. 3, d.lg. 30 luglio 1999, n. 281.

(13) Comma così modificato dall'art. 1, d.lg. 9 maggio 1997, n. 123.

f) [14] il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare, *del suo rappresentante nel territorio dello Stato e di almeno un responsabile, da indicare nel soggetto eventualmente designato ai fini di cui all'articolo 13, indicando il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili.*

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.[15] La disposizione di cui al comma 3 non si applica quando l'informativa all'interessato comporta un impiego di mezzi che il Garante dichiari 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 difensive di cui alla legge 7 dicembre 2000, n. 397*, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

Sezione II - DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

Art. 11. (Consenso)

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 10.

Art. 12. (Casi di esclusione del consenso)

1. Il consenso non è richiesto quando il trattamento:

a) riguarda dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) [16] è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o *per l'esecuzione di misure precontrattuali adottate* 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) [17] *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) [18] 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;

(14) Lettera così modificata dall'art. 4, d.lg. 28 dicembre 2001, n. 467. In base all'art. 24, comma 1, di quest'ultimo d.lg., la disposizione in oggetto si applica a decorrere dal 1 marzo 2002.
(15) Comma così modificato dall'art. 19, d.lg. 28 dicembre 2001, n. 467.
(16) Lettera così modificata dall'art. 5, comma 1, d.lg 28 dicembre 2001, n. 467.
(17) Lettera così sostituita dall'art. 4, comma 1, d.lg. 30 luglio 1999, n. 281.
(18) Lettera così modificata dall'art. 12, comma 1, d.lg. 13 maggio 1998, n. 171.

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) [19] è necessario ai fini dello svolgimento delle *investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397*, 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;

h-bis) [20] *è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.*

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'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati, secondo le modalità ed entro i limiti stabiliti dal regolamento di cui all'articolo 33, comma 3.

3. I diritti di cui al comma 1 riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia interesse.

4. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

5. Restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

Art. 14. (Limiti all'esercizio dei diritti)

(19) Lettera così modificata dall'art. 19, d.lg. 28 dicembre 2001, n. 467.

(20) Lettera inserita dall'art. 5, comma 2, d.lg. 28 dicembre 2001, n. 467. Ai sensi dell'art. 24, comma 2, di quest'ultimo decreto, "I provvedimenti attuativi delle disposizioni di cui agli articoli 5, comma 2, e 9 sono adottati, in sede di prima applicazione del presente decreto, entro centoventi giorni a decorrere dal 1 ottobre 2002."

90

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);

e-bis) [21] *da fornitori di servizi di telecomunicazioni accessibili al pubblico, limitatamente ai dati personali identificativi di chiamate telefoniche entranti, salvo che possa derivarne pregiudizio per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397.*

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 UTILIZZABILITA' 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

(21) Lettera inserita dall'art. 6, d.lg. 28 dicembre 2001, n. 467.

dati sono raccolti;

c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

c-bis) [22] *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.

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;

a-bis) [23] *qualora siano necessarie per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'esecuzione di misure precontrattuali adottate su richiesta di quest'ultimo;*

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) [24] 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;

(22) Lettera inserita dall'art. 5, d.lg. 30 luglio 1999, n. 281.
(23) Lettera inserita dall'art. 7, comma 1, d.lg. 28 dicembre 2001, n. 467.
(24) Lettera così modificata dall'art. 12, comma 2, d.lg. 13 maggio 1998, n. 171.

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) [25] limitatamente alla comunicazione, qualora questa sia necessaria ai fini dello svolgimento delle *investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397*, 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 1° settembre 1993, n. 385, nonché tra società controllate e società collegate ai sensi dell'articolo 2359 del codice civile, i cui trattamenti con finalità correlate sono stati notificati ai sensi dell'articolo 7, comma 2, per il perseguimento delle medesime finalità per le quali i dati sono stati raccolti;

h-bis) [26] *limitatamente alla comunicazione, quando questa sia necessaria, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.*

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) [27] *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;*

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) [28]

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.

(25) Lettera così modificata dall'art. 19, d.lg. 28 dicembre 2001, n. 467.
(26) Lettera inserita dall'art. 7, comma 2, d.lg. 28 dicembre 2001, n. 467.
(27) Lettera così sostituita dall'art. 4, comma 2, d.lg. 30 luglio 1999, n. 281.
(28) 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".

1-bis. [29] *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.*

1-ter. [30] *Il comma 1 non si applica, altresì, ai dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.*

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. [31] *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. [32] *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. [33] *I dati personali indicati al comma 1 possono essere oggetto di trattamento previa autorizzazione del Garante:*

a) qualora il trattamento sia effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, confessioni e comunità religiose, per il perseguimento di finalità lecite, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati o diffusi fuori del relativo ambito e l'ente, l'associazione o l'organismo determinino idonee garanzie relativamente ai trattamenti effettuati;

b) qualora il trattamento 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;

c) qualora il trattamento sia necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, di rango pari a quello dell'interessato quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale, 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.

---

(29) Comma inserito dall'art. 5, comma 1, d.lg. 11 maggio 1999, n. 135.

(30) Comma inserito dall'art. 8, comma 1, d.lg. 28 dicembre 2001, n. 467.

(31) Comma così sostituito dall'art. 5, comma 2, d.lg. 11 maggio 1999, n. 135.

(32) Comma inserito dall'art. 5, comma 3, d.lg. 11 maggio 1999, n. 135.

(33) Comma così sostituito dall'art. 8, comma 2, d.lg. 28 dicembre 2001, n. 467. Si ricorda, a proposito di questo comma, quanto previsto dall'art. 24, comma 3, d.lg. 28 dicembre 2001, n. 467: "In sede di prima applicazione della disposizione di cui alla lettera a) del comma 4 dell'articolo 22 della legge 31 dicembre 1996, n. 675, introdotta dall'articolo 8 del presente decreto, le garanzie previste nella medesima lettera a) sono determinate dall'associazione, dall'ente o dall'organismo entro il 30 giugno 2002."

90

Art. 23. (Dati inerenti alla salute) [34]

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. [35] *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. [35] *Il decreto di cui al comma 1 disciplina anche quanto previsto dall'articolo 22, comma 3-bis, della legge.*

1-quater. [35] *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. [36] 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.

3. L'autorizzazione di cui al comma 1 è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità. E' 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.

---

(34) 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".
(35) Commi inseriti dall'art. 2, comma 1, d.lg. 30 luglio 1999, n. 282.
(36) Comma così modificato dall'art. 2, comma 2, d.lg. 30 luglio 1999, n. 282.

Articolo 24-bis (Altri dati particolari) [37]

1. Il trattamento dei dati diversi da quelli di cui agli articoli 22 e 24 che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante sulla base dei principi sanciti dalla legge nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, sulla base di un eventuale interpello del titolare.

Art. 25. (Trattamento di dati particolari nell'esercizio della professione di giornalista)

1.[38] *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. [39] 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. [40] 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. [41] *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.*

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.

---

(37) Articolo inserito dall'art. 9, d.lg. 28 dicembre 2001, n. 467. Ai sensi dell'art. 24, comma 2, di quest'ultimo decreto, "I provvedimenti attuativi delle disposizioni di cui agli articoli 5, comma 2, e 9 sono adottati, in sede di prima applicazione del presente decreto, entro centoventi giorni a decorrere dal 1 ottobre 2002."
(38) Comma così sostituito dall'art. 12, comma 3, d.lg. 13 maggio 1998, n. 171.
(39) Comma così modificato dall'art. 12, comma 4, d.lg. 13 maggio 1998, n. 171.
(40) Comma così modificato dall'art. 2, comma 1, d.lg. 9 maggio 1997, n. 123.
(41) Comma aggiunto dall'art. 2, comma 2, d.lg. 9 maggio 1997, n. 123.

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. [42] 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 e *ricorra uno dei casi individuati ai sensi dell'articolo 7, comma 1*.

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. [43] 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. 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) [44] sia necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o *per l'esecuzione di misure precontrattuali adottate* 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) [45] sia necessario ai fini dello svolgimento delle *investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397*, 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) [46] sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche

(42) Comma così modificato dall'art. 10, comma 1, d.lg. 28 dicembre 2001, n. 467.
(43) Comma così modificato dall'art. 10, comma 2, d.lg. 28 dicembre 2001, n. 467, che ha soppresso in fine le parole "ovvero, se si tratta dei dati di cui agli articoli 22 e 24, di grado pari a quello assicurato dall'ordinamento italiano."
(44) Lettera così modificata dall'art. 10, comma 3, d.lg. 28 dicembre 2001, n. 467.
(45) Lettera così modificata dall'art. 19, d.lg. 28 dicembre 2001, n. 467.
(46) Lettera così modificata dall'art. 10, comma 4, d.lg. 28 dicembre 2001, n. 467.

con un contratto, *ovvero individuate dalla Commissione europea con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995;*

g-bis) [47] *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* [48] giorni dalla data di presentazione, equivale a rigetto.

5. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento cessa di avere ogni effetto se, entro i successivi venti giorni, non è adottata la decisione di cui al comma 4 ed è impugnabile unitamente a tale decisione.

6. Avverso il provvedimento espresso o il rigetto tacito di cui al comma 4, il titolare o l'interessato possono proporre opposizione al tribunale del luogo ove risiede il titolare, entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. L'opposizione non sospende l'esecuzione del provvedimento.

6-bis [49]*. 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*

(47) Lettera inserita dall'art. 4, comma 3, d.lg. 30 luglio 1999, n. 281.
(48) Parola così sostituita dall'art. 13, comma 1, lett. a), d.lg. 30 luglio 1999, n. 281.
(49) Comma inserito dall'art. 13, comma 1, lett. b), d.lg. 30 luglio 1999, n. 281.

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 PERSONALI [50]

Art. 30. (Istituzione del Garante)

1.[51] E' istituito il *Garante per la protezione dei dati personali.*

2. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

3. Il Garante è organo collegiale costituito da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. Essi eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. I membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

4. Il presidente e i membri durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i membri non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

5. All'atto dell'accettazione della nomina il presidente e i membri sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai membri compete un'indennità di funzione non eccedente, nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate, con il regolamento di cui all'articolo 33, comma 3, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

Art. 31. (Compiti del Garante)

1. Il Garante ha il compito di:

a) istituire e tenere un registro generale dei trattamenti sulla base delle notificazioni ricevute;

b) controllare se i trattamenti sono effettuati nel rispetto delle norme di legge e di regolamento e in conformità alla notificazione;

c) [52] segnalare ai relativi titolari o responsabili le modificazioni *necessarie o opportune* al fine di rendere il trat-

(50) Denominazione così modificata dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123.
(51) Comma così modificato dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123.
(52) Lettera così modificata dall'art. 11, comma 1, d.lg. 28 dicembre 2001, n. 467.

tamento 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) [53] vietare, in tutto o in parte, il trattamento dei dati o disporne il blocco *se il trattamento risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera c), oppure* 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.

(53) Lettera così modificata dall'art. 11, comma 2, d.lg 28 dicembre 2001, n. 467.

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*,[54] da dipendenti dello Stato e di altre amministrazioni pubbliche, collocati fuori ruolo nelle forme previste dai rispettivi ordinamenti, il cui servizio presso il medesimo ufficio è equiparato ad ogni effetto di legge a quello prestato nelle rispettive amministrazioni di provenienza. Il relativo contingente è determinato, in misura non superiore a quarantacinque unità, su proposta del Garante medesimo, con decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri del tesoro e per la funzione pubblica, entro novanta giorni dalla data di elezione del Garante. *Il segretario generale può essere scelto anche tra magistrati ordinari o amministrativi.* [55]

1-bis. [56] *E' 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*

(54) Parole inserite dall'art. 1, comma 1, d.lg. 26 febbraio 1999, n. 51.
(55) Parole aggiunte dall'art. 3, comma 2, d.lg. 9 maggio 1997, n. 123.
(56) Comma aggiunto dall'art. 1, comma 2, d.lg. 26 febbraio 1999, n. 51.

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 [57] *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. [58] *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. [58] *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. [58] *All'ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e quelli concernenti le funzioni di gestione attribuite ai dirigenti.*

2. Le spese di funzionamento dell'ufficio del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero del tesoro. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

3.[59] *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. [60]

(57) Comma aggiunto dall'art. 1, comma 2, d.lg. 26 febbraio 1999, n. 51.
(58) Commi aggiunti dall'art. 2, comma 1, d.lg. 26 febbraio 1999, n. 51.
(59) Comma così modificato dall'art. 2, comma 2, d.lg. 26 febbraio 1999, n. 51.
(60) 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."

3-bis. [61] *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. [62] 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. [63] *Il personale dell'ufficio del Garante addetto agli accertamenti di cui all'articolo 32 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.*

CAPO VIII - SANZIONI

Art. 34. (Omessa o incompleta notificazione) [64]

1. [65] *Chiunque, essendovi tenuto, non provvede tempestivamente alle notificazioni in conformità a quanto previsto dagli articoli 7, 16, comma 1, e 28, ovvero indica in esse notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da lire dieci milioni a lire sessanta milioni e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione.*

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. [66] 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 21, 22, 23, *24 e 24-bis, 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) [67]

1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in vio-

(61) Comma inserito dall'art. 2, comma 3, d.lg. 26 febbraio 1999, n. 51.
(62) Comma così modificato dall'art. 2, comma 4, d.lg. 26 febbraio 1999, n. 51.
(63) Comma aggiunto dall'art. 2, comma 5, d.lg. 26 febbraio 1999, n. 51.
(64) Articolo così sostituito dall'art. 12, d.lg. 28 dicembre 2001, n. 467.
(65) In relazione al presente articolo, si rammenta il disposto dell'art. 12, comma 2, d. lg. 28 dicembre 2001, n. 467: "Alle violazioni dell'articolo 34 della legge 31 dicembre 1996, n. 675, commesse prima dell'entrata in vigore del presente decreto si applicano, in quanto compatibili, le disposizioni di cui agli articoli 100, 101 e 102 del decreto legislativo 30 dicembre 1999, n. 507."
(66) Comma così modificato dall'art. 13, d.lg. 28 dicembre 2001, n. 467.
(67) Articolo così sostituito dall'art. 14, comma 1, d.lg. 28 dicembre 2001, n. 467. L'art. 14, comma 2, di quest'ultimo d.lg. prevede, inoltre, che "Per i procedimenti penali per il reato di cui all'articolo 36 della legge 31 dicembre 1996, n. 675 in corso, entro quaranta giorni dall'entrata in vigore del presente decreto l'autore del reato può fare richiesta all'autorità giudiziaria di essere ammesso alla procedura indicata all'articolo 36, comma 2, della medesima legge n. 675 del 1996, come sostituito dal presente decreto. L'Autorità giudiziaria dispone la sospensione del procedimento e trasmette gli atti al Garante per la protezione dei dati personali che provvede ai sensi del medesimo articolo 36, comma 2".

lazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con l'arresto sino a due anni o con l'ammenda da lire dieci milioni a lire ottanta milioni.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, in quanto applicabili.

Art. 37. (Inosservanza dei provvedimenti del Garante)

1. [68] Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 22, comma 2*, o degli articoli 29, commi 4 e 5, e 31, comma 1, lettera l),* è punito con la reclusione da tre mesi a due anni.

Art. 37-bis. (Falsità nelle dichiarazioni e nelle notificazioni al Garante) [69]

1. Chiunque, nelle notificazioni di cui agli articoli 7, 16, comma 1, e 28 o in atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre 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. [70] Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 29, comma 4, e 32, comma 1, è punito con la sanzione amministrativa del pagamento di una somma *da lire cinquemilioni a lire trentamilioni.*

2. [71] *La violazione delle disposizioni di cui all'articolo 10 è punita con la sanzione amministrativa del pagamento di una somma da lire tre milioni a lire diciotto milioni o, nei casi di cui agli articoli 22, 24 e 24-bis o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da lire cinque milioni a lire trenta milioni. La somma può essere aumentata sino al triplo quando essa risulti inefficace in ragione delle condizioni economiche del contravventore. La violazione della disposizione di cui all'articolo 23, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da lire cinquecentomila a lire tre milioni.*

3. [72] L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al *presente capo* [73] 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.*

(68) Comma così modificato dall'art. 15, d.lg. 28 dicembre 2001, n. 467.
(69) Articolo inserito dall'art. 16, d.lg. 28 dicembre 2001, n. 467.
(70) Comma così modificato dall'art. 17, comma 1, d.lg. 28 dicembre 2001, n. 467.
(71) Comma così sostituito dall'art. 14, comma 2, d.lg. 28 dicembre 2001, n. 467.
(72) Comma così modificato dall'art. 14, d.lg. 30 luglio 1999, n. 281.
(73) Parole così sostituite dall'art. 14, comma 3, d.lg. 28 dicembre 2001, n. 467.

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. [74] 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. *Le disposizioni del presente comma restano in vigore sino alla data del 30 giugno 2003.*

2. [75] *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. [76] 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. [77] *Le disposizioni della presente legge che prevedono un'autorizzazione del Garante si applicano limitatamente alla medesima autorizzazione e fatta eccezione per la disposizione di cui all'articolo 28, comma 4, lettera g), a decorrere dal 30 novembre 1997. Le medesime disposizioni possono essere applicate dal Garante anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti.*

7-bis. [78] *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 [79]. Il controllo sul Centro elaborazione dati è esercitato dal *Garante per la protezione dei dati personali*, nei modi previsti dalla legge e dai regolamenti.

2. [79] I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti

(74) Comma così modificato dall'art. 18, d.lg. 28 dicembre 2001, n. 467.
(75) Comma così sostituito dall'art. 2, d.lg. 28 luglio 1997, n. 255.
(76) Comma da ultimo così modificato dall'art. 1, comma 1, d.lg. 6 novembre 1998, n. 389.
(77) Comma così sostituito dall'art. 4, comma 1, d.lg. 9 maggio 1997, n. 123.
(78) Comma aggiunto dall'art. 4, comma 2, d.lg. 9 maggio 1997, n. 123.
(79) Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

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. [80] Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre venti giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni 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. E' istituita l'Autorità per l'informatica nella pubblica amministrazione, denominata Autorità ai fini del presente decreto; tale Autorità opera in piena autonomia e con indipendenza di giudizio e di valutazione.".

3. Il comma 1 dell'articolo 5 del decreto legislativo 12 febbraio 1993, n. 39, è sostituito dal seguente: "1. Le norme concernenti l'organizzazione ed il funzionamento dell'Autorità, l'istituzione del ruolo del personale, il relativo trattamento giuridico ed economico e l'ordinamento delle carriere, nonché la gestione delle spese nei limiti previsti dal presente decreto, anche in deroga alle disposizioni sulla contabilità generale dello Stato, sono adottate con regolamento emanato con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato, su proposta del Presidente del Consiglio dei ministri, di concerto con il Ministro del tesoro e su parere conforme dell'Autorità medesima. Il parere del Consiglio di Stato sullo schema di regolamento è reso entro trenta giorni dalla ricezione della richiesta, decorsi i quali il regolamento può comunque essere emanato. Si applica il trattamento economico previsto per il personale del Garante per l'editoria e la radiodiffusione ovvero dell'organismo che dovesse subentrare nelle relative funzioni, fermo restando il limite massimo complessivo di centocinquanta unità. Restano altresì fermi gli stanziamenti dei capitoli di cui al comma 2, così come determinati per il 1995 e tenendo conto dei limiti di incremento previsti per la categoria IV per il triennio 1996-1998.".

4. [80] 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 amministra-

(80) Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

tivi 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.

91 Decreto Legislativo 28 dicembre 2001, n. 467 Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'art. 1 della legge 24 marzo 2001, n. 127

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;

Vista la direttiva 95/46/CE del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati;

Vista la legge 24 marzo 2001, n. 127, recante differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676;

Vista la direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni;

Vista la raccomandazione del Consiglio d'Europa n. (95) 4 del 7 febbraio 1995, sulla protezione dei dati personali nel settore dei servizi di telecomunicazioni, con particolare riguardo ai servizi telefonici;

Visto il decreto legislativo 13 maggio 1998, n. 171, recante disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio;

Sentito il Garante per la protezione dei dati personali;

Vista la deliberazione preliminare del Consiglio dei Ministri, adottata nella riunione del 21 novembre 2001;

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 21 dicembre 2001;

Sulla proposta del Presidente del Consiglio dei Ministri, di concerto con il Ministro della giustizia;

EMANA
il seguente decreto legislativo

CAPO I - MODIFICAZIONI ED INTEGRAZIONI ALLA LEGGE N. 675/1996

Art. 1. Definizioni e diritto nazionale applicabile

1. Agli effetti dell'applicazione del presente decreto si applicano le definizioni elencate nell'articolo 1, comma 2, della legge 31 dicembre 1996, n. 675.

2. Nell'articolo 2 della legge 31 dicembre 1996, n. 675, sono aggiunti i seguenti commi:

"1-*bis*. La presente legge si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, mezzi situati nel territorio dello Stato anche diversi da quelli elettronici o comunque automatizzati, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea.

1-*ter*. Nei casi di cui al comma 1-*bis* il titolare stabilito nel territorio di un Paese non appartenente all'Unione europea deve designare ai fini dell'applicazione della presente legge un proprio rappresentante stabilito nel territorio dello Stato.".

Art. 2. Trattamenti per fini esclusivamente personali

1. Nell'articolo 3, comma 2, della legge 31 dicembre 1996, n. 675, le parole: "le disposizioni di cui agli articoli 18 e 36" sono sostituite dalle seguenti: "l'articolo 18".

Art. 3. Semplificazione dei casi e delle modalità di notificazione

1. Nell'articolo 7, comma 1, della legge 31 dicembre 1996, n. 675, è aggiunto in fine il seguente periodo: "se il trattamento, in ragione delle relative modalità o della natura dei dati personali, sia suscettibile di recare pregiudizio ai diritti e alle libertà dell'interessato, e nei soli casi e con le modalità individuati con il regolamento di cui all'articolo 33, comma 3.".

2. Nell'articolo 7, comma 2, della legge 31 dicembre 1996, n. 675, le parole: "indicati nel comma 4" sono sostituite dalle seguenti: "che devono essere indicati".

3. Nell'articolo 7, comma 4, lettera *b)*, della legge 31 dicembre 1996, n. 675, le parole: "del responsabile;" sono sostituite dalle seguenti: "del rappresentante del titolare nel territorio dello Stato e di almeno un responsabile, da indicare nel soggetto eventualmente designato ai fini di cui all'articolo 13;".

4. Le disposizioni di cui all'articolo 7, commi 3, 4, 5, 5-*bis*, 5-*ter*, 5-*quater* e 5-*quinquies*, 13, comma 1, lettera *b)* e 28, comma 7, della legge 31 dicembre 1996, n. 675 sono abrogate a decorrere dalla data di entrata in vigore delle modifiche apportate al regolamento di cui all'articolo 33, comma 3, della medesima legge in applicazione del comma 1 del presente articolo.

Art. 4. Informativa all'interessato

1. Nell'articolo 10, comma 1, lettera *f)*, della legge 31 dicembre 1996, n. 675, le parole: "e, se designato, del responsabile" sono sostituite dalle seguenti: ", del suo rappresentante nel territorio dello Stato e di almeno un responsabile, da indicare nel soggetto eventualmente designato ai fini di cui all'articolo 13, indicando il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili.".

Art. 5. Misure precontrattuali e bilanciamento di interessi

1. Nell'articolo 12, comma 1, lettera *b)*, della legge 31 dicembre 1996, n. 675, le parole: "per l'acquisizione di informative precontrattuali attivate" sono sostituite dalle seguenti: "per l'esecuzione di misure precontrattuali adottate".

2. Nell'articolo 12, comma 1, della legge 31 dicembre 1996, n. 675, è inserita in fine la seguente lettera: "*h-bis)* è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.".

Art. 6. Limiti al diritto di accesso

1. Nell'articolo 14, comma 1, della legge 31 dicembre 1996, n. 675, è aggiunta in fine la seguente lettera:

"*e-bis)* da fornitori di servizi di telecomunicazioni accessibili al pubblico, limitatamente ai dati personali

identificativi di chiamate telefoniche entranti, salvo che possa derivarne pregiudizio per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397.".

Art. 7. Presupposti per la comunicazione e la diffusione dei dati

1. Nell'articolo 20, comma 1, della legge 31 dicembre 1996, n. 675, dopo la lettera *a)* è inserita la seguente:

"*a-bis)* qualora siano necessarie per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'esecuzione di misure precontrattuali adottate su richiesta di quest'ultimo,".

2. Nell'articolo 20, comma 1, della legge 31 dicembre 1996, n. 675, è inserita in fine la seguente lettera:

"*h-bis)* limitatamente alla comunicazione, quando questa sia necessaria, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.".

Art. 8. Dati sensibili

1. Nell'articolo 22 della legge 31 dicembre 1996, n. 675, dopo il comma 1-*bis* è inserito il seguente:

"1-*ter*. Il comma 1 non si applica, altresì, ai dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria".

2. Nell'articolo 22 della legge 31 dicembre 1996, n. 675, il comma 4 è sostituito dal seguente:

"4. I dati personali indicati al comma 1 possono essere oggetto di trattamento previa autorizzazione del Garante:

a) qualora il trattamento sia effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, confessioni e comunità religiose, per il perseguimento di finalità lecite, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati o diffusi fuori del relativo ambito e l'ente, l'associazione o l'organismo determinino idonee garanzie relativamente ai trattamenti effettuati;

b) qualora il trattamento 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;

c) qualora il trattamento sia necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, di rango pari a quello dell'interessato quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale, 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. 9. Verifiche preliminari

1. Dopo l'articolo 24 della legge 31 dicembre 1996, n. 675, è inserito il seguente:

"Art. 24-*bis (Altri dati particolari).*

1. Il trattamento dei dati diversi da quelli di cui agli articoli 22 e 24 che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante sulla base dei princìpi

sanciti dalla legge nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, sulla base di un eventuale interpello del titolare.".

Art. 10. Semplificazione e garanzie per i trasferimenti di dati personali all'estero

1. Nell'articolo 28, comma 1, della legge 31 dicembre 1996, n. 675, le parole: "o riguardi taluno dei dati di cui agli articoli 22 e 24" sono sostituite dalle seguenti: "e ricorra uno dei casi individuati ai sensi dell'articolo 7, comma 1".

2. Nell'articolo 28, comma 3, della legge 31 dicembre 1996, n. 675, le parole da: "ovvero," fino alla fine del periodo sono soppresse.

3. Nell'articolo 28, comma 4, lettera *b)*, della legge 31 dicembre 1996, n. 675, le parole: "per l'acquisizione di informative precontrattuali attivate" sono sostituite dalle seguenti: "per l'esecuzione di misure precontrattuali adottate".

4. Nell'articolo 28, comma 4, lettera *g)*, della legge 31 dicembre 1996, n. 675, sono inserite in fine le seguenti parole: ", ovvero individuate dalla Commissione europea con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995".

Art. 11. Misure per il trattamento illecito o non corretto

1. Nella lettera *c)* del comma 1 dell'articolo 31 della legge 31 dicembre 1996, n. 675, la parola: "opportune" è sostituita dalle seguenti: "necessarie o opportune".

2. Nella lettera *l)* del comma 1 dell'articolo 31 della legge 31 dicembre 1996, n. 675, dopo la parola: "blocco" sono inserite le seguenti: "se il trattamento risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera *c)*, oppure".

Art. 12. Sanzione in tema di notificazione

1. L'articolo 34 della legge 31 dicembre 1996, n. 675 è sostituito dal seguente:

"Art. 34 *(Omessa o incompleta notificazione)*.

1. Chiunque, essendovi tenuto, non provvede tempestivamente alle notificazioni in conformità a quanto previsto dagli articoli 7, 16, comma 1, e 28, ovvero indica in esse notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da lire dieci milioni a lire sessanta milioni e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione.".

2. Alle violazioni dell'articolo 34 della legge 31 dicembre 1996, n. 675, commesse prima dell'entrata in vigore del presente decreto si applicano, in quanto compatibili, le disposizioni di cui agli articoli 100, 101 e 102 del decreto legislativo 30 dicembre 1999, n. 507.".

Art. 13. Trattamento illecito di dati personali

1. Nell'articolo 35, comma 2, della legge 31 dicembre 1996, n. 675, le parole: "comunica o diffonde" sono sostituite dalle seguenti: "procede al trattamento di" e le parole: "e 24, ovvero" sono sostituite dalle parole: ", 24 e 24-*bis*, ovvero".

Art. 14. Omessa adozione di misure minime di sicurezza

1. L'articolo 36 della legge 31 dicembre 1996, n. 675, è sostituito dal seguente:

"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 l'arresto sino a due anni o con l'ammenda da lire dieci milioni a lire ottanta milioni.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, in quanto applicabili.".

2. Per i procedimenti penali per il reato di cui all'articolo 36 della legge 31 dicembre 1996, n. 675 in corso, entro quaranta giorni, dall'entrata in vigore del presente decreto l'autore del reato può fare richiesta all'autorità giudiziaria di essere ammesso alla procedura indicata all'articolo 36, comma 2, della medesima legge n. 675 del 1996, come sostituito dal presente decreto. L'Autorità giudiziaria dispone la sospensione del procedimento e trasmette gli atti al Garante per la protezione dei dati personali che provvede ai sensi del medesimo articolo 36, comma 2.

Art. 15. Inosservanza di provvedimenti di divieto o di blocco

1. Nell'articolo 37, comma 1, della legge 31 dicembre 1996, n. 675, le parole: "o dell'articolo 29, commi 4 e 5," sono sostituite dalle seguenti: "o degli articoli 29, commi 4 e 5, e 31, comma 1, lettera *l)*,".

Art. 16. False comunicazioni e dichiarazioni

1. Dopo l'articolo 37 della legge 31 dicembre 1996, n. 675, è inserito il seguente:

"Art. 37-*bis (Falsità nelle dichiarazioni e nelle notificazioni al Garante)*

1. Chiunque, nelle notificazioni di cui agli articoli 7, 16, comma 1, e 28 o in atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.".

Art. 17. Adeguamento di sanzioni amministrative

1. Nell'articolo 39, comma 1, della legge 31 dicembre 1996, n. 675, le parole: "da lire un milione a lire sei milioni" sono sostituite dalle seguenti: "da lire cinquemilioni a lire trentamilioni".

2. L'articolo 39, comma 2, della legge 31 dicembre 1996, n. 675, è sostituito dal seguente:

"2. La violazione delle disposizioni di cui all'articolo 10 è punita con la sanzione amministrativa del pagamento di una somma da lire tre milioni a lire diciotto milioni o, nei casi di cui agli articoli 22, 24 e 24-*bis* o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da lire cinque milioni a lire trenta milioni. La somma può essere aumentata sino al triplo quando essa risulti inefficace in ragione delle condizioni economiche del contravventore. La violazione della disposizione di cui all'articolo 23, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da lire cinquecentomila a lire tre milioni.".

3. Nell'articolo 39, comma 3, della legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, le parole: "presente articolo" sono sostituite dalle seguenti: "presente capo".

Art. 18. Adeguamento dei trattamenti alla disciplina comunitaria

1. Nell'articolo 41, comma 1, della legge 31 dicembre 1996, n. 675, è aggiunto in fine il seguente periodo: "Le disposizioni del presente comma restano in vigore sino alla data del 30 giugno 2003.".

Art. 19. Investigazioni difensive

1. Negli articoli 10, comma 4, 12, comma 1, lettera *h)*, 20, comma 1, lettera *g)* e 28, comma 4, lettera *d)*, della legge 31 dicembre 1996, n. 675, le parole: "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," sono sostituite dalle parole: "investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397,".

Capo II - Attuazione dei principi di protezione dei dati in determinati settori

Art. 20. Codici di deontologia e di buona condotta

1. Al fine di garantire la piena attuazione dei principi previsti dalla disciplina in materia di trattamento dei dati personali, ai sensi dell'articolo 31, comma 1, lettera *h)*, della legge 31 dicembre 1996, n. 675, il Garante promuove entro il 30 giugno 2002 la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali nei settori indicati al comma 2, tenendo conto della specificità dei trattamenti nei diversi ambiti, nonché dei criteri direttivi delle raccomandazioni del Consiglio d'Europa indicate nell'articolo 1, comma 1, lettera *b)*, della legge 31 dicembre 1996, n. 676.

2. I codici di cui al comma 1 riguardano il trattamento di dati personali:

a) effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica, con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di telecomunicazione gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole ed interattivo, per favorire una piu' ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 9 della legge 31 dicembre 1996, n. 675, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato;

b) necessari per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di *curricula* contenenti dati personali anche sensibili;

c) effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni;

d) svolto a fini di informazione commerciale, prevedendo anche, in correlazione con quanto previsto dall'articolo 10, comma 4, della legge 31 dicembre 1996, n. 675, modalità semplificate per l'informativa all'interessato e idonei meccanismi per favorire la qualità e l'esattezza dei dati raccolti e comunicati;

e) effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati, individuando anche specifiche modalità per favorire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato;

f) provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui debba essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla raccomandazione del Consiglio d'Europa N. R (91) 10 in relazione all'articolo 9 della legge 31 dicembre 1996, n. 675;

g) effettuato con strumenti automatizzati di rilevazione di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantirne la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 9 della legge 31 dicembre 1996, n. 675.

3. Il rispetto delle disposizioni in essi contenute costituisce condizione essenziale per la liceità del trattamento dei dati.

4. I codici sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante e riportati in allegato al testo unico delle disposizioni in materia previsto dall'articolo 1, comma 4, della legge 24 marzo 2001, n. 127.

CAPO III - MODIFICAZIONI ED INTEGRAZIONI AL DECRETO LEGISLATIVO N. 171/1998

Art. 21. Modalità di pagamento alternative alla fatturazione

1. All'articolo 5, comma 1, del decreto legislativo 13 maggio 1998, n. 171, le parole: "consentono che" sono sostituite dalle seguenti: "sono tenuti a predisporre ogni misura idonea affinchè".

2. Dopo il comma 1 dell'articolo 5 del decreto legislativo 13 maggio 1998, n. 171, è inserito il seguente:

"1-*bis*. I fornitori di cui al comma 1 sono tenuti a documentare al Garante, entro il 30 giugno 2002, le misure predisposte. In caso di mancata documentazione si applica la sanzione amministrativa prevista dall'articolo 39, comma 1, della legge 31 dicembre 1996, n. 675. In mancanza di idonee misure il Garante provvede altresi' ai sensi dell'articolo 31, comma 1, lettere *c)* ed *l)*, della medesima legge.".

Art. 22. Informazione al pubblico sull'identificazione della linea chiamante e collegata

1. All'articolo 6, comma 6, del decreto legislativo 13 maggio 1998, n. 171, le parole "di tale servizio" sono sostituite dalle seguenti: "di tale servizio e delle possibilità previste ai commi 1, 2, 3 e 4".

Art. 23. Chiamate di emergenza

1. L'articolo 7 del decreto legislativo 13 maggio 1998, n. 171, è cosi' modificato:

"*a)* la rubrica è sostituita dalla seguente: "*(Chiamate di disturbo e di emergenza)*";

b) dopo il comma 2, è aggiunto il seguente:

"2-*bis*. Il fornitore di una rete di telecomunicazioni pubblica o di un servizio di telecomunicazioni accessibili al pubblico deve predisporre procedure adeguate e trasparenti per garantire, linea per linea, l'annullamento della soppressione dell'identificazione della linea chiamante da parte dei servizi abilitati a ricevere chiamate d'emergenza.".

Art. 24. Disposizioni transitorie

1. Le disposizioni di cui agli articoli 3, comma 3, 4, 22 e 23 del presente decreto si applicano a decorrere dal 1 marzo 2002.

2. I provvedimenti attuativi delle disposizioni di cui agli articoli 5, comma 2, e 9 sono adottati, in sede di prima applicazione del presente decreto, entro centoventi giorni a decorrere dal 1° ottobre 2002.

3. In sede di prima applicazione della disposizione di cui alla lettera *a)* del comma 4 dell'articolo 22 della legge 31 dicembre 1996, n. 675, introdotta dall'articolo 8 del presente decreto, le garanzie previste nella medesima lettera *a)* sono determinate dall'associazione, dall'ente o dall'organismo entro il 30 giugno 2002.

Art. 25. Entrata in vigore

1. Le disposizioni di cui al presente decreto entrano in vigore il 1° febbraio 2002.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

92 Legge 24 marzo 2001, n. 127
Differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali

Art. 1.

1. I decreti legislativi di cui all'articolo 1, comma 1, lettere *b)*, numeri 2), 3), 4), 5) e 6), *c)*, *d)*, *e)*, *i)*, *l)*, *n)*, ed *o)*, e all'articolo 2 della legge 31 dicembre 1996, n. 676, e successive modificazioni, in materia di trattamento dei dati personali, sono emanati entro il 31 dicembre 2001, sulla base dei principi e dei criteri direttivi indicati nella medesima legge.

2. I decreti legislativi di cui al comma 1, sono emanati previo parere delle Commissioni permanenti del Senato della Repubblica e della Camera dei deputati competenti per materia. Il parere è espresso entro trenta giorni dalla richiesta, indicando specificamente le eventuali disposizioni non ritenute corrispondenti ai principi e ai criteri direttivi contenuti nella legge di delegazione.

3. Il Governo procede comunque alla emanazione dei decreti legislativi qualora il parere non sia espresso entro trenta giorni dalla richiesta.

4. Il Governo emana, entro dodici mesi dallo scadere del termine di cui al comma 1 e previa acquisizione dei pareri previsti nel comma 2, da esprimersi entro sessanta giorni dalla richiesta, un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse, coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurarne la migliore attuazione.

5. Il Governo procede comunque alla emanazione del testo unico qualora il parere non sia espresso entro sessanta giorni dalla richiesta.

Art. 2.

1. La presente legge entra in vigore il giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

93

Legge 28 marzo 2001, n. 145
Ratifica ed esecuzione della Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano riguardo all'applicazione della biologia e della medicina: Convenzione sui diritti dell'uomo e sulla biomedicina, fatta a Oviedo il 4 aprile 1997, nonché del Protocollo addizionale del 12 gennaio 1998, n. 168, sul divieto di clonazione di esseri umani

Art. 1.

1. Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano riguardo all'applicazione della biologia e della medicina: Convenzione sui diritti dell'uomo e sulla biomedicina, fatta a Oviedo il 4 aprile 1997, nonché il Protocollo addizionale del 12 gennaio 1998, n. 168, sul divieto di clonazione di esseri umani.

Art. 2.

1. Piena e intera esecuzione è data alla Convenzione e al Protocollo di cui all'articolo 1, a decorrere dalla data della loro entrata in vigore, in conformità a quanto disposto, rispettivamente, dall'articolo 33 della Convenzione e dall'articolo 5 del Protocollo.

Art. 3.

1. Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti ulteriori disposizioni occorrenti per l'adattamento dell'ordinamento giuridico italiano ai princìpi e alle norme della Convenzione e del Protocollo di cui all'articolo 1.

2. Gli schemi dei decreti legislativi, di cui al comma 1, sono trasmessi al Senato della Repubblica e alla Camera dei deputati perché sia espresso dalle competenti Commissioni permanenti un parere entro il termine di quaranta giorni, decorso il quale i decreti legislativi sono emanati anche in mancanza del parere.

94 Autorizzazione n. 1/2002 al trattamento dei dati sensibili nei rapporti di lavoro

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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 i dati personali "sensibili";

Considerato che i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998 n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

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;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato nell'ambito dei rapporti di lavoro;

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

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:

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, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lett. b) e c);

b) ad organismi paritetici o che gestiscono osservatori in materia di lavoro, previsti dalla normativa comunitaria, dalle leggi, 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 dalla normativa comunitaria, da leggi, 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), che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, 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 d.P.R. n. 318/1999, 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).

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 23, comma 2, della legge n. 675/1996), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Restano inoltre fermi gli obblighi di informare l'interessato e di acquisirne il consenso scritto, 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, lett. 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 controlli periodici, 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, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. 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 l'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

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 dalle 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 e disciplina transitoria.
La presente autorizzazione ha efficacia a decorrere dal 1° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 1/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

95 Autorizzazione n. 2/2002 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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 i dati personali "sensibili";

Considerato che i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati;

Visti gli artt. 22, comma 3 e comma 3-bis e 23 della medesima legge n. 675/1996;

Visto l'art. 17 del decreto legislativo 11 maggio 1999, n. 135 e successive modificazioni ed integrazioni, nonché il provvedimento del Garante n. 1/P/2000 del 30 dicembre 1999 – 13 gennaio 2000, pubblicato sulla Gazzetta Ufficiale n. 26 del 2 febbraio 2000, con il quale sono state individuate le rilevanti finalità di interesse pubblico di cui all'art. 22 comma 3 della legge n. 675/1996;

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; considerato che analoghe modalità semplificate sono previste dall'art. 17, comma 3, del decreto legislativo n. 135/1999;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Visto l'art. 17, comma 5, del decreto legislativo 11 maggio 1999, n. 135 (come integrato e modificato dall'art. 16 del d.lg. 30 luglio 1999, n. 281), secondo cui il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione; considerato che il trattamento dei dati genetici può essere proseguito nei limiti di quanto disposto dalla presente autorizzazione fino al rilascio della predetta autorizzazione;

Ritenuto opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998 n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno

95

o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, 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 e di efficacia pari a quelle previste in tale ambito;

Considerato che un elevato numero di trattamenti idonei a rivelare lo stato di salute e la vita sessuale è effettuato per finalità di prevenzione o di cura, per la gestione di servizi socio-sanitari, per ricerche scientifiche o per la fornitura all'interessato di prestazioni, beni o servizi;

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15, del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

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;

b) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare con il consenso i dati idonei a rivelare lo stato di salute e la vita sessuale;

c) gli organismi sanitari pubblici, istituiti anche presso università, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute, anche per il perseguimento delle finalità di rilevante interesse pubblico individuate dall'art. 17, comma 1, del decreto legislativo n. 135/1999 o dal provvedimento del Garante n. 1/P/2000 del 30 dicembre 1999-13 gennaio 2000, o da altro provvedimento di questa Autorità parimenti adottato ai sensi dell'art. 22, comma 3 bis, della legge n. 675/1996, qualora ricorrano contemporaneamente le seguenti condizioni:

1) il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;

2) manchi il consenso (articolo 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;

d) anche soggetti diversi da quelli di cui alle lettere a), b) e c) a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora il trattamento 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.

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:

a) ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;

b) al personale sanitario infermieristico, tecnico e della riabilitazione che esercita l'attività in regime di libera professione;

c) alle istituzioni e agli organismi sanitari privati, anche quando non operino in rapporto con il Servizio sanitario nazionale.

In tali casi, l'autorizzazione è rilasciata al fine di consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, 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 diffusive, di tutela della salute mentale, di assistenza farmaceutica e di assistenza sanitaria alle attività sportive o di accertamento, in conformità alla legge, degli illeciti previsti dall'ordinamento sportivo. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario, ovvero di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini suindicati.

Qualora il perseguimento di tali fini richieda l'espletamento di compiti di organizzazione o di gestione amministrativa, i destinatari della presente autorizzazione devono esigere che i responsabili e gli incaricati del trattamento preposti a tali compiti osservino le stesse regole di segretezza alle quali sono sottoposti i medesimi destinatari della presente autorizzazione, 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, nn. 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 reli-

giose 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, ove necessario attinenti anche alla vita sessuale, 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 ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o comunque 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) che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, 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 d.P.R. n.

318/1999, 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, lett. 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, anche mediante controlli periodici, 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, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. 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 l'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

5) Comunicazione e diffusione dei dati.

Ai sensi dell'articolo 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 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 e disciplina transitoria.

La presente autorizzazione ha efficacia a decorrere dal 1° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 2/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

96 Autorizzazione n. 3/2002 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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'art. 22, comma 1, della citata legge n. 675/1996, il quale individua i dati personali "sensibili";

Visto, in particolare, l'art. 22, commi 1 bis e 1 ter, rispettivamente introdotti dall'art. 5, comma 1, del decreto legislativo n. 135/1999 e dall'art. 8 comma 1, del decreto legislativo n. 467/2001;

Visto altresì l'art. 22, comma 4, della citata legge n. 675/1996, come modificato dal decreto legislativo n. 467/2001, e considerato che i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998 n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

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;

Considerato che un elevato numero 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;

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

96

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

autorizza

il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996 da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, alle condizioni di seguito indicate.

1) Ambito di applicazione e finalità del trattamento.

La presente autorizzazione è rilasciata:

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'articolo 310 del decreto legislativo 16 aprile 1994, n. 297.

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi, sempreché il diritto da far valere o difendere sia di rango pari a quello dell'interessato quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale, 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 registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.

Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi e persone giuridiche.

I soggetti di cui alle lettere a), b) e c), possono comunicare alle persone giuridiche e agli organismi con scopo di lucro, titolari di un autonomo trattamento, i soli dati sensibili strettamente indispensabili per le attività di effettivo ausilio alle

predette finalità, con particolare riferimento alle generalità degli interessati e ad indirizzari, sulla base di un atto scritto che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo e le particolari misure di sicurezza adottate. La dichiarazione scritta di consenso degli interessati deve porre tale circostanza in particolare evidenza, e deve recare la precisa menzione dei titolari del trattamento e delle finalità da essi perseguite. Le persone giuridiche e gli organismi con scopo di lucro, oltre a quanto previsto nei punti 3) e 5) in tema di pertinenza e di non eccedenza dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

2) Interessati ai quali i dati si riferiscono.

Il trattamento può riguardare i dati sensibili attinenti:

a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;

b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l'associazione, la fondazione o il diverso organismo;

c) ai soggetti che ricoprono cariche sociali o onorifiche;

d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall'associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all'atto costitutivo, ove esistenti;

e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;

f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

3) Categorie di dati oggetto di trattamento.

L'autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l'autorizzazione generale n. 2/2002.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 22, comma 1, della legge 31 dicembre 1996, n. 675, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, che non possano essere perseguite o adempiuti, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

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, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

4) Modalità di trattamento.

Fermi restando gli obblighi previsti dagli artt. 9, 15, 17 e 28 della legge n. 675/1996 e dal d.P.R. n. 318/1999, 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).

I dati sono raccolti, di regola, presso l'interessato.

Restano fermi gli obblighi di informare l'interessato e di acquisirne il consenso scritto nei casi previsti dagli articoli 10 e 22 della legge n. 675/1996, come modificati dal decreto legislativo n. 467/2001.

5) Conservazione dei dati.
Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lett. 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 dalla normativa comunitaria, da norme di legge 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 e disciplina transitoria.
La presente autorizzazione ha efficacia a decorrere dal 1° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 3/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

97 Autorizzazione n. 4/2002 al trattamento dei dati sensibili da parte dei liberi professionisti

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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 i dati personali "sensibili";

Considerato che i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998 n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

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;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da liberi professionisti iscritti in albi o elenchi professionali per l'espletamento delle rispettive attività professionali;

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

97

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, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96, o 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. 2/2002;

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. 1/2002;

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 strettamente pertinenti e non eccedenti rispetto ad incarichi conferiti che non possano essere svolti mediante il trattamento di dati anonimi o di dati personali di natura diversa.

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. 2/2002.

3) Finalità del trattamento.

Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che il libero professionista può eseguire in base al proprio ordinamento professionale, e in particolare:

a) per curare gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro;

b) per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi;

c) ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, 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 d.P.R. n. 318/1999.

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 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 o di esercizio della professione in forma societaria ai sensi del decreto legislativo 2 febbraio 2001, n. 96.

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, lett. e) della legge n. 675/1996, i dati sensibili possono essere conservati, per il periodo di tempo previsto dalla normativa comunitaria, da leggi, 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 in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. 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 l'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

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 dalla normativa comunitaria, da norme di legge, 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 e disciplina transitoria.

La presente autorizzazione ha efficacia a decorrere dal 1° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 4/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

98 Autorizzazione n. 5/2002 al trattamento dei dati sensibili da parte di diverse categorie di titolari

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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 i dati personali "sensibili";

Considerato che i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998 n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

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;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da parte di soggetti operanti in diversi settori di attività economiche di seguito individuate;

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Gaetano Rasi;

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, agenzie di viaggio e 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 normativa comunitaria, dalla legge, 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 contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

3) Interessati ai quali i dati si riferiscono e categorie di dati trattati.

Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

4) Comunicazione e diffusione dei dati.

I dati sensibili possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società con-

trollate 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. 1/2002, rilasciata il 31 gennaio 2002, 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. 4/2002, rilasciata il 31 gennaio 2002, 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 e l'origine razziale ed etnica 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 e l'origine razziale ed etnica 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.

98

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. 2/2002, rilasciata il 31 gennaio 2002.

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 d.P.R. n. 318/1999, 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.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 23, comma 2, della legge n. 675/1996), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

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, lett. e) della legge 31 dicembre 1996, n. 675, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità ovvero per adempiere agli obblighi o agli incarichi menzionati nei precedenti capi. A tal fine, anche mediante controlli periodici, 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, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. 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 l'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

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 dalla normativa comunitaria, da norme di legge o di regolamento 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, previsti anche dai codici deontologici e di buona condotta adottati in attuazione dell'art. 20 del decreto legislativo n. 467/2001, 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 e disciplina transitoria.

La presente autorizzazione ha efficacia a decorrere dal 1° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 5/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

99 Autorizzazione n. 6/2002 al trattamento di dati sensibili da parte degli investigatori privati

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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 i dati personali "sensibili";

Considerato che i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati;

Considerato che una speciale disposizione (art. 22, comma 4, legge n. 675/1996, come modificato dal decreto legislativo n. 467/2001) permette di trattare i dati sensibili senza il consenso degli interessati, quando il trattamento autorizzato dal Garante è necessario per svolgere una investigazione difensiva ai sensi della legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, di rango pari a quello dell'interessato quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998 n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

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;

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. 2/2002, rilasciata il 31 gennaio 2002), 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 anche le prescrizioni dell'autorizzazione n. 2/2002 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;

Considerato che ulteriori misure ed accorgimenti saranno prescritti dal Garante all'atto della sottoscrizione dell'apposito codice di deontologia e di buona condotta in via di emanazione (art. 22, comma 4, legge n. 675/1996);

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Gaetano Rasi;

autorizza

gli investigatori privati 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 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, che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato, deve essere 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 in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (art. 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397).

Restano ferme le altre autorizzazioni generali rilasciate ai fini dello svolgimento delle investigazioni in relazione ad un procedimento penale o per l'esercizio di un diritto in sede giudiziaria, in particolare:

a) nell'ambito dei rapporti di lavoro (autorizzazione n. 1/2002, rilasciata il 31 gennaio 2002);

b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione generale n. 2/2002, rilasciata il 31 gennaio 2002);

c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione generale n. 3/2002, rilasciata il 31 gennaio 2002);

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. 4/2002, rilasciata il 31 gennaio 2002);

e) relativamente ai dati di carattere giudiziario (autorizzazione generale n. 7/2002, rilasciata il 31 gennaio 2002).

99

2) Categorie di dati e interessati ai quali i dati si riferiscono.

Il trattamento può riguardare i dati sensibili di cui all'art. 22, comma 1, della legge n. 675/1996, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità di cui al punto 1), che non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

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. 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. 2/2002, 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, in via di definizione 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, lett. 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 dalla normativa comunitaria, ovvero da norme di legge o di regolamento, 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 d. P.R. n. 318/1999.

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 legge n. 675/1996).

8) Efficacia temporale e disciplina transitoria.

La presente autorizzazione ha efficacia a decorrere dal 1° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 6/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

100 Autorizzazione n. 7/2002 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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 legge n. 675/1996, che ammette il trattamento dei dati personali idonei a rivelare i provvedimenti giudiziari ivi richiamati, anche da parte di soggetti pubblici, "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";

Considerato che diversi trattamenti dei predetti dati da parte di soggetti pubblici sono disciplinati nel decreto legislativo 11 maggio 1999, n. 135, nonché nel provvedimento del Garante n. 1/P/2000 del 30 dicembre 1999 - 13 gennaio 2000, pubblicato sulla Gazzetta Ufficiale n. 26 del 26 febbraio 2000;

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;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 41, comma 7, legge n. 675/1996);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti autorizzatori da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 gennaio 2002, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Considerato che l'art. 8, par. 5, della direttiva 95/46/CE 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;

100

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 opportuno che anche tali nuove autorizzazioni provvisorie siano a tempo determinato ai sensi dell'art. 14 del d.P.R. 31 marzo 1998, n. 501, in relazione alla prevista emanazione del testo unico della normativa in materia di protezione dei dati personali, in attuazione della legge n. 127 del 2001;

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;

Visto l'art. 35 della legge n. 675/1996;

Visto il regolamento recante norme sulle misure minime di sicurezza adottato con d.P.R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

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;

c) conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

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 1886, 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, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96 o 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;

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, lett. a) della legge 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 tale 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 in riferimento ad un 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 legge 7 dicembre 2000, n. 397);

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, in conformità a quanto previsto dalla normativa in materia di appalti pubblici.

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, lett. 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, lett. 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° febbraio 2002 fino al 30 giugno 2003.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 7/2000, il titolare deve adeguarsi ad esse entro il 31 maggio 2002.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 gennaio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

101 Autorizzazione al trasferimento di dati personali verso organizzazioni aventi sede negli Stati Uniti secondo i "Principi di approdo sicuro in materia di riservatezza" - 10 ottobre 2001 (*)

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. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) secondo la quale i "Principi di approdo sicuro in materia di riservatezza" allegati alla medesima decisione, applicati in conformità agli orientamenti forniti da talune "Domande più frequenti" (FAQ) parimenti allegate, garantiscono un livello adeguato di protezione dei dati personali trasferiti dalla Comunità ad organizzazioni aventi sede negli Stati Uniti sulla base della documentazione pubblicata dal Dipartimento del commercio statunitense ivi menzionata;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 6 del citato art. 25 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: a) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; b) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; c) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare una misura necessaria per l'applicazione della decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE;

Ritenuto che i sette Principi allegati alla decisione e precisati in n. 15 FAQ, su cui si è espresso con vari pareri ed osservazioni anche il Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono alcune garanzie per i diritti dell'interessato che in conformità al diritto comunitario vanno ritenute adeguate ai sensi del citato art. 28, comma 4, lett. g);

Considerato che i soggetti che applicano i predetti Principi possono prevedere ulteriori garanzie per le persone cui si riferiscono i dati, rispetto a quelle minime previste dalla richiamata decisione;

(*) v. par. 128 e 132 della presente Relazione per il richiamo ipertestuale

101

Rilevato che la decisione della Commissione può essere adattata alla luce dell'esperienza acquisita nella sua attuazione o alla luce di nuove normative intervenute negli Stati Uniti (art. 4);

Visti gli articoli 2 e 3 della decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

Vista la FAQ n. 5 sul ruolo che le autorità di garanzia degli Stati membri dovrebbero svolgere con la cooperazione delle organizzazioni statunitensi che ricevano dati personali dall'Unione europea, anche nell'ambito di un comitato (panel) informale di autorità costituito a livello europeo cui il Garante intende partecipare;

Rilevato che le autorità di garanzia degli Stati membri, riunite nel Gruppo di cui all'art. 29 della direttiva europea n. 95/46/CE, hanno aderito all'inserimento della FAQ n. 5 nel pacchetto di misure previsto dalla decisione della Commissione;

Ritenuta la necessità di assicurare ulteriore pubblicità ai predetti Principi disponendo la loro pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Giuseppe Santaniello;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti effettuati sulla base e in conformità ai "Principi di approdo sicuro in materia di riservatezza", applicati in conformità alle "Domande più frequenti" (FAQ) e all'ulteriore documentazione allegata alla decisione della Commissione europea del 26 luglio 2000, n. 2000/520/CE;

2) si riserva di svolgere, in conformità alla normativa comunitaria, alla legge n. 675/1996, all'art. 3 della decisione della Commissione e all'allegata FAQ. n. 5, i necessari controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti medesimi, nonché sul rispetto dei predetti Principi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 10 ottobre 2001

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

102 Autorizzazione al trasferimento di dati personali verso Paesi terzi in conformità alle clausole contrattuali standard approvate dalla Commissione europea - 10 ottobre 2001 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Stefano Rodotà, presidente, del Prof. Giuseppe Santaniello, vicepresidente, del Prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, nei termini previsti nel paragrafo 2 del medesimo articolo;

Visto l'art. 26 della predetta direttiva il quale individua alcune deroghe al menzionato principio, prevedendo anche che uno Stato membro possa autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un Paese terzo che non garantisce un livello di protezione adeguato, qualora il titolare del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, risultanti anche da clausole contrattuali appropriate;

Visto il comma 4 del medesimo articolo 26 sulle decisioni della Commissione europea in materia di clausole contrattuali tipo;

Vista la decisione della Commissione europea del 15 giugno 2001 n. 2001/497/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 181 del 4 luglio 2001) secondo la quale alcune clausole contrattuali tipo, allegate alla medesima decisione, costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, in caso di trasferimento di dati personali verso Paesi terzi a norma della direttiva 95/46/CE;

Considerato che gli Stati membri devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 4 del citato art. 26 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: a) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; b) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; c) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare, in conformità al citato art. 28, una misura necessaria per l'applicazione della decisione della Commissione;

Ritenuto che le citate clausole contrattuali tipo, che sono state articolate dalla Commissione in n. 11 clausole e n. 3 allegati anche sulla base del parere favorevole del Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono alcune garanzie per i diritti dell'interessato da ritenere adeguate ai sensi del citato art. 28, comma 4, lett. g);

Considerato che i soggetti che utilizzano le citate clausole contrattuali possono prevedere ulteriori garanzie per le persone cui si riferiscono i dati, rispetto alle garanzie minime previste dalle clausole medesime;

(*) v. par. 107 della presente Relazione per il testo della decisione della Commissione

102

Rilevato che la decisione della Commissione riguarda unicamente i trasferimenti di dati effettuati a partire dal territorio dello Stato da un titolare del trattamento avente sede nella Comunità (soggetto esportatore) ad un diverso titolare del trattamento (soggetto importatore) e che un'ulteriore decisione della Commissione individuerà altre clausole contrattuali tipo per i trasferimenti di dati effettuati da un titolare del trattamento avente sede nella Comunità ad un responsabile del medesimo trattamento;

Ritenuta la necessità di assicurare ulteriore pubblicità alle predette clausole contrattuali tipo, disponendo la loro pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana in allegato alla presente autorizzazione;

Ritenuta la necessità di formulare nel dispositivo alcune precisazioni nell'esercizio dei compiti demandati a questa Autorità dall'art. 28 della citata direttiva e dalla legge n. 675/1996, richiamati anche dalla citata decisione della Commissione, nei limiti necessari per la prima fase di applicazione del presente provvedimento;

Ritenuto di dover riservare la scelta del Garante di svolgere o meno, caso per caso, il ruolo di mediazione previsto dalla clausola n. 7, paragrafo 1, lett. a) della decisione;

Riservata la specificazione di ulteriori criteri e modalità in base all'esperienza maturata nell'utilizzazione delle clausole, anche in sede comunitaria;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Stefano Rodotà;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati sulla base e in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea del 15 giugno 2001 n. 2001/497/CE, con effetto dal 3 settembre 2001 e sulla base dei seguenti presupposti:

- il soggetto esportatore e il soggetto importatore devono richiamare o incorporare le clausole nei contratti relativi al trasferimento dei dati in modo da renderle riconoscibili anche alle persone cui si riferiscono i dati e che chiedano di averne conoscenza, evitando altresì la previsione di clausole limitative o incompatibili (clausole nn. 4, lett. c) e 5, lett. e); considerando alla decisione n. 5);
- la copia del contratto relativo al trasferimento e le altre informazioni necessarie devono essere fornite al Garante solo a richiesta di questa Autorità (clausole nn. 4, 5 e 8; art. 32, comma 1, legge n. 675/1996);
- deve essere comunicata al Garante la scelta che è stata effettuata in caso di controversia non risolta in via amichevole e sottoposta all'esame di un soggetto diverso dal Garante o dall'autorità giudiziaria (clausola 7, par. 2 e par. 1, lett. a); art. 32, comma 1, legge n. 675/1996);

2) si riserva in ogni caso di svolgere i necessari controlli e di adottare eventuali provvedimenti anche di blocco o di divieto di trasferimento in conformità alla legge n. 675/1996 e alla normativa comunitaria (art. 4 e considerando n. 15 della decisione);

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 10 ottobre 2001

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

103 Autorizzazione al trasferimento di dati personali verso Paesi extra-europei in conformità alle clausole contrattuali tipo di cui alla decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/CE - 10 aprile 2002

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. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto l'art. 26 della predetta direttiva il quale individua alcune deroghe al menzionato principio, prevedendo anche che uno Stato membro possa autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un Paese terzo che non garantisce un livello di protezione adeguato, qualora il titolare del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, risultanti anche da clausole contrattuali appropriate;

Visto il comma 4 del medesimo art. 26 sulle decisioni della Commissione europea in materia di clausole contrattuali tipo;

Vista la decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 6 del 10 gennaio 2002) secondo la quale alcune clausole contrattuali tipo, allegate alla medesima decisione, costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, in caso di trasferimento di dati personali a responsabili del trattamento residenti in paesi terzi, a norma degli artt. 17, paragrafo 3, e 26, paragrafo 2, della direttiva 95/46/CE;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 4 del citato art. 26 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675, come modificato dall'art. 10 del decreto legislativo 28 dicembre 2001, n. 467, secondo cui il trasferimento dei dati personali all'estero può avvenire: a) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato; b) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; c) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto, ovvero individuate dalla Commissione europea con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva n. 95/46/CE del Parlamento e del Consiglio del 24 ottobre 1995 (comma 4, lett. g));

Vista la deliberazione n. 35 del 10 ottobre 2001 con la quale questa Autorità ha autorizzato il trasferimento di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea del 15 giugno 2001, n. 2001/497/CE;

Ritenuto che le nuove clausole contrattuali tipo, che sono state articolate dalla Commissione in n. 11 clausole e n. 2 appendici anche sulla base del parere favorevole del Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono alcune garanzie per i diritti dell'interessato da ritenere adeguate ai sensi del citato art. 28, comma 4, lett. g);

Considerato che i soggetti che utilizzano le citate clausole contrattuali possono prevedere ulteriori garanzie per le persone cui si riferiscono i dati, rispetto alle garanzie minime previste dalle clausole medesime;

Rilevato che la decisione della Commissione riguarda unicamente i trasferimenti di dati effettuati a partire dal ter-

103

ritorio dello Stato da un titolare del trattamento avente sede nella Comunità (soggetto esportatore) ad un responsabile del medesimo trattamento (soggetto importatore) residente in un Paese terzo che non assicura un livello di protezione adeguato, e che la citata decisione n. 2001/497/CE della Commissione ha già individuato le clausole contrattuali tipo per i trasferimenti di dati effettuati da un titolare del trattamento avente sede nella Comunità ad un diverso titolare del trattamento residente al di fuori della Comunità medesima;

Ritenuta la necessità di assicurare ulteriore pubblicità alle predette clausole contrattuali tipo, disponendo la loro pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana in allegato alla presente autorizzazione;

Ritenuta la necessità di formulare nel dispositivo alcune precisazioni nell'esercizio dei compiti demandati a questa Autorità richiamati anche dalla citata decisione della Commissione, nei limiti necessari per la prima fase di applicazione del presente provvedimento;

Ritenuto di dover riservare la scelta del Garante di svolgere o meno, caso per caso, il ruolo di mediazione previsto dalla clausola n. 7, paragrafo 1, lett. a) della decisione;

Riservata la specificazione di ulteriori criteri e modalità in base all'esperienza maturata nell'utilizzazione delle clausole, anche in sede comunitaria;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Gaetano Rasi;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati sulla base e in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/CE, con effetto dal 3 aprile 2002 e sulla base dei seguenti presupposti:

- il soggetto esportatore e il soggetto importatore devono richiamare o incorporare le clausole nei contratti relativi al trasferimento dei dati in modo da renderle riconoscibili anche alle persone cui si riferiscono i dati e che chiedano di averne conoscenza, provvedendo a rendere conoscibile su richiesta di queste ultime anche una descrizione generale delle misure di sicurezza adottate, ed evitando altresì la previsione di clausole limitative o incompatibili (clausole nn. 4, lett. h) e 5, lett. g); considerando alla decisione n. 4);
- la copia del contratto relativo al trasferimento e le altre informazioni necessarie devono essere fornite al Garante solo a richiesta di questa Autorità (clausola n. 8 e art. 32, comma 1, legge n. 675/1996);
- deve essere comunicata al Garante la scelta che è stata effettuata in caso di controversia non risolta in via amichevole e sottoposta all'esame di un soggetto diverso dal Garante o dall'autorità giudiziaria (clausola 7, par. 2 e par. 1, lett. a));

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e all'art. 4 della decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 10 aprile 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

104 Autorizzazione al trasferimento di dati personali verso l'Ungheria - 17 ottobre 2001 (*)

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. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 26 luglio 2000, n. 2000/519/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) con la quale si è constatato che l'Ungheria garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 6 del citato art. 25 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: a) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; b) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; c) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare una misura necessaria per l'applicazione della Decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE;

Ritenuto che le disposizioni di rango costituzionale e le altre norme vigenti in Ungheria in materia di protezione dei dati personali, valutate dalla Commissione e anche dal Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono diverse garanzie per i diritti dell'interessato che in conformità al diritto comunitario vanno ritenute adeguate ai sensi del citato art. 28, comma 4, lett. g);

Rilevato che la Decisione della Commissione può essere adattata alla luce dell'esperienza acquisita nel corso della sua applicazione o di innovazioni intervenute nell'ordinamento ungherese (art. 4);

Visti gli articoli 2 e 3 della Decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

(*) v. par. 129 della presente Relazione per il richiamo ipertestuale alla decisione della Commissione europea

104

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta Decisione disponendo la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Gaetano Rasi;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso l'Ungheria, in conformità a quanto previsto alla Decisione della Commissione europea del 26 luglio 2000, n. 2000/519/CE;

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e agli artt. 2 e 3 della Decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 17 ottobre 2001

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

Autorizzazione al trasferimento di dati personali verso la Svizzera - 17 ottobre 2001 (*)

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. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 26 luglio 2000, n. 2000/518/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) con la quale si è constatato che la Svizzera garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 6 del citato art. 25 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: a) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; b) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; c) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare una misura necessaria per l'applicazione della decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE;

Ritenuto che le disposizioni di rango costituzionale e le altre norme vigenti in Svizzera in materia di protezione dei dati personali, valutate dalla Commissione e anche dal Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono diverse garanzie per i diritti dell'interessato che in conformità al diritto comunitario vanno ritenute adeguate ai sensi del citato art. 28, comma 4, lett. g);

Rilevato che la decisione della Commissione può essere adattata alla luce dell'esperienza acquisita nel corso della sua applicazione o di innovazioni intervenute nell'ordinamento svizzero (art. 4);

Visti gli articoli 2 e 3 della decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

(*) v. par. 130 della presente Relazione per il richiamo ipertestuale alla decisione della Commissione europea

104

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta decisione disponendo la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Gaetano Rasi;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso la Svizzera, in conformità a quanto previsto alla decisione della Commissione europea del 26 luglio 2000, n. 2000/518/CE;

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e agli artt. 2 e 3 della decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 17 ottobre 2001

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

105 Provvedimento del 7 marzo 2001 - Partiti e movimenti politici - Un 'decalogò per l'utilizzazione di dati da parte di partiti e movimenti politici nella propaganda elettorale

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, con la partecipazione del prof. Giuseppe Santaniello, che presiede la riunione, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTE le numerose note pervenute in merito alla conformità alle disposizioni della legge 31 dicembre 1996, n. 675 di alcune iniziative di propaganda politica ed elettorale;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

RELATORE il prof. Giuseppe Santaniello;

PREMESSO

In relazione allo svolgimento di consultazioni elettorali e referendarie sono pervenute a questa Autorità, sia da parte di formazioni politiche, sia di singoli cittadini, numerose segnalazioni e richieste di parere in ordine alle modalità di trattamento dei dati personali utilizzati per la propaganda elettorale o per la presentazione di liste e candidature o per la sottoscrizione di richieste di referendum.

Su alcune questioni il Garante si è già pronunciato fin dal primo periodo della propria attività con alcune decisioni (consultabili sul sito internet dell'Autorità www.garanteprivacy.it e sul bollettino "Cittadini e società dell'informazione"), riassunte nelle relazioni annuali presentate al Parlamento e al Governo.

Con il presente provvedimento, al fine di tracciare linee-guida per i titolari del trattamento e per tutti gli interessati sono richiamati in un quadro organico i principi che regolano la protezione dei dati personali nella materia elettorale, quali risultano dalla legge n. 675/1996 e dai successivi decreti legislativi che hanno integrato quest'ultima.

1. Possibilità di utilizzare i dati personali ricavati da registri o elenchi "pubblici".

In base agli artt. 12, comma 1, lettera c), e 20, comma 1, lettera b), della legge n. 675 è possibile trattare e divulgare, anche senza il consenso degli interessati, dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Tale particolare categoria comprende registri, elenchi, atti o documenti "pubblici" (in quanto formati o tenuti da uno o più soggetti pubblici) e da tutti accessibili, nonché analoghi registri, elenchi, atti o documenti eventualmente formati da privati, ma sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque (come l'elenco degli abbonati al servizio di telefonia vocale per la rete fissa).

Fra le predette categorie vi rientrano gli elenchi degli iscritti a vari albi e collegi professionali (vedi sul punto i provvedimenti del Garante del 30 giugno 1997 e del 20 aprile 1998), i dati contenuti in taluni registri detenuti dalle camere di commercio e, soprattutto, le liste elettorali (che chiunque, come precisato dall'art. 51 del d.P.R. 20 marzo 1967, n. 223, può visionare ed ottenere in copia presso i competenti uffici comunali), queste

105

ultime più comunemente usate per attività di propaganda elettorale, unitamente ai dati ricavati dagli elenchi telefonici.

L'insieme dei nominativi presenti nelle liste elettorali può anzi integrare una base di dati ampia riferita alla popolazione adulta, da cui è possibile ricavare un insieme di informazioni (quale cognome e nome, luogo e data di nascita, residenza, professione e titolo di studio). La lecita acquisizione dei dati contenuti in tali liste spiega pertanto come molti cittadini il cui nominativo non compare, ad esempio, nell'elenco telefonico per la rete fissa abbiano potuto ricevere messaggi e sollecitazioni elettorali presso l'indirizzo risultante dalle liste.

2. Utilizzazione di altri tipi di dati personali.

Le categorie di dati prima richiamate riguardano un insieme di informazioni predeterminato per legge e quindi facilmente riscontrabile. Qualora pertanto un cittadino riceva messaggi pubblicitari e di propaganda da parte di un soggetto politico, in favore del quale non abbia manifestato uno specifico consenso al trattamento delle informazioni che lo riguardano, e queste ultime non corrispondano ai dati effettivamente presenti negli elenchi predetti, tale circostanza può essere significativa di una raccolta illecita o non corretta dei dati. In questi casi è possibile inviare una circostanziata segnalazione al Garante cui spetta il potere di svolgere accertamenti anche attraverso il proprio servizio ispettivo.

3. L'informativa all'interessato: obblighi ed esoneri.

Il trattamento dei dati estratti dalle liste elettorali o da altri elenchi pubblici deve avvenire nel rispetto delle disposizioni della legge n. 675. Per quanto riguarda l'informativa agli interessati, il Garante ha disposto di recente un parziale esonero fino al 30 giugno 2001 in favore di partiti e movimenti politici, comitati promotori e sostenitori di liste e di candidati che utilizzino dati estratti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque senza però contattare gli interessati, o qualora inviino semplice materiale di propaganda diverso da lettere articolate o messaggi di posta elettronica che non permetta l'inserimento dell'informativa (provvedimento del 7 febbraio 2001, in Gazzetta Ufficiale n. 36 del 13 febbraio 2001, pag. 65).

Fuori di questi casi, ciascun partito politico, comitato elettorale, ecc. deve fornire la prevista informativa ai singoli cittadini interessati almeno in occasione dell'invio del primo messaggio pubblicitario o propagandistico. In tale informativa, che può essere redatta anche con formule sintetiche e con stile colloquiale, deve essere indicata, tra l'altro, con chiarezza, la denominazione e l'indirizzo del titolare o del responsabile del trattamento, onde permettere all'interessato di individuare il destinatario delle richieste ai sensi dell'art. 13 della legge n. 675 volte ad opporsi all'ulteriore invio di materiale o ad ottenere, a seconda dei casi, l'aggiornamento, la correzione, l'integrazione o la cancellazione dei dati.

Tali richieste comportano poi un dovere per i titolari del trattamento di darvi riscontro ed obbligano, nel caso di opposizione dell'interessato all'ulteriore invio di materiale, a non recapitare più a tale soggetto altri messaggi, anche in occasione di successive campagne elettorali. Infine, qualora un titolare di trattamento non fornisca un idoneo riscontro ad una richiesta di esercizio dei diritti di cui al predetto art. 13, l'interessato, in ordine a tale istanza, ha diritto di presentare ricorso ai sensi dell'art. 29 della legge n. 675 rivolgendosi al giudice ordinario o, in via alternativa, direttamente a questa Autorità.

4. Casi nei quali è necessario acquisire il consenso dell'interessato.

L'utilizzazione di altri tipi di dati non estratti da atti, documenti, elenchi o registri pubblici (da intendersi nel senso sopra precisato) può essere effettuato solo in presenza del consenso espresso del soggetto interessato, manifestato (in forma scritta se si tratta di dati sensibili) in relazione ad una informativa nella quale la finalità dell'utilizzo a fini di comunicazione politica o di propaganda elettorale dei dati dell'interessato deve essere posta chiaramente in evidenza. La necessità del consenso si impone altresì nell'ipotesi in cui determinati dati personali siano stati conoscibili semplicemente su un piano di fatto, anche momentaneamente e da parte di una pluralità di soggetti, come nel caso di indirizzi di posta elettronica ricavati da pagine web o nell'ambito di forum o *newsgroup* in rete (come precisato dal Garante nel già citato provvedimento dell'11 gennaio 2001).

5. Dati "sensibili".

La raccolta e l'utilizzazione da parte di partiti o associazioni politiche di dati relativi ad iscritti alle loro stesse organizzazioni, nonché di partecipanti ad iniziative politiche in occasione delle quali siano stati raccolti dati sui partecipanti, oppure di dati acquisiti in occasione della sottoscrizione di petizioni, proposte di legge, manifesti o richieste di referendum, comporta un trattamento di dati personali sensibili (ai sensi dell'art. 22, comma 1, della citata legge) e richiede l'espressione da parte dell'interessato di un consenso scritto. Per gli aderenti a partiti ed associazioni politiche questo viene in genere espresso con l'atto di adesione al partito stesso (vedi in proposito il comunicato stampa del Garante del 16 ottobre 1997 in "Cittadini e società dell'informazione", n. 2, pag. 82). In assenza di questo consenso o per dati acquisiti in altre occasioni politiche, occorre che l'informativa evidenzi con chiarezza, oltre all'indicazione delle principali finalità ed ai trattamenti ad esse specificamente connessi, un utilizzo più ampio di tali dati (ad esempio comunicazione degli stessi ai comitati elettorali di candidati delle medesime formazioni politiche). Qualora si intenda ipotizzare la possibile comunicazione di tali dati anche ad altri soggetti (organizzazioni di simpatizzanti, enti, associazioni, società e persone fisiche non direttamente connesse all'attività del titolare del trattamento…) tale possibilità (indipendente ed ulteriore rispetto alle ragioni precipue della raccolta dei dati) deve essere associata all'espressione di un consenso, specifico e distinto da quello previsto per il trattamento principale.

6. Obblighi in caso di uso di dati di aderenti a organizzazioni diverse da quelle politiche.

L'utilizzazione a fini di propaganda elettorale di dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politico-partitica, è possibile qualora venga espressamente prevista nell'informativa resa agli iscritti al momento dell'adesione o del rinnovo della stessa (e qualora gli organi dirigenti dell'associazione decidano, con loro autonoma determinazione, di prevedere una tale possibilità). È pertanto illegittima la prassi, riscontrata in alcuni casi segnalati a questa Autorità, di utilizzare gli indirizzari associativi per iniziative di propaganda elettorale a favore di dirigenti o ex dirigenti di associazioni o addirittura di soggetti estranei alle stesse, candidatisi successivamente ad elezioni politiche o amministrative. (v. provvedimenti del Garante del 5 ottobre 1999 e del 9 ottobre 2000).

7. Utilizzazione di dati personali acquisiti in ragione dell'esercizio di un mandato politico o amministrativo.

I titolari di determinate cariche elettive, politiche o amministrative, nell'esercizio del loro mandato e sulla base di specifiche disposizioni volte a favorire il pieno esercizio del mandato elettorale medesimo (es. art. 31 legge n. 142 del 1990, ecc.), possono legittimamente venire a conoscenza di numerosi dati personali. I dati in tal modo acquisiti devono essere però utilizzati esclusivamente per le finalità pertinenti all'esercizio del mandato (presentazione di interrogazioni, svolgimento di attività di controllo e di denuncia nelle competenti sedi istituzionali, ecc.). Non è pertanto legittimo utilizzare gli stessi dati per finalità non pertinenti quale l'attività di propaganda elettorale (vedi parere del 20 maggio 1998 in Bollettino ufficiale del Garante "Cittadini e società dell'informazione", n. 4, pag. 7 ss.).

8. Dati personali trattati da scrutatori e rappresentanti di lista: limiti e doveri.

In materia elettorale e in particolare in occasione di consultazioni elettorali, di referendum e di verifica della loro regolarità, è possibile, in conformità alla legge, la raccolta di alcuni dati sensibili. Ciò è considerato lecito anche dall'art. 8 del d.lg. 11 maggio 1999 n. 135, in materia di trattamento di dati sensibili da parte di soggetti pubblici, che espressamente colloca tale attività tra quelle di rilevante interesse pubblico che giustificano il trattamento. In questo quadro particolari cautele in tema di riservatezza devono essere osservate da scrutatori e rappresentanti di lista che, nell'esercizio delle funzioni e dei compiti loro affidati o riconosciuti dalla legge, vengano a conoscenza di dati personali anche di natura sensibile. La funzione svolta da tali soggetti è collegata al corretto svolgimento delle operazioni elettorali. I dati di cui i medesimi soggetti vengano a conoscenza per effetto delle funzioni svolte (quali quelli relativi alla partecipazione o meno al voto dei cittadini votanti presso una determinata sezione elettorale) devono essere trattati con ogni opportuna cautela anche a tutela del principio costituzionale della libertà e segretezza del voto. Ciò, tanto più, in quelle ipotesi (quali referendum abrogativi o votazioni di ballottaggio) nelle quali la partecipazione o la mancata partecipazione al voto può evidenziare di per sé anche una particolare opzione politica dell'elettore. È illegittima la compilazione da parte degli stessi soggetti, per un successivo utilizzo a fini politici da parte della stessa persona o della formazione politica

di riferimento, di elenchi di persone astenutesi dalla partecipazione al voto (ad esempio, allo scopo di sollecitare le stesse rispetto a futuri appuntamenti elettorali). Tenendo presente anche che l'elenco degli elettori astenutisi nelle elezioni per la Camera dei Deputati a suo tempo previsto dall'art. 115 del d.P.R. 30 marzo 1957, n. 361 (in base al quale tale elenco formato dal sindaco era esposto per un mese nell'albo comunale) non è più previsto e che il citato art. 115 è stato abrogato dall'art. 3 del d.lg. 20 dicembre 1993, n. 534.

9. Adozione di misure di sicurezza ed altri adempimenti.

Ciascun partito, movimento o comitato elettorale, anche se esonerato dall'obbligo della notificazione del trattamento di cui all'art. 7, comma 5 *ter*, lettera l), della legge n. 675, è tenuto, oltre che agli adempimenti di cui agli artt. 8 e 19 della medesima legge in ordine all'individuazione e alla nomina dei responsabili e degli incaricati del trattamento, ad adottare le misure minime di sicurezza di cui al d.P.R. n. 318 del 1999 con riferimento ai trattamenti di dati cartacei e automatizzati.

TUTTO CIÒ PREMESSO IL GARANTE:

segnala a tutti i titolari del trattamento interessati, ai sensi dell'art. 31, comma 1, lettera c), della legge n. 675 del 1996 la necessità di conformare il trattamento dei dati ai principi della medesima legge n. 675 richiamati nel presente provvedimento.

Roma, 7 marzo 2001

IL PRESIDENTE
Santaniello

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

106 Provvedimento in materia di codici di deontologia e di buona condotta - 10 aprile 2002

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, 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, lettera 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;

Visto il decreto legislativo 28 dicembre 2001, n. 467, recante disposizioni integrative e correttive della normativa in materia di protezione dei dati personali ai sensi della legge 24 marzo 2001, n. 127, e in particolare l'art. 20, comma 1, il quale prevede che il Garante, al fine di garantire la piena attuazione dei princìpi previsti dalla disciplina in materia di trattamento dei dati personali deve promuovere entro il 30 giugno 2002 la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali nei settori indicati al comma 2 del medesimo articolo, tenendo conto della specificità dei trattamenti nei diversi ambiti, nonché dei criteri direttivi delle raccomandazioni del Consiglio d'Europa indicate nell'articolo 1, comma 1, lettera b), della legge n. 676/1996;

Considerato che il citato comma 2 dell'art. 20 del d.lg. n. 467/2001 prevede la sottoscrizione di codici riguardanti il trattamento di dati personali:

a) effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica (con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di telecomunicazione gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole ed interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei princìpi di cui all'articolo 9 della legge n. 675/1996, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato);

b) necessari per finalità previdenziali o per la gestione del rapporto di lavoro (prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione di annunci per finalità di occupazione e alla ricezione di curricula contenenti dati personali anche sensibili);

c) effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva (prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni);

d) svolto a fini di informazione commerciale (prevedendo anche, in correlazione con quanto previsto dall'articolo 10, comma 4, della legge n. 675/1996, modalità semplificate per l'informativa all'interes-

sato e idonei meccanismi per favorire la qualità e l'esattezza dei dati raccolti e comunicati);

e) effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati (individuando anche specifiche modalità per favorire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato);

f) provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (anche individuando i casi in cui debba essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla raccomandazione del Consiglio d'Europa N. R (91) 10 in relazione all'articolo 9 della legge n. 675/1996);

g) effettuato con strumenti automatizzati di rilevazione di immagini (prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantirne la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 9 della legge n. 675/1996);

Considerato che, ai sensi dell'art. 20, comma 3, del d.lg. n. 467/2001, il rispetto delle disposizioni contenute nei codici deontologici sopra indicati costituisce condizione essenziale per la liceità del trattamento dei dati;

Considerato che, ai sensi dell'art. 20, comma 4, del d.lg. n. 467/2001, i codici sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante e riportati in allegato al testo unico delle disposizioni in materia previsto dall'articolo 1, comma 4, della legge 24 marzo 2001, n. 127;

Considerata la necessità di adempiere alle predette disposizioni di legge osservando 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 nella *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 eventuali 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. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000;

Relatore il prof. Stefano Rodotà;

TUTTO CIÒ PREMESSO IL GARANTE:

1. promuove la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali in relazione alle finalità ed ai criteri indicati dal citato art. 20 e richiamati in premessa, nei settori di seguito indicati:

a) trattamenti di dati personali effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica;

b) trattamenti di dati personali necessari per finalità previdenziali o per la gestione del rapporto di lavoro;

c) trattamenti di dati personali effettuati a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva;

d) trattamenti di dati personali svolti a fini di informazione commerciale;

e) trattamenti di dati personali effettuati nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati;

f) trattamenti di dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici;

g) trattamenti di dati personali effettuati con strumenti automatizzati di rilevazione di immagini;

2. invita tutti i soggetti pubblici e privati aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività di cui all'art. 31, comma 1, lettera h), della legge n. 675/1996, a darne comunicazione a questa Autorità entro il 31 maggio 2002 al seguente indirizzo: Garante per la protezione dei dati personali, Piazza di Monte Citorio 121 - 00186 Roma – fax 06/69677715 - *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, lettera h), per garantirne la diffusione e il rispetto.

Roma, 10 aprile 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

Commissione europea

107 Decisione della Commissione del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso Paesi terzi a norma della direttiva 95/46/CE (*)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], in particolare l'articolo 26, paragrafo 4,

considerando quanto segue:

(1) A norma della direttiva 95/46/CE, gli Stati membri devono assicurarsi che un trasferimento di dati a carattere personale verso un paese terzo possa avere luogo soltanto se il paese terzo in questione garantisce un livello adeguato di protezione dei dati e se la legislazione degli Stati membri attuativa delle altre disposizioni della direttiva viene rispettata prima del trasferimento.

(2) L'articolo 26, paragrafo 2, della direttiva 95/46/CE prevede tuttavia che gli Stati membri possano autorizzare, nel rispetto di determinate garanzie, un trasferimento o una serie di trasferimenti di dati personali verso paesi terzi che non assicurino un livello adeguato di protezione dei dati. Dette garanzie possono in particolare essere fornite dalla previsione di appropriate clausole contrattuali.

(3) A norma della direttiva 95/46/CE, il livello di protezione dei dati deve essere valutato alla luce di tutte le circostanze relative all'operazione o serie di operazioni di trasferimento di dati. Il gruppo di lavoro sulla protezione degli individui per quanto riguarda il trattamento dei dati personali costituito ai sensi della direttiva [2] ha elaborato una serie di linee direttrici per l'effettuazione di questa valutazione [3].

(4) L'articolo 26, paragrafo 2, della direttiva 95/46/CE, che consente una certa flessibilità nei riguardi di organizzazioni che debbano trasferire dati personali in paesi terzi, nonché l'articolo 26, paragrafo 4, che prevede clausole contrattuali tipo, costituiscono elementi essenziali per il mantenimento del necessario flusso di dati personali fra la Comunità europea e i paesi terzi, senza creare inutili oneri per gli operatori economici. Tali disposizioni rivestono particolare importanza in quanto è probabile che la Commissione, a breve o anche a medio termine, constati l'adeguatezza del livello di protezione ai sensi dell'articolo 25, paragrafo 6, soltanto per un numero limitato di paesi.

(5) Le clausole contrattuali tipo costituiscono soltanto una delle possibilità previste dalla direttiva 95/46/CE per la liceità dei trasferimenti di dati personali in paesi terzi, oltre a quanto previsto agli articoli

(*) notificata con il numero C(2001)1539 - testo rilevante ai fini del SEE - 2001/497/CE

(1) GU L 281 del 23.11.1995, pag.31.

(2) Indirizzo Internet del gruppo di lavoro: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

(3) WP 4 (5020/97): «Primi orientamenti sui trasferimenti di dati personali verso paesi terzi —possibili modalità di verifica dell'adeguatezza», documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997.
WP 7 (5057/97): «Valutazione dell'autoregolamentazione dell'industria:quando reca un contributo significativo al livello di protezione dei dati in un paese terzo?», documento di lavoro:approvato dal gruppo di lavoro il 14 gennaio 1998.
WP 9 (5005/98): «Pareri preliminari sull'impiego delle clausole contrattuali nel contesto dei trasferimenti di dati personali a paesi terzi », documento di lavoro:approvato dal gruppo di lavoro il 22 aprile 1998.
WP12: «Trasferimenti di dati personali a paesi terzi:applicazione degli articoli 25 e 26 della direttiva UE per la protezione dei dati», documento di lavoro: approvato dal gruppo di lavoro il 24 luglio 1998, disponibile sul sito Internet «europa.eu.int/comm/internal_markt/en/media.dataprot/wpdocs/wp12/en» della Commissione europea.

25 e 26, paragrafi 1 e 2. Sarà più agevole per le organizzazioni trasferire i dati in paesi terzi incorporando tali clausole nei contratti. Le clausole contrattuali tipo riguardano soltanto la protezione dei dati. Gli esportatori e importatori dei dati sono liberi di inserire altre clausole a carattere commerciale ritenute pertinenti ai fini del contratto, ad esempio in materia di assistenza reciproca in caso di controversie con le persone interessate dai dati o con un'autorità di controllo, purché esse non siano incompatibili con le clausole tipo.

(6) La presente decisione deve applicarsi fatte salve le eventuali autorizzazioni concesse dagli Stati membri ai sensi delle disposizioni nazionali di attuazione dell'articolo 26, paragrafo 2. La presente decisione ha esclusivamente l'effetto di vietare che gli Stati membri rifiutino di riconoscere come adeguate garanzie le clausole contrattuali in essa contenute, e non produce alcun effetto su clausole contrattuali diverse.

(7) La presente decisione si limita a prevedere che le clausole di cui all'allegato possono essere utilizzate da un responsabile del trattamento con sede nella Comunità europea come garanzie sufficienti ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE. Il trasferimento di dati personali in paesi terzi costituisce un'operazione di trattamento in uno Stato membro la cui legittimità è soggetta alla legislazione nazionale. Le autorità di controllo in materia di protezione dei dati degli Stati membri, nell'esercizio di funzioni e poteri loro attribuiti ai sensi dell'articolo 28 della direttiva 95/46/CE, restano competenti per determinare se l'esportatore dei dati ha rispettato la legislazione nazionale che recepisce le disposizioni della direttiva 95/46/CE, ed in particolare eventuali norme specifiche per quanto riguarda l'obbligo di fornire informazioni a norma della direttiva.

(8) L'ambito di applicazione della presente decisione non si estende al trasferimento di dati personali, operato da responsabili del trattamento aventi sede nella Comunità a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici. Detti trasferimenti non richiedono le stesse garanzie in quanto l'incaricato del trattamento agisce esclusivamente per conto del responsabile del trattamento. La Commissione intende provvedere in ordine a questo genere di trattamenti con una successiva decisione.

(9) È opportuno stabilire le informazioni minime che le parti devono specificare nel contratto relativo al trasferimento. Gli Stati membri devono mantenere il potere di specificare le informazioni che le parti sono tenute a fornire. L'applicazione della presente decisione sarà rivista alla luce dell'esperienza acquisita.

(10) La Commissione potrà inoltre considerare in futuro se altre clausole tipo presentate da organizzazioni commerciali o altre parti interessate offrano garanzie adeguate ai sensi della direttiva 95/46/CE.

(11) Le parti devono essere libere di convenire le prescrizioni alle quali deve conformarsi l'importatore dei dati ai fini dell'effettiva protezione degli stessi, ma determinati principi di protezione devono essere applicati in qualunque circostanza.

(12) I dati devono essere trattati e successivamente utilizzati o comunicati ulteriormente soltanto per scopi determinati e non devono essere trattenuti che per il tempo strettamente necessario.

(13) Ai sensi dell'articolo 12 della direttiva 95/46/CE le persone interessate dai dati devono avere accesso a tutti i dati che le riguardano e se del caso diritto di rettifica, di cancellazione o di congelamento di determinati dati.

(14) L'ulteriore trasferimento di dati personali ad altro responsabile del trattamento, avente sede in un paese terzo, deve essere consentito soltanto subordinatamente al rispetto di determinate condizioni, tendenti in particolare a garantire che le persone interessate dai dati siano adeguatamente informate ed abbiano la possibilità di formulare osservazioni e, in casi determinati, di negare il proprio consenso al trasferimento.

(15) Oltre a verificare se i trasferimenti in paesi terzi sono conformi alla legislazione nazionale, le autorità di controllo devono inoltre svolgere un ruolo fondamentale nel meccanismo contrattuale, al fine di garantire che i dati personali siano adeguatamente protetti dopo il trasferimento. In determinate fattispecie le autorità degli Stati membri devono avere la possibilità di proibire o sospendere un trasferimento o

serie di trasferimenti di dati basati sulle clausole contrattuali tipo, in relazione a casi eccezionali in cui si accerti che un trasferimento su base contrattuale avrebbe la probabile conseguenza di recare sostanziale pregiudizio alle garanzie di adeguata tutela delle persone interessate dai dati.

(16) Deve potersi esigere l'esecuzione delle clausole contrattuali tipo non soltanto su istanza delle parti che stipulano il contratto, ma anche delle persone interessate dai dati, in particolare qualora le stesse subiscano pregiudizio in conseguenza di violazioni del contratto.

(17) Il contratto deve essere retto dalla legge dello Stato membro in cui ha sede l'esportatore dei dati, che abiliti il terzo beneficiario di un contratto a ottenerne l'esecuzione. Le persone interessate dai dati devono poter essere rappresentate da associazioni o altre organizzazioni se lo desiderano e se ciò è autorizzato dalla legislazione nazionale.

(18) Per ridurre le difficoltà pratiche che le persone interessate dai dati potrebbero incontrare all'atto dell'esercizio dei loro diritti in base alle clausole contrattuali tipo, l'esportatore e l'importatore dei dati devono essere tenuti responsabili separatamente e in solido per danni derivanti da qualsiasi violazione di disposizioni soggette alla clausola del terzo beneficiario.

(19) Le persone interessate dai dati hanno diritto di azione nonché diritto al risarcimento del danno a carico dell'esportatore e dell'importatore dei dati stessi, o di entrambi, per i danni derivanti da qualsiasi atto incompatibile con gli obblighi di cui alle clausole contrattuali tipo. Entrambe le parti possono essere esonerate da tale responsabilità se dimostrano di non essere responsabili del danno.

(20) La responsabilità separatamente e in solido non si estende alle disposizioni escluse dalla clausola del terzo beneficiario, e non espone necessariamente una delle parti a responsabilità per illecito trattamento ad opera dell'altra. Benché tale reciproco indennizzo fra le parti non costituisca un requisito per l'adeguatezza della tutela delle persone interessate dai dati e le parti possano quindi eliminarlo dal contratto, esso deve essere incluso nelle clausole contrattuali tipo a fini di chiarezza e per evitare che le parti siano obbligate a concordare di volta in volta le clausole in materia di indennizzo.

(21) Qualora una disputa fra le parti e le persone interessate dai dati non possa essere risolta amichevolmente e le persone interessate invochino la clausola del terzo beneficiario, le parti convengono di riconoscere alle persone interessate dai dati la possibilità di scegliere fra la mediazione, l'arbitrato e l'azione in giudizio. La misura in cui le persone interessate dai dati potranno effettivamente esercitare tale scelta dipenderà dalla disponibilità di sistemi attendibili e riconosciuti di mediazione e di arbitrato. La mediazione ad opera delle autorità di controllo degli Stati membri deve costituire un'alternativa nel caso in cui esse la forniscano.

(22) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito in virtù dell'articolo 29 della direttiva 95/46/CE, ha emesso un parere sul livello di protezione raggiunto in base alle clausole contrattuali tipo allegate alla presente decisione che è stato preso in considerazione per la stesura della stessa [4].

(23) Le disposizioni di cui alla presente decisione sono conformi al parere del comitato istituito in virtù dell'articolo 31 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Le clausole contrattuali tipo di cui all'allegato della presente decisione costituiscono garanzie sufficienti ai fini della tutela della riservatezza, dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi a norma dell'articolo 26, paragrafo 2, della direttiva 95/46/CE.

(4) Parere n.1/2001 adottato dal gruppo di lavoro in data 26.1.2001 (DG MARKT 5102/00 WP 38), disponibile sul sito «Europa» della Commissione europea.

Articolo 2

La presente decisione concerne esclusivamente l'adeguatezza della tutela assicurata dalle clausole contrattuali tipo per il trasferimento di dati personali di cui all'allegato. Essa si applica fatte salve le disposizioni nazionali di attuazione di altre disposizioni della direttiva 95/46/CE relative al trattamento dei dati personali negli Stati membri.

La presente decisione non si applica al trasferimento di dati personali operato da responsabili del trattamento, aventi sede nella Comunità, a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici.

Articolo 3

Ai fini della presente decisione:

a) si applicano le definizioni della direttiva 95/46/CE;

b) per «categorie particolari di dati» si intendono i dati di cui all'articolo 8 di detta direttiva;

c) per «autorità di controllo» si intende l'autorità di cui all'articolo 28 di detta direttiva;

d) per «esportatore di dati» si intende il responsabile del trattamento che trasferisce dati personali;

e) per «importatore di dati» si intende il responsabile del trattamento che conviene di ricevere dati personali dall'esportatore di dati, a fini di ulteriore trattamento ai sensi della presente decisione.

Articolo 4

1. Fatta salva la possibilità delle competenti autorità degli Stati membri di adottare provvedimenti, al fine di garantire il rispetto delle disposizioni nazionali di attuazione delle disposizioni di cui ai capi II, III, V e VI, della direttiva 95/46/CE, dette autorità possono avvalersi dei poteri loro attribuiti per proibire o sospendere flussi di dati verso paesi terzi, a fini di tutela delle persone per quanto riguarda il trattamento dei rispettivi dati personali, qualora:

a) sia accertato che la legislazione cui è sottoposto l'importatore dei dati lo obbliga a deroghe dai pertinenti principi di protezione dei dati che eccedano quelle ritenute necessarie in una società democratica ai sensi dell'articolo 13 della direttiva 95/46/CE, e che tali deroghe siano probabilmente destinate a recare sostanziale pregiudizio alle garanzie di cui alle clausole contrattuali tipo; oppure

b) un'autorità competente abbia accertato che l'importatore dei dati non ha rispettato le clausole contrattuali; oppure

c) sia sostanzialmente probabile che le clausole contrattuali tipo di cui all'allegato non siano o non saranno rispettate, e che la prosecuzione del trasferimento comporterebbe un rischio imminente di grave pregiudizio alle persone interessate dai dati.

2. Il divieto o la sospensione cessano non appena vengono meno le ragioni che li hanno imposti.

3. Quando uno Stato membro prende provvedimenti di cui ai paragrafi 1 e 2 ne informa la Commissione, che trasmette le informazioni agli altri Stati membri.

Articolo 5

La Commissione valuta il funzionamento della presente decisione sulla base delle informazioni disponibili tre anni dopo la notifica della stessa agli Stati membri, e riferisce in merito alle eventuali risultanze al comitato istituito ai sensi dell'articolo 31 della direttiva 95/46/CE, ivi compreso qualsiasi elemento suscettibile di interessare la valutazione di cui all'articolo 1 della presente decisione nonché qualsiasi elemento tale da indicare che la presente deci-

sione viene applicata in maniera discriminatoria.

Articolo 6

La presente decisione si applica dal 3 settembre 2001.

Articolo 7

La presente decisione è indirizzata agli Stati membri.

Fatto a Bruxelles, il 15 giugno 2001.

Per la Commissione
Frederik BOLKESTEIN
Membro della Commissione

ALLEGATO

Clausole contrattuali tipo
A norma dell'articolo 26, paragrafo 2, della direttiva 95/46/CE per il trasferimento di dati personali a paesi terzi che non garantiscono un livello adeguato di protezione

Nome dell'organizzazione che esporta dati: …….....

Indirizzo: .....……..…

Tel…….....…… Fax.... …… E-mail:.....……

Altre informazioni identificative:…….....……
(«l'**esportatore** dei dati»)

e

Nome dell'organizzazione che importa dati: ……
……..

Indirizzo:……

Tel…….....…… Fax.... …… E-mail:.....……

Altre informazioni identificative: …….....……
(«l'**importatore** dei dati»)

HANNO CONVENUTO le seguenti clausole contrattuali (le «**clausole**») al fine di addurre salvaguardie adeguate per quanto riguarda la protezione della riservatezza nonché delle libertà e dei diritti fondamentali degli individui per il trasferimento dall'esportatore all'importatore dei dati personali specificati nell'appendice 1.

Clausola 1

Definizioni
Ai fini delle clausole:

a) «**dati personali**», «**categorie particolari di dati**», «**trattamento**», «**responsabile del trattamento**», «**incaricato del trattamento**», «**persona interessata**» e «**autorità di controllo**» hanno la stessa accezione di cui alla 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 («la direttiva»);

b) «**l'esportatore dei dati**» è il responsabile del trattamento che trasferisce i dati personali;

c) «l'**importatore dei dati**» è il responsabile del trattamento che accetta di ricevere dati personali dall'esportatore per ulteriore trattamento in conformità alle presenti clausole, e che non è soggetto ad un sistema vigente in un paese terzo per assicurare un'adeguata protezione.

Clausola 2

Particolari del trasferimento
I particolari del trasferimento, e in particolare le categorie di dati personali ed i fini a cui vengono trasferite, sono specificati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

Clausola 3

Clausola del terzo beneficiario

Le persone interessate dai dati possono chiedere l'esecuzione della presente clausola nonché della clausola 4, lettere b), c) e d), della clausola 5, lettere a), b), c), ed e), della clausola 6, paragrafi 1 e 2, nonché delle clausole 7, 9 e 11, in qualità di terzi beneficiari. Le parti non si oppongono a che le persone interessate dai dati siano rappresentate da un'associazione o da altre organizzazioni se lo desiderano, e se ciò è autorizzato dalla legislazione nazionale.

Clausola 4

Obblighi dell'esportatore dei dati

L'esportatore dei dati s'impegna e garantisce quanto segue:

a) il trattamento dei dati personali, compreso il loro trasferimento, viene effettuato, e continua ad essere effettuato fino al momento del trasferimento stesso, in conformità a tutte le pertinenti disposizioni (e viene notificato, se del caso, alle autorità competenti) dello Stato membro in cui ha sede l'esportatore, nel pieno rispetto delle leggi vigenti in tale Stato;

b) qualora il trasferimento riguardi speciali categorie di dati, le persone interessate vengono informate che i dati che li riguardano potrebbero essere trasmessi ad un paese terzo che non fornisce una protezione adeguata, al più tardi all'atto del trasferimento;

c) mette a disposizione, a richiesta delle persone interessate, copia delle presenti clausole; e

d) risponde entro un termine ragionevole e nella misura del possibile ad eventuali richieste delle autorità di controllo per quanto riguarda il trattamento dei dati personali in questione da parte dell'importatore dei dati, nonché a qualsiasi richiesta delle persone interessate per quanto riguarda il trattamento dei relativi dati da parte dell'importatore degli stessi.

Clausola 5

Obblighi dell'importatore dei dati

L'importatore dei dati s'impegna e garantisce quanto segue:

a) di non aver ragione di ritenere che la legge applicabile nel suo caso gli impedisca di adempiere agli obblighi di cui al contratto. Qualora la suddetta legge venisse modificata in termini tali da essere probabilmente destinata ad esercitare un sostanziale effetto avverso alle garanzie di cui alle clausole, l'importatore dei dati notifica la variazione all'esportatore dei dati e all'autorità di controllo del paese in cui ha sede l'esportatore. In tal caso l'esportatore dei dati ha diritto di sospendere il trasferimento e/o di rescindere il contratto;

b) a trattare i dati personali conformemente ai principi obbligatori di tutela dei dati di cui all'appendice 2, oppure, su esplicito consenso delle parti espresso barrando le caselle che seguono e fatto salvo il rispetto dei principi obbligatori di protezione dei dati di cui all'appendice 3, a trattare i dati sotto ogni punto di vista rispettando:

- le pertinenti disposizioni di diritto nazionale per la protezione dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare il diritto alla riservatezza per quanto riguarda il trattamento dei dati personali, applicabili a un responsabile dei trattamento nel paese in cui ha sede l'esportatore dei dati, oppure,

- le pertinenti disposizioni di cui a decisioni della Commissione a norma dell'articolo 2 5, paragrafo 6, della direttiva 95/46/CE, accertanti che un paese terzo fornisce adeguata protezione soltanto in

taluni settori d'attività, purché l'importatore dei dati avente sede in tale paese terzo non sia assoggettabile a dette disposizioni, nella misura in cui le disposizioni stesse siano applicabili nel settore del trasferimento;

c) a rispondere prontamente e adeguatamente a tutte le ragionevoli richieste dell'esportatore dei dati o delle persone interessate dai dati, per quanto riguarda il trattamento dei dati personali soggetti a trasferimento, a collaborare con la competente autorità di controllo nel corso di tutte le indagini e a rispettare il parere ditale autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

d) a sottoporre a controllo, su richiesta dell'esportatore dei dati, i propri servizi di trattamento, il controllo viene effettuato dall'esportatore dei dati o da un ente ispettivo indipendente e in possesso delle necessarie qualifiche professionali, selezionato dall'esportatore dei dati e, ove necessario, di concerto con le autorità di controllo;

e) fornire su richiesta copia delle clausole stipulate alle persone interessate dai dati, e ad indicare la sede competente per eventuali reclami.

Clausola 6

Responsabilità

1. Le parti convengono che le persone interessate dai dati che abbiano subito pregiudizio per qualsiasi violazione delle disposizioni di cui alla clausola 3 hanno diritto di essere indennizzate dalle parti per il danno sofferto. Le parti convengono che non sussista responsabilità soltanto se dimostrino che nessuna di essi si è resa responsabile di violazioni delle dette disposizioni.

2. L'esportatore e l'importatore dei dati convengono di assumersi separatamente e in solido la responsabilità dei danni causati alle persone interessate dai dati a seguito di violazioni di cui al paragrafo 1. In caso di violazione di dette disposizioni le persone interessate dai dati possono citare in giudizio sia l'esportatore sia l'importatore dei dati, sia entrambi.

3. Le parti concordano che se una di esse viene riconosciuta responsabile di una violazione commessa dall'altra di qualsiasi disposizione di cui al paragrafo 1, la seconda delle parti indennizza la prima per ogni costo, onere, danno, spesa o perdita sostenuta dalla prima, nei limiti che gli sono imputabili (*).

Clausola 7

Mediazione e giurisdizione

1. In caso di controversie che non possano essere risolte in via amichevole fra le persone interessate dai dati e una delle parti, e qualora le persone interessate dai dati invochino la disposizione relativa al terzo beneficiario di cui alla clausola 3, le parti convengono di accettare la decisione delle persone interessate dai dati di:

a) ricorrere alla mediazione ad opera di un terzo indipendente o, se del caso, dell'autorità di controllo;

b) deferire la controversia ai tribunali dello Stato membro in cui ha sede l'esportatore dei dati.

2. Le parti convengono che, di comune accordo fra le persone interessate dai dati e la relativa controparte, la risoluzione di una specifica controversia possa essere deferita ad un organo arbitrale, purché tale parte abbia sede in un paese che ha ratificato la convenzione di New York sull'applicazione dei lodi arbitrali.

3. Le parti convengono che i paragrafi 1 e 2 si applicano fatti salvi i diritti soggettivi o di azione di cui le persone interessate dai dati possono avvalersi al fine del risarcimento dei danni, in forza di altre disposizioni di diritto nazionale o internazionale.

(*) Il paragrafo 3 è facoltativo.

107

Clausola 8

Collaborazione con l'autorità di controllo

Le parti convengono di depositare copia del presente contratto presso l'autorità di controllo su richiesta di tale autorità o se tale deposito è previsto dalla legge nazionale.

Clausola 9

Scadenza delle clausole

Le parti convengono che la scadenza delle presenti clausole, in qualsiasi circostanza e per qualsiasi motivo, non esonera le parti stesse dagli obblighi e/o condizioni di cui alle clausole stesse per quanto riguarda il trattamento dei dati trasferiti.

Clausola 10

Legislazione applicabile

Alle presenti clausole si applica la legge dello Stato membro in cui ha sede l'esportatore dei dati.

……..……..

Clausola 11

Modifica del contratto

Le parti si impegnaro a non alterare o modificare i termini qui convenuti delle presente clausole.

Per conto dell'esportatore dei dati:

Cognome e nome .....……

Qualifica:……..……..

Indirizzo:……...……..

Altre eventuali informazioni per convalidare il contratto: ……..

……..……..

(Firma) (Sigillo dell'organizzazione)

Per conto dell'importatore dei dati:

Nome (per esteso):…....……...

Qualifica:…….....……..

Indirizzo:….……..

Altre eventuali informazioni per convalidare il contratto: …….....……..

…….....……..

(Firma) (Sigillo dell'organizzazione)

Appendice 1
Alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti.

(Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, in conformità alle rispettive procedure nazionali, qualsiasi altra informazione che debba fare parte della presente appendice).

Esportatore dei dati
(specificare brevemente le attività pertinenti al trasferimento):

……...

Importatori dei dati
(specificare brevemente le attività pertinenti al trasferimento):

……...

Persone interessate dai dati
I dati personali trasferiti interessano le seguenti categorie di persone (specificare):

……...

Fini del trasferimento
Il trasferimento è necessario ai fini seguenti (specificare):

……...

Categorie di dati oggetto di trasferimento
I dati trasferiti interessano le seguenti categorie di dati (specificare):

……...

Dati delicati (se del caso)
Il trasferimento interessa le seguenti categorie di dati a carattere delicato (specificare):

……...

Destinatari
I dati personali trasferiti possono essere comunicati esclusivamente ai seguenti destinatari o categorie di destinatari (specificare):

……...

Limite di durata
I dati personali trasferiti possono essere conservati soltanto per (specificare): ……. (mesi/anni)

L'esportatore dei dati	L'importatore dei dati
Nome:……..	Nome:……..
…….	…….
(Firma del rappresentante autorizzato)	(Firma del rappresentante autorizzato)

Appendice 2
Alle clausole contrattuali tipo

Principi obbligatori di protezione di cui alla clausola 5, lettera b), primo capoverso

Questi principi di tutela dei dati devono essere letti ed interpretati alla luce delle disposizioni della direttiva 95/46/CE.

Essi si applicano fatte salve le norme imperative di diritto nazionale, cui sia soggetto l'importatore dei dati, che non eccedano quanto necessario, in una società democratica, per i motivi elencati all'articolo 13, paragrafo 1, della direttiva 95/46/CE, cioè se esse costituiscono misure necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato o della protezione della persona interessata o dei diritti e delle libertà altrui.

1. *Limitazione del fine:* i dati devono essere elaborati e successivamente utilizzati ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presenti clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2. *Qualità e proporzionalità dei dati:* i dati devono essere corretti e, ove necessario, aggiornati. I dati devono essere adeguati, pertinenti e non esuberanti in relazione ai fini per cui vengono trasferiti e ulteriormente trattati.

3. *Trasparenza:* gli individui interessati dai dati devono essere informati sui fini del trattamento e sull'identità del responsabile dello stesso paese terzo, e su qualsiasi altro aspetto necessario per garantire la correttezza del trattamento, salvo che queste informazioni siano già state fornite dall'esportatore dei dati.

4. *Sicurezza e riservatezza:* il responsabile del trattamento è tenuto a prendere provvedimenti tecnici ed organizzativi di sicurezza appropriati ai rischi presentati dal trattamento, come accesso non autorizzato. Qualsiasi persona che agisca in virtù dell'autorità del responsabile del trattamento non deve effettuare operazioni di trattamento dei dati se non per disposizione del responsabile del trattamento stesso.

5. *Diritti di accesso, rettifica, cancellazione e congelamento dei dati:* come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi. Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

6. *Restrizioni sui trasferimenti successivi:* ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE (trasferimenti successivi) possono essere effettuati soltanto:

a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

— gli scopi del successivo trasferimento,
— l'identità dell'esportatore di dati con sede nella Comunità,
— le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e

— l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui, oppure

b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

7. *Speciali categorie di dati:* nel caso che il trattamento riguardi dati che possano rivelare l'origine razziale o etnica, ovvero le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione a sindacati, dati relativi allo stato di salute o alla vita sessuale, nonché dati relativi a reati, condanne penali o provvedimenti di sicurezza, devono essere previste ulteriori salvaguardie ai sensi della direttiva 95/46/CE, ed in particolare idonee misure di sicurezza come trasmissione cifrata o registrazione di ogni accesso ai dati.

8. *Marketing diretto:* quando i dati vengono trattati a fini di marketing diretto, devono essere previste procedure tali da consentire ai soggetti dei dati di negare in qualsiasi momento il proprio consenso all'utilizzazione a tali fini dei dati che li riguardano.

9. *Decisioni individuali automatizzate:* le persone interessate dai dati hanno il diritto di non essere assoggettate a decisioni basate unicamente sul trattamento automatizzato di dati, a meno che non vengano presi altri provvedimenti per salvaguardare i loro legittimi interessi ai sensi dell'articolo 15 della direttiva 95/46/CE. Qualora l'obiettivo del trasferimento sia una decisione automatizzata ai sensi del citato articolo 15 la persona interessata deve avere il diritto di conoscere le motivazioni su cui si basa detta decisione.

Appendice 3
Alle clausole contrattuali tipo

Principi obbligatori di protezione di cui alla clausola 5, lettera b), secondo capoverso

1. *Limitazione del fine:* i dati devono essere elaborati e successivamente utilizzati ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presente clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2. *Diritti di accesso, rettifica, cancellazione e congelamento dei dati:* come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi. Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

3. *Restrizioni sui trasferimenti successivi:* ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE (trasferimenti successivi) possono essere effettuati soltanto:

a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

— gli scopi del successivo trasferimento,

— l'identità dell'esportatore di dati con sede nella Comunità,
— le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e
— l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui, oppure

b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

108 Decisione della Commissione del 27 dicembre 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in Paesi terzi, a norma della direttiva 95/46/CE (*)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, [1] in particolare l'articolo 26, paragrafo 4,

considerando quanto segue:

(1) In base alla direttiva 95/46/CE, gli Stati membri devono provvedere affinché il trasferimento di dati personali verso un determinato paese terzo possa avere luogo soltanto se tale paese garantisce un livello adeguato di protezione dei dati, e se vengono osservate, previamente al trasferimento, le disposizioni adottate dagli Stati membri in attuazione di altre norme della direttiva.

(2) L'articolo 26, paragrafo 2, della direttiva 95/46/CE prevede che gli Stati membri possano autorizzare, subordinatamente a talune garanzie, il trasferimento di dati personali verso paesi terzi che non garantiscono un livello adeguato di protezione dei dati. Tali garanzie possono essere costituite in particolare da apposite clausole contrattuali.

(3) A norma della direttiva 95/46/CE, il livello di protezione dei dati deve essere valutato alla luce di tutte le circostanze relative all'operazione di trasferimento. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali costituito in forza della direttiva [2] ha elaborato una serie di orientamenti per tale valutazione [3].

(4) Le clausole contrattuali tipo riguardano soltanto la protezione dei dati. Ma gli esportatori e gli importatori dei dati sono liberi di inserire qualsiasi altra clausola commerciale ritenuta pertinente ai fini del contratto, purché non incompatibile con le clausole tipo.

(5) La presente decisione non incide sulle autorizzazioni nazionali che gli Stati membri possono concedere in base alle disposizioni nazionali adottate in attuazione dell'articolo 26, paragrafo 2, della direttiva 95/46/CE. Essa prevede semplicemente che gli Stati membri riconoscano come garanzie sufficienti le clausole contrattuali in essa contenute e non produce alcun effetto sulle clausole contrattuali di altra natura.

(*) Notificata con il numero C(2001)4540 - testo rilevante ai fini del SEE - 2002/16/CE.

(1) GU L 281 del 23.11.1995, pag.31.

(2) Indirizzo Internet del gruppo di lavoro:
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

(3) WP 4 (5020/97): «Primi orientamenti sui trasferimenti di dati personali verso paesi terzi—possibili modalità di verifica dell'adeguatezza», documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997.
WP 7 (5057/97) Documento di lavoro: «Valutazione dell'autoregolamentazione dell'industria: quando reca un contributo significativo al livello di protezione dei dati in un paese terzo?», approvato dal gruppo di lavoro il 14 gennaio 1998.
WP 9 (5005/98) Documento di lavoro: «Pareri preliminari sull'impiego delle clausole contrattuali nel contesto dei trasferimenti di dati personali a paesi terzi », approvato dal gruppo di lavoro il 22 aprile 1998.
WP 12: Trasferimenti di dati personali a paesi terzi:applicazione degli articoli 25 e 26 della direttiva UE per la protezione dei dati,approvato dal gruppo di lavoro il 24 luglio 1998, disponibile sul sito Internet della Commissione europea: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

(6) La presente decisione si limita a stabilire che le clausole da essa previste possano essere utilizzate dal responsabile del trattamento con sede nella Comunità come garanzie sufficienti per il trasferimento di dati personali a incaricati del trattamento residenti in paesi terzi ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE.

(7) Essa attua pertanto l'articolo 17, paragrafo 3, della direttiva e non pregiudica il contenuto dei contratti o degli atti giuridici adottati in materia. Appare tuttavia opportuno prevedere determinate clausole tipo, riguardanti in particolare gli obblighi dell'esportatore, affinché vi sia maggiore chiarezza sulle disposizioni che possono essere inserite nei contratti fra i responsabili e gli incaricati del trattamento.

(8) Le autorità di controllo degli Stati membri svolgono un ruolo fondamentale in tale ambito garantendo che i dati personali siano adeguatamente tutelati in seguito al trasferimento. Nei casi eccezionali in cui gli esportatori si rifiutino o non siano in grado di impartire le istruzioni necessarie agli importatori, e le persone cui si riferiscono i dati siano esposte ad un imminente rischio di gravi danni, le clausole tipo devono consentire alle autorità di controllo di vigilare sugli importatori dei dati ed adottare, se del caso, decisioni vincolanti nei loro confronti. Le autorità di controllo devono avere la facoltà di vietare o sospendere i trasferimenti di dati effettuati in base alle clausole contrattuali tipo nei casi eccezionali in cui il trasferimento su base contrattuale possa pregiudicare le garanzie e gli obblighi destinati a fornire adeguata protezione alle persone interessate dai dati.

(9) La Commissione potrà valutare in futuro se le garanzie sufficienti ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE possano altresì essere costituite da altre clausole contrattuali tipo, proposte da organizzazioni di categoria o a altri soggetti interessati per il trasferimento di dati personali ad incaricati del trattamento residenti in paesi terzi che non garantiscono un livello adeguato di protezione.

(10) La comunicazione di dati personali ad incaricati del trattamento residenti al di fuori della Comunità costituisce un trasferimento internazionale protetto ai sensi del capo IV della direttiva 95/46/CE. La presente decisione non riguarda il trasferimento di dati personali da responsabili del trattamento residenti nella Comunità a responsabili del trattamento residenti al di fuori della Comunità. Tale trasferimento rientra nel campo di applicazione della decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a caratteri personale verso paesi terzi a norma della direttiva 95/46/CE [4].

(11) Le clausole contrattuali tipo devono prevedere le misure tecniche e organizzative di sicurezza che devono essere applicate dall'incaricato del trattamento, residente in un paese terzo che non garantisce un livello di protezione adeguato, affinché il livello di sicurezza sia commisurato ai rischi inerenti al trattamento e alla natura dei dati da tutelare. Nel contratto le parti devono prevedere le misure tecniche e organizzative che, tenuto conto della normativa sulla protezione dei dati, della più recente tecnologia e dei costi di attuazione, sono necessarie allo scopo di proteggere i dati personali contro la distruzione accidentale o illecita, la perdita accidentale, l'alterazione, l'accesso o la rivelazione non autorizzati, e qualsiasi altra forma di trattamento illecito.

(12) Allo scopo di agevolare i flussi di dati in uscita dalla Comunità deve essere consentito agli incaricati del trattamento, che forniscano servizi di trattamento a più responsabili nella Comunità, d'applicare le stesse misure tecniche e organizzative di sicurezza indipendentemente dallo Stato membro da cui si effettua il trasferimento, in particolare nel caso in cui l'importatore riceva i dati ai fini dell'ulteriore trattamento da diverse sedi dell'esportatore situate nella Comunità. In questa ipotesi deve applicarsi la legge dello Stato designato.

(13) Devono essere previste le informazioni minime che le parti devono includere nel contratto relativo al trasferimento. Gli Stati membri hanno comunque la facoltà di specificare in termini più particolareggiati le informazioni che le parti sono tenute a fornire. Il funzionamento del sistema istituito dalla presente decisione sarà valutato alla luce dell'esperienza futura.

(14) L'importatore è tenuto a trattare i dati personali trasferiti esclusivamente per conto dell'esportatore e in conformità alle istruzioni da questi impartite, nonché in ottemperanza agli obblighi stabiliti dalle clausole

(4) GU L 181 del 4.7.2001, pag.19.

stesse. L'importatore deve astenersi segnatamente dal rivelare i dati personali a terzi, salvo che sussistano determinate circostanze. L'esportatore è tenuto a trasmettere opportune istruzioni all'importatore durante l'intero periodo in cui vengano prestati i servizi di trattamento affinché i dati siano trattati conformemente alle istruzioni impartite, alla normativa sulla protezione dei dati e agli obblighi contenuti nelle clausole tipo. Il trasferimento di dati personali a incaricati del trattamento residenti al di fuori della Comunità lascia impregiudicato il fatto che le attività di trattamento debbano comunque essere conformi alla normativa sulla protezione dei dati.

(15) È opportuno che le clausole contrattuali tipo possano essere fatte valere non solo dalle organizzazioni che stipulano il contratto ma anche dalle persone interessate dai dati, in particolare laddove l'eventuale violazione del contratto rechi ad esse pregiudizio.

(16) Le persone interessate dai dati devono poter agire in giudizio, anche ai fini del risarcimento dei danni, nei confronti dell'esportatore che è il responsabile del trattamento dei dati personali trasferiti.
Eccezionalmente le persone interessate dai dati devono potere agire in giudizio nei confronti dell'importatore, anche ai fini del risarcimento dei danni, per la violazione degli obblighi stabiliti dalla clausola 3, qualora l'esportatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente.

(17) Nelle controversie sorte con persone interessate dai dati che si avvalgano della clausola del terzo beneficiario, l'importatore, ove non sia possibile la composizione in via amichevole, deve consentire all'interessato di scegliere fra la mediazione, l'arbitrato o l'azione legale. L'effettiva possibilità di scelta dipenderà dall'esistenza di sistemi di mediazione ed arbitrato affidabili e riconosciuti. La mediazione ad opera delle autorità di controllo dello Stato membro in cui ha sede l'esportatore deve essere ammessa, sempre che dette autorità prestino tale servizio.

(18) Il contratto deve essere soggetto alla legge dello Stato membro in cui ha sede l'esportatore, di modo che il terzo beneficiario possa far valere le disposizioni contrattuali. È opportuno che le persone interessate dai dati possano essere rappresentate da associazioni o altre organizzazioni, qualora lo desiderino e qualora ciò sia ammesso dalla normativa nazionale.

(19) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito in forza dell'articolo 29 della direttiva 95/46/CE ha emesso un parere sul livello di protezione garantito dalle clausole contrattuali tipo allegate alla presente decisione, che è stato preso in considerazione nella stesura della decisione stessa [5].

(20) Le misure previste dalla presente decisione sono conformi al parere del comitato istituito in forza dell'articolo 31 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Le clausole contrattuali tipo riportate in allegato costituiscono garanzie sufficienti ai fini della tutela della riservatezza, dei diritti fondamentali e della libertà delle persone nonché per l'esercizio dei relativi diritti ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE.

Articolo 2

La presente decisione concerne esclusivamente l'adeguatezza della tutela conferita dalle clausole contrattuali tipo per il trasferimento di dati personali riportate in allegato. Essa lascia impregiudicata l'applicazione delle disposizioni nazionali sul trattamento dei dati personali negli Stati membri adottate in attuazione della direttiva 95/46/CE.

La presente decisione si applica al trasferimento dei dati personali effettuato da responsabili del trattamento residenti nella Comunità a destinatari residenti al di fuori della Comunità che agiscano esclusivamente in veste di incaricati del trattamento.

(5) Parere n.7/2001 approvato dal gruppo di lavoro in data 13 settembre 2001; vedi par. 120 della presente Relazione.

Articolo 3
Ai fini della presente decisione:

a) si applicano le definizioni di cui alla direttiva 95/46/CE; inoltre

b) per «speciali categorie di dati» s'intendono i dati di cui all'articolo 8 di detta direttiva;

c) per «autorità di controllo» s'intende l'autorità di cui all'articolo 28 di detta direttiva;

d) per «esportatore» s'intende il responsabile del trattamento che trasferisce i dati personali;

e) per «importatore» s'intende l'incaricato del trattamento residente in un paese terzo, che s'impegni a ricevere dall'esportatore dati personali al fine di trattarli per conto e secondo le istruzioni dell'esportatore stesso nonché a norma della presente decisione e che non sia assoggettato dal paese terzo ad un sistema che garantisca una protezione adeguata;

f) per «normativa sulla protezione dei dati» s'intende la normativa che protegge i diritti e le libertà fondamentali delle persone fisiche e in particolare il diritto alla riservatezza riguardo al trattamento di dati personali, applicabile ai responsabili del trattamento nello Stato membro in cui ha sede l'esportatore;

g) per «misure tecniche e organizzative di sicurezza» s'intendono le misure destinate a proteggere i dati personali contro la distruzione accidentale o illecita, la perdita accidentale, l'alterazione e la rivelazione o l'accesso non autorizzati, in particolare ove il trattamento comporti la trasmissione di dati su rete, nonché contro qualsiasi altra forma di trattamento illecito.

Articolo 4
1. Fatto salvo il potere di provvedere all'osservanza delle disposizioni nazionali adottate in attuazione dei capi II, III, V e VI della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei poteri loro attribuiti per vietare o sospendere i flussi di dati verso paesi terzi allo scopo di proteggere le persone con riguardo al trattamento dei dati personali, qualora:

a) sia accertato che, in base alla legge ad esso applicabile, l'importatore è tenuto ad applicare deroghe alla normativa sulla protezione dei dati che eccedano le restrizioni ritenute necessarie in una società democratica ai sensi dell'articolo 13 della direttiva 95/46/CE, e pregiudichino significativamente le garanzie previste dalla normativa sulla protezione dei dati e dalle clausole contrattuali tipo, oppure

b) un'autorità competente abbia accertato che l'importatore non ha rispettato le clausole contrattuali riportate in allegato, oppure

c) sia probabile che le clausole contrattuali tipo in allegato non vengano rispettate, e che la prosecuzione del trasferimento determini un imminente rischio di gravi danni per le persone interessate dai dati.

2. Il divieto o la sospensione ai sensi del paragrafo 1 sono revocati non appena ne vengano meno le ragioni.

3. Quando prende i provvedimenti di cui ai paragrafi 1 e 2, lo Stato membro informa senza indugio la Commissione; questa trasmette l'informazione agli altri Stati membri.

Articolo 5
Decorsi tre anni dalla notificazione della presente decisione agli Stati membri, la Commissione valuta il funzionamento del sistema previsto dalla decisione stessa sulla base delle informazioni disponibili. Essa riferisce in merito alle risultanze della valutazione al comitato istituito in forza dell'articolo 31 della direttiva 95/46/CE. La relazione comprende qualsiasi circostanza rilevante ai fini della valutazione dell'adeguatezza delle clausole contrattuali tipo riportate in allegato nonché qualsiasi eventuale circostanza indicante che la presente decisione viene applicata in maniera discriminatoria.

Articolo 6

La presente decisione si applica a decorrere dal 3 aprile 2002.

Articolo 7

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 27 dicembre 2001.

Per la Commissione
Frederik BOLKESTEIN
Membro della Commissione

108

ALLEGATO

Clausole contrattuali tipo («Incaricati del trattamento»)

Ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE per il trasferimento di dati personali a responsabili del trattamento residenti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati.

Nome dell'organizzazione esportatrice: …….....……

Indirizzo …….....……

tel……..; fax……..; e-mail:…….

Altre informazioni identificative: …….....……...

(«**l'esportatore**»)

e

Nome dell'organizzazione importatrice: …….....……

Indirizzo …….....……

tel……..; fax……..; e-mail:…….

Altre informazioni identificative: …….....……...

(«**l'importatore**»)

HANNO CONVENUTO le seguenti clausole contrattuali («nel prosieguo: le clausole») al fine di prestare garanzie sufficienti per la tutela della riservatezza, delle libertà e dei diritti fondamentali delle persone con riguardo al trasferimento dall'esportatore all'importatore dei dati personali indicati nell'appendice 1.

Clausola 1

Definizioni

Ai fini delle presenti clausole:

a) I termini «dati personali», «speciali categorie di dati», «trattamento», «responsabile del trattamento», «incaricato del trattamento», «persona interessata» e «autorità di controllo» hanno la stessa accezione attribuita nella direttiva 95/46/CE, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel prosieguo: «la direttiva») [1];

b) per «esportatore» s'intende il responsabile del trattamento che trasferisce i dati personali;

c) per «importatore» s'intende il responsabile del trattamento residente in un paese terzo che s'impegni a ricevere dall'esportatore dati personali al fine di trattarli per conto e secondo le istruzioni dell'esportatore stesso nonché a norma della presente decisione, e che non sia soggetto nel paese terzo ad un sistema che garantisca una protezione adeguata;

d) «per normativa sulla protezione dei dati» s'intende la normativa, applicabile ai responsabili del trattamento nello Stato membro in cui ha sede l'esportatore, che protegge i diritti e le libertà fondamentali delle persone fisiche ed in particolare il diritto alla riservatezza riguardo al trattamento dei dati personali;

(1) Le parti hanno facoltà di avvalersi delle definizioni di cui alla direttiva 95/46/CE nell'ambito della presente clausola se ritenuto preferibile ai fini del contratto.

e) per «misure tecniche e organizzative di sicurezza» s'intendono le misure intese a proteggere i dati personali da distruzione accidentale o illecita, da perdita accidentale, da alterazione, o da rivelazione e accesso non autorizzati, in particolare ove il trattamento comporti la trasmissione di dati su rete, nonché da qualsiasi altra forma illecita di trattamento.

Clausola 2

Particolari del trasferimento

I particolari del trasferimento, segnatamente le eventuali categorie di dati personali, sono indicati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

Clausola 3

Clausola del terzo beneficiario

Le persone interessate dai dati possono far valere, nei confronti dell'esportatore, la presente clausola nonché le clausole 4, lettere b), c), d), e) ed f), 5, lettere a), b), c), d), e) e g), 6, lettere a) e b), 7, 8, paragrafo 2, 9, 10 e 11 in qualità dei terzi beneficiari.

Le persone interessate dai dati possono far valere, nei conformi dell'importatore, la presente clausola nonché le clausole 5, lettere a), b), c), d), e) e g), 6, lettere a) e b), 7, 8, paragrafo 2, 9, 10 e 11 qualora l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere.

Le parti non si oppongono a che la persona interessata dai dati sia rappresentata da un'associazione o altra organizzazione, ove siffatta rappresentanza corrisponda alla esplicita volontà dell'interessato e sia ammessa dalla legge nazionale.

Clausola 4

Obblighi dell'esportatore

L'esportatore dichiara e garantisce quanto segue:

a) che il trattamento dei dati personali, compreso il loro trasferimento, viene effettuato, e continuerà ad essere effettuato in conformità a tutte le disposizioni pertinenti della normativa sulla protezione dei dati e verrà comunicato, se del caso, alle competenti autorità dello Stato membro in cui ha sede l'esportatore) nel pieno rispetto delle leggi vigenti in questo Stato;

b) che egli ha prescritto all'importatore - e continuerà a farlo durante l'intero periodo in cui sono prestati i servizi di trattamento dei dati - di elaborare i dati personali trasferiti soltanto per suo conto e in conformità alla normativa sulla protezione dei dati e alle presenti clausole;

c) che l'importatore fornisce sufficienti garanzie per quanto riguarda le misure tecniche e organizzative di sicurezza indicate nell'appendice 2;

d) che alla luce della normativa sulla protezione dei dati le misure di sicurezza sono idonee a proteggere i dati personali contro la distruzione accidentale o illecita, l'alterazione, e la trasmissione o l'accesso non autorizzati, in particolare qualora il trattamento comprenda la trasmissione di dati su rete, nonché contro ogni altra forma di trattamento illecito, e garantiscono un livello di sicurezza commisurato ai rischi connessi al trattamento ed alla natura dei dati che devono essere protetti, tenuto conto della più recente tecnologia e dei costi d'attuazione;

e) che provvederà all'osservanza delle misure di sicurezza;

f) che, qualora il trasferimento riguardi speciali categorie di dati, le persone interessate sono state o

saranno informate, prima del trasferimento o immediatamente dopo lo stesso, che i dati che li riguardano potrebbero essere trasmessi ad un paese terzo che non fornisce una protezione adeguata;

g) di trasmettere all'autorità di controllo la comunicazione presentata dall'importatore ai sensi della clausola 5 b) qualora decida di proseguire il trasferimento o revocare la sospensione;

h) i mettere a disposizione delle persone interessate dai dati, su richiesta, una copia delle clausole del presente allegato recante, anziché l'appendice 2, una descrizione generale delle misure di sicurezza.

Clausola 5

Obblighi dell'importatore (1)

L'importatore dichiara e garantisce quanto segue:

a) che tratterà i dati personali soltanto per conto dell'esportatore e in conformità alle sue istruzioni nonché alle presenti clausole; egli si impegna ad informare prontamente l'esportatore qualora non possa per qualsiasi ragione ottemperare a tale disposizione; in tal caso l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto;

b) che non ha alcuna ragione di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali che egli comunicherà all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole; in tal caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;

c) che ha applicato le misure tecniche e organizzative di sicurezza indicate nell'appendice 2 prima di effettuare il trattamento dei dati personali trasferiti;

d) che comunicherà prontamente all'esportatore:

i) qualsiasi richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della rivelazione di dati personali, salvo che la comunicazione sia vietata da norne specifiche, ad esempio da norme di diritto penale miranti a tutelare il segreto delle indagini;

ii) qualsiasi accesso accidentale o non autorizzato e

iii) qualsiasi richiesta ricevuta direttamente dalle persone interessate dai dati cui egli non abbia risposto, salvo che sia stato autorizzato a non rispondere;

e) che risponderà prontamente e adeguatamente a tutte le richieste dell'esportatore relative al trattamento dei dati personali soggetti a trasferimento e che si conformerà al parere dell'autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

f) che sottoporrà i propri impianti di trattamento, su richiesta dell'esportatore, al controllo dell'esportatore o di un organismo ispettivo composto da soggetti indipendenti, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall'esportatore, eventualmente di concerto con l'autorità di controllo;

g) che fornirà, su richiesta, alle persone interessate dai dati, una copia delle clausole del presente allegato

(1) Disposizioni vincolanti della legislazione nazionale applicabile all'importatore che non vanno oltre quanto è necessario in una società democratica sulla base di uno degli interessi di cui all'articolo 13, paragrafo 1, della direttiva 95/46/CE ossia, i provvedimenti necessari per la sicurezza nazionale, la difesa, l'ordine pubblico, la prevenzione, l'investigazione, l'individuazione ed il perseguimento dei reati o delle violazioni delle norme disciplinanti le professioni regolamentate, la salvaguardia di rilevanti interessi economici o finanziari dello Stato, la tutela delle persone interessate dai dati o dei diritti o delle libertà di altri, non sono in contraddizione con le clausole contrattuali tipo. Costituiscono esempi di disposizioni vincolanti che non vanno oltre quanto è necessario in una società democratica le sanzioni internazionalmente riconosciute, o obblighi di informazioni in materia fiscale o contro il riciclaggio di capitali.

recante, anziché l'appendice 2, una descrizione generale delle misure di sicurezza, qualora le persone interessate non siano in grado di ottenerne copia direttamente dall'esportatore.

Clausola 6

Responsabilità

1. Le parti convengono che le persone interessate dai dati che abbiano subito un pregiudizio per qualsiasi violazione delle disposizioni di cui alla clausola 3 hanno diritto di ottenere dall'esportatore il risarcimento del danno sofferto.

2. Qualora la persona interessata dai dati non sia in grado di agire in giudizio nei confronti dell'esportatore per violazione di uno degli obblighi di cui alla clausola 3 in quanto l'esportatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'importatore riconosce alla persona stessa il diritto di agire nei suoi confronti così come se egli fosse l'esportatore.

3. Le parti convengono che se una di esse viene riconosciuta responsabile di una violazione delle clausole commessa dall'altra, quest'ultima, nei limiti della sua responsabilità, è tenuta a indennizzare la prima per ogni costo, onere, danno, spesa o perdita sostenuti.

Tale indennizzo è subordinato al fatto che

a) l'esportatore informi prontamente l'importatore in merito alle istanze presentate; e

b) l'importatore abbia la possibilità di collaborare con l'esportatore nella difesa e nella risoluzione della controversia.[1].

Clausola 7

Arbitrato e giurisdizione

1. L'importatore dichiara che qualora una persona interessata dai dati faccia valere il diritto del terzo beneficiario ai sensi della clausola 3 e/o chieda il risarcimento dei danni in base alle presenti clausole, egli accetterà la decisione della persona stessa:

a) di sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente dell'autorità di controllo;

b) di deferire la controversia agli organi giurisdizionali dello Stato membro in cui ha sede l'esportatore.

2. L'importatore dichiara che, previo accordo con la persona interessata dai dati, una determinata controversia potrà essere deferita ad un organo arbitrale, sempre che l'importatore stesso risieda in un paese che abbia ratificato la convenzione di New York sull'esecuzione dei lodi arbitrali.

3. Le parti dichiarano che la scelta compiuta dalla persona interessata dai dati non pregiudica i diritti sostanziali o procedurali spettanti alla stessa relativamente ai rimedi giuridici previsti dalla normativa nazionale o internazionale.

Clausola 8

Collaborazione con le autorità di controllo

1. L'esportatore si impegna a depositare una copia del presente contratto presso l'autorità di controllo, qualora questa ne faccia richiesta a qualora il deposito sia prescritto dalla legge nazionale.

(1) Il paragrafo 3 è facoltativo.

2. Le parti dichiarano che l'autorità di controllo ha il diritto di sottoporre a controlli l'importatore nella stessa misura e secondo le stesse modalità previste per l'esportatore dalla normativa nazionale sulla protezione dei dati.

Clausola 9

Legge applicabile

Le presenti clausole sono soggette alla legge dello Stato membro in cui ha sede l'esportatore, ossia .....

Clausola 10

Modifica del contratto

Le parti si impegnano a non alterare o modificare il contenuto delle presenti clausole.

Clausola 11

Obblighi al termine dell'attività di trattamento dei dati personali

1. Le parti convengono che al termine dell'attività di trattamento l'importatore provvede, a scelta dell'esportatore, a restituire a quest'ultimo tutti i dati personali trasferiti e le relative copie o a distruggere tali dati, certificando all'esportatore l'avvenuta distruzione, salvo che gli obblighi di legge impediscano di restituire o distruggere in tutto o in parte i dati personali trasferiti. In questo caso, l'importatore si impegna a garantire la riservatezza dei dati personali trasferiti e ad astenersi dal trattare di propria iniziativa tali dati.

2. L'importatore si impegna a sottoporre a controllo i propri impianti di trattamento su richiesta dell'esportatore e/o dell'autorità di controllo, ai fini della verifica dell'esecuzione dei provvedimenti di cui al paragrafo 1.

Per conto dell'esportatore:

Cognome e nome:…….....……
Qualifica:……..……..
Indirizzo:……
Altre informazioni necessarie per convalidare il contratto: …….....

Firma:.....

(timbro dell'organizzazione)

Per conto dell'importatore:

Cognome e nome:…….....……
Qualifica:……..……..
Indirizzo:……
Altre informazioni necessarie per convalidare il contratto: …….....

Firma:.....

(timbro dell'organizzazione)

Appendice I
Alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti

(* Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, in conformità alle rispettive procedure nazionali, qualsiasi altra informazione che debba fare parte della presente appendice.)

Esportatore
(specificare brevemente le attività pertinenti al trasferimento):

……...

Importatore
(specificare brevemente le attività pertinenti al trasferimento):

……...

Persone interessate dai dati
I dati personali trasferiti interessano le seguenti categorie di persone (specificare):

……...

Categorie di dati oggetto di trasferimento
I dati trasferiti interessano le seguenti categorie di dati (specificare):

……...

Speciali categorie di dati (se del caso)
Il trasferimento interessa le seguenti speciali categorie di dati (specificare):

……...

Operazioni di trattamento
I dati personali trasferiti saranno sottoposti alle seguenti attività principali di trattamento (specificare):

L'ESPORTATORE L'IMPORTATORE

Nome …….

Firma del rappresentante autorizzato

……

Appendice 2
Alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole e dev'essere compilata e sottoscritta dalle parti

Descrizioni delle misure tecniche e organizzative attuate dall'importatore in conformità alle clausole 4, lettera c), e 5, lettera c) o al documento/legislazione allegata:

……....

109 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows - Strasbourg, 8.11.2001 (ETS no. 181) (*)

COUNCIL OF EUROPE CONSEIL DE L'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 element 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 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 a 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 of Article 1 of this Protocol.

b Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with 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.

(*) Protocollo addizionale alla Convenzione per la protezione delle persone fisiche con riguardo al trattamento di dati personali, relativo alle autorità di controllo ed ai flussi transfrontalieri

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 of Article 2 of this Protocol, 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 and are found adequate by 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 a 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 five of its Signatories have expressed their consent to be bound by the Protocol in accordance with the provisions of paragraph 2 of Article 3.

b 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 a After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

b 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 a Any Party may at any time denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

b 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 receipt of such notification by the Secretary General.

6 The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the European Communities and any other State which has 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 8th day of November 2001, 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.

110 Council of Europe Convention on Cybercrime Budapest, 23.11.2001 (*)

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning

(*) Convenzione del Consiglio d'Europa sulla criminalità informatica

the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a

form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be

subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its

sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, 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 the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be 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 of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, 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 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State 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 the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt

with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that

have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede 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 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, 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, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Autorità di controllo comune Schengen

111 Quinta relazione di attività dell'Autorità di controllo comune: marzo 2000 - dicembre 2001

SOMMARIO

NOTA DI SINTESI

PRIMA PARTE: RIEPILOGO

SECONDA PARTE: UN ANNO DI ATTIVITÀ DELL'ACC

CAPITOLO I : PARERI E RACCOMANDAZIONI
I.1. Sicurezza degli uffici SIRENE
I.2. Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione
I.3. Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata
I.4. Accesso al SIS da parte dei servizi competenti per l'immatricolazione dei veicoli
I.5. Riconoscimento dello status di osservatore al Regno Unito
I.6. Messa in applicazione dell'acquis di Schengen nei paesi nordici
I.7. Progetto di risoluzione del Consiglio sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea
1.8. Attuazione del sistema d'informazione Schengen nel Regno Unito

CAPITOLO II: ATTIVITÀ DI CONTROLLO
II.1. Controllo del C.SIS
II.2. Gruppi tecnici ed esperti
II.3. Criptazione dei collegamenti SIS
II.4. Elenco delle autorità autorizzate a consultare direttamente il SIS

CAPITOLO III: CAMPAGNA DI INFORMAZIONE
III.1. Campagna d'informazione sui diritti dei cittadini nei confronti del SIS
III.2. Pagina Internet dell'ACC
III.3. Presentazione della quarta relazione annuale dell'ACC in occasione della conferenza stampa di Bruxelles

CAPITOLO IV: INTEGRAZIONE DELL'UNIONE EUROPEA E ACQUIS DELL'ACC

CAPITOLO V: FUNZIONAMENTO DELL'ACC
V.1. Riunioni
V.2. Elezioni del Presidente e del Vicepresidente
V.3. Bilancio dell'ACC e supporto di segreteria
V.4. Regolamento interno

TERZA PARTE: RELAZIONI DELL'ACC ALL'INTERNO E AL DI FUORI DELLA STRUTTURA SCHENGEN E DEL CONSIGLIO
I.1. Relazioni con la Commissione per le libertà pubbliche del Parlamento europeo
I.2. Relazioni con il Comitato dell'articolo 36, il Comitato dei Rappresentanti Permanenti e il Consiglio
I.3. Commissione di valutazione – Paesi nordici
I.4. Posizione del Regno Unito e dell'Irlanda

QUARTA PARTE: REAZIONI DELLE AUTORITÀ SCHENGEN ALLA RELAZIONE ANNUALE DELL'ACC

QUINTA PARTE: IL FUTURO DELL'ACC NEL NUOVO QUADRO ISTITUZIONALE

ALLEGATI
1. Elenco dei membri dell'autorità di controllo comune
2. Quadro dei pareri dell'ACC e reazioni degli organi esecutivi e tecnici
3. 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 allegato al trattato di Amsterdam

4. Dati inseriti nel SIS

NOTA DI SINTESI

Fedele alla sua tradizione di trasparenza e di apertura democratica, l'autorità di controllo comune Schengen (ACC) ha voluto presentare, per la quinta volta, una relazione sulla sua attività. La difesa degli interessi dell'individuo nella tutela della vita privata è stata, anche nel periodo compreso tra il marzo 2000 e il dicembre 2001, al centro delle attività dell'ACC, di cui ha così confermato la specificità nell'ambito della struttura Schengen.

L'ACC, basandosi su relazioni, raccomandazioni o pareri, ha formulato varie proposte e suggerimenti riguardanti sia il controllo della sicurezza del Sistema d'informazione Schengen (SIS) sia la tutela degli interessi dei singoli di cui sopra sia ancora l'adempimento dell'obbligo d'informazione nei confronti del cittadino e la verifica dell'esistenza dei presupposti per l'attuazione dell'acquis di Schengen nei nuovi paesi.

Negli ultimi tempi, dalle discussioni sull'evoluzione di un nuovo SIS è emersa forte la volontà di ampliare il contenuto e l'utilizzo del SIS. Per poter contribuire attivamente a tale evoluzione, è assolutamente indispensabile che quanti sono coinvolti nello sviluppo del SIS riconoscano l'importanza di coinvolgere l'ACC fin dall'inizio. Si tratta di una condizione essenziale per lo sviluppo di un nuovo SIS con un corretto equilibrio tra contenuto e uso del SIS e protezione dei dati.
L'ACC nota con soddisfazione che sta delineandosi in modo costruttivo una tendenza a coinvolgere l'ACC.

L'anno appena trascorso ha permesso all'ACC di migliorare notevolmente la visibilità grazie ai contatti con la Commissione per le libertà pubbliche del Parlamento europeo. Anche l'ingresso dei paesi nordici come membri effettivi dell'ACC, il 25 marzo 2001, è stato occasione di numerosi contatti con la stampa che hanno permesso all'Autorità di sottolineare l'importanza del suo ruolo.

La decisione del Consiglio di istituire un segretariato comune di tutte le autorità di controllo nel settore di polizia europeo (Schengen, Europol, Sistema d'informazione doganale, ecc.) rappresenta indubbiamente un passo nella buona direzione e l'ACC non può che compiacersene. Tale soluzione permetterà infatti alle autorità di controllo interessate, tra cui l'ACC, di contare su un maggiore supporto di segreteria, che l'ACC ha chiesto fin dal 1995. Sebbene a tale decisione non si associno risorse di bilancio separate, l'ACC è certa di poter godere, grazie ad essa, di una maggiore autonomia a beneficio della tutela dei diritti dei cittadini alla vita privata.

Bruxelles, gennaio 2002

Il Presidente
Giovanni Buttarelli

111

PRIMA PARTE: RIEPILOGO

Sono trascorsi 15 anni da quel giorno del 1985 in cui, in un villaggio della Mosella lussemburghese da cui avrebbe tratto il nome, fu firmato l'accordo di Schengen.

Precursore dello spazio di libertà, sicurezza e giustizia che avrebbe poi creato il trattato di Amsterdam, l'accordo ha indubbiamente avuto successo, come dimostra il numero crescente di paesi che hanno aderito all'accordo stesso e alla relativa convenzione di applicazione firmata nel 1990. Ai cinque paesi firmatari del 1985 se ne sono aggiunti altri dieci, l'ultimo dei quali il 25 marzo 2001. (1)

Si ricorda che lo scopo dell'accordo di Schengen e della relativa convenzione di applicazione è l'abolizione dei controlli alle frontiere interne degli Stati membri e, quindi, la creazione di un grande spazio di libera circolazione delle persone. Per conseguire questo obiettivo garantendo nel contempo, all'interno di tale spazio, un livello di sicurezza almeno pari a quello esistente in precedenza, la convenzione di applicazione dell'accordo di Schengen prevede misure compensative, principalmente: armonizzazione della politica dei visti, definizione di una politica comune in materia di determinazione dello Stato responsabile dell'esame di una domanda di asilo, miglioramento della cooperazione di polizia e giudiziaria, intensificazione della lotta al traffico illecito di stupefacenti, armonizzazione del livello dei controlli alle frontiere esterne dello spazio Schengen e creazione di un sistema d'informazione Schengen (SIS).

Il SIS è un sistema comune che collega tutti i paesi che applicano la convenzione 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 uno degli Stati membri che applicano 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).

Alla creazione del SIS si è affiancata quella di un'Autorità di controllo comune per la protezione dei dati personali, incaricata segnatamente di vigilare sul rispetto delle disposizioni della convenzione relative all'unità di supporto tecnico del SIS (articolo 115). A quest'organo, composto di due rappresentanti di ogni autorità di controllo nazionale delle Parti contraenti, è inoltre attribuito un compito di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

Sin dal giugno 1992, una decisione ministeriale ha istituito un'autorità di controllo comune provvisoria, organo che ha compiuto i primi passi nella preparazione dell'applicazione dei principi della protezione dei dati.

Il 26 marzo 1995, contestualmente alla messa in applicazione della convenzione nei sette paesi membri che soddisfacevano le condizioni preliminari, l'autorità di controllo provvisoria si è trasformata in definitiva, ossia nell'Autorità di controllo comune Schengen (ACC) prevista all'articolo 115 della convenzione.

Fin dalla messa in applicazione della convenzione, il 26 marzo 1995, l'ACC ha dovuto faticare molto perché ne fossero riconosciute le competenze e l'indipendenza rispetto agli organi esecutivi di Schengen. Prova ne è la prima relazione di attività, che sottolinea in particolare le difficoltà incontrate per ottenere un bilancio autonomo o quelle sperimentate dal gruppo di esperti cui l'ACC aveva affidato il controllo dell'unità centrale del SIS (C.SIS) installata a Strasburgo. A oltre un anno di distanza l'ACC non aveva ancora ottenuto dagli organi esecutivi di Schengen una risposta alle raccomandazioni formulate in base al controllo del C.SIS, cui aveva replicato soltanto il ministero dell'interno francese. Soltanto dal febbraio 1998 l'ACC può disporre delle informazioni inerenti al SIS che le sono necessarie per svolgere i propri compiti, perché le autorità responsabili del sistema esaminavano le richieste d'informazioni caso per caso.

Nonostante i progressi compiuti il cammino è ancora lungo. Nelle visite di controllo che l'ACC ha effettuato nel 1996 e 1999 presso il sistema centrale di Strasburgo si è sì constatato il buon funzionamento complessivo del sistema, ma si sono anche rilevati diversi problemi, tra cui alcuni che pongono reali difficoltà in termini d'integrità. Gli incon-

(1) I paesi che applicano l'acquis di Schengen sono: Belgio, Paesi Bassi, Lussemburgo, Francia, Germania, Italia, Portogallo, Spagna, Austria, Grecia, Svezia, Danimarca, Finlandia, Islanda e Norvegia.

venienti patiti dai legittimi titolari di identità usurpate inserite nel SIS indicano un'altra debolezza del sistema.

I problemi rilevati dall'ACC hanno acquisito un'importanza vieppiù significativa quando, il numero di Stati Schengen che applicano la convenzione è passato da 7 a 10 alla fine del 1997, e poi a 15 il 25 marzo 2001. Il numero dei dati inseriti nel SIS aumenta infatti di conseguenza (v. allegato 4).

Al pari di tutti i sistemi d'informazione nel settore della polizia, anche quello di Schengen registra un'evoluzione. L'accesso al SIS è stato peraltro esteso ad altri servizi e sono in corso riflessioni per allargarlo anche a servizi non governativi e per aggiungere altre categorie di dati a quelle esistenti. All'evoluzione deve affiancarsi un potenziamento del ruolo delle pertinenti autorità di controllo indipendenti. L'integrazione di Schengen nell'Unione europea risultante dal trattato di Amsterdam[1] deve migliorare la trasparenza e offrire maggiori garanzie per i diritti fondamentali del cittadino. I parlamenti nazionali e gli organi europei possono ora intervenire più attivamente per la realizzazione di questi obiettivi.

SECONDA PARTE: UN ANNO DI ATTIVITÀ DELL'ACC

CAPITOLO I: PARERI E RACCOMANDAZIONI

I.1. Sicurezza degli uffici SIRENE

La sicurezza degli uffici SIRENE è di responsabilità diretta delle autorità di controllo nazionali competenti della protezione dei dati. Il compito di armonizzazione che la convenzione assegna loro ha indotto l'autorità a interessarsi della questione, in particolare a seguito di una fuga di documenti e di informazioni prodottasi presso un ufficio SIRENE nel 1997.

Avvalendosi delle relazioni di controllo degli uffici SIRENE, elaborate dalle autorità nazionali, l'ACC ha formulato 10 raccomandazioni per il miglioramento della sicurezza di tali uffici, che ha trasmesso ai competenti organi di Schengen. Tali autorità hanno risposto[2] affermando che gli *Stati membri ritengono che buona parte delle raccomandazioni dell'Autorità di controllo comune siano già attuate negli uffici SIRENE* e che non avrebbero messo in pratica quelle raccomandazioni che sono *piuttosto onerose sotto il profilo tecnico ed organizzativo rispetto all'obiettivo perseguito.*

L'ACC, nel prendere atto della risposta, ha deciso di perseverare affinché la sicurezza degli uffici SIRENE fosse migliorata e uniformata. Ha quindi steso un questionario uniforme che permetterà alle autorità nazionali di controllo di effettuare le verifiche in modo armonizzato. L'ACC ha approvato il questionario uniforme il 30 giugno 2000:[3] esso servirà di base ai controlli degli uffici SIRENE cui procederanno le autorità nazionali ed è già stato utilizzato dall'Autorità di controllo dell'Europol nel 2000.

I.2. Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

Fin dal 1997 uno dei membri dell'ACC aveva chiesto all'Autorità come andasse interpretato l'articolo 102, paragrafo 1 della convenzione, relativo alla conservazione dei documenti ad avvenuta cancellazione di una segnalazione. Gli Stati membri davano infatti interpretazioni diverse alla disposizione: alcuni di essi conservano i documenti relativi alle segnalazioni dopo che queste sono state cancellate e li utilizzano per completare gli schedari di polizia.

L'articolo 102, paragrafo 1 vieta però alle Parti contraenti di utilizzare i dati di cui agli articoli da 95 a 100 per fini diversi da quelli enunciati per ciascuna delle segnalazioni di cui ai detti articoli.

Nel parere 98/1 del 3 febbraio 1998 l'ACC ha chiesto che ciascuna Parte contraente distruggesse immediatamente tutta la documentazione relativa a una segnalazione cancellata, conformemente all'articolo 112

(1) Cfr. articolo 7 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea, allegato al trattato di Amsterdam
(2) Risposta del 19 novembre 1999 (SCHAC 2512/99).
(3) Doc. SCHAC 2514/00.

della convenzione e che il manuale SIRENE fosse riveduto per eliminare le disposizioni che violano la convenzione di Schengen. Ha poi completato questa raccomandazione con una lettera del 22 ottobre 1999 in cui insisteva sull'obbligo di rispettare il principio di finalità, in base al quale il dossier può essere utilizzato soltanto per i fini che hanno motivato l'inserimento della segnalazione, e sottolineava che i requisiti di finalità e di conservazione limitata alla finalità per la quale la segnalazione è stata effettuata sono altresì enunciati nell'articolo 5 della convenzione n. 108 del Consiglio d'Europa, del 28 gennaio 1981, che tutti gli Stati sono tenuti a osservare (articolo 126, paragrafo 1 della convenzione di Schengen).

Il Comitato dell'articolo 36 del 15 dicembre 1999 ha constatato che secondo il *Servizio giuridico del Consiglio "il parere dell'ACC si riferisce alla prassi seguita in alcuni Stati membri e non alle regole del Consiglio*". Il Comitato dell'articolo 36 ha deciso di consultare il Gruppo SIS per verificare se occorresse modificare il manuale SIRENE alla luce delle osservazioni dell'ACC.

Sebbene non abbia da allora ricevuto alcuna notizia, l'ACC ha potuto constatare le difficoltà che il Consiglio incontra nel modificare l'acquis di Schengen relativo al SIS, ad esempio il Manuale SIRENE. Nel determinare la base giuridica dell'acquis di Schengen non si è riusciti a giungere ad un accordo per il SIS, il quale si fonda perciò su una doppia base giuridica (primo e terzo pilastro) che paralizza qualsiasi evoluzione dell'acquis in materia. L'ACC mantiene pertanto vivo l'auspicio che il Consiglio dia seguito al suo parere, cui peraltro si attiene la maggior parte degli Stati membri.

I.3. Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata

In caso di usurpazione d'identità alcuni Stati membri introducono nel SIS il nome del titolare legittimo dell'identità usurpata, mentre il bersaglio è piuttosto l'usurpatore.

In altre parole, l'identità segnalata nel sistema non corrisponde, né di fatto né di diritto, all'identità del ricercato, bensì a quella della vittima dell'usurpazione. Tuttavia, il titolare legittimo non è assolutamente informato del fatto che la sua identità sia stata introdotta nel SIS.

Alcuni Stati sono favorevoli ad una procedura secondo la quale i dati di carattere personale relativi alle persone la cui identità è stata usurpata dovrebbero essere immediatamente cancellati, mentre altri sostengono che la segnalazione contenente l'identità usurpata dovrebbe essere mantenuta anche se il titolare legittimo dell'identità inserita nel SIS ne richiedesse la cancellazione: l'argomento da essi addotto a sostegno della loro tesi è la necessità di trovare il responsabile.

Nel parere 98/1 del febbraio 1998 l'ACC ha ricordato i diritti fondamentali e i principi della convenzione in materia di protezione dei dati, sottolineando soprattutto il principio di proporzionalità, che impone di raggiungere un equilibrio fra i diritti della persona la cui identità è stata usurpata e la necessità di individuare gli usurpatori.

L'Autorità ha proposto che, fino all'avvio del SIS II, si cerchi di definire una soluzione comune e, se possibile, si indichi che la segnalazione riguarda un'identità usurpata.

In risposta a tale parere il Comitato dell'articolo 36 ha comunicato all'ACC le soluzioni ipotizzate per tale problema (nel prossimo futuro, misure temporanee per il SIS I +, a fine 2000, e soluzione definitiva a più lungo termine per il SIS II).

In base a tali informazioni l'ACC ha formulato un altro parere nel marzo 2000. In esso ribadisce il principio di proporzionalità, in virtù del quale non tutti i casi di usurpazione d'identità giustificano la segnalazione del nome del titolare legittimo e sottolinea che l'elaborazione dei dati relativi alle persone la cui identità è stata usurpata potrà essere consentita solo previo libero ed esplicito accordo delle stesse o dietro loro richiesta. Devono inoltre essere previste altre misure, quali la possibilità di rilasciare al titolare legittimo dell'identità usurpata un documento supplementare, ad esempio integrativo al passaporto, che attesti che il titolare non è la persona che usurpa l'identità.

L'ACC constata con rammarico che le misure temporanee annunciate per fine 2000 non sono granché soddisfacenti, almeno a giudicare dai reclami che continuano ad arrivare alle autorità di controllo nazionali.

I.4. Accesso al SIS da parte dei servizi competenti per l'immatricolazione dei veicoli

Il Presidente del Comitato dell'articolo 36 ha risposto al parere reso dall'ACC nel 1998 sull'accesso al SIS da parte dei servizi competenti per l'immatricolazione dei veicoli[1] comunicando all'ACC, con lettera del 28 aprile 2000,[2] le diverse soluzioni che gli Stati membri hanno adottato o ipotizzano affinché le loro rispettive autorità competenti per l'immatricolazione dei veicoli possano verificare se esista nel SIS una segnalazione riguardante un veicolo di cui è chiesta l'immatricolazione. L'ACC ha rilevato che le soluzioni adottate o ipotizzate si attengono sì al suo parere in materia, ma purtroppo non sono armonizzate.

I.5. Riconoscimento dello status di osservatore al Regno Unito

Il 30 giugno 2000 l'ACC ha votato sul riconoscimento dello status di osservatore al Regno Unito. Il 29 maggio 2000 il Consiglio aveva infatti adottato la decisione riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen.[3] Presa visione del contenuto di tale decisione, l'ACC ha constatato che il Regno Unito poteva legittimamente chiedere di partecipare ai suoi lavori in veste di osservatore. Dalla votazione effettuata a norma dell'articolo 2, paragrafo 2 del regolamento interno dell'ACC è emerso un accordo unanime su tale partecipazione del Regno Unito in veste di osservatore.

La richiesta del Regno Unito di partecipare a una parte dell'acquis di Schengen comporterà la verifica che il paese soddisfi i presupposti per la messa in applicazione di detto acquis, alla quale sarà opportuno associare l'ACC (v. infra, terza parte, punto I.4).

I.6. Messa in applicazione dell'acquis di Schengen nei paesi nordici

Perché l'acquis di Schengen possa essere messo in applicazione nel territorio di uno Stato membro occorre che questo soddisfi i presupposti stabiliti dalla convenzione di Schengen, fra cui l'esistenza di una normativa sulla protezione dei dati personali conforme ai requisiti fissati dalla convenzione (articolo 117, paragrafo 2). Come per gli altri presupposti, neanche in questo caso la convenzione precisa come vada verificata la conformità a tale requisito.

Tuttavia, fin dal suo avvio come organo provvisorio, l'ACC - cui la convenzione attribuisce competenze esclusive in materia di protezione dei dati - ha effettuato tale verifica nel settore in questione quando la convenzione è stata messa in applicazione nel 1995 in sette paesi e successivamente in Italia, Austria e Grecia. Ha poi informato il Gruppo centrale che detto presupposto era soddisfatto.[4]

Da allora sono state istituite delle Commissioni di valutazione incaricate di verificare se i requisiti che l'acquis di Schengen impone negli Stati membri che lo applicano, siano applicati correttamente, soprattutto riguardo al controllo delle frontiere esterne. Nel 1998 a tali controlli si è aggiunta la protezione dei dati, in connessione con il controllo degli uffici SIRENE e N.SIS. All'epoca il Comitato esecutivo di Schengen non ha precisato in che misura l'ACC dovesse essere associata a detti controlli. Interpellato dall'ACC, l'allora Presidente del Gruppo centrale ha comunque confermato che il Presidente dell'ACC poteva assistere alla prevista riunione fra la Commissione di valutazione e il Presidente dell'Autorità tedesca per la protezione dei dati, ma non al resto della valutazione (N.SIS e uffici SIRENE). L'ACC ha declinato l'invito, perché il Presidente dell'Autorità tedesca era un suo membro e non era necessaria l'autorizzazione del Gruppo centrale per consentire al Presidente dell'ACC di assistere a tale riunione.

Questa posizione del Gruppo centrale ha determinato che il controllo dell'osservanza dei principi di protezione dei dati sanciti dalla convenzione fosse affidato a dei rappresentanti dei servizi che, negli Stati che applicano l'acquis di Schengen o in quelli che vi si preparano, si occupano del funzionamento del SIS o lo utilizzano. All'epoca l'ACC aveva denunciato quella che considera una violazione della convenzione, la quale le attribuisce la competenza primaria in materia di controllo dell'osservanza dei principi di protezione dei dati.

(1) Parere 98/5.
(2) Lettera SCHAC 2527/00.
(3) GU L 131 dell'1.6.2000, pag. 43.
(4) Lettera SCH/Aut-cont (97) 35.

Per i paesi nordici la valutazione ha seguito le stesse regole e, al pari del Gruppo centrale nel 1998, il Comitato dell'articolo 36 non ha fatto nulla per renderla accessibile all'ACC tramite una sua partecipazione diretta.

L'ACC ha tuttavia ottenuto dal Presidente del Gruppo centrale di poter prendere visione della relazione inerente alla visita di valutazione Schengen sulla protezione e la sicurezza dei dati nei paesi nordici.[1] Nella riunione del 30 giugno 2000 ha ricevuto tale relazione e ha preso atto delle conclusioni del Consiglio GAI del 29 maggio 2000, il quale ha fatto il punto delle valutazioni sino ad allora effettuate nel quadro della preparazione degli Stati nordici alla piena applicazione di Schengen. Il Consiglio ha preso atto con compiacimento dei notevoli progressi compiuti, constatando che gli Stati nordici si preparavano in maniera adeguata. A suo parere, se tutti gli obiettivi descritti nelle relazioni fossero raggiunti entro il termine previsto e se nel frattempo non fossero constatate divergenze, non sarebbe più il caso di tornare sugli argomenti in merito ai quali erano state effettuate visite o fornite risposte al questionario. Il Consiglio ha indicato che il buon funzionamento del SIS sarebbe stato verificato nel corso del primo trimestre del 2001 e ha confermato l'obiettivo politico di giungere entro il 2000 ad una decisione sulla piena applicazione dell'acquis di Schengen negli Stati nordici a decorrere dal 25 marzo 2001.

Nella medesima riunione l'ACC ha esaminato le risposte che vari paesi nordici avevano trasmesso in merito alla lettera del Presidente dell'ACC del 4 maggio 2000,[2] in cui si chiedevano precisazioni soprattutto sul seguito che tali paesi avrebbero riservato ai pareri dell'ACC, che costituiscono acquis di Schengen, sugli adeguamenti apportati alla normativa per conformarsi ai requisiti di Schengen e sul modo in cui sarebbe stata garantita l'indipendenza dell'autorità di controllo.

Nella riunione dell'11 ottobre 2000 l'ACC ha constatato che, in materia di protezione dei dati personali, nei 5 paesi nordici esistevano i presupposti per la messa in applicazione dell'acquis di Schengen. Ha trasmesso tale parere positivo[3] al Comitato dell'articolo 36 e al Consiglio, il quale ne ha preso atto il 15 marzo 2001, data in cui ha confermato la messa in applicazione dell'acquis di Schengen nei paesi nordici a decorrere dal 25 marzo 2001.

I.7. Progetto di risoluzione del Consiglio sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea

L'ACC aveva chiesto di essere tenuta al corrente dell'andamento dei lavori del Gruppo "Sistemi di informazione e protezione dei dati" che esaminava il progetto di risoluzione del Consiglio sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea. Udita la relazione orale espostale nella riunione del 2 febbraio 2001, l'ACC ha rilevato con soddisfazione che nelle previsioni il Consiglio avrebbe adottato il progetto di risoluzione in tempi brevi. Ha tuttavia deplorato che lo strumento avesse soltanto valore indicativo, a suo avviso poco consono a garantire un'armonizzazione delle norme relative alla protezione dei dati nell'ambito del terzo pilastro. Il Presidente dell'ACC ha fatto presenti tali perplessità al Presidente del Comitato dell'articolo 36 e al Presidente del Gruppo "Sistemi di informazione e protezione dei dati", da cui attende una risposta.

I.8. Attuazione del sistema d'informazione Schengen nel Regno Unito

L'ACC Schengen ha riesaminato una proposta del Regno Unito concernente l'attuazione tecnica della sua partecipazione al SIS.

La soluzione del Regno Unito consiste nel trasmettere tutti i dati SIS al Regno Unito. Poiché tale Stato membro non applica l'articolo 96 dell'accordo di Schengen, i dati sono filtrati prima che gli utenti possano accedervi.

Il principio base nel settore della protezione dei dati è costituito dal principio di necessità. Con l'applicazione di detto principio si può argomentare che, poiché le intenzioni originarie dell'accordo di Schengen, a norma dell'articolo 92, non sussistono per alcune parti contraenti, una parte contraente può trattare i dati solo

(1) Doc. 8110/1/00 REV 1 SCH-EVAL 26 COMIX 365.
(2) Doc. SCHAC 2528/00.
(3) Parere 2000/1 (doc. SCHAC 2543/00), allegato.

nella misura in cui sono necessari ai fini di cui agli articoli da 95 a 100 e se detta parte contraente applica tali articoli.

La soluzione proposta dal Regno Unito fa sì che quest'ultimo possa trattare i dati riguardanti l'articolo 96 in violazione dell'articolo 94 dell'accordo di Schengen.

Nel suo parere l'ACC ha inoltre sottolineato che va difeso il principio secondo il quale un individuo può esercitare i propri diritti in ogni Stato Schengen. Si deve prevedere una procedura in base alla quale le richieste di accesso e di verifica riguardanti i dati di cui all'articolo 96 possono essere inoltrate tramite il commissario per la protezione dei dati nel Regno Unito.

CAPITOLO II: ATTIVITÀ DI CONTROLLO

II.1. Controllo del C.SIS

Nel 1999 un gruppo tecnico costituito di esperti delle autorità di controllo nazionali ha proceduto al controllo del C.SIS. La relazione sulla visita di controllo, di carattere riservatissimo, è stata approvata nel febbraio 2000 e trasmessa, unitamente ad una sintesi, al Comitato dell'articolo 36. Del suo esame è stato incaricato il Gruppo SIS del Consiglio, la cui risposta del 10 maggio è stata trasmessa all'ACC dal Comitato dell'articolo 36.

L'ACC giudica incoraggiante il seguito che è stato dato alla sua ultima relazione sulla visita di controllo della C.SIS, e in particolare alle sue raccomandazioni. Ha rilevato con soddisfazione che 10 di queste sono state già adottate nel C.SIS I+, mentre deplora che altre cinque non possano per il momento essere messe in pratica, anche se la situazione dovrebbe evolvere in senso positivo, probabilmente già per il SIS II al più tardi.

Seppur consapevole che l'attuazione di alcune delle sue raccomandazioni pone difficoltà, l'ACC ha ricordato che, poiché la convenzione le assegna il compito di controllare che le misure di sicurezza del C.SIS siano rispettate, è suo dovere formulare le raccomandazioni del caso affinché il C.SIS si attesti sempre su un livello di sicurezza fra i più elevati. Le quattro raccomandazioni dell'ACC che non saranno messe in pratica vertono sulla sicurezza fisica, il blocco dei terminali dopo un dato tempo, l'assenza di barriere fisiche fra il personale del Ministero dell'interno e il C.SIS e la gestione dei dispositivi di cifratura e di altri elementi relativi alle comunicazioni. L'ACC ha insistito affinché i gruppi tecnici continuassero a valutare con attenzione le conseguenze dell'aver scartato tali raccomandazioni e vagliassero i rischi per la sicurezza insiti nel non intervenire sulle situazioni da essa rilevate.

II.2. Gruppi tecnici ed esperti

Per poter verificare se nel quadro del SIS II si tenesse debitamente conto degli aspetti connessi alla sicurezza, l'ACC aveva chiesto di prendere visione del capitolato d'oneri della futura rete SIS II e di essere tenuta al corrente dei problemi giuridici dovuti al fatto che il SIS non si fonda su una base giuridica unica.

Per quanto riguarda la mancanza di base giuridica, nella riunione del 13 dicembre 2000 l'ACC è stata informata che, all'atto dell'adozione della decisione del 20 maggio 1999 che determina, in conformità delle pertinenti disposizioni del trattato che istituisce la Comunità europea e del trattato sull'Unione europea, la base giuridica per ciascuna delle disposizioni o decisioni che costituiscono l'acquis di Schengen il Consiglio non era riuscito a classificare le disposizioni dell'acquis di Schengen relative al SIS. Durante le discussioni erano infatti emerse divergenze d'opinione fondamentali fra le delegazioni - Commissione compresa - quanto alla base giuridica da adottare per tali disposizioni dell'acquis di Schengen. Nessuna delegazione ha nel frattempo comunicato di aver mutato posizione.

Da allora sono state avanzate diverse proposte intese ad ampliare le funzionalità del SIS II rispetto al SIS attuale, ma molte di esse comporterebbero una modifica delle vigenti disposizioni dell'acquis di Schengen integrato nell'ambito dell'Unione europea, al cui riguardo sussistono divergenze d'opinione. Queste dovranno essere sanate in tempi rapidi e con soluzioni inattaccabili se si vorranno concretare le proposte degli Stati membri.

Sempre dopo averla sollecitata, l'ACC ha ottenuto, nella riunione del 2 febbraio 2001, una sintesi delle

nuove funzionalità previste per il SIS II. Ha preso atto dell'intenzione del Gruppo SIS di esaminare in un secondo tempo le questioni relative alla protezione dei dati personali che alcune delle nuove funzionalità porranno. L'ACC dovrà essere tenuta al corrente dei lavori al riguardo per potersi accertare che le conclusioni del Gruppo rispecchino il suo parere e lascino impregiudicata la protezione dei dati.

I requisiti funzionali della futura rete non sono comunque ancora stati stabiliti.

II.3. Criptazione dei collegamenti SIS

Nel febbraio 2000 l'ACC aveva chiesto informazioni sull'algoritmo di cifratura utilizzato nei collegamenti SIS e messo a punto dall'Ufficio federale tedesco per la sicurezza in materia di tecnologie dell'informazione[1] e dalla società Bosch Telecom. Tali informazioni, che le sono state comunicate nel luglio 2000,[2] l'hanno indotta a chiedere, nel dicembre dello stesso anno,[3] che si realizzasse uno studio per valutare effettivamente le conseguenze economiche e organizzative che comporterebbe l'attuazione, già nel quadro di SISNET, delle misure necessarie per modificare periodicamente le chiavi di cifratura dei dispositivi. Queste infatti non sono state mai modificate dopo l'entrata in funzione del SIS e l'ACC ritiene che il loro mantenimento a tempo indefinito possa costituire un grave rischio per la sicurezza del traffico di dati SIS, dato che, secondo i criteri più elementari in materia di sicurezza, la validità di un sistema di cifratura dipende direttamente dal periodo fissato per modificare le sue chiavi. L'ACC ha inoltre chiesto informazioni sullo stato del progetto SISNET e una documentazione sui requisiti tecnici di questo nuovo sistema, mediante il quale saranno in futuro modificate le chiavi.

L'ACC si compiace che, il 23 marzo 2001, il Comitato dell'articolo 36 abbia approvato un progetto di risposta, sottopostogli dal Gruppo SIS, in cui si propone di dar seguito al parere dell'ACC modificando periodicamente le chiavi di cifratura dei dispositivi.

II.4. Elenco delle autorità autorizzate a consultare direttamente il SIS

L'ACC ha ottenuto, dopo averlo sollecitato, l'elenco aggiornato delle autorità autorizzate a consultare il SIS (doc. 5002/00 SIS 2 COMIX 2), che è stato presentato al Consiglio GAI del 27 marzo 2000.

L'ACC ha invitato i presidenti delle autorità di controllo nazionali a verificare, in base all'articolo 114 della convenzione, se le condizioni di accesso al SIS siano rispettate. Ha inoltre ricordato al Comitato dell'articolo 36 il ruolo che le autorità di controllo nazionali svolgono per l'aggiornamento dell'elenco delle autorità autorizzare a consultare il SIS.

CAPITOLO III: CAMPAGNA D'INFORMAZIONE

III.1. Campagna d'informazione sui diritti dei cittadini nei confronti del SIS

Nel 1997, l'ACC aveva deciso di varare in tutti paesi una campagna d'informazione destinata ai cittadini dal titolo "Il sistema di informazione Schengen vi riguarda". L'ACC aveva 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 informazione diretta al pubblico. Essa ha dunque deciso di informare i cittadini dei loro diritti nei confronti del SIS mediante opuscoli.

L'ACC ha ottenuto che gli organi di Schengen sostenessero la sua campagna di informazione, incaricandosi della stampa degli opuscoli informativi e della loro diffusione alle frontiere esterne di Schengen.

L'ACC ha proceduto a varie riprese alla valutazione di tale campagna. A quattro anni dal suo avvio, gli opuscoli dell'ACC sono diffusi in sette Stati membri che applicano l'acquis di Schengen. Il numero di domande

(1) Il BSI, ossia il "Bundesamt für die Sicherheit in der Informationstechnik".
(2) Doc. 9998/00 CATS 49 SIS 61 COMIX 522.
(3) Doc. SCHAC 2544/1/00.

di accesso presentate da cittadini ai quali è stato rifiutato l'ingresso nel territorio Schengen è notevolmente aumentato in seguito a tale campagna, dimostrandone l'efficacia. Gli Stati membri hanno ricevuto numerose domande di accesso relative a segnalazioni di cui i cittadini erano oggetto.

L'ACC deplora tuttavia che finora le autorità competenti francese e lussemburghese non abbiano ancora fornito gli strumenti necessari al lancio di tale campagna di informazione dei cittadini. I paesi nordici hanno invece dichiarato di attribuire la massima importanza a questa campagna e stanno esaminando le possibilità di realizzarla. In taluni paesi nordici alcune attività d'informazione sono già state svolte insieme alle autorità competenti. Per migliorare il trattamento delle domande per le quali è necessaria l'applicazione della procedura di cooperazione definita dall'ACC in base all'articolo 114, paragrafo 2, della convenzione, il gruppo di esperti che ha ideato l'opuscolo informativo ha redatto, basandosi sulle risposte degli Stati membri, un progetto di vademecum sul diritto dei cittadini di accedere alle informazioni contenute nel SIS e sulla cooperazione tra le autorità di controllo. Il vademecum, la cui stesura definitiva è attesa a breve, si rivolgerà alle autorità di controllo nazionali ma anche ai professionisti del diritto, che vi troveranno tutte le informazioni utili in merito alle procedure che una persona deve seguire per far valere il suo diritto di accedere ai dati che la riguardano inseriti nel SIS e di ottenerne, se del caso, la rettifica.

III.2. 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 sull'attività dell'ACC. In conseguenza all'integrazione di Schengen nell'ambito dell'Unione europea, sarà il sito del Consiglio ad ospitare la pagina dell'ACC non appena saranno stati apportati gli adeguamenti necessari al progetto. La pagina dell'ACC è provvisoriamente ospitata dall'autorità di controllo portoghese e può essere consultata sul sito di questa (http://www.cnpd.pt/schengen).

III.3. Presentazione della quarta relazione annuale dell'ACC in occasione della conferenza stampa di Bruxelles

L'ACC ha presentato la quarta relazione sulle sue attività (marzo 1999 - febbraio 2000)[1] nella conferenza stampa organizzata l'11 ottobre 2000 a Bruxelles. La stampa internazionale, in particolare quella dei paesi candidati all'adesione all'Unione europea, si è mostrata particolarmente interessata al ruolo e alle competenze dell'ACC nel sistema Schengen, al funzionamento del SIS, al tipo di dati in esso contenuti e agli strumenti di accesso di cui dispone il cittadino, così come al futuro dell'ACC.

Interviste sulle attività dell'ACC sono state rilasciate alle televisioni svedese e danese e sono state pubblicate su quotidiani e su periodici specializzati in Danimarca, Norvegia e Svezia.

Le relazioni sono state diffuse dalle autorità di controllo nazionali utilizzando gli stessi canali di cui si avvalgono per le loro relazioni nazionali e, in taluni casi, Internet. Sono state altresì trasmesse dal Presidente dell'ACC al Presidente e alla Commissione per le libertà pubbliche del Parlamento europeo. In alcuni paesi si sono tenute conferenze stampa per presentare il documento e per sensibilizzare il pubblico.

CAPITOLO IV: INTEGRAZIONE DELL'UNIONE EUROPEA E ACQUIS DELL'ACC

Ai sensi del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea 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 ecc.

(1) Doc. SCHAC 2533/1/00 REV1.

111

Su richiesta del Gruppo centrale Schengen, l'ACC ha redatto l'elenco del suo acquis, nella prospettiva dell'integrazione dell'acquis di Schengen nell'Unione europea (allegato 7), nel quale erano enumerati i pareri adottati dall'ACC e le decisioni adottate dagli organi esecutivi di Schengen in merito al funzionamento dell'ACC e alla sua indipendenza. Tale elenco è stato trasmesso al Consiglio dell'Unione europea e al Presidente del Gruppo centrale il 18 maggio 1998, così come, nel dicembre 1998, una nota supplementare relativa all'acquis istituzionale e funzionale dell'ACC.

Tale punto non è stato trattato dal Gruppo centrale né nella riunione del 19 febbraio 1999 né successivamente, nonostante un sollecito rivolto dall'ACC al Presidente di tale gruppo.

Nessuno dei pareri dell'ACC o delle decisioni che la riguardano è stato incorporato nell'acquis di Schengen integrato nell'ambito dell'Unione europea. Il Consiglio dei Ministri ha adottato, il 20 maggio 1999, una *decisione del Consiglio concernente l'Autorità di controllo comune istituita dall'articolo 115 della convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmata il 19 giugno 1990.*[1] Con tale decisione il Consiglio si impegna a provvedere al segretariato dell'ACC e a fornirle i mezzi logistici necessari all'organizzazione delle sue riunioni a Bruxelles, oltre che a rimborsare le spese di viaggio dei suoi membri per le riunioni dell'ACC a Bruxelles o dei suoi esperti per i controlli a Strasburgo. Nella decisione si constata inoltre che l'ACC dovrà adattare il suo regolamento interno alla nuova situazione.

L'ACC insiste nel deplorare che, a causa di questa interpretazione restrittiva del Protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea allegato al trattato di Amsterdam, l'acquis dell'ACC continui ad avere come base giuridica quella dell'ACC stessa.

L'ACC rileva quindi che i suoi pareri e le sue raccomandazioni costituiscono un insieme la cui base giuridica è fondata su quella dell'ACC stessa, che deve essere presa in considerazione dagli Stati che applicano attualmente l'acquis di Schengen e da ogni nuovo Stato che si unirà ad essi.

Nel parere 2000/1 l'ACC ha annunciato che incaricherà le autorità di controllo nazionali di verificare il rispetto di tale acquis.

CAPITOLO V: FUNZIONAMENTO DELL'ACC

V.1. Riunioni

Dal marzo 2000 l'ACC ha tenuto otto riunioni plenarie, alle quali si aggiungono una riunione del gruppo ristretto sul diritto di accesso e una riunione di esperti sul controllo del C.SIS e degli uffici SIRENE.

V.2. Elezioni del Presidente e del Vicepresidente

Nel dicembre 2000, i Sigg. B. De Schutter (delegazione belga) e G. Buttarelli (delegazione italiana) sono stati confermati nelle rispettive cariche di Presidente e Vicepresidente.

Nel dicembre 2001 il Sig. G. Butarelli è stato eletto Presidente.

V.3. Bilancio dell'ACC e supporto di segreteria

L'ACC non ha ancora riottenuto una linea di bilancio autonoma. Eppure, i bilanci relativi al funzionamento del SIS sono stati ripresi nell'acquis e la linea di bilancio autonoma assegnata all'ACC rientrava nella definizione dell'acquis di Schengen ai sensi del protocollo allegato al trattato di Amsterdam.

L'ACC deplora che, nella sua decisione, il Consiglio non abbia tenuto conto di talune missioni che la convenzione le attribuisce. Ai sensi della decisione infatti, se sono a carico del Consiglio le spese di viaggio dei

(1) Decisione adottata dal Consiglio il 20 maggio 1999 e pubblicata nella GU L 176 del 10 luglio 1999, pag. 34.

membri per le riunioni plenarie a Bruxelles, non lo sono invece le spese di soggiorno per le visite di controllo del C.SIS né quelle indotte, ad esempio, da una campagna d'informazione dei cittadini sui loro diritti nei confronti del SIS. L'efficienza dell'ACC dipende quindi in gran parte dalla buona volontà del Consiglio, e in particolare della Presidenza in carica, la quale si trova di fronte ad una scelta difficile fra le proprie priorità, in cui l'ACC non necessariamente viene al primo posto, e le limitate risorse del Consiglio in termini di, segnatamente, disponibilità delle sale di riunione e degli interpreti.

Quanto al supporto di segreteria, dal 1° settembre 2001 l'ACC condivide un segretariato con l'autorità dell'Europol e quella doganale. Il Consiglio ha infatti approvato, con decisione del 17 ottobre 2000, l'istituzione di un segretariato comune per le autorità di controllo comuni del terzo pilastro del trattato sull'Unione europea.[1] Il personale assegnato a tale segretariato (due persone nel settembre 2001, cui se ne aggiungerà una terza nei mesi successivi) lavorerà per le tre autorità, segnando così un netto miglioramento rispetto alla situazione attuale.

Detta decisione del Consiglio segna una prima tappa verso un ravvicinamento delle autorità di controllo comuni stesse. Questa fase potrà essere superata solo svolgendo una riflessione approfondita sul ruolo delle autorità di controllo istituite a livello europeo e sui mezzi da assegnare loro affinché possano onorare il loro ruolo fondamentale di custode dei diritti dei cittadini a fronte di un sistema di trattamento dei dati inquadrato nell'ambito di polizia a livello europeo.

V.4. Regolamento interno

Il regolamento interno dell'ACC è riportato in allegato. Esso non è stato modificato nel senso chiesto dal Consiglio nella decisione del 20 maggio 1999 e l'ACC continua ad applicarlo per quanto esso è compatibile con la situazione venutasi a creare a seguito della decisione del Consiglio. Si rilevi che le incompatibilità tra il regolamento interno dell'ACC e la decisione del Consiglio riguardano solo aspetti pratici e organizzativi, che l'ACC peraltro contesta.

TERZA PARTE:

RELAZIONI DELL'ACC ALL'INTERNO E AL DI FUORI DELLA STRUTTURA SCHENGEN E DEL CONSIGLIO

I.1. Relazioni con la Commissione per le libertà pubbliche del Parlamento europeo

Dal 1997 l'ACC ha proposto alla Presidenza della Commissione per le libertà pubbliche del Parlamento europeo di poterle presentare la sua relazione annuale. Una serie di esemplari della stessa sono stati inviati ogni anno a questa Commissione del Parlamento europeo. Il Presidente dell'ACC vi è stato invitato ad un'audizione dedicata al tema "Unione europea e protezione dei dati" svoltasi il 22 e 23 febbraio 2000. Ha così potuto illustrare il ruolo dell'ACC e i suoi principali risultati. I partecipanti si sono interessati in modo particolare al problema dell'usurpazione d'identità. L'ACC si compiace per tale iniziativa del Parlamento europeo che risponde al suo desiderio di trasparenza e d'informazione.

Il 27 giugno 2000 il Presidente dell'ACC ha partecipato, assieme ad una rappresentante della Presidenza portoghese, al Presidente portoghese del Gruppo "Sistemi d'informazione e protezione dei dati" e al suo successore francese, a una riunione con il deputato europeo Hernández Mollar, relatore della Commissione per le libertà pubbliche, in cui si è discusso del progetto di decisione relativa al segretariato comune delle autorità di controllo. Il Parlamento ha espresso timori riguardo all'indipendenza delle autorità di controllo, segnatamente a livello di bilancio, e ha manifestato l'intenzione di proporre l'assegnazione di una linea di bilancio autonoma alle autorità di controllo, come avviene per il mediatore.

---

(1) Decisione del Consiglio, del 17 ottobre 2000, che istituisce un segretariato delle autorità di controllo comuni preposte alla protezione dei dati istituite dalla convenzione che istituisce un ufficio europeo di polizia (convenzione Europol), dalla convenzione sull'uso dell'informatica nel settore doganale e dalla convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni (convenzione di Schengen) - GU L 271 del 24.10.2000, pag. 1.

Il Presidente dell'ACC è stato inoltre invitato ad assistere alla seduta della Commissione per le libertà pubbliche del 12 luglio 2000, durante la quale è stato esaminato il progetto di decisione.

I.2. Relazioni con il Comitato dell'articolo 36, il Comitato dei Rappresentanti Permanenti e il Consiglio

Prima dell'integrazione di Schengen nell'Unione europea, il Gruppo centrale aveva accettato di associare l'ACC alle attività sullo studio preliminare della rete SIRENE fase II e sul SIS I+. L'ACC doveva in tal modo accertarsi che il sistema futuro comprendesse specifiche tecniche che consentissero di esercitare i controlli previsti dalla convenzione. Da allora i lavori dei gruppi tecnici sono stati portati avanti senza che l'ACC vi fosse associata: essa non ha ricevuto nessuna informazione sull'integrazione dei cinque paesi nordici nel SIS, mentre le informazioni sugli sviluppi tecnici in preparazione (SIS I+ e SIS II) le sono state comunicate soltanto dopo ripetuti solleciti.

Dall'integrazione di Schengen nell'ambito dell'Unione europea, i Presidenti successivi dell'ACC hanno sempre voluto allacciare contatti informali con le varie Presidenze del Consiglio in carica. Il primo incontro ha avuto luogo sotto Presidenza finlandese e verteva su un progetto di segretariato comune alle autorità di controllo comuni del terzo pilastro, mentre il secondo si è svolto sotto Presidenza portoghese e riguardava la valutazione del livello di protezione dei dati di carattere personale nei paesi nordici. Sotto Presidenza francese non c'è stata nessuna riunione, mentre l'attuale Presidenza svedese dà prova di un'apertura incoraggiante: nel febbraio 2001 il Presidente del Comitato dell'articolo 36 ha infatti assicurato al Presidente dell'ACC che avrebbe sostenuto l'ACC nelle sue attività.

I.3. Commissione di valutazione – Paesi nordici

Nel gennaio e febbraio 2001 sono state effettuate altre visite di valutazione nei paesi nordici per verificare l'esistenza dei presupposti per la messa in applicazione dell'acquis di Schengen per quanto riguarda il controllo alle frontiere esterne e il funzionamento del SIS.

L'ACC, benché abbia un interesse diretto in questo campo, non è stata associata in nessun modo alla valutazione e neppure i suoi risultati le sono stati comunicati ufficialmente.

I.4. Posizione del Regno Unito e dell'Irlanda

Questi due paesi sono gli unici dell'Unione europea che non applicano ancora l'acquis di Schengen.

L'articolo 4 del protocollo Schengen offre la possibilità al Regno Unito e all'Irlanda, i quali non sono vincolati dall'acquis di Schengen, di chiedere di partecipare, in tutto o in parte, alle disposizioni di detto acquis.

Il Regno Unito si è avvalso di tale disposizione nel 1999 e, su tale base, applicherà in parte l'acquis di Schengen, in particolare il SIS. Il progetto di decisione prevede che il regime in materia di protezione dei dati della convenzione di Schengen sarà applicabile al Regno Unito nella misura in cui questo paese applicherà l'acquis di Schengen. Allo stato attuale del fascicolo, solo l'articolo 96 della convenzione dovrebbe essere escluso dal campo di applicazione. Il 30 giugno 2000 l'ACC ha riconosciuto al Regno Unito lo status di osservatore (v. supra, seconda parte, punto I.5).

La richiesta dell'Irlanda di partecipare in parte alle disposizioni dell'acquis di Schengen è attualmente all'esame.

L'ACC auspica di poter svolgere la propria funzione venendo associata alla verifica dei presupposti per la messa in applicazione dell'acquis di Schengen in questi due paesi.

QUARTA PARTE: REAZIONI DELLE AUTORITÀ SCHENGEN ALLA RELAZIONE ANNUALE DELL'ACC

L'ACC non ha registrato nessuna reazione degli organi del Consiglio alla sua quarta relazione di attività.

QUINTA PARTE: IL FUTURO DELL'ACC NEL NUOVO QUADRO ISTITUZIONALE

I sistemi d'informazione in Europa sono in continua evoluzione. Il sistema d'informazione Schengen è applicato in 15 paesi, la convenzione Europol è entrata in vigore e la sua autorità di controllo funziona e anche il sistema d'informazione doganale e il sistema Eurodac saranno tra breve operativi.

A fronte di tale evoluzione costante, relativamente al trattamento dei dati personali nel settore della cooperazione di polizia il ruolo dell'ACC - al pari di quello dell'autorità di controllo comune dell'Europol e dell'autorità istituita dalla convenzione sull'uso dell'informatica nel settore doganale - è indispensabile per garantire l'equilibrio fra il buon funzionamento dell'apparato di polizia e la massima tutela dei diritti umani. Se l'istituzione di un segretariato unico segna un importante primo passo verso il consolidamento del sistema di controllo, si dovrà altresì vagliare seriamente la possibilità di armonizzare, se non addirittura di fondere, gli organi di controllo. Il nuovo interesse del Parlamento europeo e la maggiore consapevolezza da parte dei cittadini dell'importanza dei garanti del corretto funzionamento di tali organi sono peraltro segnali incoraggianti dell'interesse sempre maggiore che converge sulle attività dell'ACC nell'Unione europea, spazio di libertà, sicurezza e giustizia.

1. COMPOSIZIONE DELLE DELEGAZIONI DELL'AUTORITÀ DI CONTROLLO COMUNE

aggiornamento: 31 dicembre 2001

Presidente: **Sig. Bart DE SCHUTTER**
Vicepresidente: **Sig. Giovanni BUTTARELLI**

AUSTRIA

MEMBRI
Sig.ra Waltraut KOTSCHY
Sig.ra Eva SOUHRADA-KIRCHMAYER
SUPPLENTI
Sig.ra Birgit HROVAT-WESENER

BELGIO

MEMBRI
Sig. Bart DE SCHUTTER
Sig.ra Bénédicte HAVELANGE

DANIMARCA

MEMBRI
Sig.ra Lotte N. JØRGENSEN
Sig. Peter AHLESON

FINLANDIA

MEMBRI
Sig.ra Maija KLEEMOLA
Sig. Reijo AARNIO

111

SUPPLENTE
Sig. Heiki HUHTINIEMI

FRANCIA

MEMBRI
Sig. Alex TÜRK
Sig.ra Florence FOURETS
SUPPLENTI
Sig. Olivier COUTOR

GERMANIA

MEMBRI
Sig. Joachim JACOB
rappresentato dal Sig. Wolfgang von POMMER ESCHE
Sig. Friedrich VON ZEZSCHWITZ
rappresentato dalla Sig.ra Angelika SCHRIEVER-STEINBERG

GRECIA

MEMBRI
Sig. Constantinos DAFERMOS
SUPPLENTI
Sig. Georgios DELYANNIS
Sig. Dimitrios GRITZALIS

ISLANDA

MEMBRI
Sig. Sigrun JÖHANNESDOTTIR
Sig.ra Margret STEINARSDOTTIR

ITALIA

MEMBRI
Sig. Sebastiano NERI
Sig. Giovanni BUTTARELLI

LUSSEMBURGO

MEMBRI
Sig. René FABER
SUPPLENTI
Sig. Jean WAGNER
Sig. Georges WIVENES

PAESI BASSI

MEMBRI
Sig. Peter HUSTINX
Sig. Ulco van de POL

NORVEGIA

MEMBRI
Sig. Georg APENES
Sig.a Guro SLETTEMARK

PORTOGALLO

MEMBRI
Sig. Luis BARROSO
Sig.a Isabel CRUZ

SPAGNA

MEMBRI
Sig. Juan Manuel FERNANDEZ LOPEZ
Sig. Miguel Angel LOPEZ HERRERO
SUPPLENTI
Sig. Emilio ACED FELEZ
Sig.a María Concepción ROMERO CIQUE

SVEZIA

MEMBRI
Sig. Leif LINDGREN
Sig.a Britt-Marie WESTER
SUPPLENTI
Sig.a Birgitta ABJORNSSON
Sig.a Anna-Karin WALDTON

2. 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	– Vigilare sul trasporto e sulla conservazione del back-up dei dati. – Migliorare l'affidabilità dei collegamenti tra il C.SIS e gli N.SIS. – Garantire una separazione fisica tra le apparecchiature del C.SIS e quelle del Ministero dell'Interno francese situate nello stesso edificio.	– 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	Poiché la Convenzione non prevede una base giuridica per l'esistenza degli uffici SIRENE, tale base va creata modificando la Convenzione o modificando in modo armonizzato le legislazioni nazionali.	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	Vigilare sull'identità degli archivi delle Parti contraenti.	Definizione di una nuova procedura di raffronto dei dati che non evidenzia più le differenze riscontrate dall'ACC	Le differenze continuano ad esistere, ma non sono più evidenziate
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 e 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.

	Contenuto	Attività	Osservazioni
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 ha constatato, nel 1999, che il numero di "super utenti" è stato 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 esperti 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.	

	Contenuto	Attività	Osservazioni
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. 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.	Nel 1998 la questione era ancora allo studio del Comitato di orientamento SIS.	

	Contenuto	Attività	Osservazioni
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.		

	Contenuto	Attività	Osservazioni
Parere supplementare dell'11 ottobre 1999 sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione		Il Comitato dell'articolo 36 conferma l'analisi del gruppo centrale e invita il gruppo SIRENE ad adeguare, se necessario, il manuale SIRENE.	
Parere supplementare del 15 febbraio 2000 sulla segnalazione nel SIS di persone vittime di un'usurpazione d'identità			
Nordic SCHAC 2543/000	Analisi dell'ottemperanza alle condizioni preliminari per la messa in applicazione dell'acquis di Schengen nei paesi nordici – protezione dei dati di carattere personale		
Attuazione del SIS nel R.U SCHAC 2520/01	Attuazione del SIS nel Regno Unito		

3. 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 modalit‡ 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 dellíACC del 27 marzo 1997) e SCH/Aut-cont (97) L 5
Decisione dell'ACC relativa alle leggi sulla protezione dei dati dellíItalia	Dichiarazione dell'ACC sull'entrata in vigore delle leggi sulla protezione dei dati dellíItalia	SCH/Aut-cont (97) PV 7 (riunione dellíACC del 4 luglio 1997) e SCH/Aut-cont (97) 35
Elenco delle autorit‡ 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 dellíACCP del 22 febbraio 1995)
Raccomandazioni dell'ACCP sul C.SIS	Raccomandazioni relative alla sicurezza presso il C.SIS, all'affidabilit‡ 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 autorit‡ 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 attivit‡ 1995-1997.	• SCH/Aut-cont (96) 40, 2a rev. (dicembre 1996, versione definitiva del 27 marzo 1997) ñ (RISERVATO) • SCH/Aut-cont (97) 27, 2a rev. (Relazione di attivit‡ 1995-1997 del 17 marzo 1997) ñ pagg. 24-28
Parere sul progetto pilota relativo ai veicoli rubati	Principi da rispettare in materia di scambio di informazioni provenienti dal SIS, nellíambito 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
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.)

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)
Parere sull'attuazione del SIS nel Regno Unito	Categorie di dati da trasmettere al Regno Unito	Parere del 23 ottobre 2001 SCHAC 2520/01
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. È 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.

4. DATI INSERITI NEL SIS

SIS Data Base from C.SIS point of view the 31/12/2001 at 00:00 utc

	NAT	NBE	NDE	NDK	NES	NFI	NFR	NGR	NIS	NIT	NLU	NNL	NNO	NPT	NSE	Total
Valid records (not expired)																
BK	378	421	213 157	72	342	270	328 297	0	0	27 676	196	602	0	76	1	571 488
DB	111	19 954	137 449	2	10 564	0	27 429	165	2	9 344	21	6 090	3	98	443	211 673
FA	3 286	2 574	137 049	23	21 192	4 321	71 946	8 770	0	4 469	800	1 197	105	13 793	8 465	277 990
ID	172 519	40 089	1 437 150	48 910	47 505	9 343	2 291 354	2 160	0	1 718 978	4 829	1 148 365	8 772	937	258 252	7 189 163
VE	6 842	29 144	154 776	4 455	132 262	1 129	256 830	25 614	0	343 800	532	40 159	4 094	24 432	32 268	1 056 337
WP	40 784	4 706	636 639	494	19 799	3 350	146 865	57 065	11	299 586	970	12 880	421	6 483	4 567	1 234 620
Total	223 920	96 888	2 716 220	53 956	231 664	18 413	3 122 721	93 774	13	2 403 853	7 348	1 209 293	13 395	45 817	303 996	10 541 271
Logicaly deleted records existing at N.SIS																
BK	0	0	193	0	0	0	231	0	0	0	0	0	0	0	0	424
DB	0	1	0	0	0	0	0	0	0	6	0	0	0	0	0	7
FA	0	3	9	0	5	0	2	11	0	0	0	0	0	5	0	35
ID	369	97	1 782	63	2	16	3 695	27	0	6 390	9	498	3	0	343	13 294
VE	36	255	974	175	871	14	3 512	247	0	2 281	7	343	91	200	311	9 317
WP	192	19	2 146	1	170	46	724	16	0	210	4	80	2	7	6	3 623
Total	597	375	5 104	239	1 048	76	8 164	301	0	8 887	20	921	96	212	660	26 700
Requests from previous day																
DB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FA	0	3	4	0	0	0	0	0	0	1	0	0	0	0	0	8
ID	72	6	185	17	2	7	2	0	0	72	0	44	14	0	9	430
VE	2	70	156	69	545	6	1 098	60	0	174	2	73	24	90	118	2 487
WP	9	2	152	2	56	2	213	0	0	14	2	5	0	0	0	457
Total	83	81	497	88	603	15	1 313	60	0	261	4	122	38	90	127	3 382

Broadcasts from previous day							
	BK	DB	FA	ID	VE	WP	Total
Requests	0	0	8	430	2 487	457	3 382
Phy del at N.SIS	0	4	6	1 296	1 900	546	3 752
Total	0	4	14	1 726	4 387	1 003	7 134

Distribution of logicaly deleted records present at N.SIS (per day)								
Expiration dates								
31/12/2001	30/12/2001	29/12/2001	28/12/2001	27/12/2001	26/12/2001	25/12/2001	Older	Total
4 344	3 014	4 196	3 912	5 644	5 590	0	0	26 700
					Can be physicaly deleted at N.SIS from today			

SIS Data Base from C.SIS point of view the 31/12/2001 at 00:00 utc

	NAT	NBE	NDE	NDK	NES	NFI	NFR	NGR	NIS	NIT	NLU	NNL	NNO	NPT	NSE	Total
Distribution of WP records per type																
Main	38 598	3 565	295 403	482	18 686	2 895	98 734	56 918	8	296 007	887	9 525	378	6 459	4 044	832 589
Alias	2 186	1 141	341 236	12	1 113	455	48 131	147	3	3 579	83	3 355	43	24	523	402 031
Total	40 784	4 706	636 639	494	19 799	3 350	146 865	57 065	11	299 586	970	12 880	421	6 483	4 567	1 234 620
Distribution of 'WP main records' by article																
(95)	847	1 113	3 951	73	777	83	2 335	256	5	2 193	112	400	53	331	126	12 655
(96)	33 400	456	286 266	56	8 862	2 666	53 823	56 288	3	277 480	336	7 913	233	1 302	3 820	732 904
(97) Adult	175	692	1 012	30	5 552	37	4 819	295	0	1 689	59	530	16	1 294	21	16 221
(97) Under age	83	686	1 112	20	2 436	9	8 270	79	0	1 754	35	621	6	732	26	15 869
(98)	3 693	594	2 461	99	802	85	19 741	0	0	2 199	345	27	54	2 800	6	32 906
(99,2) Observation	400	5	601	204	194	14	5 353	0	0	9 823	0	33	16	0	45	16 688
(99,2) Check	0	19	0	0	63	1	4 393	0	0	869	0	1	0	0	0	5 346
Total	38 598	3 565	295 403	482	18 686	2 895	98 734	56 918	8	296 007	887	9 525	378	6 459	4 044	832 589
Distribution of VE records per type																
Main	6 842	29 143	154 776	4 455	132 262	1 129	254 857	25 614	0	343 800	532	40 159	4 094	24 432	32 268	1 054 363
Alias	0	1	0	0	0	0	1 973	0	0	0	0	0	0	0	0	1 974
Total	6 842	29 144	154 776	4 455	132 262	1 129	256 830	25 614	0	343 800	532	40 159	4 094	24 432	32 268	1 056 337
Distribution of 'VE main records' by article																
(99) Observation	25	7	595	2	87	0	583	1	0	77	0	11	0	0	0	1 388
(99) Check	0	36	0	0	758	1	3 328	1	0	80	0	8	1	0	0	4 213
(100) Lost or stolen	6 814	29 100	32 458	4 429	131 359	1 126	250 946	25 612	0	339 476	523	40 055	3 762	23 934	32 268	921 862
(100) In search	3	0	121 723	24	58	2	0	0	0	4 167	9	85	331	498	0	126 900
Total	6 842	29 143	154 776	4 455	132 262	1 129	254 857	25 614	0	343 800	532	40 159	4 094	24 432	32 268	1 054 363

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (art. 29 direttiva 95/46/CE)

112 Raccomandazione 1/2001 concernente i dati relativi alla valutazione del personale Adottata il 22.3.2001

GRUPPO DI LAVORO "ARTICOLO 29" - PROTEZIONE DEI DATI PERSONALI

5008/01/IT def.
WP 42

Raccomandazione 1/2001
concernente i dati relativi alla valutazione del personale
Adottata il 22.3.2001

Il gruppo, istituito dall'articolo 29 della direttiva 95/46/CE è l'organo comunitario indipendente e avente carattere consultivo per la protezione dei dati e della vita privata. Le sue mansioni sono definite dall'articolo 30 della direttiva 95/46/CE e dall'articolo 14 della direttiva 97/66/CE. Il Segretariato è fornito dalla:

Commissione europea, Mercato interno, Unità libera circolazione dell'informazione e protezione dei dati. B-1049 Bruxelles/B-1049 Brussel - Belgio - Ufficio: C100-6/136 Indirizzo Internet: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

IL GRUPPO DI LAVORO PER LA PROTEZIONE DELLE PERSONE PER QUANTO CONCERNE IL 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 paragrafi 1 (a) e 3 della direttiva,

visto il suo regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

La direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati impone agli Stati membri di tutelare le libertà e i diritti fondamentali delle persone fisiche, in particolare il diritto alla vita privata, con riguardo al trattamento dei dati personali.

La direttiva fa parte delle misure adottate dalla Comunità intese a rimuovere gli ostacoli ai flussi di dati personali in diversi ambiti dell'economia, dell'amministrazione e dell'attività sociale del mercato interno, mirando ad armonizzare le norme relative al trattamento dei dati personali, garantendo nel contempo un elevato livello di protezione nella Comunità.

Ai sensi della definizione dell'articolo 2(a) della direttiva 95/46/CE, si intende per "dati personali" qualsiasi informazione concernente una persona fisica identificata o identificabile, ad esempio dati relativi alla sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

Il campo d'applicazione di questa definizione implica che la definizione di dato personale può comprendere non solamente i dati amministrativi o che risultano da fattori obiettivi che possono essere verificati o rettificati, ma anche qualsiasi altro elemento, informazione o circostanza che ha un contenuto informativo che può fornire elementi supplementari di informazione concernenti una persona identificata o identificabile.

Dati personali possono quindi essere trovati nel quadro di valutazioni e giudizi soggettivi, che possono includere elementi specifici che caratterizzano l'identità fisica, fisiologica, mentale, economica, culturale o sociale della persona interessata. Quanto detto vale anche se un giudizio o una valutazione sono formulati sotto forma di un punteggio, di una scala di valori o di altri parametri di valutazione.

Il fatto che, ai sensi di una legge nazionale, taluni di questi dati soggettivi non possono sempre essere accessibili e rettificabili, o che questi siano rettificabili con una dichiarazione o un'annotazione fatta dal soggetto, non evita che si tratti di dati personali, con riguardo alla trasparenza del loro trattamento e all'esercizio del diritto d'accesso.

Considerazioni simili valgono per quanto riguarda il fatto che l'accesso diretto ai dati inclusi in giudizi soggettivi o valutazioni può essere negato o limitato ai sensi della legge nazionale.

Fatto a Bruxelles, il 22 marzo 2001
Per il gruppo di lavoro
Il Presidente
Stefano RODOTA'

113 Raccomandazione relativa ai requisiti minimi per la raccolta di dati *on-line* nell'Unione europea

ARTICOLO 29 - GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI

5020/01
WP 43

RACCOMANDAZIONE 2/2001
relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea

Adottata il 17 maggio 2001

Il gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta dell'organo indipendente di consulenza dell'UE per la protezione dei dati e della vita privata. I suoi compiti sono stabiliti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 14 della direttiva 97/66/CE. Il servizio di segretariato è fornito da:

Commissione europea, DG Mercato interno, Funzionamento ed impatto del mercato interno. Coordinamento. Protezione dei dati.
Rue de la Loi 200, B - 1049 Bruxelles - Belgio - Ufficio: C100-6/136
Telefono: linea diretta (32-2)295.72.58 o 299.27.19. centralino: 299.11.11. Fax: (32-2)296.80.10.
Indirizzo internet: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995[1],

visti gli articoli 29 e 30, paragrafo 1, lettera a), e paragrafo 3 di detta direttiva,

visto il regolamento interno, in particolare gli articoli 12 e 14,

ha adottato la presente raccomandazione:

I. Introduzione

1. Nel documento di lavoro intitolato "Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line", del 21 novembre 2000[2], il Gruppo di lavoro ha evidenziato come sia importante garantire la messa in atto di strumenti adeguati per assicurare che l'utente Internet riceva tutte le informazioni necessarie affinché possa riporre la propria fiducia, con cognizione di causa, sui siti visitati e, se necessario, esercitare determinate scelte conformemente ai propri diritti come previsto dalla normativa europea.

Tale fattore risulta particolarmente importante in considerazione del fatto che l'uso di Internet moltiplica le possibilità di raccolta di dati personali e, conseguentemente, i pericoli per i diritti fondamentali e le libertà degli individui, soprattutto per quel che riguarda la loro vita privata. Nel suo Parere n. 4/2000 del 16 maggio 2000 sul livello di tutela dei dati offerto dai principi dell'"approdo sicuro" (Safe Harbor), il Gruppo di lavoro ha invitato la Commissione a valutare con urgenza l'opportunità di creare un marchio di qualità per i siti Internet, che si basi su criteri comuni che potrebbero essere stabiliti a livello comunitario.

Questa raccomandazione fa seguito ai due documenti sopracitati. Essa intende contribuire all'effettiva ed omogenea applicazione delle disposizioni nazionali adottate in conformità alle direttive[3] sulla tutela dei dati personali fornendo indicazioni concrete sull'attuazione delle norme contenute in tali direttive relativamente alle pratiche più comuni esercitate attraverso Internet. Tali pratiche si verificano soprattutto al momento del "contatto iniziale" tra l'utente Internet ed un sito Web sia nel caso di esclusiva ricerca di informazioni, sia nel caso di esecuzione di operazioni commerciali su base graduale.

Le indicazioni fornite di seguito riguardano in particolar modo la raccolta di dati personali su Internet e si prefiggono di identificare le misure che dovranno essere attuate nei confronti delle persone interessate per garantire la lealtà e la liceità di tali pratiche (applicazione degli articoli 6, 7, 10 e 11 della direttiva 95/46/CE). Tali indicazioni focalizzano in particolare sul come, quando e quali informazioni occorre fornire all'utente individuale, con l'aggiunta di dettagli pratici relativi a diritti ed obblighi risultanti da dette direttive.

Il principale obiettivo di questa raccomandazione consiste dunque nel fornire un concreto valore aggiunto all'attuazione dei principi generali della direttiva. Il Gruppo di lavoro considera la presente raccomandazione come la prima iniziativa per la presentazione a livello europeo dell'insieme "minimo" di obblighi ai quali i responsabili del trattamento (le persone fisiche o giuridiche responsabili del trattamento dati nell'ambito di un sito Web) [4] che si occupano di siti Internet in cui vengono richieste informazioni particolareggiate o la specificazione del campo d'azione [5] possano facilmente conformarsi. Certamente questa raccomandazione non eso-

(1) Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile su: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

(2) WP 37 (5063/00): documento di lavoro - Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line. Adottato il 21 novembre 2000. Disponibile su: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.htm

(3) Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e direttiva 97/66/CE del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni.Disponibili su: http://europa.eu.int/comm/inernal_market/en/media/dataprot/law.htm

(4) A titolo di riferimento, l'articolo 2 della direttiva 95/46/CE definisce il responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario".

(5) Le raccomandazioni concrete della presente raccomandazione costituiscono i requisiti minimi nel senso che non sono le uniche. In futuro tali raccomandazioni dovrebbero essere integrate da altre relative al trattamento di dati personali ancor più sensibili, come il trattamento riguardante siti sanitari e siti rivolti a bambini o i servizi offerti dai portali. In quanto ad altre specifiche modalità di trattamento, come la divulgazione di dati personali in un sito o la conservazione

nera i responsabili del trattamento dall'obbligo attualmente vigente di verificare la conformità di tali trattamenti all'intera serie di requisiti e condizioni precisati nel diritto nazionale applicabile per renderlo legittimo, verifica senza la quale tale trattamento non risulta idoneo.

Tale raccomandazione si applica nel caso in cui il responsabile del trattamento abbia sede in uno degli Stati membri dell'Unione europea. In questa circostanza sarà applicato il diritto nazionale dello Stato membro in oggetto al trattamento dei dati personali che avvenga nel contesto delle attività di tale stabilimento. Tale raccomandazione si applica altresì quando il responsabile del trattamento non ha sede nel territorio della Comunità ma ricorre, ai fini del trattamento di dati personali, a strumenti automatizzati o non automatizzati situati nel territorio di uno degli Stati membri dell'UE. Tale trattamento è contemplato dalla legislazione nazionale dello Stato membro in cui si trovano i supporti tecnici o le risorse [6].

2. La raccomandazione, per poter conseguire tale obiettivo, è rivolta particolarmente:

- ai responsabili del trattamento che raccolgono dati on-line, dotandoli di una guida pratica che elenchi l'insieme minimo delle misure concrete da attuare;

- ai singoli utenti Internet affinché siano informati a riguardo e affinché possano esercitare i propri diritti;

- alle istituzioni desiderose di assegnare un'etichetta certificante la conformità delle procedure di trattamento impiegate alle direttive europee sulla protezione dei dati, dotandole di criteri di riferimento per l'assegnazione di tale etichetta riguardo alle informazioni da apporre e alla raccolta di dati personali. È ovvio che, al momento dell'assegnazione dell'etichetta, occorrerà tener conto di separati criteri concernenti altri obblighi e diritti oltre ai suddetti criteri di riferimento. Il Gruppo di lavoro pubblicherà successivamente un esauriente documento relativo a detta problematica;

- alle autorità europee responsabili della protezione dei dati per poterle dotare di un quadro di riferimento comune per il loro compito di verifica della conformità alle disposizioni nazionali adottate dagli Stati membri, conformemente alle direttive sopracitate;

3. Il Gruppo di lavoro è inoltre del parere che tale raccomandazione dovrebbe servire da riferimento per la definizione dei criteri per software e hardware preposti alla raccolta e al trattamento di dati personali su Internet.

II. Raccomandazioni sulle informazioni da fornire in caso di raccolta di dati nel territorio degli Stati membri dell'Unione europea

2.1. Informazioni da fornire alla persona interessata e tempi da rispettare.

4. Qualsiasi raccolta di dati personali individuali ottenuta attraverso un sito Web richiede l'anticipata fornitura di determinate informazioni. In termini di contenuto la conformità a tale obbligo rende necessario:

---

dei dati sul traffico da parte dei fornitori di servizi Internet e dei fornitori di contenuti e servizi Internet, si rimanda alle raccomandazioni del Gruppo di lavoro contenute nel documento citato nella nota n. 1 e alle altre posizioni del caso assunte dal Gruppo di lavoro, come il WP 25 (5085/99): Raccomandazione 3/99 relativa alla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari. Approvata il 7 settembre 1999. WP 18 (5005/99): Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni. Approvata il 3 maggio 1999. WP 17 (5093/98): Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software ed hardware. Approvata il 23 febbraio 1999. Tutto disponibile su: cfr. nota n. 1.

(6) Cfr. articolo 4, paragrafo 1, punti a) e c) della direttiva 95/46/CE. È necessario mantenere nettamente distinto tale aspetto dalla questione del trasferimento legale di dati personali dall'UE ad un paese terzo. Tale problematica è trattata dagli articoli 25 e 26 della direttiva 95/46/CE e dalle connesse decisioni della Commissione europea relative all'adeguatezza della tutela nei paesi terzi. Ad esempio, se un sito Web americano fa uso di strumenti situati all'interno dell'UE per la raccolta ed il trattamento di dati personali sarà applicata alle operazioni di raccolta e di trattamento la legislazione dello stato europeo in questione, a prescindere dall'adeguatezza del livello di protezione fornito da tale compagnia e conformemente alla decisione della Commissione europea relativa all'approdo sicuro. Tale problematica relativa all'adesione o meno del destinatario di dati all'approdo sicuro sarà pertinente esclusivamente in merito alla liceità delle successive cessioni di dati personali dalla compagnia con sede all'interno dell'UE a quell'altra.

5. menzionare l'identità, l'indirizzo fisico e quello elettronico del responsabile del trattamento e, ove possibile, quello dell'eventuale rappresentante in forza all'articolo 4.2 della direttiva;

6. menzionare chiaramente la/le finalità del trattamento con il quale il responsabile raccoglie dati attraverso un sito Web. Ad esempio, nel caso in cui tali dati vengano raccolti per stipulare un contratto (abbonamento ad Internet, ordine di prodotti, ecc.) ed anche per la commercializzazione diretta, occorre che il responsabile specifichi chiaramente le due finalità in questione;

7. menzionare chiaramente il carattere obbligatorio o facoltativo delle informazioni richieste.
Le informazioni obbligatorie sono quelle indispensabili all'espletamento del servizio richiesto. Ad esempio, è possibile evidenziare il carattere obbligatorio o facoltativo apponendo un asterisco all'informazione di carattere obbligatorio oppure, in alternativa, è possibile scrivere "facoltativo" accanto all'informazione non obbligatoria. Il fatto che la persona interessata non fornisca informazioni facoltative non deve tornarle a svantaggio in nessun modo;

8. menzionare l'esistenza di diritti, e delle condizioni per il loro esercizio, in base ai quali l'interessato possa esprimere il proprio consenso o, eventualmente, opporsi al trattamento di dati personali(7). È necessario parimenti fornire indicazioni sulle modalità di accesso, di rettifica o di cancellazione di tali dati o informazioni, sia riguardo la persona o il servizio al quale occorre rivolgersi per l'esercizio di tali diritti, che relativamente alla possibilità di esercitarli on-line e all'indirizzo fisico del responsabile;

9. elencare i destinatari o le categorie di destinatari delle informazioni raccolte. Al momento della raccolta di dati i siti Internet dovrebbero specificare se i dati raccolti saranno comunicati o resi disponibili a terzi – tra cui, in particolare, partner commerciali, imprese figlie, ecc. – e le relative motivazioni (con finalità diverse dalla fornitura del servizio richiesto e per la commercializzazione diretta(8)).

In questi casi è fondamentale che gli utenti Internet dispongano di un'effettiva possibilità di opporsi on-line a detta comunicazione cliccando su di una casella di spunta ed esprimendo così il proprio favore alla comunicazione dei dati con finalità diverse dalla fornitura del servizio richiesto. Dal momento che il diritto di opporsi può essere esercitato in qualunque momento, occorre menzionare anche nelle informazioni fornite alla persona interessata la possibilità di esercitare tale diritto on-line. Il Gruppo di lavoro, consapevole degli svantaggi recati dal sovraccarico di informazioni negli schermi, è del parere che, se non appaiono nomi di destinatari, il responsabile del trattamento si impegna a non comunicare le informazioni raccolte a terzi i cui nomi ed indirizzi non siano stati forniti (a meno che la loro identità sia ovvia), garantisce che la comunicazione dei dati sia necessaria all'espletamento del servizio richiesto dall'utente Internet e che tale comunicazione sia effettuata esclusivamente con quella finalità.

10. Nel caso in cui sia previsto che il responsabile del trattamento trasmetta i dati a paesi esterni all'Unione europea, specificare se tali paesi garantiscono una protezione adeguata degli individui riguardo al trattamento dei loro dati personali, in forza dell'articolo 25 della direttiva 95/46/CE. In questo caso è necessario fornire informazioni specifiche a proposito dell'identità e dell'indirizzo dei destinatari (indirizzo fisico e/o elettronico)(9);

---

(7) Il trattamento a finalità specifiche è consentito solo se motivato da una delle considerazioni elencate nell'articolo 7 della direttiva 95/46/CE (tra l'altro nei casi in cui la persona interessata abbia fornito esplicitamente il proprio consenso, in cui il trattamento risulti indispensabile per l'esecuzione del contratto con la persona interessata, in cui il trattamento risulti indispensabile per adempiere ad un obbligo legale del responsabile del trattamento e in cui tale trattamento risulti indispensabile per il perseguimento dell'interesse legittimo del responsabile oppure di quello di terzi che hanno fatto uso di tali dati, a meno che l'interesse della persona in oggetto non risulti prevalente).
Il diritto ad opporsi (cfr. articolo 14) è fissato dagli Stati membri in almeno due situazioni di cui all'articolo 7, inclusa l'ultima menzionata sopracitata. L'individuo ha il diritto, salvo disposizione contraria prevista dalla normativa nazionale, di opporsi in qualsiasi momento per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che lo riguardano. Il diritto di opporsi su richiesta e gratuitamente sussiste in ogni caso quando il trattamento in oggetto è finalizzato alla commercializzazione diretta. La persona interessata può inoltre opporsi gratuitamente (una volta informata ed a partire dalla prima comunicazione) alla comunicazione di dati personali a terzi o al loro utilizzo per conto di terzi per la commercializzazione diretta.
(8) La comunicazione a terzi è consentita solo nel caso in cui la finalità prevista non sia incompatibile con quella per la quale i dati sono stati raccolti e se motivata da una delle considerazioni elencate nell'articolo 7, condizioni che rendono legittimo il trattamento.
(9) Informazioni riguardo l'adeguatezza delle decisioni sono disponibili sul sito Web della Commissione al seguente indirizzo:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

11. fornire nome ed indirizzo (indirizzo fisico e/o elettronico) del servizio o della persona incaricata di rispondere ad eventuali quesiti riguardanti la protezione di dati personali;

12. menzionare chiaramente l'esistenza di procedure di raccolta automatica di dati prima di utilizzare simili metodi per detta raccolta[10].

Nel caso di un ricorso a tali procedure è necessario che la persona interessata riceva le informazioni contenute in questo documento. Detta persona dovrà inoltre essere informata circa il nome del dominio dal quale il *server* del sito trasmette le procedure di raccolta automatica, le finalità di dette procedure, il loro periodo di validità, l'eventualità in cui l'accettazione di tali procedure sia necessaria per visitare il sito e le possibili conseguenze di una loro disattivazione. Se vi sono altri responsabili del trattamento coinvolti nella raccolta dei dati personali occorre che la persona interessata riceva tutte le informazioni riguardanti l'identità del responsabile e le finalità del trattamento relativamente a ciascun responsabile di detto trattamento.

È necessario comunicare la possibilità di opporsi alla raccolta prima di ricorrere a qualsiasi procedura automatica che provochi la connessione di un utente PC ad un altro sito Web.

Es. allo scopo di evitare che un secondo sito possa raccogliere dati ad insaputa di un utente Internet nel caso in cui questo venga automaticamente connesso da un sito Web ad un altro per visualizzare pubblicità sotto forma di *banner*.

Ad esempio, se un *cookie* viene collocato dal *server* del responsabile del trattamento è necessario comunicare detta informazione prima che venga spedito all'*hard disk* dell'utente Internet, in aggiunta alle informazioni fornite grazie alla tecnologia esistente che si limita a specificare il nome del sito di trasmissione ed il periodo di validità di detto cookie[11].

13. Indicare le misure di sicurezza a garanzia dell'autenticità del sito, del grado di completezza e riservatezza delle informazioni trasmesse nella detta rete in applicazione della legislazione nazionale applicabile.[12]

14. Fornire le informazioni in tutte le lingue usate nel sito Web e, specialmente, in quei passaggi ove avviene la raccolta dei dati personali.

15. Che i responsabili del trattamento verifichino la coerenza delle informazioni contenute nei vari documenti destinati al sito (le sezioni "dati personali e protezione della vita privata", i moduli elettronici, testi relativi alle condizioni generali di vendita e ad altre comunicazioni commerciali).

2.2. Modalità di presentazione delle informazioni

16. Il Gruppo di lavoro ritiene che le seguenti informazioni debbano apparire direttamente sullo schermo prima che avvenga la raccolta, così da assicurare un giusto trattamento dei dati.

Dette informazioni riguardano:

- l'identità del responsabile del trattamento;
- la/le finalità;
- la natura obbligatoria o facoltativa delle informazioni richieste;
- i destinatari o le categorie di destinatari dei dati raccolti;
- l'esistenza del diritto di accesso e di rettifica;

(10) Il trattamento "invisibile" ed automatico dei dati personali è soggetto alle medesime modalità, condizioni e garanzie delle altre tipologie di trattamento di dati personali. Cfr. Raccomandazione 1/99 del Gruppo di lavoro sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware (23 febbraio 1999), disponibile sul sito Web citato nella nota n. 1.

(11) Se il *cookie* è collocato da un'organizzazione attraverso il proprio sito Web e soltanto questa è in grado di accedere al contenuto di detto cookie non occorre fornire informazioni aggiuntive riguardo l'organizzazione responsabile del collocamento del cookie, purché l'organizzazione che ospita tale sito Web sia già stata adeguatamente identificata.

(12) Cfr. le norme specifiche dell'articolo 17, paragrafi 1 e 3 secondo trattino della direttiva 95/46/CE.

- l'esistenza del diritto di opporsi a qualsiasi comunicazione dei dati a terzi con finalità diverse dalla fornitura del servizio richiesto e le modalità per esercitare tale diritto (ad esempio fornendo la possibilità di cliccare su una casella di spunta);

- le informazioni da fornire in caso di utilizzo di procedure di raccolta automatica;

- il livello di sicurezza nel corso di tutte le fasi del trattamento compresa la trasmissione, ad esempio sulle reti.

In tali situazioni le informazioni devono essere fornite interattivamente e devono apparire sullo schermo. Così, nel caso di metodi automatici di raccolta dati, dette informazioni possono essere fornite, se necessarie, tramite la tecnica delle finestre *pop-up*.

A proposito del livello di sicurezza nel corso della trasmissione dei dati dall'apparecchiatura occorre visualizzare un'intestazione del tipo "Stai accedendo ad una connessione protetta" oppure le procedure di informazione automatica presenti nei *browser*, come la comparsa di icone specifiche sotto forma di chiave o di lucchetto.

17. Il Gruppo di lavoro ritiene inoltre che sia necessario poter accedere ad informazioni esaustive riguardo alla politica di tutela della sfera privata (comprese le modalità per l'esercizio del diritto d'accesso) direttamente dalla pagina d'entrata del sito e ovunque vengano raccolti dati personali on-line. Il titolo dell'intestazione su cui cliccare deve essere sufficientemente messo in risalto, chiaro e preciso in modo da consentire all'utente Internet di crearsi un'idea chiara del contenuto al quale sta per accedere. Ad esempio, l'intestazione potrebbe asserire "Stiamo raccogliendo e trattando dati personali che La riguardano. Per ulteriori informazioni clicchi qui" oppure "Dati personali o tutela della sfera privata". Il contenuto delle informazioni alle quali l'utente Internet è indirizzato deve altresì essere sufficientemente preciso.

III. Raccomandazioni per il perfezionamento degli altri diritti e doveri

Il Gruppo di lavoro desidera inoltre attirare l'attenzione dei destinatari della presente Raccomandazione su altri diritti dell'individuo ed obblighi dei responsabili del trattamento basati su direttive di particolare attinenza nell'ambito della raccolta di dati personali su siti Web. Il Gruppo di lavoro ritiene che le raccomandazioni seguenti, così come le indicazioni sulle informazioni, abbiano un'utilità pratica immediata sia per i responsabili del trattamento che per gli utenti Internet.

18. Raccogliere esclusivamente i dati necessari per il conseguimento dello scopo prefisso;

19. garantire che i dati siano trattati esclusivamente nelle suddette legittime modalità, conformemente ad uno dei criteri elencati nell'articolo 7 della direttiva 95/46/CE;

20. garantire l'effettivo esercizio del diritto di accesso e di rettifica; l'esercizio di tali diritti dovrebbe essere possibile sia all'indirizzo fisico del responsabile del trattamento che *on-line*.
È necessario predisporre particolari misure di sicurezza affinché esclusivamente la persona interessata abbia accesso on-line alle informazioni che la riguardano;

21. conformarsi al principio della "finalità" o "scopo" in base al quale occorre far uso di dati personali solo se necessario e per finalità determinate. In altri termini, in assenza di un motivo legittimo, non è possibile fare uso di dati personali ed è necessario mantenere l'anonimato degli individui (articolo 6, paragrafo 1, punto b) della direttiva 95/46/CE).
Detto principio è altresì denominato "principio di minimizzazione".

22. Fornire ed incoraggiare la consultazione in modalità anonima di siti commerciali, nello stesso ambito descritto nel punto 21, senza richieste di identificazione degli utenti per cognome, nome, indirizzo di posta elettronica o altri dati identificativi.

Qualora sia necessario un collegamento ad una persona senza completa identificazione della stessa è bene suggerire ed accogliere l'uso di pseudonimi di qualsivoglia natura.

Ove non sussistano necessità di identificazione legale occorre incoraggiare ed accogliere l'uso di pseudonimi, anche nel caso di determinate operazioni. Un esempio è dato dall'uso di certificati pseudonimi per le firme elettroniche (cfr. articolo 8 della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche).

23. Stabilire un periodo di conservazione per i dati raccolti. È possibile conservare detti dati esclusivamente per il tempo necessario allo scopo del trattamento indicato e perseguito (articolo 6 della direttiva 95/46/CE e articolo 6 della direttiva 97/66/CE).

24. Adottare gli accorgimenti necessari per garantire la sicurezza dei dati nel corso del loro trattamento e della loro trasmissione (ad esempio limitare e determinare il numero delle persone che hanno accesso ai dati, far uso di trasmissioni cifrate, ecc.; articolo 17 della direttiva 95/46/CE).

25. Se è coinvolto un responsabile per l'elaborazione, ad esempio per ospitare un sito Web, stipulare un contratto che gli imponga di attuare appropriate misure di sicurezza in conformità anche della normativa dello Stato membro in cui si trova il responsabile per l'elaborazione, nonché effettuare il trattamento dei dati personali attenendosi esclusivamente alle indicazioni del responsabile di detto trattamento.

26. A seconda dei casi e in forza della legge nazionale, procedere alla notificazione dell'autorità di controllo (se il responsabile dell'elaborazione del sito si trova nell'Unione europea o se lo stesso dispone di un rappresentante nell'Unione europea). Il numero di registrazione di detta notifica può essere indicato all'interno del sito, in modo vantaggioso, al di sotto dell'intestazione destinata alla protezione dei dati.

27. Se vengono trasferite informazioni ad un paese terzo in cui non è garantito un adeguato livello di protezione è necessario assicurare che il trasferimento dei dati avvenga esclusivamente se lo stesso è in linea con le deroghe all'articolo 26 della direttiva 95/46/CE. In questi casi occorre informare le persone delle adeguate garanzie fornite affinché il trasferimento risulti lecito.

IV. Raccolta di indirizzi per la commercializzazione diretta tramite posta elettronica e per la spedizione di *newsletter*

28. Per ciò che concerne la commercializzazione diretta per posta elettronica:

- il Gruppo di lavoro ripropone il proprio parere secondo il quale gli indirizzi di posta elettronica reperiti nelle aree pubbliche di Internet all'insaputa delle persone interessate, ad esempio nei gruppi di discussione, non sono stati raccolti lecitamente. Tali indirizzi non possono perciò essere utilizzati con finalità diverse da quelle per le quali sono stati originariamente resi pubblici; in particolar modo non possono essere utilizzati per la commercializzazione diretta; [13]

- fare uso di indirizzi di posta elettronica per la commercializzazione diretta a condizione che questi siano stati raccolti lealmente e legalmente. Affinché la raccolta sia leale e legale è necessario che le persone interessate siano state informate della possibilità dell'uso di tali dati per la commercializzazione diretta e che dette persone abbiano potuto acconsentire a tale uso direttamente al momento della raccolta (cliccando su una casella di spunta)[14]. L'invio di posta elettronica a scopo promozionale deve altresì prevedere la possibilità di

(13) Cfr. WP 28 (5007/00): "Parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali", approvato il 3.2.2000, WP 29 (5009/00): "Parere 2/2000 concernente la revisione generale del quadro giuridico delle telecomunicazioni", approvato il 3.2.2000, e, specialmente, riguardo l'applicazione degli articoli 6 e 7 della direttiva 95/46/CE, WP 36 (5042/00): "Parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 (COM(2000)385)", approvato il 2.11.2000 e WP 37 (5063/00): "Documento di lavoro: Tutela della vita privata su Internet, un approccio integrato dell'UE

(14) All'interno dell'Unione europea cinque Stati membri (Germania, Austria, Italia, Finlandia e Danimarca) hanno adottato misure intese a vietare le comunicazioni commerciali non sollecitate. In altri Stati membri esiste un sistema di possibilità di recesso oppure permane una situazione poco chiara. È bene notare che la proposta di direttiva della Commissione relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM(2000) 385) del 12 luglio 2000 è in favore di una soluzione armonizzata basata sulla possibilità di adesione; tale approccio è stato unanimemente

esercitare il recesso on-line dall'elenco di indirizzi impiegato [15].

29. Per ciò che concerne la spedizione di *newsletter*:
- Procurarsi il previo consenso delle persone interessate e garantire la possibilità di un loro recesso da tali spedizioni in qualsiasi momento; occorrerà pertanto informare dette persone riguardo a questa possibilità ogniqualvolta viene spedita una *newsletter*.

Il gruppo di lavoro invita il Consiglio, la Commissione europea, il Parlamento europeo e gli Stati membri a tener conto della presente raccomandazione.

Il gruppo si riserva la facoltà di formulare ulteriori osservazioni.

Fatto a Bruxelles, 21 maggio 2001
Per il gruppo
Il Presidente
Stefano RODOTÀ

sostenuto dal Gruppo di lavoro nel Parere 7/2000 (WP 36 sopracitato). Si veda inoltre lo studio di S. Gauthronet e di E. Drouard (ARETE) per la Commissione, "Messaggi pubblicitari indesiderati e protezione dei dati personali", gennaio 2001, http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamsumit.pdf

(15) La direttiva sul commercio elettronico stabilisce ulteriori requisiti relativi alle comunicazioni commerciali non sollecitate in quei casi in cui è consentita la possibilità di recesso conformemente alla direttiva 97/66/EC.

114 Parere 8/2001 del Gruppo di lavoro "Articolo 29"(1) sul trattamento dei dati nel contesto lavorativo Adottato il 13 settembre 2001 (5062/01 WP 48)

SOMMARIO

Il trattamento dei dati personali nel contesto lavorativo è oggetto di discussione a livello sia comunitario che nazionale. I governi e i garanti della protezione dei dati degli Stati membri hanno elaborato o stanno elaborando normative, codici o raccomandazioni per regolare vari aspetti della protezione dei dati nel contesto lavorativo. Nel quadro dell'Agenda per la politica sociale la Commissione europea ha varato una consultazione delle parti sociali sulla protezione dei dati nel contesto lavorativo.

Per contribuire all'applicazione omogenea delle norme nazionali di recepimento della direttiva 95/46/CE relativa alla tutela dei dati[2] , il gruppo di lavoro ha istituito un sottogruppo per esaminare la questione [3] e ha adottato un **documento approfondito** reperibile su Internet al seguente indirizzo[4]:
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

Datori di lavori e lavoratori devono sapere che **molte delle attività svolte di solito nel contesto lavorativo comportano il trattamento di dati personali dei lavoratori**, talvolta di natura assai delicata[5]. È quasi sicuro che ogni rilevazione, uso o memorizzazione di informazioni sui lavoratori con mezzi elettronici rientri nel campo d'applicazione della legislazione di protezione dei dati, come avviene anche per il controllo dell'accesso dei lavoratori alla posta elettronica o a Internet da parte del datore di lavoro. **Il controllo della posta elettronica comporta necessariamente il trattamento di dati personali.** Il trattamento di dati sotto forma di suono e di immagine nel contesto lavorativo rientra nel campo d'applicazione della legislazione di protezione dei dati ed anche la sorveglianza video dei lavoratori è disciplinata dalle disposizioni della direttiva e dalle leggi nazionali che la recepiscono.

Se trattano dati personali dei lavoratori, i datori di lavoro dovrebbero sempre tenere presenti **I SEGUENTI PRINCIPI FONDAMENTALI DELLA PROTEZIONE DEI DATI:**

• **FINALITÀ**: i dati devono essere rilevati per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità.

• **TRASPARENZA**: i lavoratori devono come minimo sapere quali dati il datore di lavoro sta raccogliendo su di loro (direttamente o per altre vie), e quali sono gli scopi dei trattamenti di questi dati eseguiti o previsti al momento o in futuro. La trasparenza viene anche garantita accordando alla persona interessata il diritto d'accesso ai propri dati personali e obbligando i responsabili del trattamento dei dati a darne notifica alle autorità di sorveglianza come previsto nella legislazione nazionale.

• **LEGITTIMITÀ**: il trattamento dei dati personali dei lavoratori deve essere legittimo. L'articolo 7 della direttiva elenca i criteri di legittimazione del trattamento.

• **PROPORZIONALITÀ**: i dati personali devono essere adeguati, pertinenti e non eccedenti rispetto

(1) Il gruppo di cui all'articolo 29 è composto da rappresentanti dei garanti della protezione dei dati degli Stati membri. Il gruppo ha carattere consultivo e indipendente che, tra l'altro, ha il compito di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della direttiva relativa alla tutela dei dati per contribuire alla loro applicazione omogenea.
(2) 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 23.11.95, pag. 31.
(3) All'attività del sottogruppo hanno contribuito le seguenti autorità di controllo: AT, BE, DE, EL, ES, FR, IRL, IT, NL, UK.
(4) Il documento include un elenco delle più significative leggi di protezione dei dati degli Stati membri con qualche incidenza nel contesto lavorativo.
(5) Costituiscono esempi di registrazioni che comportano il trattamento di dati personali tutelati dalla direttiva 95/46/CE: le domande di lavoro e le referenze professionali, le informazioni sulle retribuzioni e le imposte, le informazioni fiscali e sulle prestazioni sociali, le registrazioni relative alle ferie annuali, alle assenze straordinarie/non retribuite, alle note informative/di valutazione annuali, alle promozioni, ai trasferimenti, la formazione, ai problemi di disciplina, agli infortuni sul lavoro, etc.

alle finalità per le quali vengono rilevati e/o successivamente trattati. Ammesso che i lavoratori siano stati informati del trattamento, e che il trattamento sia legittima e proporzionato, è comunque necessario che sia leale nei confronti del lavoratore.

• **ESATTEZZA E CONSERVAZIONE DEI DATI**: i dati sull'occupazione devono essere esatti e se occorre aggiornati. Il datore di lavoro deve adottare tutte le misure opportune affinché i dati inesatti o incompleti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati vengano cancellati o rettificati.

• **SICUREZZA**: sul luogo di lavoro il datore di lavoro deve adottare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dei propri lavoratori. Una particolare protezione deve essere accordata rispetto alla diffusione o all'accesso non autorizzati.

• **CONSAPEVOLEZZA DEL PERSONALE**: il personale con competenze o responsabilità nel trattamento di dati personali di altri lavoratori deve essere informato in materia di tutela dei dati e ricevere una formazione adeguata. Senza un'idonea formazione degli addetti al trattamento dei dati personali il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito.

CONSENSO. Il gruppo di lavoro "articolo 29" ritiene che, se un datore di lavoro deve trattare dati personali come conseguenza necessaria e inevitabile del rapporto di lavoro, sbaglia se cerca di legittimare il trattamento mediante il consenso. Il ricorso al consenso va limitato ai casi in cui il lavoratore è effettivamente libero di scegliere e può successivamente ritirare il proprio consenso senza pregiudizio.

I LAVORATORI SONO PERSONE INTERESSATE titolari dei diritti conferiti dalla direttiva relativa alla tutela dei dati, il più importante dei quali è il diritto di accesso di cui all'articolo 12 della direttiva stessa.[6]

INTERAZIONE TRA DIRITTO DEL LAVORO E DIRITTO DELLA PROTEZIONE DEI DATI. Il gruppo di lavoro intende sottolineare che il diritto della protezione dei dati e le prassi e il diritto del lavoro non operano separatamente e senza reciproche interferenze.

L'interazione è necessaria e apprezzabile e deve contribuire allo sviluppo di soluzioni che proteggano adeguatamente gli interessi dei lavoratori.

SORVEGLIANZA E CONTROLLO. Il controllo e la sorveglianza dei lavoratori rispetto all'uso della posta elettronica, all'accesso a Internet, alle riprese televisive o ai dati sulla localizzazione sono soggetti alle norme che tutelano i dati. **Ogni controllo deve essere una risposta proporzionata** del datore di lavoro ai rischi che corre nel tener conto della riservatezza e di altri interessi legittimi dei lavoratori. **Tutti i dati personali** detenuti o utilizzati durante i controlli devono essere **adeguati, pertinenti e non eccedenti rispetto alle finalità che giustificano il controllo**. I controlli devono essere eseguiti nel modo meno intrusivo possibile.

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI. L'articolo 25 della direttiva stabilisce che il trasferimento di dati personali verso un paese esterno all'UE può aver luogo soltanto se il paese terzo garantisce un livello di protezione dei dati adeguato. Va tenuto presente che, indipendentemente dalla base giuridica del trasferimento ai sensi degli articoli 25 e 26, il trattamento connesso al trasferimento deve comunque conformarsi agli articoli da 6 a 8 e a tutte le altre disposizioni della direttiva.

---

(6) Ogni persona interessata ha il diritto di ottenere dal responsabile del trattamento (in questo caso il datore di lavoro):

a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessive:

• La conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatati cui sono comunicati i dati,

• La comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati,

• La conoscenza della logica applicata nei trattamenti automatizzati dei dati che la interessano, per lo meno nel caso delle decisioni automatizzate

b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati;

c) la notificazione ai terzi, ai quali sono stati comunicati i dati di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato.

114

Il gruppo di lavoro **ritiene preferibile contare su un'adeguata protezione del paese destinatario piuttosto che sulle deroghe di cui all'articolo 26, come ad esempio il consenso dei lavoratori.** Quando ci si affida al consenso, questo deve essere inequivocabile e dato liberamente. Sbagliano i datori di lavoro che si affidano **esclusivamente** al consenso, eccettuato il caso in cui un suo eventuale ritiro successivo non causi problemi.

ULTERIORI ORIENTAMENTI. Il gruppo di lavoro sta esaminando ulteriori orientamenti per i casi in cui l'applicazione dei principi generali della tutela dei dati solleva specifici problemi inerenti al contesto lavorativo, quali la sorveglianza e il controllo sul luogo di lavoro, i dati di valutazione dei lavoratori ed altri.

RICHIAMI IPERTESTUALI

Per esigenze di spazio i documenti riportati in questa sezione sono indicati solo con il relativo frontespizio, accompagnato dall'indicazione del sito web dove sono interamente riportati

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (art. 29 direttiva 95/46/CE)

115 Parere 1/2001 sul progetto di decisione della Commissione ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso Paesi terzi in conformità all'articolo 26(4) della direttiva (*)

GRUPPO PER LA TUTELA DEI DATI PERSONALI - ARTICOLO 29

5006/02/IT
WP 38 def

Parere 1/2001 sul

progetto di decisione della Commissione ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi in conformità all'articolo 26(4) della direttiva

(progetto presentato al gruppo il 17 gennaio 2001)

Adottato il 26 gennaio 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp38it.pdf

116 Parere 2/2001 sul livello di adeguatezza del Personal Information and Electronic Documents Act (legge sui dati personali e i documenti elettronici) canadese (*)

ARTICOLO 29 - GRUPPO DI LAVORO PER LA PROTEZIONEDEI DATI

5109/00/IT
WP 39

Parere 2/2001 sul

Livello di adeguatezza del
Personal Information and Electronic Documents Act
(Legge sui dati personali e i documenti elettronici) canadese

Adottato il 26 gennaio 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp39it.pdf

117 Parere 3/2001 sul livello di protezione della legge 2000 di modifica della legge australiana sulla tutela della vita privata (settore privato)

ARTICOLO 29 – GRUPPO PER LA TUTELA DELLE PERSONE
CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

5095/00/IT/Rev. 1
WP 40

Articolo 29 – Gruppo per la tutela delle persone con
riguardo al trattamento dei dati personali

Parere 3/2001
sul livello di protezione della legge 2000 di modifica della legge australiana sulla
tutela della vita privata (settore privato)

Adottato il 26 gennaio 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40it.pdf

118 Parere 4/2001 sul progetto di Convenzione sulla cybercriminalità del Consiglio d'Europa (*)

ARTICOLO 29 – GRUPPO PER LA TUTELA DELLE PERSONE
CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

5001/01/IT/def.
WP 41

Parere 4/2001
sul progetto di convenzione sulla cibercriminalità del Consiglio d'Europa

Adottato il 22 marzo 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41it.pdf

119 Parere 5/2001 sulla relazione speciale del Mediatore europeo al Parlamento europeo a seguito del progetto di raccomandazione alla Commissione europea nella denuncia 713/98/IJH.

GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI
ARTICOLO 29

5003/00/IT/def.
WP 44

Parere 5/2001

sulla relazione speciale del Mediatore europeo al Parlamento europeo a seguito del progetto di raccomandazione alla Commissione europea nella denuncia 713/98/IJH.

Adottato il 17 maggio 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp44it.pdf

120 Quarta relazione annuale sulla situazione relativa alla tutela delle persone con riguardo al trattamento dei dati personali e alla vita privata nella Comunità e nei Paesi terzi concernente l'anno 1999 (*)

GRUPPO PER LA TUTELA DEI DATI PERSONALI
(ARTICOLO 29)

5019/02/IT
WP 46

QUARTA RELAZIONE ANNUALE

SULLA SITUAZIONE RELATIVA ALLA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI E ALLA VITA PRIVATA NELLA COMUNITÀ E NEI PAESI TERZI

ANNO 1999

Adottata il 17.5.2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp46it.pdf

121

Parere 7/2001 sul progetto di decisione della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili di attività di elaborazione con sede in Paesi terzi ai sensi dell'articolo 26(4) della direttiva 95/46/CE (*)

ARTICOLO 29 - GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI

5061/01/IT/def.
WP 47

Parere 7/2001

sul progetto di decisione della Commissione

(versione del 31 agosto 2001)

relativa alle clausole contrattuali tipo per il trasferimento di dati personali a responsabili di attività di elaborazione con sede in paesi terzi ai sensi dell'articolo 26(4) della direttiva 95/46

Approvato il 13 settembre 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp47it.pdf

122 Prassi raccomandata IATA n. 1774 - Protezione della riservatezza e dei flussi transfrontalieri di dati personali utilizzati per il trasporto aereo internazionale di passeggeri e merci (*)

GRUPPO DELL'ARTICOLO 29 PER LA TUTELA DEI DATI

5032/01/IT/def.
WP 49

Documento di lavoro relativo alla

Prassi raccomandata IATA n° 1774
Protezione della riservatezza e dei flussi transfrontalieri di dati personali utilizzati per il trasporto aereo internazionale di passeggeri e merci

Adottato il 14 settembre 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp49it.pdf

123 Parere 9/2001 sulla comunicazione della Commissione intitolata «Creare una società dell'informazione più sicura rafforzando la sicurezza delle infrastrutture dell'informazione e lottando contro la criminalità informatica» (*)

GRUPPO "ARTICOLO 29" SULLA TUTELA DEI DATI PERSONALI

5074/01/IT/def.
WP 51

Parere 9/2001

sulla comunicazione della Commissione intitolata
«Creare una società dell'informazione più sicura rafforzando la sicurezza delle infrastrutture dell'informazione e lottando contro la criminalità informatica»

adottato il 5 novembre 2001

(*)http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp51it.pdf

124 Parere 10/2001 sulla necessità di un approccio equilibrato alla lotta contro il terrorismo(*)

ARTICOLO 29 - GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI

0901/02/IT/def.
WP 53

Parere 10/2001

sulla necessità di un approccio equilibrato alla lotta contro il terrorismo

Approvato il 14 dicembre 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp53it.pdf

125 Quinta relazione annuale sulla situazione relativa alla tutela delle persone con riguardo al trattamento dei dati personali e alla vita privata nell'Unione europea e nei Paesi terzi concernente l'anno 2000 (*)

ARTICLE 29 - DATA PROTECTION WORKING PARTY

WP 54

FIFTH ANNUAL REPORT
ON THE SITUATION REGARDING THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND PRIVACY IN THE EUROPEAN UNION AND IN THIRD COUNTRIES
COVERING THE YEAR 2000

PART I

Adopted on 6th March 2002

(*) Parte I: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp54en_1.pdf
Parte 2: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp54en_2.pdf

ARTICLE 29 - DATA PROTECTION WORKING PARTY

WP 54

FIFTH ANNUAL REPORT ON THE SITUATION REGARDING THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND PRIVACY IN THE EUROPEAN UNION AND IN THIRD COUNTRIES COVERING THE YEAR 2000

PART II

Adopted on 6 th March 2002

126 Posizione comune adottata dal Consiglio il 28 gennaio 2002 in vista dell'adozione della direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (*)

CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 29 gennaio 2002 (31.01)
(OR. fr)

15396/2/01 REV 2 ADD 1

Fascicolo interistituzionale:
2000/0189 (COD)

ECO 395
CODEC 1375

Oggetto: Posizione comune adottata dal Consiglio del 28 gennaio 2002 in vista dell'adozione della direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

(*) http://register.consilium.eu.int/pdf/it/01/st15/15396-yyi1.pdf

127 Comunicazione della Commissione europea al Parlamento europeo sulla Posizione comune del Consiglio in merito all'adozione della direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, del 30 gennaio 2002 (*)

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.01.2002
SEC(2002) 124 final

2000/0189 (COD)

COMMUNICATION FROM THE COMMISSION
TO THE EUROPEAN PARLIAMENT

pursuant to the second subparagraph of Article 251 (2) of the EC Treaty

concerning the

common position of the Council on the adoption of a Directive of the European Parliament and of the Council on processing of personal data and the protection of privacy in the electronic communications sector

(*) http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/data%20prot%20cion%20posi%20on%20council%20com%20po-en.pdf

Commissione europea

128 Decisione della Commissione europea, del 26 luglio 2000, sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal dipartimento del commercio degli Stati Uniti (con rettifica) (*)

[notificata con il numero C(2000) 2441]

(Testo rilevante ai fini del SEE)

(2000/520/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1), in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

A norma della direttiva 95/46/CE, gli Stati membri sono tenuti a consentire il trasferimento verso un paese terzo di dati personali soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se vengono rispettate, prima del trasferimento stesso, norme di attuazione delle altre disposizioni della direttiva adottate dagli Stati membri.

La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

A norma della direttiva 95/46/CE, il livello di protezione dei dati personali deve essere valutato con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni; il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali (2) ha fornito indicazioni circa le modalità di effettuazione di tali valutazioni (3).

Tenuto conto della diversità degli approcci in materia di tutela dei dati nei paesi terzi, la valutazione dell'adeguatezza e le decisioni a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE devono essere eseguite in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti dei paesi terzi o fra questi, qualora sussistano condizioni analoghe, e da non costituire ostacoli dissimulati agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

(*) http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=it&numdoc=32000D0520&model=guichett

129 Decisione della Commissione europea, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati in Ungheria (*)

[notificata con il numero C(2000) 2305]

(Testo rilevante ai fini del SEE)

(2000/519/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1), in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

La direttiva 95/46/CE prescrive agli Stati membri di assicurarsi che i trasferimenti di dati personali verso un determinato paese terzo abbiano luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se le leggi dello Stato membro che attuano le altre disposizioni della direttiva sono rispettate prima del trasferimento.

La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma della direttiva, ha fornito indicazioni sull'effettuazione di tali valutazioni (2).

Tenuto conto dei distinti modi in cui vengono protetti i dati nei paesi terzi, sia la verifica dell'adeguatezza di tale protezione, sia l'applicazione di ogni decisione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE, devono avvenire in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti di o tra paesi terzi in cui sussistono condizioni analoghe e da non costituire ostacoli occulti agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

In Ungheria vigono in materia di protezione dei dati personali norme di legge che producono effetti giuridici vincolanti.

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/hu_00-519_it.pdf

130 Decisione della Commissione europea, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati in Svizzera (*)

[notificata con il numero C(2000) 2304]

(Testo rilevante ai fini del SEE)

(2000/518/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1), in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

La direttiva 95/46/CE prescrive agli Stati membri di assicurarsi che i trasferimenti di dati personali verso un determinato paese terzo abbiano luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se le leggi dello Stato membro che attuano le altre disposizioni della direttiva sono rispettate prima del trasferimento.

La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma della direttiva, ha fornito indicazioni sull'effettuazione di tali valutazioni (2).

Tenuto conto dei distinti modi in cui vengono protetti i dati nei paesi terzi, sia la verifica dell'adeguatezza di tale protezione, sia l'applicazione di ogni decisione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE, devono avvenire in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti di o tra paesi terzi in cui sussistono condizioni analoghe e da non costituire ostacoli occulti agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

Nella Confederazione svizzera vigono in materia di protezione dei dati personali norme di legge che producono effetti giuridici vincolanti a livello federale e cantonale.

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/ch_00-518_it.pdf

131 Decisione della Commissione del 20 dicembre 2001 conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act) (*)

[notificata con il numero C(2001)4539]

(2002/2/CE)

LACOMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1), in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

Conformemente alla direttiva 95/46/CE gli Stati membri sono tenuti ad operare affinché i trasferimenti di dati personali verso paesi terzi possano avvenire solo se il paese terzo in questione garantisce un livello adeguato di tutela e se,prima del trasferimento, viene rispettata la legislazione dello Stato membro che attua altre disposizioni della direttiva.

La Commissione può constatare che un paese terzo garantisce un livello adeguato di tutela. In tal caso gli Stati membri vi possono trasferire dati personali senza richiedere ulteriori garanzie.

Conformemente alla direttiva 95/46/CE, il livello di tutela dei dati deve essere valutato tenendo presenti tutte le circostanze in cui si svolgono le operazioni di trasferimento dei dati e tenendo conto di determinate condizioni.Il gruppo di lavoro sulla tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito indicazioni per effettuare tale valutazione (2).

Data la diversità degli approcci alla protezione dei dati nei paesi terzi,è opportuno che la valutazione dell'adeguatezza avvenisse e che ogni decisione, basata sull'articolo 25, §6, della direttiva 95/46/CE, fosse presa ed attuata senza da luogo a discriminazioni arbitrarie o ingiustificate verso o tra paesi terzi in cui esistono condizioni analoghe e senza dar luogo a barriere occulte per gli scambi commerciali,visti gli attuali impegni della Comunità a livello internazionale.

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/canadadecisionit.pdf

132 Documento di lavoro dei servizi della Commissione sull'applicazione della decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal dipartimento del commercio degli Stati Uniti (*)

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 13.02.2002
SEC(2002) 196

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

sull'applicazione della decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal dipartimento del commercio degli Stati Uniti

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/news/02-196_it.pdf

133 Proposta di decisione del Parlamento europeo, del Consiglio e della Commissione relativa allo statuto e alle condizioni generali d'esercizio delle funzioni di garante europeo della protezione dei dati – COM(2001) 411 (*)

COM (2001) 411

RELAZIONE

Il trattamento dei dati personali è un'operazione correntemente praticata da istituzioni e organismi comunitari nell'ambito della loro attività. Ad esempio, la Commissione procede allo scambio di dati personali con gli Stati membri nel quadro della politica agricola comune, per la gestione del regime doganale, dei fondi strutturali e nel quadro di altre politiche comunitarie, quali l'istruzione, la formazione, la cultura e la ricerca. Per garantire la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, e per evitare che gli scambi d'informazione vengano rimessi in discussione dagli Stati membri per motivi di protezione dei dati, il trattato firmato ad Amsterdam ha inserito nel trattato che istituisce la Comunità europea una disposizione finalizzata a questo scopo. Il nuovo articolo 286 prevede che a decorrere dal 1° gennaio 1999 le istituzioni e gli organismi comunitari applichino le norme comunitarie sulla protezione dei dati personali stabilite prevalentemente dalle direttive 95/46/CE e 97/66/CE. Esso prevede inoltre che un organo di controllo indipendente vigili sull'applicazione di tali norme. D'altro canto le stesse motivazioni hanno portato all'inclusione del diritto alla protezione dei dati di carattere personale nella Carta dei diritti fondamentali dell'Unione europea. Per adempiere a questa disposizione del trattato il legislatore comunitario ha adottato il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati. Il regolamento stabilisce una serie di principi ai quali sono soggetti i trattamenti dei dati personali ad opera delle istituzioni e degli organismi comunitari. Oltre a tali disposizioni sostanziali, il regolamento istituisce un'autorità di controllo indipendente, denominata garante europeo della protezione dei dati, che ha il compito di assicurare l'applicazione delle disposizioni del regolamento. Il garante è assistito da un garante aggiunto.

Il regolamento prevede inoltre che il Parlamento europeo, il Consiglio e la Commissione fissino di comune accordo lo statuto e le condizioni generali d'esercizio delle funzioni del garante europeo della protezione dei dati e, in particolare, la retribuzione, le indennità e ogni altro compenso sostitutivo.

(*) http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=it&numdoc=52001PC0411&model=guichett

134 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (*)

European Treaty Series -No.164
Série des Traités européens -n ° 164

Convention for the Protection
of Human Rights and Dignity of the
Human Being with regard to the
Application of Biology and Medicine:

Convention on Human Rights
and Biomedicine

Convention pour la protection
des Droits de l'Homme et de la dignité
de l'être humain à l'égard des
applications de la biologie
et de la médecine:

Convention sur les Droits de l'Homme
et la biomédecine

Oviedo,4.IV.1997

(*) http://www.legal.coe.int/bioethics/gb/pdf/convention.pdf

135 Additional Protocol to the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine on the Prohibition of Cloning Human Beings (*)

European Treaty Series - No. 168

ADDITIONAL PROTOCOL TO THE CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND DIGNITY OF THE HUMAN BEING WITH REGARD TO THE APPLICATION OF BIOLOGY AND MEDICINE, ON THE PROHIBITION OF CLONING HUMAN BEINGS

Paris, 12.I.1998

(*) http://conventions.coe.int/Treaty/en/Treaties/Word/168.doc

136 Protection of Personal Data with regard to Surveillance (*)

Protection of personal data with regard to surveillance

Report by Mr. Giovanni BUTTARELLI,
Secretary General of the Italian Data Protection Authority (Italy)

Notice

The importance of the phenomenon of surveillance and surveillance activities by technical means which are becoming increasingly sophisticated demands serious thought at both national and international level with regard to the advantages and risks for democratic societies and individuals.

Several states have undertaken work in this field, even considering it necessary to draft specific legislative provisions on data protection in the field of (video-)surveillance.

In this context, the Council of Europe wishes to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe asked a consultant, Dr Giovanni BUTTARELLI, to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context.

It was therefore wished to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account when preparing specific legislative provisions on data protection with relation to video surveillance. These principles could, where appropriate, be applied to other forms or technical means of
surveillance after making any necessary adjustments to them.

At the present stage the Report and the Guiding Principles are to be the subject of public consultation. Any comments on these texts may be transmitted to the Secretariat General of the Council of Europe before 21st January 2001, at the following address : judith.ledoux@coe.int.

1) FOREWORD

Any research and/or report on surveillance is related to the technological development of control systems and is therefore to be considered in connection with the relevant historical context.

(*) http://www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapButtarelliE.htm

(5601252/1) Roma 2002 - Istituto Poligrafico e Zecca dello Stato - S.