ATTI PARLAMENTARI

XIV LEGISLATURA

CAMERA DEI DEPUTATI

Doc. CXXXVI
n. 3

RELAZIONE

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

(Anno 2002)

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

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

Trasmessa alla Presidenza il 26 maggio 2003

TIPOGRAFIA DEL SENATO (200)

PAGINA BIANCA

INDICE

Elenco delle abbreviazioni

I. STATO DI ATTUAZIONE DELLA LEGGE N. 675/1996

Le principali novità sul piano normativo

1. Il testo unico e i codici deontologici . . . . . *Pag.* 15
2. Altre attività normative . . . . . » 17
3. Iniziative legislative . . . . . » 21
4. L'attività consultiva del Garante sugli atti del Governo » 23

Pubblica amministrazione

5. Profili generali . . . . . » 26
6. Informazioni sensibili e altri dati particolari . . . . . » 28
7. Trasparenza dell'attività amministrativa . . . . . » 31
8. Accesso ai documenti amministrativi . . . . . » 33
9. Banche dati di rilevanti dimensioni . . . . . » 36
10. Carta d'identità elettronica, carta nazionale dei servizi e tessera elettorale . . . . . » 39
11. Documentazione anagrafica e materiale elettorale . . . . » 42
12. Istruzione . . . . . » 45
13. Canone radiotelevisivo . . . . . » 47
14. Enti locali . . . . . » 49

Attività giudiziarie e di polizia

15. Profili generali . . . . . » 51
16. Trattamento di dati nell'ambito dell'attività giudiziaria » 52
17. Notificazione di atti e comunicazioni . . . . . » 53
18. Attività di polizia . . . . . » 55
19. Sistema di informazione Schengen . . . . . » 57

Sanità

20. Trattamento di dati idonei a rilevare lo stato di salute » 59
21. Informazioni genetiche . . . . . » 62

Rapporto di lavoro

22. Tutela dei dati personali dei lavoratori . . . . . » 64
23. Controllo a distanza dei lavoratori . . . . . » 70

24. Annunci di lavoro, riforma del collocamento e del sistema informativo in materia di lavoro ..... *Pag.* 71

Statistica e ricerca scientifica

25. Il codice deontologico per il trattamento dei dati a scopi statistici e di ricerca scientifica ..... » 74

Associazioni, movimenti politici e partiti

26. Trattamento dei dati e realtà associative ..... » 76
27. Confessioni religiose ..... » 78
28. Condomini e multiproprietà ..... » 80

Attività forense, investigazione privata e liberi professionisti

29. Liberi professionisti e albi professionali ..... » 82
30. Raccolta di dati per finalità di difesa ..... » 83

Settore del credito, finanziario e assicurativo

31. Istituti di credito ..... » 85
32. Intermediazione finanziaria ..... » 88
33. Centrali rischi e società finanziarie ..... » 90
34. Registro dei protesti ..... » 94
35. Raccolte di dati in ambito assicurativo e banca dati Isvap ..... » 95
36. Perizie medico-legali ..... » 98

Attività giornalistiche a mezzi di informazione

37. Attività giornalistica e rispetto dei princìpi della legge n. 675/1996 ..... » 100
38. Tutela dei minori ..... » 101
39. Cronache giudiziarie ..... » 103
40. Foto segnaletiche o di persone arrestate ..... » 105
41. Diffusione di informazioni raccolte mediante l'uso di telecamere nascoste ..... » 106
42. Dignità della persona e dati idonei a rilevare lo stato di salute ..... » 107
43. Esercizio dei diritti nei confronti degli organismi di informazione ..... » 109

Sorveglianza e sistemi biometrici

44. Videosorveglianza ..... » 110
45. Rilevazioni biometriche ..... » 114

Marketing

46. *Marketing* e diritti dell'interessato ..... » 116

Telefonia e reti di comunicazione

47. Profili generali . . . . . *Pag.* 118
48. Accesso ai dati di traffico telefonico e altre questioni . » 120
49. Servizi non richiesti e consenso dell'interessato . . . . . » 123
50. Comunicazioni indesiderate dirette a utenze telefoniche mobili . . . . . » 124
51. Messaggi multimediali (*Mms*) . . . . . » 127
52. Localizzazione . . . . . » 128
53. Attività di cooperazione con l'Autorità per le garanzie nelle comunicazioni . . . . . » 129

Trattamento dei dati personali in Internet

54. Profili generali . . . . . » 130
55. Comunicazioni indesiderate . . . . . » 131
56. Il codice deontologico . . . . . » 133
57. Pubblicazione di fotografie sui siti *web* . . . . . » 134
58. Fotografie e immagini su cataloghi pubblicitari, giornali, riviste o altri strumenti di diffusione . . . . . » 135

Sicurezza dei dati e dei sistemi

59. Misure di sicurezza: novità normative e casi applicativi » 136

I trasferimenti all'estero di dati

60. Paesi che offrono una protezione adeguata . . . . . » 139
61. «*Safe Harbor*» . . . . . » 141

II. Il Garante

La trattazione dei ricorsi

62. Principali problemi esaminati . . . . . » 145
63. Profili procedurali, impugnazione dei provvedimenti dell'Autorità . . . . . » 151

Attività ispettive e applicazione di sanzioni amministrative

64. Tipologia degli accertamenti ispettivi e criteri adottati. » 153
65. La collaborazione con organi dello Stato. Il protocollo d'intesa con la Guardia di finanza . . . . . » 155
66. La programmazione delle ispezioni e i risultati . . . . . » 157
67. L'attività sanzionatoria del Garante . . . . . » 158

L'attività di informazione e comunicazione

68. Profili generali . . . . . » 160
69. Seminari, convegni ed altre iniziative . . . . . » 163
70. Il nuovo *Internet* dell'Autorità . . . . . » 166

La gestione amministrativa dell'Ufficio

71. I regolamenti del Garante e la nuova organizzazione dell'Ufficio ..... *Pag.* 168
72. Il bilancio, gli impegni di spesa e l'attività contrattuale » 170
73. Lo sviluppo del sistema informativo ..... » 173
74. Il personale e i collaboratori esterni ..... » 176

Il registro dei trattamenti

75. Organizzazione e sviluppi futuri ..... » 178

Dati statistici

76. Prospetto analitico. Tabelle e grafici ..... » 181

III. Attività comunitarie e Internazionali

Il recepimento delle trattative comunitarie

77. Le direttive sulla protezione dei dati ..... » 187
78. Stato di recepimento delle direttive 95/46/CE e 97/66/Ce negli Stati membri ..... » 188
79. *Privacy* nelle telecomunicazioni ..... » 192

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

80. Profili generali ..... » 194

La cooperazione tra Autorità garanti in Europa

81. Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ..... » 197
82. La partecipazione ad altri comitati e gruppi di lavoro . » 201

L'Autorità di controllo comune Schengen

83. L'attività dell'Autorità ..... » 203

Europol

84. L'attività dell'Autorità comune di controllo e i primi casi di contenzioso ..... » 205

Il controllo sul Sistema informativo doganale

85. La creazione dell'Autorità di controllo ..... » 206

Eurodac

86. Collaborazione tra Stati membri e garanzie per gli interessati ..... » 207

Consiglio d'Europa

87. La convenzione sul *cybercrime* . . . . . *Pag.* 208
88. L'attività dei gruppi di esperti . . . . . » 210
89. Linee-guida in materia di sorveglianza . . . . . » 212

O.C.S.E.

90. I risultati conseguiti nel 2002 . . . . . » 213
91. Ulteriori iniziative . . . . . » 215

IV. DOCUMENTAZIONE

Testi

Normativa

92. Legge 31 dicembre 1996, n. 675 - Tutela delle persone e di altri soggetti rispetto al trattamenti dei dati personali . . . . . » 220
93. 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 . . . . . » 243
94. Legge 3 febbraio 2003, n. 14 - "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2002" . . . . . » 250
95. Codice dei deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale . . . . . » 251

Provvedimenti del Garante.

96. Autorizzazioni generali 2002 . . . . . » 259
97. 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 . . . . . » 260
98. Autorizzazione al trasferimento di dati personali verso il Canada - 30 aprile 2003 . . . . . » 272
99. Provvedimento in materia di codici di deontologia e di buona condotta - 10 aprile 2002 . . . . . » 278

Unione europea

100. Direttiva 2002/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle

comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) . . . . . *Pag.* 281

101. Raccomandazione del Parlamento europeo al Consiglio sul futuro sviluppo di *Europol* e la sua integrazione a pieno titolo nel sistema istituzionale dell'Unione europea . . . . . » 295

102. Risoluzione del Parlamento europeo del 13 marzo 2003 sulla trasmissione dei dati personali da parte delle compagnie aeree in occasione di voli transatlantici . . . . . » 298

103. Decisione del Consiglio del 28 febbraio 2002 riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'*acquis* di Schengen (2002/192/CE) . . » 301

104. Decisione del Consiglio del 14 ottobre 2002 relativa alla declassificazione di talune parti del manuale Sirene adottato dal comitato esecutivo istituito dalla convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 (2003/19/CE) . . . . . » 302

105. UE Catalogo Schengen. - Sistema d'Informazione Schengen. SIRENE: Raccomandazioni e migliori pratiche. Dicembre 2002 . . . . . » 303

106. Manuale SIRENE. Informazioni supplementari richieste all'ingresso nazionale . . . . . » 304

Commissione europea

107. Dichiarazione del Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie in merito alla pubblicazione di *test* genetici via *Internet* - 24 febbraio 2003 » 305

Consiglio d'Europa

108. Raccomandazione R(2002)9 del Comitato dei ministri agli Stati membri sulla protezione dei dati personali raccolti e trattati per scopi assicurativi . . . . . » 306

109. *Protection of personal data with regard to surveillance* (2000) *and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance* . . . . . » 314

110. *Guiding principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance* . . . . . » 330

Autorità di controllo comune Schengen

111. *Implementation of Schengen in the UK* . . . . . » 333

112. *SIS II devolopments* . . . . . » 337

113. *Opinon concerning the relation between Article 112 and 113 of the Schengen Convention* . . . . . *Pag.* 342
114. *SIS II devolopments* . . . . . » 345
115. Quinta relazione di attività dell'Autorità di controllo comune: marzo 2000 - dicembre 2001 . . . . . » 348

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

116. Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro . . . . . » 350
117. Documento di lavoro sulla determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento dei dati personali su *Internet* da parte dei siti *web* non stabiliti nell'UE . » 351
118. Parere 1/2002 riguardo alla relazione CEN/ISSS sulla standardizzazione delle modalità di tutela della vita privata in Europa . . . . . » 362
119. Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6 . . . . . » 363
120. Parere 3/2002 sulle prescrizioni in merito alla tutela dei dati contenute nella proposta della Commissione di una direttiva relativa all'armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di credito al consumo . . . . . » 364
121. Documento di lavoro sul funzionamento dell'Accordo di approdo sicuro . . . . . » 365
122. Parere 4/2002 sul livello di tutela dei dati personali in Argentina . . . . . » 367
123. Parere 5/2002 sulla dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica di dati di traffico delle telecomunicazioni . . . . . » 368
124. Documento di lavoro sulle "liste nere" . . . . . » 370
125. Parere 6/2002 relativo alla trasmissione da parte delle compagnie aeree d'informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti . . . . . » 371
126. Documento di lavoro sul trattamento di dati personali tramite videosorveglianza . . . . . » 378
127. Documento di lavoro relativo ai servizi di autenticazione *on-line* . . . . . » 394
128. Parere 1/2003 sulla memorizzazione dei dati relativi al traffico a fini di fatturazione . . . . . » 395

O.C.S.E.

129. Raccomandazione del Consiglio Ocse relativa alle linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza . . . . . *Pag.* 401

Consiglio dell'Unione europea

130. Risoluzione del Consiglio dell'Unione europea del 18 febbraio 2003 su un approccio europeo per una cultura della sicurezza delle reti e dell'informazione . . . . . » 407

ELENCO DELLE ABBREVIAZIONI

La presente Relazione è riferita al 2002 e contiene alcune ulteriori notizie già anticipate nella precedente Relazione nonché alcune ulteriori informazioni, aggiornate al 30 aprile 2003, 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

PAGINA BIANCA

Stato di attuazione della legge n.675/1996

PAGINA BIANCA

Le principali novità sul piano normativo

1 Il testo unico e i codici deontologici

Nel 2002 è proseguito il consolidamento degli interventi normativi del 2001 che hanno integrato la disciplina in materia di protezione dei dati personali in vista dell'adozione di un testo unico in materia.

Dopo la legge 24 marzo 2001, n. 127, recante una nuova delega al Governo, e il decreto legislativo 28 dicembre 2001 n. 467, che ne rappresenta la prima fase di attuazione, sono state poste le basi per completare la disciplina in materia di protezione dei dati personali, con l'adozione, entro il 30 giugno 2003, di un testo unico (art. 1, comma 4, l. n. 127/2001) e con il varo di codici deontologici in alcuni importanti settori (art. 20, d.lg. n. 467/2001).

La previsione di un testo unico delle disposizioni normative in materia di protezione dei dati personali renderà possibile introdurre integrazioni e modifiche di coordinamento o finalizzate alla migliore attuazione della disciplina vigente, anche in settori, come quelli relativi alle attività giudiziarie e di polizia, nei quali è avvertita l'esigenza di completare il percorso previsto dalle leggi delega che si sono succedute dal 1996 ad oggi (leggi nn. 676/1996, 344/1996 e, appunto, 127/2001).

Il termine per completare i lavori per l'adozione del testo unico, originariamente fissato al 31 dicembre 2002, è stato prorogato al 30 giugno 2003 dalla legge comunitaria 2002 (art. 26, l. 3 febbraio 2003, n. 14) su iniziativa del Governo che potrà rendere possibile un esame ancora più approfondito della materia, già di per sé complessa, anche al fine di attuare la nuova direttiva relativa alla protezione dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva del Consiglio e del Parlamento europeo n. 2002/58/CE del 12 luglio 2002).

Nel 2002 e nei primi mesi del 2003 è proseguito l'impegno della commissione di esperti istituita presso la Presidenza del Consiglio dei ministri-Dipartimento della funzione pubblica per la messa a punto di uno schema del testo unico.

Al tema dei codici di deontologia e di buona condotta le recenti norme hanno dato notevole risalto, prevedendo anche che il rispetto delle relative disposizioni costituisca condizione essenziale per la liceità del trattamento dei dati. Come già riportato nella precedente *Relazione del 2001*, in ragione della sperimentata efficacia del ricorso a tali strumenti normativi, il d.lg. n. 467/2001 ha esteso l'utilizzo di tale fonte regolatrice al fine di specificare i principi della legge n. 675/1996 in alcuni settori, fra quelli indicati nella legge-delega n. 127/2001, nei quali è sentita, anche da parte delle categorie di soggetti interessati, l'esigenza di una disciplina dettagliata e al tempo stesso flessibile nei suoi sviluppi (art. 20, d.lg. n. 467/2001).

I nuovi codici, che si aggiungeranno a quelli già sottoscritti o in via di completamento,

riguardano, in sintesi, i trattamenti:

- effettuati nell'ambito dei servizi di comunicazione e informazione offerti per via telematica e in particolare attraverso *Internet* ;
- necessari per la gestione del rapporto di lavoro e per finalità previdenziali;
- effettuati per fini di *direct marketing* o di invio di materiale pubblicitario;
- svolti a fini di informazione commerciale;
- provenienti da archivi pubblici ed accessibili al pubblico;
- effettuati nell'ambito di sistemi informativi utilizzati per la concessione di crediti al consumo (centrali rischi private);
- effettuati con strumenti automatizzati di rilevazione di immagini (videosorveglianza).

Tali codici dovranno ispirarsi ai criteri direttivi delle pertinenti raccomandazioni del Consiglio d'Europa indicate nella legge-delega n. 676 del 1996 e ad alcuni principi integrativi di carattere generale per specifiche categorie di trattamenti, espressamente indicati nelle norme del 2001.

Sinora, in base all'art. 31, comma 1, lett. *h)* della legge n. 675/1996 -che attribuisce al Garante il compito di promuovere la sottoscrizione di codici deontologici- e ad altre disposizioni normative (art. 25, l. n. 675/1996; art. 6, d.lg. 30 luglio 1998, n. 281), sono stati sottoscritti: a) il codice relativo all'attività giornalistica, pubblicato a seguito del provvedimento del Garante del 29 luglio 1998; b) quello per i trattamenti effettuati a scopi storici, pubblicato a seguito del provvedimento del Garante del 14 marzo 2001; e c) nel decorso anno, il codice per i trattamenti effettuati a scopi statistici e di ricerca scientifica nell'ambito del SISTAN, pubblicato a seguito del provvedimento del Garante del 31 luglio 2002 (per quest'ultimo si veda, più diffusamente, il paragrafo 25). Sono, inoltre, in avanzato stato i procedimenti per l'adozione del codice per l'attività forense e l'investigazione privata (art. 22, comma 4, l. n. 675/1996) e il codice per gli altri trattamenti effettuati a scopi statistici e di ricerca scientifica.

I codici di deontologia e di buona condotta, che saranno allegati al testo unico al fine di garantire completezza ed omogeneità al processo normativo di attuazione della delega (art. 20, comma 4, d.lg. n. 467/2001), costituiranno così una fonte significativa anche per gli effetti sul piano della liceità dei trattamenti. Il Garante ha avviato le procedure per l'approvazione dei nuovi codici con deliberazione del 10 aprile 2002, adottata in anticipo rispetto al termine previsto dal menzionato art. 20, fissato al 30 giugno, con la quale ha invitato *"a partecipare all'adozione"* dei codici tutti i soggetti pubblici o privati *"aventi titolo ...in base al principio di rappresentatività"* (art. 31, comma 1, lett. *h)*, l. n. 675/1996). Numerose sono risultate le richieste di partecipazione pervenute all'Autorità.

2 Altre attività normative

Nel corso del 2002, nel quale è entrata nel vivo l'attività normativa della XIV legislatura, sono stati approvati vari provvedimenti d'interesse per la materia del trattamento dei dati personali. Si segnalano i più rilevanti, relativi anche ai primi mesi del 2003:

a) il decreto legislativo 9 aprile 2003, n. 70, recante *"Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico"*. Il decreto, diretto a promuovere la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico, rinvia espressamente alla legge n. 675/1996 e al d.lg. n. 171/1998 per le questioni relative al diritto alla riservatezza e al trattamento dei dati personali nel settore delle telecomunicazioni. Il testo contiene peraltro specifiche cautele in merito alle comunicazioni elettroniche non sollecitate (art. 9);

b) la legge 24 aprile 2003, n. 88, di conversione del d.l. 24 febbraio 2003, n. 28, recante *"Disposizioni urgenti per contrastare i fenomeni di violenza in occasione di competizioni sportive"*. Le novità emerse anche a seguito della conversione del decreto prevedono che con uno o più decreti del Ministro dell'interno, di concerto con il Ministro per i beni e le attività culturali e con il Ministro per l'innovazione e le tecnologie, sentito il Garante, siano stabilite modalità per l'attuazione delle disposizioni riguardanti la disciplina dell'ingresso agli impianti sportivi mediante varchi dotati di *metal detector*, finalizzati all'individuazione di strumenti di offesa e presidiati da personale incaricato previa verifica elettronica della regolarità del titolo di accesso. Con decreto del Ministro dell'interno, di concerto con il Ministro per i beni e le attività culturali e con il Ministro per l'innovazione e le tecnologie, sentito il Garante, saranno inoltre stabilite modalità per attuare le disposizioni concernenti la dotazione dei medesimi impianti sportivi di strumenti che consentano la registrazione televisiva delle aree riservate al pubblico, sia all'interno dell'impianto, sia nelle sue immediate vicinanze;

c) la legge 14 febbraio 2003, n. 30, recante *"Delega al Governo in materia di occupazione e mercato del lavoro"* in base alla quale dovrebbe essere ridefinito il regime del trattamento dei dati relativi all'incontro tra domanda e offerta di lavoro, nel rispetto della legge 31 dicembre 1996, n. 675, al fine di:

- evitare oneri aggiuntivi e ingiustificati rispetto alle esigenze di monitoraggio statistico;
- prevenire forme di esclusione sociale e vigilanza sugli operatori, con previsione (art. 1, comma 2, lett. *g)*) del divieto assoluto per gli operatori privati e pubblici di qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione dei lavoratori, anche con il loro consenso, in base all'affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale, o di famiglia, o di gravidanza, nonché ad eventuali controversie con i precedenti datori di lavoro.
- In base alla l. n. 30/2003 è inoltre espressamente vietato raccogliere, memorizzare o diffondere informazioni sui lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo. Tale delega dovrà essere armonizzata con quella relativa al testo unico in materia di trattamento dei dati personali;

d) la legge 5 febbraio 2003, n. 17, recante *"Nuove norme per l'esercizio del diritto di voto da parte degli elettori affetti da gravi infermità"* che, modificando l'articolo 55 del testo unico di cui al decreto del Presidente della Repubblica n. 361 del 1957, nonché l'articolo 41 del testo unico di cui al decreto del Presidente della Repubblica n. 570 del 1960, ha aggiunto il seguente comma: *"L'annotazione del diritto al voto assistito, di cui al secondo comma, è inserita, su richiesta dell'interessato, corredata della relativa documentazione, a cura del Comune di iscrizione elettorale, mediante apposizione di un corrispondente simbolo o codice, nella tessera elettorale personale, nel rispetto delle disposizioni vigenti in materia di riservatezza personale ed in particolare della legge 31 dicembre 1996, n. 675, e successive modificazioni"*;

e) la legge 3 febbraio 2003, n. 14, recante *"Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2002"*, cui si è fatto cenno, che proroga al 30 giugno 2003 il termine previsto dalla legge n. 127 del 2001 per l'adozione del testo unico in materia di protezione dei dati personali;

f) la legge 16 gennaio 2003, n. 3, recante *"Disposizioni ordinamentali in materia di pubblica amministrazione"*, collegato alla finanziaria 2002. Il testo normativo prevede alcuni interventi in materia di innovazione tecnologica nella pubblica amministrazione, da attuare con uno o più regolamenti governativi (art. 27), con riguardo, in particolare, alla diffusione della carta nazionale dei servizi e all'accesso telematico agli atti della pubblica amministrazione. In proposito va segnalato che il testo in esame non reca più il riferimento alla diffusione della carta d'identità elettronica, a seguito di un emendamento parlamentare soppressivo il cui proponente ha precisato che una materia come quella della carta d'identità elettronica, investendo il controllo sui dati e richiedendo adeguate garanzie per la riservatezza delle persone, non può essere affidata a regolamenti adottati sulla base di una delega affidata al Governo;

g) il decreto-legge 9 settembre 2002 n. 195, convertito dalla legge 9 ottobre 2002, n. 222, con il quale il Governo ha ampliato gli interventi di legalizzazione del lavoro irregolare di cui alla predetta legge n. 189/2002, estendendo, com'è noto, le misure già previste per colf e badanti nel campo del lavoro subordinato nell'impresa. Nel corso dei lavori per la conversione del provvedimento d'urgenza, l'Autorità ha segnalato al Governo (ai sensi dell'art. 31, comma 1, lett. *m)* l. 675/1996) l'opportunità di interventi emendativi a due disposizioni di particolare interesse in materia di rilevazione di impronte digitali. Il decreto-legge prevedeva, nella sua stesura originaria, che ai trattamenti dei dati personali degli extracomunitari acquisiti attraverso i rilievi dattiloscopici si applicasse il particolare regime normativo previsto per i trattamenti effettuati nell'ambito del Centro elaborazione dati del Dipartimento della pubblica sicurezza (art. 2, comma 6, d.l. n. 195/2002 e art. 4, comma 1, lett. *a)*, l. n. 675/1996). Inoltre, ha introdotto l'obbligo di sottoporre a rilievi dattiloscopici anche i cittadini italiani al momento del rilascio della carta d'identità elettronica, integrando, di fatto, la disciplina prevista per il documento d'identità dall'articolo 36 del d.P.R. 28 dicembre 2000, n. 445, recante il testo unico in materia di documentazione amministrativa (art. 2, comma 7, d.l. n. 195/2002). Tale ultima disposizione è stata adottata in "attuazione" dell'ordine del giorno citato alla successiva lettera *i)* a proposito della legge n. 189/2002. I chiarimenti forniti dall'Ufficio del Garante hanno consentito di ricondurre in parte le due previsioni nel quadro dei principi previsti dalla legge n. 675 del 1996. Da un lato, il vigente comma 6 dell'art. 2 del decreto-legge contiene un rinvio più corretto ai principi appli-

cabili in materia di trattamenti effettuati da organismi di polizia (art. 4, comma 2, l. n. 675/1996); ciò, non necessariamente, però, per le specifiche finalità di sicurezza pubblica o prevenzione e accertamento di reati cui è preposto il C.e.d. del Dipartimento della pubblica sicurezza, in quanto la raccolta delle impronte digitali degli extracomunitari non è di per sé sempre effettuata per finalità di sicurezza pubblica, ma principalmente per fini di identificazione delle persone. Dall'altro, la legge di conversione ha in ogni caso integrato il comma 7 del medesimo articolo 2 del decreto-legge prevedendo che la pur disposta sottoposizione a rilievi dattiloscopici di tutti i cittadini italiani avvenga secondo modalità che rispettino i principi in materia di dati personali in tema di utilizzazione, conservazione e accesso ai dati, modalità da stabilirsi con regolamento governativo. A tale scopo, nel corso dei lavori di conversione del decreto-legge il Governo, accogliendo un ordine del giorno della Camera, si è impegnato a riferire al Parlamento sui criteri che intenderebbe seguire per l'attuazione delle due disposizioni, per quanto riguarda, in particolare, le modalità di raccolta e di gestione delle impronte digitali. L'Autorità, nel quadro delle più ampie indicazioni fornite, ha comunque confermato la propria disponibilità a cooperare per l'individuazione di tali modalità tecniche, nell'ambito dei più ampi interventi in ordine alla predisposizione e diffusione della carta d'identità elettronica e della carta nazionale dei servizi, per i quali sono avviati i necessari contatti con il Ministero dell'interno e con il Ministero dell'innovazione e delle tecnologie;

h) la legge 1 agosto 2002, n. 166, recante *"Disposizioni in materia di infrastrutture e trasporti"* il cui art. 41 (Riassetto delle telecomunicazioni) attribuisce al Governo una delega per l'attuazione delle recenti direttive comunitarie in materia di comunicazioni elettroniche (direttive del Parlamento e del Consiglio nn. 2002/19/CE, 2002/20/CE, 2002/21/CE e 2002/22/CE del 7 marzo 2002), ivi comprese quelle approvate entro il termine di esercizio della delega, riguardanti, fra l'altro, i diritti degli utenti e la sicurezza dei dati personali. In tale quadro è compresa anche la già citata direttiva n. 2002/58/CE del 12 luglio 2002 in materia di tutela della vita privata nel settore delle comunicazioni elettroniche, alla quale, peraltro, fa riferimento anche l'art. 26 della l. 3 febbraio 2003, n. 14 (legge comunitaria 2003) e, implicitamente, la legge n. 127/2001. Tale direttiva sostituisce la direttiva n. 97/66/CE e comprende alcuni aspetti di particolare importanza per la protezione dei dati personali che necessitano di una piena attuazione nel nostro ordinamento, quali, fra l'altro, le modalità di inserimento degli abbonati negli elenchi telefonici, la conservazione dei dati di traffico, la localizzazione degli utenti e l'invio di comunicazioni indesiderate attraverso la posta elettronica o altri mezzi elettronici (c.d. *spamming*);

i) la legge 30 luglio 2002, n. 189, di riforma della normativa in materia di immigrazione ed asilo, che contiene disposizioni in base alle quali ogni straniero che richiede il permesso di soggiorno o lo rinnovi è sottoposto a rilievi fotodattiloscopici (artt. 5 e 7). Nel corso dei lavori il Governo ha accolto l'ordine del giorno già indicato alla lettera *g)* in base al quale si è impegnato ad adottare le misure necessarie perché nella carta d'identità elettronica siano inserite le impronte digitali dei cittadini italiani e gli altri dati biometrici. Sull'argomento della raccolta delle impronte digitali il Garante ha inoltrato in data 27 giugno 2002 ai Presidenti delle Camere e ad alcune commissioni parlamentari una nota con la quale, nel richiamare il quadro di garanzie previsto a livello internazionale, ha segnalato la necessità del rispetto, in tale delicata materia, dei principi in mate-

ria di protezione dei dati personali, specie per quanto attiene alla raccolta, alla conservazione e alla successiva utilizzazione di tali dati. La legge n. 189 prevede, l'adozione di regolamenti attuativi anche per gli aspetti di interconnessione fra diversi archivi esistenti, in relazione ai quali il Garante non mancherà di fornire le indicazioni di competenza in occasione del rilascio del previsto parere (art. 34, comma 2, l. n. 189/2002 e art. 31, comma 2, l. n. 675/1996);

l) il decreto legge 20 giugno 2002, n. 121, convertito dalla legge 1 agosto 2002, n. 168, recante alcune disposizioni urgenti in materia di sicurezza della circolazione stradale, il quale, fra l'altro, innova la disciplina dei controlli "a distanza" delle violazioni concernenti i limiti di velocità, prevedendo, a determinate condizioni, l'uso di strumenti di rilevazione (del tipo *autovelox* e simili) anche senza la presenza della pattuglia (art. 4). La disposizione fa salva l'applicazione delle cautele in materia di riservatezza e a tale riguardo l'Autorità ha collaborato con il Ministero dell'interno per la predisposizione di una circolare applicativa della materia per quanto riguarda gli aspetti relativi alla protezione dei dati personali;

m) 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.

3 Iniziative legislative

Oltre ai provvedimenti normativi approvati decritti al paragrafo precedente, sono stati seguiti i lavori parlamentari relativi ad altre iniziative legislative riconducibili alla tematica della protezione dei dati personali. Tra i progetti di legge più importanti vanno ricordati:

a) il disegno di *legge di semplificazione del 2001* (AS 776-B-BIS). Nel corso dell'esame presso la Commissione affari costituzionali della Camera il Governo ha presentato un emendamento che inserisce un articolo volto a promuovere il processo di informatizzazione giudiziaria. Esso prevede, in particolare, l'accesso - riservato a chi vi abbia interesse - ai dati identificativi delle questioni pendenti innanzi alla magistratura amministrativa e contabile mediante pubblicazione sui siti *web* delle autorità emananti, nonché la pubblicazione nei medesimi siti delle relative decisioni giudiziarie. Al riguardo l'Autorità ha fornito alla Commissione elementi utili di valutazione al fine di rendere pienamente compatibile tale processo con i principi in tema di protezione dei dati personali nel settore dell'informatica giuridica, in relazione anche alle specifiche cautele che potranno essere previste nel menzionato testo unico in attuazione di uno specifico criterio di delega della legge n. 127/2001. La Commissione ha tenuto conto con un emendamento degli elementi forniti dal Garante;

b) una proposta di legge in materia di accesso delle forze di polizia ai dati detenuti da vettori aerei e navali (AC 2630). Nell'ambito dei lavori presso la Commissione affari costituzionali della Camera si è tenuta, in data 14 gennaio 2003, l'audizione del Presidente del Garante, prof. Stefano Rodotà, il quale ha rappresentato l'esigenza che il progetto normativo rispetti i principi in materia di protezione dei dati personali applicabili ai trattamenti effettuati per finalità di polizia (art. 4, l. n. 675/1996). In particolare l'Autorità, richiamando quanto già osservato dal Garante in un provvedimento adottato nel 1999 in relazione ad una segnalazione presentata su tale problematica dalla compagnia aerea Alitalia, si è soffermata sull'esigenza che le richieste di informazioni siano il più possibile circostanziate, selettive e finalizzate unicamente al perseguimento di gravi reati di terrorismo o di criminalità organizzata e che i dati acquisiti, ove non di specifico interesse per le indagini, siano appena possibile cancellati;

c) il disegno di legge recante *modifiche ed integrazioni alla legge 7 agosto 1990, n. 241* (AS 1281) il cui articolo 13 modifica l'art. 25 della legge n. 241/1990 prevedendo che il Garante debba essere "sentito" dalla Commissione per l'accesso in sede di decisione su provvedimenti di diniego di accesso adottati da amministrazioni statali per motivi inerenti ai dati personali di terzi. Nel corso dei lavori, la Commissione ha approvato un emendamento del Governo in base al quale il Garante, a sua volta, dovrebbe richiedere il parere, non vincolante, della predetta Commissione qualora un procedimento relativo al trattamento di dati personali da parte di soggetti pubblici interessi l'accesso a documenti amministrativi;

d) il disegno di legge recante *"Norme in materia di pluralismo informatico e sulla adozione e diffusione del software libero nella pubblica amministrazione"* (AS 1188), in discus-

sione presso la Commissione affari costituzionali del Senato;

e) il disegno di legge delega al Governo in materia di *protezione giuridica delle invenzioni biotecnologiche*, approvato dalla Camera il 26 settembre 2002 e dal Senato, con modificazioni, il 2 aprile 2003.

Sono stati, infine, seguiti i lavori relativi ad alcune indagini conoscitive riguardanti tematiche d'interesse, fra le quali ricordiamo:

- l'indagine sulle potenzialità e le prospettive di Europol, presso il Comitato di controllo sull'attuazione dell'Accordo di Schengen, sull'attività di Europol e in materia di immigrazione, nell'ambito della quale il 9 ottobre 2002 si è tenuta un'audizione del dr. Giovanni Buttarelli, segretario generale dell'Autorità, nella qualità di Presidente dell'Autorità comune di controllo Schengen;
- l'indagine conoscitiva sul funzionamento e sulle modalità di gestione dell'anagrafe tributaria, presso la competente Commissione bicamerale, nell'ambito della quale si è tenuta, in data 6 novembre 2002, l'audizione del Presidente del Garante, prof. Stefano Rodotà e del Vicepresidente prof. Giuseppe Santaniello.

4 L'attività consultiva del Garante sugli atti del Governo

L'articolo 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. Norme speciali prevedono poi specificamente altri pareri.

In relazione a tale competenza, nel corso dell'anno il Garante ha espresso alcuni pareri in importanti materie, fra i quali si segnalano, in particolare, quelli riguardanti:

- il testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti (d.P.R. 14 novembre 2002, n. 313 - in suppl. G.U. n. 36 del 13 febbraio 2003). Oggetto del testo unico sono le norme che disciplinano l'iscrizione, l'eliminazione, la trasmissione e conservazione dei dati del casellario giudiziale, del casellario dei carichi pendenti, dell'anagrafe delle sanzioni amministrative dipendenti da reato, dell'anagrafe dei carichi pendenti degli illeciti amministrativi dipendenti da reato e quelle che riguardano i relativi servizi certificativi, le competenze degli uffici coinvolti e le loro procedure. L'approvazione del testo unico ha comportato l'abrogazione di 19 testi, dei quali 14 di rango primario e 5 di rango secondario. Fulcro delle innovazioni proposte è il sistema informativo automatizzato, che è posto al centro di tutte le attività degli uffici. L'aver disciplinato procedure e organizzazione con norme di rango secondario consentirà un rapido adeguamento alle esigenze poste dal continuo sviluppo tecnologico, favorito, ancor più, dalla scelta di rimettere a decreti dirigenziali le modalità tecniche operative del funzionamento del sistema;
- il decreto direttoriale 31 maggio 2002 dell'Amministrazione autonoma dei monopoli di Stato, recante "*Norme disciplinanti l'accettazione telefonica e telematica delle scommesse sportive, in attuazione del D.M. 15 febbraio 2001, n. 156*";
- alcuni decreti dirigenziali di attuazione del predetto testo unico in materia di casellario giudiziale (parere del 31 marzo 2003);
- lo schema di regolamento recante modifiche alle disposizioni del testo unico in materia di documentazione amministrativa concernenti le firme elettroniche (parere del 17 settembre 2002);
- lo schema di regolamento recante il regolamento di attuazione della legge n. 459/2001 sull'esercizio di voto dei cittadini italiani residenti all'estero (parere del 27 settembre 2002);
- lo schema di regolamento di attuazione dell'articolo 4, comma 8, del d.lg. 25 settembre 1997, n. 374, in materia di estensione delle disposizioni antiriciclaggio ad attività non finanziarie particolarmente suscettibili di utilizzazione a fini di riciclaggio (parere del 12 marzo 2003);
- lo schema di regolamento recante disciplina delle modalità di istituzione e tenuta presso la Presidenza del Consiglio dei ministri della banca dati informatica dei compo-

nenti degli organi di amministrazione attiva, consultiva e di controllo dello stato e degli enti pubblici a carattere nazionale e delle relative modalità di nomina (parere del 9 aprile 2003);
- lo schema di d.P.R. recante il regolamento integrativo della disciplina e dell'accesso al servizio di informatica giuridica del Centro elettronico di documentazione (CED) della Corte Suprema di cassazione. Al riguardo l'Autorità ha anche richiamato l'esigenza di inserire nel testo unico previsto dalla legge n. 127 alcune disposizioni concernenti note questioni pendenti sull'informatica giuridica (in particolare, relativamente all'indicazione dei nomi delle parti e alla pubblicità in rete delle sentenze), trattandosi di aspetti oggetto delle leggi-delega nn. 676/1996 e 127/2001, la prima delle quali reca un espresso riconoscimento della rilevanza dell'informatica giuridica e dell'esigenza di norme che ne favoriscano lo sviluppo in armonia con le garanzie in materia di protezione dei dati (art. 1, comma 1, lett. *l)*, l. n. 676/1996) (parere del 29 aprile 2003);
- schema di decreto recante *"Identificazione dei tipi di dati personali e delle operazioni eseguibili in relazione a rilevanti finalità di interesse pubblico perseguite dall'amministrazione della giustizia"*(parere del 29 aprile 2003).

A fronte dei pareri espressi sopra menzionati deve segnalarsi che -anche se in misura decisamente ridotta rispetto al passato- continuano a registrarsi casi di mancata consultazione del Garante.

In proposito, vanno menzionati, in particolare i seguenti provvedimenti:
- decreto del Ministro della salute del 7 agosto 2002 (in G.U. 24 ottobre 2002, n. 250) recante norme procedurali per l'effettuazione dei controlli *anti-doping* e per la tutela della salute, adottato ai sensi dell'art. 3, comma 1, della legge 14 dicembre 2000, n. 376;
- decreto del Ministro della lavoro e delle politiche sociali del 27 settembre 2002 (in G.U. 21 marzo 2003, n. 16) recante il regolamento di esecuzione delle disposizioni di legge in materia di riordinamento dei compiti e della gestione del Casellario centrale infortuni dell'INAIL.

Il Garante non ha espresso pareri per altri provvedimenti come quelli dell'Agenzia delle entrate specie in materia di trasmissione di atti per via telematica. Fra questi ultimi, ricordiamo in particolare:
- provvedimento del 30 maggio 2002 (in G.U. 12 giugno 2002, n. 136), relativo alle modalità di trasmissione per via telematica e di conservazione dei dati relativi alle forniture di documenti fiscali (art. 3, d.P.R. 5 ottobre 2001, n. 44);
- provvedimento del 19 giugno 2002 (G.U. 19 giugno 2002, n. 149), relativo alle modalità della trasmissione telematica all'anagrafe tributaria da parte dei soggetti gestori di servizi di pubblica utilità di dati e notizie riguardanti i contratti di somministrazione dei servizi telefonici;
- provvedimento del 30 luglio 2002 (G.U. 12 agosto 2002, n. 188), concernente le modifiche al decreto del Ministro delle finanze 13 dicembre 2000, in materia di obbligo di comunicazione all'anagrafe tributaria da parte dei rappresentanti fiscali di imprese di assicurazione dei dati relativi ai contratti di assicurazione;
- provvedimento del 18 luglio 2002 (in G.U. 25 luglio 2002, n. 173), relativo alla definizione delle specifiche tecniche dei dati per la comunicazione telematica di ammissione

o diniego del credito d'imposta;
- provvedimenti del 26 settembre 2002 (in G.U. 4 ottobre 2002 n. 233) e del 27 dicembre 2002 (in G.U. 10 gennaio 2003, n. 7), concernenti l'approvazione delle specifiche tecniche per la trasmissione telematica dei dati relativi alle comunicazioni in materia di interessi, premi ed altri frutti delle obbligazioni e dei dati da utilizzare per le dichiarazioni di inizio attività, variazione dati o cessazione attività;
- provvedimento del 2 gennaio 2003 (in G.U. 11 gennaio 2003, n. 8), concernente l'approvazione del modello di dichiarazione riservata delle attività emerse ai sensi del decreto-legge n. 282 del 2003.

Pubblica amministrazione

5 Profili generali

Il 2002 è stato caratterizzato, ancora una volta, dalla mancata o incompleta attuazione, da parte di diverse amministrazioni pubbliche, delle disposizioni di cui al d.lg. 135/1999, che disciplinano il trattamento dei dati sensibili.

In particolare, non risulta ancora attuata presso vari soggetti pubblici la previsione che impone alle amministrazioni pubbliche di identificare e rendere pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni eseguibili, in relazione alle rilevanti finalità di interesse pubblico dei trattamenti di competenza individuati legislativamente o con provvedimento del Garante.

Il quadro di diffusa disapplicazione di quanto previsto dal citato decreto legislativo è risultato, anche da uno specifico ciclo di ispezioni a campione disposto dal Garante nel corso dell'anno passato.

Tale verifica, unitamente alla valutazione del contenuto dei numerosi quesiti pervenuti, conferma la percezione che in diversi uffici pubblici non sia ancora maturato il richiesto grado di sensibilità sulle regole introdotte dalla legge n. 675/1996 e sugli effetti che le stesse comportano sul modo di amministrare.

Anche dai numerosi quesiti pervenuti da amministrazioni locali e centrali emerge la conferma che il livello di idonea applicazione della legge n. 675/1996 negli uffici pubblici non è ancora soddisfacente.

Sebbene siano trascorsi sei anni dall'entrata in vigore di tale legge, permangono ingiustificate incertezze e lacune, solo in parte derivanti dai tempi obiettivamente necessari per far maturare un ottimale approccio culturale ai principi di garanzia fissati dalla legge, e in larga parte determinati, invece, dalla tendenza ad esaurire l'impegno nell'attuazione - spesso tardiva, inesatta o incompleta - della legge n. 675/1996 assolvendo in modo riduttivo i soli adempimenti di ordine formale.

A tutt'oggi manca inoltre, come si è evidenziato anche nelle precedenti relazioni, una visione di insieme delle problematiche connesse alla protezione dei dati personali. Continua ad essere spesso privilegiato un approccio meramente formale che rende di fatto fini a se stessi e inutilmente burocratici gli adempimenti posti a tutela dei diritti delle persone e della sicurezza delle informazioni, senza alcun concreto beneficio per i diritti della personalità degli interessati.

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

La consapevolezza di tale stato di cose ha tra l'altro indotto l'Autorità ad intensificare la collaborazione già avviata con gli enti rappresentativi delle autonomie locali e con le regioni. A queste si sono affiancati, su loro specifica iniziativa, contatti e collaborazioni con alcune amministrazioni centrali, le quali hanno al momento portato a pochi risultati concreti.

Tali questioni sono state peraltro sollevate anche in ambito parlamentare dall'interrogazione a risposta scritta presentata dall'On. Del Mastro Delle Vedove, con la quale sono stati richiesti al Governo chiarimenti sulle eventuali iniziative assunte in merito.

6 Informazioni sensibili e altri dati particolari

Come si è accennato nel paragrafo precedente, l'Autorità ha continuato a focalizzare l'attenzione in particolare sull'adeguamento degli ordinamenti da parte dei soggetti pubblici alle disposizioni del d.lg. n. 135/1999 per trattare lecitamente dati sensibili e informazioni di tipo giudiziario.

Come è noto, l'art. 5 di tale decreto, modificando l'art. 22, comma 3, della legge n. 675/1996 ha stabilito che laddove la legge o, in via transitoria, il Garante, abbiano individuato le rilevanti finalità d'interesse pubblico perseguite con un determinato trattamento, i soggetti pubblici possono utilizzare i dati dopo aver previamente individuato e reso noti, "secondo i rispettivi ordinamenti", i tipi di dati e di operazioni eseguibili.

Anche nel corso dell'anno 2002, gli atti adottati in tal senso dalle amministrazioni sono risultati, purtroppo, in numero esiguo e non privi di vizi di fondo legati ad una ricognizione solo formale dell'esistente, tanto da giustificare nuovamente la considerazione, già espressa lo scorso anno, che varie disposizioni del d.lg. n. 135/99 siano rimaste sostanzialmente inapplicate e che alcuni trattamenti effettuati in ambito pubblico proseguano nell'inosservanza delle garanzie per il cittadino.

Oltre a ciò, l'adozione, da parte di alcuni enti, degli atti diretti a rendere noti i tipi di dati e di operazioni effettuabili non è avvenuta consultando preventivamente il Garante, come dovuto per legge, il che ha determinato ulteriori ripercussioni sulla loro validità.

Terminata la peraltro assai lunga fase di primo "avvio" dell'adeguamento degli ordinamenti ai sensi dell'art. 5, comma 4, del d.lg. n. 135/1999, tale stato di cose, verificato anche a seguito di una serie di ispezioni effettuate presso alcune amministrazioni estratte a campione, resta di gravità tale da esporre il nostro Paese anche a rischi di gravi violazioni della disciplina comunitaria. Ciò 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 al più presto alle disposizioni vigenti. Con la medesima segnalazione, sono state peraltro enucleate in chiave alcune linee-guida alle quali le pubbliche amministrazioni devono uniformarsi nella predisposizione degli atti (in *Bollettino* n. 24, p. 40).

Con tale provvedimento il Garante, nel ribadire l'obbligo di procedere alla rilevazione in questione attraverso atti di natura regolamentare anziché attraverso altri atti amministrativi, ha ricordato che le norme generali introdotte dal d.lg. n. 135/1999 non devono essere riprodotte nei singoli atti, apparendo pacifico che al trattamento dei dati in questione si applichino comunque le medesime disposizioni generali fissate nel decreto in tema, in particolare, di essenzialità, pertinenza, modalità di conservazione dei dati, ecc. (artt. 1-5). Piuttosto, si è osservato, risulta necessario collegare alle rilevanti finalità perseguite dal trattamento già individuate dal decreto o

dal Garante, i tipi di dati sensibili trattati e i tipi di operazioni su di essi eseguite. Ciò che occorre, in altre parole, è che la pubblica amministrazione chiarisca ai cittadini, in un quadro di piena trasparenza, quali categorie di informazioni vengono utilizzate in relazione alle singole finalità e renda note le sostanziali forme della loro utilizzazione, evitando peraltro la pedissequa, quanto inutile, menzione di tutte le operazioni che compongono l'ampia definizione legislativa di "trattamento" (art. 1, l. n. 675/1996).

Relativamente alla forma che tali provvedimenti promossi dalle amministrazioni pubbliche devono assumere, il Garante ha ribadito, come si è detto, quanto affermato in altre circostanze e cioè che il delicato profilo in questione, che incide in modo significativo sui diritti della personalità, deve essere esaminato attraverso atti di natura regolamentare anziché mediante atti amministrativi interni. Ciò anche perché la forma regolamentare, in ragione del particolare e più adeguato procedimento di formazione (interno ed esterno ai soggetti pubblici) assicura all'atto-regolamento una maggiore "autorevolezza" e 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 quindi nuovamente riservato, in presenza di accertate violazioni della disciplina in materia, di adottare specifici provvedimenti di blocco o divieto del trattamento.

Dalle verifiche ispettive svolte dall'Autorità sono inoltre risultate ulteriori violazioni di legge, quali la mancata designazione dei soggetti incaricati del trattamento, ovvero un'adozione di misure minime di sicurezza non sempre rispondente al dettato normativo.

Proprio in ragione delle difficoltà appena ricordate, e consapevole del particolare impegno che tale disciplina integrativa di dati sensibili può comportare, l'Autorità ha intrapreso anche sotto questo profilo forme di collaborazione con gli organismi rappresentativi degli enti locali, cui si accennerà nel paragrafo dedicato a questo tema (par. 12).

In materia sanitaria l'individuazione dei tipi di dati e di operazioni presenta profili specifici; l'art. 2, comma 1, d.lg. n. 282/1999, aveva infatti affidato tale compito ad un decreto del Ministro della sanità (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 avrebbe dovuto permettere una disciplina più uniforme del settore anche per quanto riguarda l'individuazione delle modalità semplificate per le informative di cui all'art. 10 della l. n. 675/1999 e per la prestazione del consenso nei confronti degli organismi sanitari pubblici, convenzionati o accreditati dal Servizio sanitario nazionale.

Un apposito gruppo di lavoro, cui ha partecipato anche questa Autorità, ha svolto un intenso lavoro terminando, sostanzialmente, l'opera intrapresa. La disciplina integrativa in questa materia è assai attesa.

Oltre a privare i cittadini di importanti garanzie a tutela dei propri diritti fondamentali, il mancato completamento della disciplina 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 che il medesimo

decreto dovrebbe introdurre.

Fra i pochi tentativi di dare esecuzione alle disposizioni introdotte dal d.lg. n. 135/1999, deve segnalarsi l'adozione del decreto del Ministero della difesa del 10 ottobre 2002, che presenta però un'individuazione non ancora idonea di dati e di operazioni, effettuata peraltro utilizzando una fonte non regolamentare e senza consultare preventivamente il Garante. Opportuni contatti sono stati intrapresi con i relativi uffici per adeguare il decreto.

Con riferimento alla materia dei dati sanitari va anche segnalato il rinnovo da parte del Garante dell'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, invece, i dati a carattere giudiziario, il loro trattamento resta al momento regolato principalmente dall'art. 24 della l. 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 perseguite 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 problemi analoghi a quelli appena ricordati a proposito dei dati sensibili. Anche in questo caso necessita, pertanto, una rapida emanazione di idonei regolamenti attuativi da parte di tutte le amministrazioni interessate.

Il Garante ha peraltro autorizzato detti trattamenti, come già in passato con l'autorizzazione n. 7 (rinnovata 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.

Con riferimento alla pratica applicazione dei principi in materia di trattamenti di dati sensibili in ambito pubblico, merita di essere da ultimo citata la richiesta presentata al Garante da parte di una comunità montana volta ad ottenere una "autorizzazione" al trattamento di dati sensibili in occasione della realizzazione di un censimento della popolazione finalizzato alla redazione di un piano di protezione civile.

In tale occasione, l'Ufficio ha avuto modo di precisare (risposta a quesito del 20 gennaio 2003) che le informazioni attinenti a persone non autosufficienti rilevabili in tale occasione, in quanto di carattere sensibile, possono essere già trattate in quanto collegate alle rilevanti finalità di interesse pubblico in materia di "protezione civile", alle quali può appunto ricondursi il trattamento in questione e che sono individuate sia dal d.lg. n. 135/1999, sia dal *Provvedimento n. 1/P/2000* del Garante (in G.U. 2 febbraio 2000, n. 26). L'Ufficio ha peraltro richiamato l'ente al rispetto del principio di pertinenza ex art. 9, legge n. 675/1996, in virtù del quale negli atti delle pubbliche amministrazioni devono essere riportati solo i dati indispensabili al raggiungimento delle finalità istituzionali.

7 Trasparenza dell'attività amministrativa

Come già evidenziato nelle precedenti relazioni, la tutela della riservatezza dei dati personali va armonizzata con le esigenze di trasparenza dell'azione amministrativa, di cui ha tenuto conto all'art. 43, comma 2, legge n. 675/1999.

Nel rinviare al successivo paragrafo una sintetica disamina di alcuni provvedimenti sul diritto d'accesso, si intende qui dar conto succintamente di alcuni chiarimenti dell'Autorità che, nel decorso anno, hanno contribuito, in diversi casi, ad offrire una chiave di lettura nel delicato bilanciamento fra esigenze di trasparenza e tutela della riservatezza.

Uno degli elementi che merita evidenziare in questa sede -e che viene a volte sottovalutato- è l'incidenza che un diverso diritto di accesso, quello introdotto dall'art. 13 della legge n. 675, ha avuto in termini di maggiore trasparenza dell'attività della p. a.

In varie occasioni, il Garante ha messo in evidenza le differenze fra i due diritti di accesso, quello previsto dal d.lg. n. 267/2000 e dalla legge n. 241 del 1990 e quello introdotto dal citato art. 13, precisando che quest'ultimo consente all'interessato di accedere solo alle informazioni che lo riguardano e che tale accesso di regola non avviene attraverso le forme previste per le prime (visione e copia). Nonostante tale più specifica area di informazioni conoscibili, l'esercizio di questo diritto da parte degli interessati ha contribuito anch'esso ad una maggiore "apertura" e trasparenza della pubblica amministrazione: si pensi, tra l'altro, agli effetti che ha avuto nei riguardi della conoscenza dei dati personali riferiti a persone decedute, nei cui confronti tale diritto può essere esercitato da chiunque vi abbia interesse (*Provv.* 22 gennaio 2003).

Nel 2002, le esigenze di trasparenza delle attività pubbliche sono venute nuovamente in evidenza in diverse situazioni, anche in riferimento alla conoscibilità di una testata giornalistica dei dati detenuti dall'INPS relativi alle contribuzioni aggiuntive versate da organizzazioni sindacali a favore di rappresentanti collocati in aspettativa non retribuita.

Al riguardo è stato preliminarmente rilevato che è prassi costante dell'Ufficio non fornire prescrizioni analitiche in caso di richieste di parere formulate da soggetti pubblici circa l'accoglibilità o meno di singole richieste di accesso a documenti. Ciò in ragione del fatto che la decisione su tali richieste pertiene alla valutazione discrezionale del soggetto pubblico, sulla base di una compiuta valutazione dello specifico quadro normativo applicabile all'ente e con possibilità di impugnazione giurisdizionale della decisione medesima.

Nel caso sottoposto è stato tuttavia brevemente osservato che l'ente previdenziale, nel valutare la richiesta della testata giornalistica, tenuto conto dell'orientamento giurisprudenziale e dell'eventuale regolamento adottato per l'applicazione della legge n. 241/1990, non sembrava incontrare ostacoli nel consentire l'accesso a dati di vario genere che ricostruissero chiaramente l'entità e le caratteristiche del fenomeno della contribuzione aggiuntiva (ammontari minimi,

massimi e medi di contribuzione; numero complessivo di interessati suddivisi per oo.ss. interessate; durata media della contribuzione; ecc.). E' stato inoltre precisato che per la conoscibilità di informazioni più dettagliate, l'ente previdenziale poteva basarsi anche sulla natura pubblica o privata dei fondi utilizzati per le contribuzioni aggiuntive anche al fine di comunicare i nomi dei beneficiari, tenendo altresì conto dell'art. 6 del codice di deontologia per l'attività giornalistica che si riferisce al diritto di cronaca in riferimento a *"persone note o che esercitano funzioni pubbliche"* (*Provv.* 23 agosto 2002).

Il tema è stato anche affrontato, sotto ulteriori profili, con la pronuncia con la quale sono stati forniti ulteriori chiarimenti in merito alla diffusione delle immagini delle sedute comunali da parte di una televisione locale. Rispondendo al quesito di un Comune, l'Autorità ha affermato che una simile eventualità deve ritenersi in generale configurabile -anche al di fuori dell'ambito locale o nel caso in cui ad esse si aggiungano 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 adottate le necessarie cautele per prevenire l'indebita divulgazione di dati sensibili, quali quelli relativi alle condizioni di salute (*Newsletter* 11-13 marzo 2002, in *www.garanteprivacy.it*).

Sempre nell'ambito dell'esigenza di trasparenza delle attività pubbliche è venuta in evidenza la delicata problematica relativa alla possibilità da parte di un comune di mettere a disposizione di varie organizzazioni sindacali e uffici giudiziari l'intera graduatoria riguardante il sostegno alle locazioni di immobili per inquilini soggetti a procedure esecutive di sfratto ed aventi nel nucleo familiare ultrasessantacinquenni o handicappati gravi.

Al riguardo si è rilevato che la selezione, e l'inserimento in graduatoria, degli inquilini beneficiari del sostegno avviene sulla base di informazioni riguardanti lo stato di salute (disabilità grave) o l'età (oltre i sessantacinque anni) di almeno uno dei componenti il nucleo familiare. Non è sembrato poi agevole estrapolare dalla graduatoria i dati sensibili relativi ai portatori di handicap da quelli relativi agli ultrasessantacinquenni in buone condizioni di salute.

In tal senso l'Autorità ha ravvisato nella diffusione dell'intera graduatoria un contrasto con la normativa sulla protezione dei dati personali, che vieta ai soggetti pubblici la diffusione dei dati idonei a rilevare lo stato di salute (art. 23, comma 4, l. n. 675/1996; art. 4, comma 4, d.lg. n. 135/1999). Lo stesso art. 13 del d.lg. n. 135/1999, che delimita il trattamento effettuato per fini di trasparenza, dei dati sensibili necessari per il riconoscimento di agevolazioni, abilitazioni e benefici di altro tipo, conferma il predetto divieto di diffusione dei dati idonei a rilevare lo stato di salute (art. 4, comma 4 d.lg. cit.: *Provv.* 13 marzo 2003).

8 Accesso ai documenti amministrativi

L'Autorità è stata nuovamente interpellata di frequente per chiarire alcuni aspetti del rapporto tra la normativa sul diritto di accesso ai documenti amministrativi e la legge n. 675/1996.

Molti interventi dell'Autorità hanno ricalcato quanto più volte ribadito circa la vigenza delle disposizioni in materia di trasparenza dell'attività amministrativa e la necessità che una compiuta valutazione dell'istanza di accesso a documenti amministrativi venga effettuata dall'amministrazione che dispone di tutti gli elementi utili ad effettuare il contemperamento fra i diversi diritti in gioco.

Fra le varie questioni segnalate degne di particolare menzione sono quelle incentrate sulla legittimità della richiesta di accedere alla documentazione riguardante l'attribuzione ai dipendenti di taluni trattamenti retributivi accessori.

Alcune di queste richieste risultano rivolte ai sensi della legge n. 241/1990 e sono generalmente presentate da persone interessate a conoscere per motivi diversi le posizioni retributive di alcuni colleghi; altre, *prima facie* non risolvibili applicando i soli principi in materia di trasparenza amministrativa, sono rivolte dalle oo.ss. all'insieme delle retribuzioni percepite dai lavoratori e, in alcuni casi, appaiono fondarsi su quanto previsto dai relativi contratti collettivi nazionali di lavoro.

In materia di dati sensibili, l'entrata in vigore del d.lg. n. 135/1999 sembra aver risolto dubbi residui circa l'applicabilità del diritto di accesso ai documenti anche nei confronti delle informazioni più delicate. L'art. 16 di tale decreto ha infatti dichiarato *"di rilevante interesse pubblico"* anche i trattamenti di dati sensibili *"necessari per far valere il diritto alla difesa in sede amministrativa o giudiziaria"* (comma 1, lett. *b)*), e quelli *"effettuati in conformità alle leggi e ai regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi"* (comma 1, lett. *c)*).

Nel caso dei dati sensibili, ovviamente, le valutazioni sul diritto di accesso devono essere effettuate con maggiore attenzione. In particolare, una fattispecie specifica si rinviene con riferimento ai dati sulla salute e sulla vita sessuale per i quali lo stesso d.lg. n. 135 prevede che consente l'accesso solo *"se il diritto da far valere o difendere ... è di rango almeno pari a quello dell'interessato"* (art. 16, comma 2).

Il tema, affrontato anche in due recenti decisioni del Consiglio di Stato (Sez. VI, n. 1882/2001 e n. 2542/2002), si è posto soprattutto con riferimento alle cartelle cliniche, che -oltre a riportare dati sensibili- contengono anche informazioni relative a varie patologie, le quali talvolta possono essere riferite anche a persone diverse dall'interessato (ad es. il caso delle anamnesi familiari).

In effetti, relativamente alla gestione di tali atti e documenti, il Garante negli ultimi tempi è stato destinatario di numerose richieste di chiarimenti circa la possibilità per le strutture ospedaliere di consentirne l'accesso -in copia (integrale o in estratto) o in visione- sulla base delle istanze formulate ai sensi della legge n. 241/1990 o degli artt. 391 *quater* e 391 *nonies* c. p.

Su tale tematica e, in particolare su quali siano i diritti da considerarsi di "rango pari" a quello dell'interessato, già nel passato l'Autorità aveva constatato (v. autorizzazione n. 6/2002, punto 1, lett. *a)*), che essi devono appartenere alla categoria dei diritti della personalità o degli altri diritti fondamentali ed inviolabili.

In materia di trasparenza amministrativa, l'Autorità ha poi ripetutamente evidenziato la piena vigenza delle disposizioni precedenti all'entrata in vigore della legge n. 675/1996, in quanto espressamente fatte salve dal suo art. 43, comma 2.

Tale vigenza è stata successivamente confermata, con specifico riferimento ai dati sensibili, dal d.lg. 11 maggio 1999, n. 135, il quale, al già menzionato all'art. 16, ha dichiarato di "rilevante interesse pubblico", fra gli altri, i trattamenti di dati sensibili *"necessari per far valere il diritto di difesa in sede amministrativa o giudiziaria"* (comma 1, lett. *b)*), e quelli *"effettuati in conformità alle leggi e ai regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi"* (comma 1, lett. *c)*).

Il secondo comma del medesimo articolo 16 ha tuttavia introdotto, seppure con una formula suscettibile di ingenerare qualche fraintendimento, un'ulteriore limitazione laddove i dati oggetto di trattamento riguardino lo stato di salute o la vita sessuale. In tali ipotesi, infatti, viene precisato che *"il trattamento è consentito se il diritto da far valere o difendere ... è di rango almeno pari a quello dell'interessato"* (art. 16, comma 2). In proposito l'Autorità ha ultimato l'istruttoria di un provvedimento volto ad individuare talune ipotesi in base alle quali il diritto da far valere o difendere si configura di rango pari a quello dell'interessato, anche in relazione ai primi casi affrontati dalla giurisprudenza.

Come già accennato, l'Autorità ha confermato il proprio positivo orientamento sulla questione relativa alla compatibilità tra la normativa sul trattamento dei dati personali e il diritto di accesso riconosciuto ai consiglieri comunali e provinciali agli atti e ai documenti delle rispettive amministrazioni locali (art. 43 d.lg. n. 267/2000, corrispondente all'art. 31, commi 5, 6 e 6 *bis*, l. n. 142/1990).

Una delle richieste presentate risultava di particolare interesse riguardando la possibilità per un assessore comunale di conoscere i nomi dei dipendenti comunali iscritti al sindacato (*Provv.* 17 febbraio 2003).

L'Autorità ha rilevato che la disciplina sull'ordinamento degli enti locali, mentre riconosce ai consiglieri comunali il diritto di ottenere dagli uffici del comune, comprese aziende ed enti collegati, ogni informazione utile all'espletamento del loro mandato, nel rispetto del segreto d'ufficio, non prevede analogo diritto per gli assessori in quanto tali. Le norme dispongono, invece, che il sindaco e i singoli assessori per gli specifici settori ad essi delegati, debbano solo

sovrintendere al funzionamento degli uffici e dei servizi e non con atti di diretta gestione, ma con direttive generali. L'ordinamento degli enti locali, infatti, prevede che si applichino le norme nella distinzione tra le funzioni di indirizzo e controllo politico-amministrativo, che spettano agli organi di governo dell'ente, e quelle di attuazione e gestione amministrativa, che spettano ai dirigenti.

Pertanto, solo nel caso in cui la richiesta di dati relativi al personale dipendente, anche di natura sensibile, è effettivamente indispensabile all'assessore per espletare la funzione di controllo politico-amministrativo sull'andamento dell'ufficio del personale, l'acquisizione dei dati può risultare conforme alle norme rilevanti in tema di protezione dei dati. Se invece sono proprio le ricordate finalità di rilevante interesse pubblico a mancare, la comunicazione di questi dati non è legittima e l'accesso da parte dell'assessore non è quindi consentito.

In tema di trasparenza sugli emolumenti pubblici, il Garante ha poi ricordato che nessuna disposizione della legge sulla tutela della riservatezza impone una segretezza al riguardo. La specifica disciplina in materia di pubblicità delle situazioni patrimoniali (leggi nn. 441/1982, 412/1991 e 127/1997) è ispirata a criteri di trasparenza. Ciò è stato evidenziato in più occasioni anche attraverso l'adozione di provvedimenti, pareri e comunicati stampa dell'Autorità dell'ultimo quinquennio, relativi ad amministrazioni statali e regionali, istituti ed enti pubblici, altri enti locali, società a capitale pubblico, aziende autonome e speciali, concessionari di servizi pubblici, dirigenti, equiparati e altri *manager* pubblici (*Comunicato* 21 gennaio 2003).

L'Autorità è intervenuta, inoltre, in numerosi altri casi nei quali si richiedeva di conoscere il rapporto tra la normativa sul diritto di accesso ai documenti amministrativi e le disposizioni che tutelano il diritto alla riservatezza dei dati personali. Si segnalano in proposito le seguenti pronunce:

- parere circa la possibilità per una persona, invalida civile, di accedere alle convenzioni tra province e aziende private, al fine di verificare il rispetto delle norme sull'assunzione delle c.d. "categorie protette" (*Provv.* 4 aprile 2003);
- parere sulla pubblicabilità nell'albo pretorio di un comune di un provvedimento con il quale si dispone l'assegnazione di un dipendente ad un altro ufficio (*Provv.* 13 gennaio 2003);
- parere in ordine alla possibilità di esporre nella bacheca di un ufficio pubblico i dati giornalieri relativi alla timbratura elettronica dell'entrata e dell'uscita del personale dipendente (*Provv.* 13 gennaio 2003);
- parere riguardante la possibilità per un comune di rilasciare ad un ufficio pubblico un elenco nominativo, completo di indirizzo, dei cittadini nati negli anni 1984-85, al fine di consentire all'ente stesso lo svolgimento di propri servizi istituzionali (*Provv.* 13 gennaio 2003);
- parere circa la possibilità per il concessionario per la riscossione dei tributi di procedere ad una serie di controlli per accertare redditi o cespiti mobiliari o immobiliari da sottoporre a procedura esecutiva per il recupero delle somme non riscosse (*Provv.* 13 marzo 2003).

9 Banche dati di rilevanti dimensioni

È stata confermata, anche nell'anno in esame, la tendenza già sottolineata nelle precedenti relazioni ad un crescente sviluppo di banche dati di grandi dimensioni, le quali -nonostante i vantaggi che esse possono comportare per l'attività amministrativa- presentano maggiori rischi nei confronti dei diritti fondamentali delle persone, specie quando risultano prive dei necessari presupposti normativi e avviate in forme non accordate fra loro.

Nel quadro delle prime iniziative in tema di *e-government*, su invito del Dipartimento per l'innovazione e le tecnologie, l'Ufficio del Garante, come anticipato nella precedente Relazione annuale, ha collaborato - per gli aspetti di propria competenza - alla redazione di un bando per progetti di *e-government* presentati nel corso del 2002 ed ha assicurato la propria disponibilità per la loro valutazione sotto il profilo del rispetto della normativa in materia di protezione dei dati personali.

Sicuramente fra le banche dati di grandi dimensioni che più hanno catalizzato l'attenzione dell'Autorità anche nel corso del 2002 figura la raccolta sistematica delle dichiarazioni di appartenenza linguistica di tutti i cittadini nella provincia di Bolzano, prevista dall'art. 18 del d.P.R. n. 752/1976.

Secondo tale disposizione, ogni cittadino di età superiore ai quattordici anni residente in quella provincia alla data del censimento generale della popolazione, è tenuto a rendere una dichiarazione individuale di appartenenza ad uno dei tre gruppi linguistici italiano, tedesco o ladino. Tale dichiarazione, sottoscritta dal dichiarante, viene ritirata dai rilevatori in busta chiusa e così conservata, a scelta del dichiarante, presso il commissariato del Governo o il comune di residenza.

Di questa disposizione si è già fatto cenno nella *Relazione per l'anno 2001*, laddove è stata evidenziata anche la valutazione non positiva del Garante nei confronti della parziale modifica legislativa intervenuta (d.lg. 18 gennaio 2002, n. 11) che, trasferendo la conservazione delle schede dai tribunali ai comuni o al commissariato del Governo, ha dato luogo ad un sistema nel quale già la scelta stessa del luogo di custodia si presta ad una possibile individuazione dell'origine etnica o delle convinzioni degli interessati, favorita anche da alcuni inviti apparsi su organi di stampa volti ad incentivare la scelta di depositare le schede presso i comuni. A seguito dell'interessamento alla vicenda da parte degli organi comunitari la materia è sotto esame ai fini delle possibili, nuove modifiche normative anche per assicurare conformità al quadro internazione e comunitario.

Per altro verso con riferimento al 14° censimento generale della popolazione, è stato rilevato che sarebbero stati trasferiti in Romania e in Croazia, per essere successivamente trattati, i dati raccolti in occasione di tale censimento. In considerazione del fatto che non è ancora

stato accertato il livello di protezione dei dati personali assicurato in questi due Paesi, il Garante è intervenuto nella vicenda e nel dicembre 2002, ha chiesto all'Istat informazioni riguardo agli adempimenti previsti dalla legge 675/1996 per il trasferimento dei dati all'estero, al fondamento giuridico delle operazioni di trattamento ivi avvenute, nonché ai rapporti intercorrenti tra l'Istituto e i soggetti operanti in tali Paesi. Il procedimento di controllo è in procinto di essere completato.

In aggiunta ai numerosi pareri forniti all'Istat allo scopo di mantenere alto il livello di tutela della riservatezza dei cittadini nell'ambito del censimento, l'Autorità ha avviato un ciclo di ispezioni e controlli, tuttora in corso di completamento, volti a verificare infine il puntuale rispetto delle indicazioni fornite.

Sempre in tema di grandi banche di dati, nel 2002 è stata promulgata la legge 30 luglio 2002, n. 189 in materia di immigrazione ed asilo, con la quale si è inteso disciplinare l'emersione del lavoro irregolare di persone extracomunitarie ai fini della legalizzazione della loro posizione.

La procedura disposta dal Ministero dell'interno ha previsto la presentazione da parte degli interessati di una dichiarazione in busta chiusa a Poste S.p.A., la quale ha avuto anche il compito di effettuare una scansione informatica delle istanze pervenute.

L'Autorità ha esaminato la circolare emanata dal Ministero dell'interno contenente disposizioni organizzative per l'attuazione di tale legge ed ha segnalato la necessità di una maggiore attenzione ai profili legati alla riservatezza delle persone coinvolte. In particolare, è stata sottolineata l'importanza di approntare idonee misure a protezione dei dati personali specie di quelli di carattere sensibile (in alcuni casi, infatti, gli interessati erano tenuti a presentare una certificazione sanitaria relativa alle persone accudite dai cittadini extracomunitari indicati per la procedura di emersione). Tali dati, secondo quanto precisato dall'Autorità, devono essere conservati nel rispetto delle disposizioni in materia di sicurezza e conservati per un periodo prestabilito.

L'Autorità ha poi chiesto chiarimenti in merito al registro informatizzato di coloro che hanno presentato l'istanza di regolarizzazione previsto dalla legge n. 189/2002, che dovrebbe peraltro contenere esclusivamente dati di carattere anagrafico. Oltre ad evidenziare la necessità di fornire adeguata informativa agli interessati in merito al trattamento dei dati raccolti, sono state esaminate le modalità di lavoro dei rappresentanti dei diversi enti coinvolti, segnalando l'opportunità di una chiara definizione della funzionalità del c.d. "sportello unico per l'immigrazione", con una precisa suddivisione delle abilitazioni all'accesso ai dati tra gli incaricati in base alle diverse attribuzioni previste dalla legge.

A seguito di tali richieste il Ministero si è attivato designando Poste S.p.A. ed i prefetti in sede responsabili per le parti di competenza, affidando loro anche il compito di individuare i rispettivi incaricati dei trattamenti.

Con particolare riferimento, poi, ai dati sensibili contenuti nelle certificazioni sanitarie da allegare alle istanze di regolarizzazione, è stato precisato che, nel dare piena attuazione alle dis-

posizioni previste dal d.P.R. n. 318/1999, tali dati saranno conservati solo in forma cartacea al fine di poterli gestire separatamente. Per quanto riguarda, invece, l'operatività del c.d. sportello unico, è stato chiarito dallo stesso Ministero che ognuno degli enti coinvolti fornisce i servizi di propria competenza, senza alcuna comunicazione di dati fra amministrazioni e nel rispetto delle proprie competenze istituzionali.

10 Carta d'identità elettronica, carta nazionale dei servizi e tessera elettorale

L'Autorità continua a seguire con particolare attenzione e in contatto con il Ministero dell'interno e le altre amministrazioni interessate, le questioni concernenti la carta di identità elettronica.

Le varie questioni via via esaminate sono state riassunte anche in occasione di iniziative pubbliche cui ha preso parte l'Autorità.

Il Prof. Gaetano Rasi, componente dell'Autorità, in un seminario organizzato nell'ambito del COM-PA, ha ad esempio richiamato l'attenzione sulla necessità di selezionare in una prospettiva di 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 (v. Newsletter del 16/22 settembre 2002). Nel corso di un analogo seminario svoltosi anch'esso al COM-PA, il Segretario generale dell'Autorità ha in particolare evidenziato i rischi e le varie problematiche pratiche derivanti dall'inserimento nella carta d'identità elettronica delle impronte digitali (v. comunicato stampa 18 settembre 2002), tenuto anche conto della remota, ma pur sempre configurabilità di una riproduzione illecita di tali impronte e di una loro ipotetica utilizzazione illecita, a detrimento anche dell'attività investigativa che si basa molto su questi elementi di prova.

Se l'apparente accantonamento del progetto di un'apposita tessera sanitaria unica ha segnato una positiva pausa di riflessione sul fronte della proliferazione delle carte "pubbliche" contenenti dati sulla salute, non si può manifestare pari ottimismo sul fronte "privato", dove prosegue la moltiplicazione di "carte" dedicate a particolari categorie di pazienti o a determinate patologie. Una tale proliferazione rende ovviamente più difficoltoso un quadro in cui si possa tenere adeguatamente conto dei profili attinenti alla riservatezza ed alla dignità della persona.

I progetti della carta d'identità elettronica e della carta nazionale dei servizi, congiuntamente alla firma digitale, sono attualmente individuati nelle politiche di *e-government* quali strumenti attraverso i quali i cittadini potranno utilmente avvalersi della rete per usufruire di nuovi servizi erogati per via telematica dalle amministrazioni pubbliche. Tali tematiche, tra l'altro, rientrano tra i progetti di emissione di una carta nazionale dei servizi, introdotta nell'ordinamento dall'articolo 8 del decreto legislativo 23 febbraio 2002 n. 10, in attuazione della direttiva 1999/93/CE in materia di firme elettroniche.

In questa prospettiva il Garante si accinge ad esprimere il parere richiesto da ultimo su uno schema di provvedimento attuativo volto a facilitare l'introduzione della carta e, in questa sede, si riserva di formulare sull'ultima versione disponibile dello schema alcune doverose riflessione sugli usi non proporzionati dei dati personali che potrebbero essere ipotizzati a vario

scopo, anche a fini di contenimento della spesa sanitaria. Ciò in utile e proficua cooperazione con gli uffici del Ministro per l'innovazione e le tecnologie, ma ponendo in chiara luce gli obiettivi limiti che la disciplina internazionale e comunitaria pone al riguardo.

L'istituzione della carta d'identità elettronica e la connessa ipotesi di sostanziale trasformazione del codice fiscale in un identificativo generale, pone delicati profili di compatibilità con la disciplina prevista dalla direttiva 95/46/CE, nella parte in cui questa dispone che gli Stati membri determinino in base a quali garanzie e condizioni un numero nazionale di identificazione o qualsiasi altro mezzo identificativo di portata generale può essere oggetto di trattamento.

Come evidenziato dal presidente del Garante (nell'ambito della audizione della Commissione parlamentare di vigilanza sull'anagrafe tributaria del 6 novembre 2002) si impone la necessità di specificare, attraverso uno o più atti normativi, le condizioni per cui un tale sistema identificativo generale potrà essere utilizzato per il trattamento delle informazioni. Identica importanza andrà attribuita alla salvaguardia del principio di finalità, da ravvisarsi in una corrispondenza tra il fine per il quale si ricorre all'identificativo generale e il tipo dei dati utilizzati; nonché alla garanzia della riservatezza e segretezza nelle modalità di utilizzazione, trasmissione e accesso ai dati che tale identificativo generale consentirà.

Appare evidente come, nell'ambito dei progetti della carta d'identità elettronica e della carta nazionale dei servizi, particolare delicatezza viene ad assumere la definizione -sulla base ed in conseguenza di una totale partecipazione degli enti locali al processo di aggiornamento dell'Indice nazionale delle anagrafi- di un sistema integrato delle anagrafi di tutti i comuni italiani che, oltre ad assicurare, attraverso l'utilizzo di una chiave di ricerca univoca individuata nel codice fiscale, la piena circolarità dell'informazione anagrafica detenuta dall'ente locale e le relative variazioni, può consentire la verifica e l'allineamento delle informazioni delle anagrafi comunali con il contenuto dell'anagrafe tributaria.

La stessa commissione parlamentare di vigilanza sopra richiamata, nella relazione conclusiva del 12 dicembre 2002, ha ritenuto che "nel processo in corso di utilizzo dello strumento informativo per la semplificazione del rapporto tra cittadino e «pubbliche amministrazioni» sarà altresì compito della Commissione - intendendosi recepire in tal senso anche le indicazioni formulate dall'Autorità garante per la *privacy* e nel quadro di una partecipazione attiva secondo lo spirito della legge n. 675 del 1996 con riguardo alla tutela della dignità e libertà delle persone coinvolte nel trattamento dei dati personali - dotarsi di un nuovo *habitus* nell'esercizio delle proprie funzioni istituzionali, vigilando anche affinché, ove presenti implicazioni di materia tributaria, sia l'istituzione dei documenti elettronici (con particolare riferimento alla carta d'identità elettronica), sia l'interconnessione tra le varie istituzioni per lo scambio e la verifica delle informazioni elettroniche, non comportino il rischio di menomare i principi di riservatezza dei dati personali, con evidente, particolare riguardo ai dati sensibili, ed intervenendo nella valutazione delle finalità sottese alla loro accessibilità ed utilizzazione.".

Una recente novità in materia di utilizzo della carta nazionale dei servizi è stata introdotta dall'art. 52 della legge 27 dicembre 2002, n. 289. Tale disposizione prevede che, al fine di potenziare il processo di attivazione del monitoraggio delle prescrizioni mediche, farmaceuti-

che, specialistiche e ospedaliere, di contenere la spesa sanitaria, nonché di accelerare l'informatizzazione del sistema sanitario e dei relativi rapporti con i cittadini e le pubbliche amministrazioni e gli incaricati dei pubblici servizi, il Ministro per l'innovazione e le tecnologie (di concerto con il Ministro dell'economia e delle finanze, il Ministro della salute, il Ministro dell'interno, e sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano), stabilisce le modalità per l'assorbimento della tessera recante il codice fiscale nella carta nazionale dei servizi e per la progressiva utilizzazione della carta medesima ai fini sopra descritti.

In materia di tessera elettorale, nonostante i solleciti formulati dall'Autorità per un complessivo riesame della materia, continua a rimanere in vigore la normativa concernente la tessera elettorale cartacea, sulla quale il Garante ha nel passato espresso un giudizio assai critico in ragione della conoscibilità dei dati relativi al comportamento elettorale degli interessati che può realizzarsi attraverso il suo uso.

Le dichiarazioni rese nel maggio 2002 dai Ministri dell'interno e per l'innovazione e le tecnologie, i quali hanno definito lo strumento in questione ormai obsoleto e ribadito la necessità di una sollecita introduzione del supporto informatico, fanno sperare che tale questione possa essere risolta in tempi brevi tenendo conto anche delle considerazioni a suo tempo formulate dal Garante.

In occasione della predisposizione da parte del Ministero dell'interno di taluni emendamenti al testo dello schema di provvedimento legislativo recante *"Nuove norme per l'esercizio del diritto di voto da parte degli elettori affetti da grave infermità"* (v. legge 5 febbraio 2003, n. 17), il Garante ha inoltre espresso il richiesto parere (5 febbraio 2003) fornendo indicazioni per evitare l'annotazione di dati relativi allo stato di salute nel documento di identità. Tale misura non appariva giustificata rispetto ai concorrenti principi generali in materia di tutela della riservatezza, tra i quali si colloca quello della pertinenza e non eccedenza dei trattamenti di dati personali rispetto alle finalità perseguite (art. 9, c. 1, lett. *d)*, l. n. 675/1996). Tenendo conto del predetto parere dell'Autorità, la legge n. 17/2003, modificando l'art. 55 del testo unico di cui al d.P.R. n. 361 del 1957, e l'art. 41 del testo unico di cui al d.P.R. n. 570 del 1960, ha aggiunto il seguente comma:

> *"L'annotazione del diritto al voto assistito, di cui al secondo comma, è inserita, su richiesta dell'interessato, corredata della relativa documentazione, a cura del Comune di iscrizione elettorale, mediante apposizione di un corrispondente simbolo o codice, nella tessera elettorale personale, nel rispetto delle disposizioni vigenti in materia di riservatezza personale ed in particolare della legge 31 dicembre 1996, n. 675, e successive modificazioni".*

11 Documentazione anagrafica e materia elettorale

Sono rimaste numerose le richieste di chiarimenti rivolte all'Autorità da enti locali e privati cittadini in ordine al trattamento di dati contenuti in atti anagrafici, dello stato civile e nelle liste elettorali.

Con riferimento alle liste anagrafiche ed elettorali relative a cittadini italiani residenti all'estero, nell'ambito della collaborazione con il Ministro per gli italiani nel mondo, l'Autorità ha reso il proprio parere (17 settembre 2002) su uno schema di decreto del Presidente della Repubblica recante il regolamento di attuazione della legge n. 459 del 27 dicembre 2001 ("*Norme per l'esercizio di voto dei cittadini italiani residenti all'estero*"), ponendo in evidenza diversi profili critici.

In primo luogo, è stata evidenziata l'esigenza di verificare l'effettiva necessità di indicare nel tagliando elettorale (che deve essere inviato all'ufficio consolare competente unitamente alla scheda elettorale sulla quale il cittadino ha espresso la propria preferenza) dati che consentano di risalire direttamente ed immediatamente all'identità dell'elettore. A tal fine è stato suggerito di apporre sul tagliando solo un numero o un codice corrispondente alla posizione del singolo, al fine di garantire meglio la segretezza del voto.

In relazione, poi, alla previsione di realizzare un "elenco aggiornato" dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle liste elettorali, è stata sottolineata la necessità che la legge specifichi quali dati debbano confluirvi, considerato anche che gli archivi già esistenti contengono informazioni non necessarie all'esercizio del diritto di voto (ad esempio, le anagrafi degli italiani residenti all'estero riportano l'indicazione dell'anno di espatrio e la motivazione di iscrizione all'AIRE, mentre gli schedari consolari "*anche degli atti o fatti che producono o possono produrre la perdita della cittadinanza o dei diritti civili ... nonché di ogni altro elemento utile ai fini della tutela degli interessi del connazionale*"). Ciò anche al fine di garantire che il nuovo trattamento rispetti i princìpi di pertinenza e non eccedenza previsti dall'art. 9 della legge n. 675/1996.

Con il medesimo parere è stato inoltre rilevato che la previsione di una rete telematica di scambio di informazioni anagrafiche ed elettorali tra uffici consolari, Ministero degli affari esteri, Ministero dell'interno e comuni, non essendo stata prevista dalla legge n. 459/2001 e neanche dalla successiva legge n. 104 del 27 maggio 2002, non poteva essere introdotta da un "decreto di attuazione", come nel caso di specie.

Sul tema il Garante è intervenuto anche per soddisfare due ulteriori richieste di chiarimenti. Nel primo caso (20 marzo 2003) un soggetto privato (un patronato che svolge attività a favore dei connazionali residenti in un paese comunitario) aveva chiesto all'ambasciata italiana gli elenchi degli iscritti all'anagrafe consolare, al fine di inviare loro una nota esplica-

tiva sulle nuove norme. Nel secondo caso (14 gennaio 2003), un comune formulava un quesito in merito alla possibilità di rilasciare ad un "Centro pari opportunità" alcuni dati personali della popolazione femminile residente.

In entrambe le ipotesi è stata esclusa la possibilità di mettere a disposizione i dati personali posseduti ai soggetti privati richiedenti. Tuttavia, nel primo caso, è stato osservato che resta comunque salva la possibilità per la stessa ambasciata italiana, in considerazione dei fini di *"pubblica utilità"* dell'iniziativa e delle funzioni istituzionali che le sono attribuite, di assumere il patrocinio del progetto e, con atto convenzionale, di affidare al patronato i compiti connessi alla realizzazione dell'iniziativa. Facendo ciò, l'ambasciata avrebbe potuto eventualmente designare formalmente il patronato quale responsabile del trattamento ai sensi dell'art. 8 della legge n. 675/1996 impartendogli per iscritto le necessarie indicazioni per procedere al trattamento dei dati nel rispetto della normativa in vigore. Altrimenti, l'ambasciata avrebbe potuto preferibilmente curare direttamente l'iniziativa ipotizzata dal patronato.

Per quanto attiene agli interventi relativi all'utilizzo dei dati nell'ambito delle norme riguardanti gli atti anagrafici, sono state fornite indicazioni ad un comune (13 gennaio 2003) in ordine alla possibilità di rilasciare all'ACI un elenco nominativo, completo di indirizzo, dei cittadini, al fine di consentire allo stesso ente automobilistico *"una gestione più corretta dei propri servizi istituzionali"*. In tal caso è stato precisato che il rilascio degli elenchi degli iscritti all'anagrafe della popolazione residente è previsto unicamente nei confronti di pubbliche amministrazioni che ne facciano richiesta per motivi di pubblica utilità. Data la natura pubblica dell'ACI, l'ente locale deve valutare l'esistenza delle ragioni di pubblica utilità, ragioni che, ad un primo esame, sono sembrate ricorrere.

In un altro caso (28 gennaio 2003) l'Autorità, interessata da un Comune in ordine alla possibilità di fornire ad un privato un estratto delle liste elettorali in forma aggregata, ha rilevato che, dato anche il regime di pubblicità di tali liste, la questione pareva riguardare non tanto la liceità della trasmissione di quei dati quanto, piuttosto, l'effettuazione - ad esclusivo vantaggio del soggetto privato - di un'attività non prevista dall'ordinamento.

Un'ulteriore questione sottoposta all'Autorità da un comune ha riguardato la possibilità di ottenere dalla locale azienda energetica una verifica dei nominativi elencati in un tabulato relativo a persone che avevano eletto domicilio presso il palazzo civico, al fine di aggiornare i registri anagrafici.

Tale attività è stata considerata (28 gennaio 2003) lecita essendo assistita dalla previsione di cui all'art. 4 della legge n. 1228/1954, la quale, ai commi 2 e 3, prevede che l'Ufficiale d'anagrafe possa ordinare *"gli accertamenti necessari ad appurare la verità dei fatti denunciati dagli interessati, relativi alle loro posizioni anagrafiche"*, potendo interpellare, per lo stesso fine, anche *"enti, amministrazioni ed uffici pubblici e privati"*.

Un tema delicato è stato affrontato con un intervento (7 novembre 2002) sollecitato da una segnalazione, nei confronti di una pubblica amministrazione per segnalare l'inopportunità di indicare lo stato di vedovanza nella corrispondenza inviata dallo stesso ente pubblico ad una cittadina. Sul punto la medesima amministrazione ha assicurato che si era trattato di

un mero errore materiale e di aver predisposto idonee misure atte ad evitare il ripetersi di tali incresciosi episodi.

Con un parere reso il 5 febbraio 2003, il Garante è tornato nuovamente sul tema del diritto di accesso alla documentazione relativa alle consultazioni elettorali per il rinnovo di un consiglio comunale. Nel caso in esame il diritto veniva esercitato da un elettore che aveva instaurato un procedimento giurisdizionale dinanzi al tribunale volto a conoscere gli atti relativi alla presentazione delle liste dei candidati elettore al quale è stato riconosciuto il diritto di accesso.

12 Istruzione

Un altro settore d'indagine oggetto di attenzione nel corso del 2002 è stato quello concernente la tutela della riservatezza in ambito scolastico, che coinvolge spesso persone minori di età.

Tra le questioni sottoposte all'attenzione dell'Autorità si ritiene opportuno citare il caso di un istituto scolastico parificato, che ha formulato un quesito in merito alla possibilità di ottenere dal comune l'elenco nominativo, completo di indirizzo, dei minori residenti, al fine di promuovere alcune offerte scolastiche.

In tale occasione, è stato rilevato (16 gennaio 2003) che, ferma restando la disciplina dettata per la pubblicità delle liste elettorali contenuta nell'art. 51 del d.P.R. 20 marzo 1967, n. 223 (secondo cui i soggetti pubblici e privati possono ottenere copia delle liste elettorali tenute dal Comune), il rilascio degli elenchi degli iscritti all'anagrafe della popolazione residente è consentito, per motivi di pubblica utilità, solamente nei confronti delle pubbliche amministrazioni che ne facciano motivata richiesta e non anche verso soggetti privati, tra i quali doveva ricomprendersi l'istituto scolastico parificato.

In un altro caso è stato fornito un riscontro ad un quesito (28 ottobre 2002) in merito alla possibilità per un istituto scolastico di comunicare alle famiglie i nominativi degli alunni iscritti ad un corso di disassuefazione dal fumo.

Al riguardo, è stato preliminarmente rilevato che tali tipi di informazioni, in determinate circostanze e condizioni, potrebbero risultare idonei a rivelare lo stato di salute dei soggetti interessati.

Nel caso specifico, è stato rilevato che la procedura seguita dall'istituto scolastico poteva essere effettuata in maniera più rispettosa della riservatezza degli alunni. In particolare, qualora i corsi in questione fossero stati tenuti al di fuori del normale orario scolastico, con conseguente necessità di indirizzare alle famiglie una richiesta di autorizzazione alla loro frequentazione, sarebbe stato opportuno riportare nella richiesta di autorizzazione non la specifica menzione dell'oggetto del corso, bensì la sua generica finalità (ad esempio, corso finalizzato "all'educazione alla salute e alla prevenzione"). Di tale comunicazione, in ogni caso si sarebbe dovuta dare informazione preventiva agli interessati in modo da consentire loro di tutelare la riservatezza e l'anonimato così come disposto anche dalle specifiche norme di settore

Un altro aspetto interessante è stato affrontato in occasione della risposta ad un quesito concernente la possibilità di considerare i c.d. "debiti formativi" degli alunni quali dati personali "sensibili", nonché relativamente alla liceità della pubblicazione di tali informazioni nell'albo degli istituti scolastici.

In proposito è stato rilevato (20 dicembre 2002) che tale genere di informazioni, senz'altro considerabili quali dati personali, non sono da ricondursi a quelli di natura sensibile. Al riguardo è stato altresì precisato che, se pur la normativa sulla riservatezza non vieta la comunicazione dei risultati degli scrutini, il punteggio attribuito quale "credito scolastico" a ciascun alunno deve essere *"pubblicato sull'albo dell'Istituto, unitamente ai voti conseguiti in sede di scrutinio finale e trascritto sulla pagella scolastica"*, mentre l'indicazione dell'eventuale promozione con "debito formativo" va indicata solo su questo ultimo documento (art. 14, comma 5, d.m. n. 90/2001, ribadito anche dal d.m. n. 56/2002).

Un'ulteriore questione affrontata ha riguardato la segnalazione di un cittadino che lamentava la diffusione, da parte di alcuni insegnanti, di informazioni relative alla salute della propria figlia.

Il lungo tempo trascorso e l'assenza di elementi probatori, tenuto anche conto della parziale discordanza delle versioni dei fatti riferite dalle parti, ha impedito, nel caso di specie, di assumere puntuali provvedimenti. L'Autorità ha tuttavia richiamato l'Istituto a conformare in futuro i trattamenti di dati personali svolti alle norme e ai principi introdotti dalla normativa sulla riservatezza (ribaditi, con specifico riferimento all'ambito scolastico, dal d.P.R. n. 249/1998 il quale, all'art. 2 comma 2, prevede che la comunità scolastica tuteli "*il diritto dello studente alla riservatezza*").

Un delicato problema è stato affrontato in occasione dell'esame di un quesito in merito alla legittimità della trasmissione effettuata da una direzione didattica di una nota - ritenuta riservata - ad una persona non direttamente coinvolta in una procedura di conciliazione obbligatoria.

In tal caso è stata rilevata (20 gennaio 2003) l'illiceità di tale comunicazione di dati personali poiché era stata effettuata in mancanza di una specifica norma di legge o di regolamento che, ai sensi dell'art. 27 della legge n. 675/1996, legittimasse il soggetto pubblico a comunicare i dati personali a soggetti privati.

13 Canone radiotelevisivo

Il trattamento dei dati personali connesso alla gestione e alla riscossione del canone di abbonamento al servizio radiotelevisivo è stato oggetto di esame da parte del Garante già nel corso dei precedenti anni (cfr. *Relazioni 2000 e 2001*, rispettivamente pp. 21 e 28). Al termine di una complessa istruttoria avviata nel febbraio 2001 e sollecitata anche da alcuni organi di informazione e associazioni di consumatori, il Garante, con provvedimenti del 5 dicembre 2001 e del 30 gennaio 2002, è intervenuto nei confronti della Rai e dell'Agenzia delle entrate stabilendo che in assenza di specifiche disposizioni normative a riguardo, non si possono raccogliere e trattare dati personali mediante accordi -con rivenditori di apparecchi televisivi e noleggiatori di videocassette- che prevedano rimborsi spese e premi per la cessione di dati.

L'Autorità ha rilevato che, se per rendere più efficace la lotta all'evasione del canone si riterrà necessaria la collaborazione dei rivenditori, questa dovrà essere prevista da una specifica normativa conforme anche alla legge n. 675, sulla base di scelte riservate al Parlamento e al Governo.

La mancanza di una normativa *ad hoc*, a parere del Garante, non può essere superata dal consenso degli acquirenti, dal momento che la legge n. 675/1996 esclude che i soggetti pubblici possano supplire con tale espediente -estraneo al contesto dei trattamenti di dati in ambito pubblico- alla mancanza di fondamenti normativi. La natura pubblica del trattamento di dati effettuato, in qualità di responsabile del trattamento, dalla Rai era, del resto, stata già riconosciuta in un provvedimento del Garante del luglio 2000: in quanto, appunto, "responsabile" del trattamento dei dati contenuti nell'archivio informatico degli abbonati, la Rai collabora con l'amministrazione finanziaria nello svolgimento dei compiti relativi alla gestione e alla riscossione dei canoni, e non può quindi essere considerata alla stregua di un soggetto privato che decide autonomamente in materia, dovendo in realtà attenersi alle prescrizioni normative e alle istruzioni impartite dall'amministrazione finanziaria.

Alla società deve applicarsi quindi il regime previsto per le amministrazioni pubbliche le quali possono effettuare solo i trattamenti di dati connessi all'esercizio delle proprie funzioni istituzionali, nei limiti stabiliti dalle previsioni di legge o di regolamento e senza richiedere il consenso degli interessati.

In base a tali considerazioni, il Garante ha stabilito che il particolare tipo di trattamento di dati personali svolto nel caso di specie dalla Rai per conto dell'amministrazione finanziaria non sia consentito e che pertanto cessino le specifiche operazioni di raccolta in corso dei dati relativi ai clienti di imprese e società di rivendita, fabbricazione e importazione di apparecchi televisivi e di vendita o noleggio di videocassette.

Avverso i provvedimenti del Garante, sia la società concessionaria, sia l'Agenzia delle entrate 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.

14 Enti Locali

Con l'introduzione del Sistema di accesso e interscambio anagrafico (SAIA), è stato sviluppato lo scambio telematico di dati e informazioni relative alle variazioni anagrafiche tra i comuni e tra questi e gli altri enti pubblici, al fine della eliminazione del rilascio di certificazioni anagrafiche e per il migliore espletamento dei compiti di vigilanza attribuiti al Ministero dell'interno.

Il fulcro del SAIA è costituito dall'Indice nazionale delle anagrafi (INA), istituito con il d.l. 27 dicembre 2000, n. 392, convertito in legge 28 febbraio 2001, n. 26. L'indice contiene nome, cognome, codice fiscale e ultima residenza delle persone iscritte in anagrafe, consentendo l'individuazione del comune al quale richiedere i dati di interesse istituzionale.

La rilevante incidenza di quest'ultima innovazione sull'ordinamento anagrafico, e l'ampia individuazione dei soggetti legittimati ad accedere all'Indice, avevano originato l'esigenza, espressamente contenuta nella previsione legislativa, che ai fini dell'adozione del decreto del Ministro dell'interno per la gestione dell'INA, fosse sentito il Garante per la protezione dei dati personali.

Con il decreto del Ministero dell'interno 23 aprile 2002, n. 513, è stato costituito il Centro nazionale per i servizi demografici presso il Dipartimento per gli affari interni e territoriali, competente, fra l'altro, in ordine alle funzioni connesse alla gestione dei processi di autenticazione e convalida dei dati anagrafici, alla gestione, all'aggiornamento e alla consultazione dell'Indice nazionale delle anagrafi, alla gestione del Centro servizi anagrafi del Sistema di accesso e interscambio anagrafico. Su questi temi, in relazione anche agli obblighi di consultazione previsti dall'art. 31, comma 2, della legge n. 675/1996 è necessario che prosegua una stretta cooperazione con il Ministero dell'interno.

Anche con specifico riguardo agli enti locali è stato affrontato con il citato provvedimento del 17 gennaio 2002 (in *Bollettino* n. 24, p. 40) il delicato problema della mancata adozione dei regolamenti previsti dal d.lg. n. 135/1999 in materia di utilizzo di dati sensibili.

La percezione di una diffusa mancata applicazione della normativa in materia in ambito locale ha indotto l'Autorità, come si è già avuto modo di ricordare, a disporre un ciclo di ispezioni presso alcuni comuni estratti a sorte.

L'esito di tali accertamenti (effettuati in diverse parti del territorio nazionale e su enti di diversa dimensione) ha confermato le impressioni iniziali. A parte un caso di assoluta mancanza di ogni atto o procedura connessa alla normativa sulla riservatezza, la maggior parte degli enti ha mostrato un'applicazione non completamente corretta dei precetti della legge n. 675/1996 e del d.lg. n. 135/1999.

Sebbene siano risultate generalmente applicate le misure di sicurezza stabilite dal

d.P.R. n. 318/1999, nessun Comune fra quelli ispezionati ha adottato ancora gli idonei atti regolamentari previsti dal citato d.lg. n. 135.

Tale stato di cose ha indotto l'Autorità anche ad intensificare i propri sforzi nella già avviata collaborazione con l'ANCI (Associazione Nazionale Comuni Italiani) e l'UPI (Unione delle Province Italiane) al fine di redigere uno schema di regolamento da mettere poi a disposizione degli enti locali tramite i rispettivi siti *web* istituzionali.

È proseguita nel corso dell'anno anche la collaborazione con le Regioni riunite nell'ambito della Segreteria della Conferenza dei Presidenti; in tal caso più che alla predisposizione di uno schema di regolamento (anche in considerazione del precedente della Regione Toscana), l'Autorità intende fornire, ove richiesta, assistenza per l'adozione di schemi regolamentari.

Tra gli altri atti adottati nel corso dell'anno, si cita, anche una risposta a quesito del Comune di Milano in merito ai soggetti legittimati a richiedere i certificati di destinazione urbanistica utilizzati negli atti tra vivi aventi ad oggetto il trasferimento, la costituzione o lo scioglimento di diritti reali relativamente a terreni (6 febbraio 2003).

Un altro aspetto è stato affrontato in occasione dell'esame della richiesta di parere del Comune di Vicenza relativa alla possibilità di comunicare ad un assessore comunale che ne aveva fatto richiesta, i nomi dei dipendenti comunali iscritti al sindacato con l'indicazione della relativa sigla sindacale. L'Autorità ha rilevato che, se non è indispensabile per una precisa finalità di interesse pubblico, l'assessore comunale non può conoscere i nomi dei dipendenti comunali iscritti al sindacato. L'iscrizione ad una determinata sigla sindacale, infatti, costituisce un dato di natura sensibile, sottoposto a specifica tutela.

Nel caso in esame, come già accennato, è stato precisato che la disciplina sull'ordinamento degli enti locali, mentre riconosce ai consiglieri comunali il diritto di ottenere dagli uffici del Comune, comprese aziende ed enti collegati, ogni informazione utile all'espletamento del loro mandato, nel rispetto del segreto d'ufficio, non prevede analogo diritto per gli assessori in quanto tali. Le norme dispongono, invece, che il sindaco e i singoli assessori per gli specifici settori ad essi delegati, debbano solo sovrintendere al funzionamento degli uffici e dei servizi e non con atti di diretta gestione, ma con direttive generali. Pertanto, solo nel caso in cui la richiesta di dati relativi al personale dipendente, anche di natura sensibile, sia effettivamente indispensabile all'assessore per espletare la funzione di controllo politico-amministrativo sull'andamento dell'ufficio del personale, l'acquisizione dei dati potrebbe risultare configurabile.

Un profilo estremamente delicato è infine stato affrontato in sede di decisione su un ricorso presentato all'Autorità da un dipendente comunale in relazione al trattamento di alcuni dati personali contenuti in certificati formati ed esibiti in giudizio dal Comune presso il quale il ricorrente presta servizio, nell'ambito di una causa civile che vedeva coinvolti l'ente stesso e il coniuge del ricorrente. Nel dichiarare infondato il ricorso, l'Autorità ha rilevato che la formazione e l'esibizione dei certificati comportavano un trattamento di dati personali lecito e finalizzato al legittimo esercizio del diritto di difesa dell'ente nel quadro delle relative finalità istituzionali, rispetto a profili per i quali il ricorrente non aveva fornito idonei elementi di valutazione tali da porre in dubbio che l'attività difensiva fosse svolta in contrasto con la legge n. 675/1996

Attività giudiziarie e di polizia

15 Profili generali

Alcuni trattamenti svolti in ambito pubblico sono temporaneamente sottratti all'ambito applicativo di alcune disposizioni in materia di protezione dei dati personali. Ci si riferisce, in particolare, ai trattamenti effettuati per ragioni di giustizia, per finalità di prevenzione e repressione dei reati, a quelli relativi a dati memorizzati o destinati a confluire nel Centro elaborazione dati del Dipartimento della pubblica sicurezza, nonché ai trattamenti effettuati dai servizi di informazione e di sicurezza (art. 4, l. n. 675/1996).

In relazione invece alle disposizioni della legge n. 675 già applicabili, in particolare quelle attinenti ai requisiti di liceità e alla sicurezza dei trattamenti di dati personali, gli uffici giudiziari o di polizia devono, in particolare, rispettare anch'essi il principio di "proporzionalità" nel trattamento dei dati (in base al quale, fra l'altro, si possono trattare solo i dati *"pertinenti ... e non eccedenti"* rispetto alle finalità istituzionali, secondo quanto previsto dall'art. 9, l. n. 675/1996) e adottare le cautele necessarie a garantire la sicurezza dei dati trattati (art. 15, commi 1 e 2, l. n. 675/1996 e d.P.R. n. 318/1999 sulle misure minime di sicurezza).

Come anticipato nella prima parte della presente Relazione, nell'ambito della ridefinizione in termini più ampi del contesto della delega, la previsione dell'emanazione entro il 30 giugno 2003 di un testo unico delle disposizioni normative in materia di protezione dei dati personali renderà possibile introdurre integrazioni e modifiche di coordinamento o finalizzate alla migliore attuazione della disciplina vigente, anche in settori, come quelli relativi alle attività giudiziarie e di polizia, nei quali è particolarmente avvertita l'esigenza di completare il percorso previsto dalla leggi delega che si sono succedute dal 1996 ad oggi.

Nelle more dell'armonizzazione del quadro normativo, il Garante, per i trattamenti in questione, ha ribadito e sviluppato anche nel corso del 2002 alcuni principi normativi, in parte già applicati in precedenti provvedimenti, tra i quali quello, richiamato, di "pertinenza e non eccedenza" del trattamento rispetto alle finalità istituzionali.

16 Trattamento di dati nell'ambito dell'attività giudiziaria

Come già riportato nella Relazione per il 2001, il Garante, in sede di decisione su un ricorso (*Provv.* 27 marzo 2002, in *Bollettino* n. 26, p. 3), ha affermato che il trattamento di dati svolto da un professionista sanitario che agisce in qualità di collaboratore del consulente tecnico d'ufficio nominato dal giudice è svolto *"per ragioni di giustizia, nell'ambito di uffici giudiziari"* (art. 4, comma 1, lett. *d)*, l. n. 675/1996). In tal caso, non può trovare quindi, applicazione il procedimento relativo al ricorso all'Autorità regolato dall'art. 29 della legge n. 675/1996.

Nell'ambito delle diverse iniziative dell'Autorità sul tema dei trattamenti di dati personali a fini di giustizia sono da ricordare, inoltre:

- il parere espresso dall'Autorità, ai sensi dell'art. 31, c. 2, della l. n. 675/1996, sullo schema di regolamento recante il testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti (d.P.R. 14 novembre 2002, in suppl. G.U. n. 36 del 13 febbraio 2003);
- il parere del 28 maggio 2002 con il quale è stato precisato che configura un trattamento di dati a fini personali (art. 3 l. 675/1996) la comunicazione -effettuata da parte dell'ex coniuge- di dati personali anche sensibili riferiti alla controparte, ad uffici o organi giudiziari, per esigenze di difesa di propri diritti. Sul punto sono stati ricordati i principi contenuti nell'autorizzazione generale n. 2/2002 relativa al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale svolto per far valere o difendere un diritto in sede giudiziaria, sempre che il diritto sia di rango pari a quello dell'interessato e i dati siano trattati esclusivamente per tale finalità;
- il parere dell'11 marzo 2003 in merito alla possibilità per la Camera arbitrale presso l'Autorità per la vigilanza sui lavori pubblici di rilasciare a privati, per motivi di studio o per la pubblicazione su riviste giuridiche, copia dei lodi pronunciati dai collegi arbitrali costituiti presso la Camera arbitrale prima che intervenga il decreto del tribunale che ne dispone l'esecutività.

17 Notificazione di atti e comunicazioni

Anche nel corso dell'anno preso in considerazione sono pervenute numerose segnalazioni da parte dei cittadini, volte a denunciare modalità non corrette o inidonee di notificazione di atti giudiziari ed amministrativi.

L'Ufficio, nelle more dell'auspicata modifica normativa, ha ricordato in diverse occasioni le specifiche indicazioni già fornite sull'argomento (*Provv.* 22 ottobre 1998 e del 26 ottobre 1999). E' stato così ribadito che la legge n. 675/1996 non ha 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- a terzi non interessati alla vicenda giudiziaria (portieri di stabili, capi di uffici e di aziende, comandanti di corpo militare, ecc.).

Le richieste di tutela formulate da numerosi cittadini evidenziano la necessità di operare un'armonizzazione della complessiva disciplina sulle notificazioni di atti con la normativa in materia di protezione dei dati personali, al fine di garantire in modo effettivo la dignità e la riservatezza di ciascun individuo e, al contempo, di prevenire incidenze negative sull'amministrazione della giustizia e sullo svolgimento di altre funzioni pubbliche.

Relativamente alle accennate modifiche normative, è all'esame della Commissione giustizia del Senato il disegno di legge AS 556 volto a modificare le norme in materia, il quale prevede, tra l'altro, che nel caso in cui la notificazione non possa essere eseguita nelle mani del destinatario, la consegna o il deposito della copia dell'atto da notificare avvengano da parte delle persone incaricate della notificazione in busta sigillata.

Un'ulteriore proposta di legge (AC 2229), riguardante *"Modifiche urgenti al codice di procedura civile"*, è stata presentata in data 25 gennaio 2002 ed è stata, di recente, oggetto di relazione (26 marzo 2003).

Nelle more dell'esame di tali norme, l'Autorità ha richiamato gli enti interessati al rispetto della disciplina vigente, laddove essa consente già modalità più aderenti alla normativa sulla riservatezza.

In particolare, in materia di notificazioni di atti tributari (cartelle esattoriali, avvisi di mora, di accertamento, ecc), il Garante ha ritenuto possibile già oggi utilizzare il sistema della notificazione per posta, salvi i divieti espressi di legge o i casi in cui la notificazione deve essere eseguita personalmente (art. 149 c.p.c. e art. 1, l. 890/1982). Un maggiore utilizzo di tale modalità è auspicabile, secondo l'Autorità, in considerazione del limitato numero di indicazioni riportate nella parte esterna della busta, anche in relazione a quanto disposto dalla legge 146/1998 che prescrive l'impiego del plico sigillato per la notifica mezzo posta quale ordina-

ria forma di comunicazione degli atti dell'amministrazione finanziaria.

Ancora nell'ambito delle prestazioni di natura tributaria, l'Ufficio si è espresso nel senso che non configura una violazione della riservatezza l'indicazione di dati relativi al coniuge negli avvisi di accertamento delle dichiarazioni dei redditi effettuate congiuntamente, poiché tale sorta di dichiarazione rappresenta una facoltà dei contribuenti con i connessi benefici ed oneri.

18 Attività di polizia

Anche nel 2002 ha assunto rilievo il profilo dei controlli sui trattamenti effettuati nell'ambito dell'attività di polizia, in particolare dal Centro elaborazione dati del Dipartimento della pubblica sicurezza.

Continuano a pervenire all'Autorità segnalazioni -a volte presentate direttamente al Garante o, più correttamente, a seguito di istanze di accesso rivolte al Dipartimento della pubblica sicurezza ai sensi della speciale normativa in materia di dati trattati per finalità di polizia (art. 10, l. n. 121/1981, modificato dall'art. 42 l. n. 675/1996)- con le quali gli interessati lamentano la presenza nel C.e.d. di dati inesatti, incompleti ovvero non aggiornati, per lo più in riferimento a provvedimenti giudiziari o amministrativi intervenuti e non registrati.

In occasione di una segnalazione avente ad oggetto trattamenti operati da uffici dell'Arma dei carabinieri e della Polizia di Stato, come già anticipato nella *Relazione del 2001*, il Garante ha nuovamente affermato che i trattamenti effettuati da organi o uffici di polizia concernenti dati memorizzati nel predetto C.e.d. ovvero trattati per finalità di prevenzione, accertamento o repressione dei reati devono essere effettuati anch'essi nel rispetto di alcuni importanti principi previsti dalla legge n. 675 e in particolare della disciplina contenuta nell'art. 9 della medesima legge, sotto il profilo della liceità, correttezza, esattezza e aggiornamento, della pertinenza, della completezza e della non eccedenza rispetto alle finalità istituzionali e, infine, della conservazione per il solo periodo di tempo necessario al raggiungimento degli scopi (*Provv.* 17 gennaio 2002).

L'Autorità ha, poi, richiamato l'attenzione degli uffici di polizia sulla necessità di verificare periodicamente la rispondenza dei dati trattati ai descritti requisiti apportandovi, ove necessario, le modifiche o integrazioni richieste, ovvero cancellando i dati detenuti, specie in ragione dei diversi esiti processuali delle vicende eventualmente documentate dagli interessati.

Resta avvertita l'esigenza di integrazioni normative che agevolino il rispetto dei principi sopra descritti, prevenendo ancor più effetti pregiudizievoli per i diritti dei cittadini e tenendo conto della specificità dell' attività investigativa.

In tal senso, il testo unico atteso entro il 30 giugno 2003 rappresenta una preziosa occasione per alcuni mirati interventi come, ad esempio, una più coerente disciplina dei flussi di informazioni fra i vari uffici competenti -dall'ufficio giudiziario all'ufficio di polizia che ha attivato il procedimento e tra uffici di polizia- in modo tale da consentire che i dati possano essere completi in ogni sede interessata. Allo stato, mancano, infatti, dispositivi che assicurino organicamente e sistematicamente un effettivo aggiornamento dei dati, soprattutto quando la vicenda giudiziaria si concluda con un provvedimento favorevole nei confronti del cittadino.

La temporanea, parziale applicazione dei principi previsti dalla legge n. 675 ai trattamenti appena descritti e la delicatezza della materia impongono all'Autorità una specifica attenzione nell'individuazione delle situazioni che effettivamente ricadono sotto tale disciplina.

Al riguardo, in occasione dello svolgimento dei campionati del mondo di calcio nella scorsa estate, l'Autorità è ad esempio intervenuta nei confronti del Ministero dell'interno in occasione della raccolta dei dati degli acquirenti dei biglietti degli incontri effettuata nell'ambito di una collaborazione internazionale di polizia per corrispondere a precise richieste delle autorità coreane e giapponesi, chiarendo che tale iniziativa comprendeva anche aspetti non direttamente finalizzati all'espletamento di attività di sicurezza pubblica o di prevenzione di reati, per i quali dovevano essere rispettati i principi della legge n. 675 (informativa all'interessato; notifica del trattamento al Garante, ecc.).

19 Sistema di informazione Schengen

Il Garante, quale Autorità di controllo sulla sezione nazionale del Sistema informativo Schengen (N.SIS), ha ricevuto anche nel corso dell'anno numerose richieste di verifica dell'eventuale registrazione, nei predetti 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 30 settembre 1993, n. 388, di ratifica del predetto Accordo.

Si tratta, in gran parte, di istanze che attengono al diniego del rilascio di visti, per lo più espresso a causa di segnalazioni a fini della non ammissione nei Paesi Schengen di persone nei cui confronti sono stati emessi provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno (espulsione, respingimento alla frontiera).

In non pochi casi è stato necessario acquisire il parere delle omologhe autorità di controllo degli altri Paesi aderenti all'Accordo di Schengen in base alla procedura di consultazione prevista dall'art. 114, comma 2, della Convenzione, trattandosi di segnalazioni inserite nel SIS da organi di quei Paesi. La collaborazione è stata sempre proficua.

In altri casi gli interessati hanno lamentato la circostanza di essere vittime di usurpazione d'identità o segnalato casi di omonimia. In talune circostanze è stato possibile attivare una procedura di comparazione degli elementi identificativi della persona oggetto di usurpazione d'identità con quelli, anche dattiloscopici, della persona effettivamente segnalata nel S.I.S. al fine di accertare l'estraneità ai fatti del richiedente l'accesso.

Si è nuovamente riscontrato un notevole afflusso di richieste di verifica o di controllo, anche in relazione alla procedura di regolarizzazione di cittadini extracomunitari introdotta dalla legge n. 189/2002.

Nei mesi precedenti il completamento di tale procedura si è registrato un sensibile incremento delle richieste, soprattutto provenienti da Paesi dell'est europeo (e in particolare dalla Romania), per lo più effettuate in assenza di specifici provvedimenti pregiudizievoli per gli interessati.

Anche in considerazione di tale "emergenza" il Garante, a seguito di una specifica richiesta di chiarimenti da parte di una cancelleria consolare, ha chiarito l'esatto ambito delle competenze spettanti in tale materia al Garante, quale autorità nazionale di controllo, e fornito alcune indicazioni circa le modalità di inoltro delle istanze utili a renderne più agevole e più spedita la trattazione.

In particolare, il Garante ha precisato che gli interessati possono rivolgere a questa Autorità

una richiesta di verifica dei dati che li riguardano inseriti nel S.I.S., come pure possono richiedere la rettifica o la cancellazione dei medesimi dati. Il Garante, invece, non ha alcun compito istituzionale, diretto o indiretto, in materia di adozione, concessione o revoca dei provvedimenti amministrativi 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 tali provvedimenti, quindi, gli interessati possono rivolgersi ai competenti organi o uffici del Ministero dell'interno.

Nell'occasione il Garante ha richiamato l'attenzione dei competenti uffici del Ministero degli affari esteri sull'opportunità di sensibilizzare -in ordine alle indicazioni suesposte- gli uffici consolari di altri Paesi che potrebbero risultare particolarmente interessati dalle richieste in esame.

A seguito di una cooperazione proficua con l'Ufficio SIRENE e con il Servizio immigrazione e polizia di frontiera del Dipartimento della pubblica sicurezza, si sono notevolmente snellite le procedure per le verifiche richieste. Va dato atto della disponibilità di tali uffici per un più accurato e tempestivo aggiornamento dei dati.

Da ultimo, anche in relazione a tale materia, l'adozione del testo unico potrebbe essere l'occasione per rimeditare la scelta operata dal legislatore nel 1993 di prevedere l'accesso "indiretto" presso questa Autorità (che il più delle volte si risolve in un inutile appesantimento della procedura), allineando così la normativa a quella di altri Paesi dell'ambito Schengen che hanno già optato per l'accesso "diretto" presso le autorità di polizia.

Sanità

20 Trattamento di dati idonei a rivelare lo stato di salute

L'assetto normativo delineato dal legislatore delegato nel 1999 per la disciplina del trattamento dei dati idonei a rivelare lo stato di salute da parte degli organismi sanitari pubblici, nonché degli organismi sanitari e degli esercenti le professioni sanitarie operanti in regime di convenzione o di accreditamento con il Servizio sanitario nazionale, non ha ancora trovato integrale definizione in ragione della mancata adozione del regolamento del Ministro della salute con il quale dovevano 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).

Tale ritardo determina difficoltà nell'applicazione della normativa -soprattutto da parte degli organismi sanitari pubblici- anche in ragione del fatto che al suddetto regolamento è stato affidato 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).

Con riferimento alle modalità di applicazione dell'art. 23 della legge n. 675/1996, in diverse occasioni l'Autorità ha segnalato a 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).

Il Garante ha poi nuovamente affrontato la questione del trattamento dei dati personali di natura sensibile dei portatori di *handicap* intervenendo in merito alla divulgazione su un sito *Internet* dei nominativi di alcuni alunni con l'indicazione della relativa patologia sofferta. In tal caso è stato disposto il blocco del trattamento dei dati idonei a rivelare lo stato di salute degli interessati e l'accertamento ispettivo presso il titolare del trattamento (*Provv.* 10 aprile 2002).

In un caso in cui si ipotizzava una diffusione di dati inerenti alla salute, l'Autorità ha applicato la prevista sanzione amministrativa nei confronti di una Asl che non aveva risposto alla richiesta di informazioni volta a verificare che la stessa non avesse -come segnalato- invitato ad una visita per l'accertamento dell'invalidità una persona con foglio privo di busta dal quale si evidenziava il motivo della convocazione. L'Autorità ha contestato alla Asl la violazione delle disposizioni della legge 675/1996 riguardanti la mancata risposta alla richiesta di informazioni o esibizioni di documenti (art. 39, comma 1).

Nell'ambito delle diverse iniziative dell'Autorità sul tema dei trattamenti di dati sanitari sono inoltre da ricordare:

- le indicazioni fornite in merito alle modalità di spedizione di alcuni prodotti per l'incontinenza. E' stato precisato che la menzione del contenuto della spedizione sulla parte esterna del pacco postale è idonea a rivelare a terzi -in talune circostanze- le condizioni di salute del destinatario del prodotto. A seguito dell'intervento dell'Autorità, la società mittente si è impegnata a variare gli impianti di stampa, al fine di eliminare dal nastro adesivo l'indicazione della natura del contenuto del pacco postale (22 agosto 2002 e 28 ottobre 2002);
- le indicazioni fornite ad alcuni datori di lavoro circa la possibilità di prevedere l'inserimento nei giustificativi di assenza per malattia non solo della prognosi, ma anche della diagnosi della patologia sofferta dal lavoratore. In merito, è stato rilevato che, dal momento che non esiste più l'obbligo dell'invio al datore di lavoro della diagnosi della malattia del lavoratore, il medico che effettua la visita di controllo deve fornire al datore di lavoro solo certificati dai quali risulti la sussistenza e la durata dello stato di incapacità del lavoratore, senza alcuna indicazione diagnostica. La diagnosi non va quindi indicata neanche nei certificati medici che il dipendente deve inviare al datore di lavoro per documentare l'assenza per malattia;
- le indicazioni fornite ad una amministrazione pubblica in merito alla legittimità della trasmissione al Ministero dell'economia e delle finanze dei verbali relativi agli invalidi civili iscritti nelle liste speciali di collocamento obbligatorio. E' stato precisato che la comunicazione potrebbe essere giustificata solo qualora detti verbali si riferiscano a soggetti assunti al lavoro ai sensi della legge n. 482/1968 che abbiano omesso di presentare la dichiarazione di responsabilità relativa alla sussistenza dei requisiti previsti per tale assunzione. Solo in tal caso, infatti, è previsto uno specifico potere di accertamento in capo al Ministero (*Provv.* 16 ottobre 2002);
- il parere in merito alla legittimità della richiesta effettuata da una Asl ai medici curanti di inviare trimestralmente i diari clinici tenuti presso il domicilio dei pazienti beneficiari del servizio di assistenza domiciliare programmata. In tal caso, dopo aver ricostruito il quadro normativo di riferimento, è stata ritenuta illegittima la richiesta della Asl di una comunicazione sistematica di tali dati sensibili. Per lo svolgimento del controllo dell'erogazione dei servizi di assistenza domiciliare è sufficiente che l'azienda sanitaria richieda la trasmissione dei soli fogli firmati dai medici in occasione delle visite domiciliari, senza alcuna indicazione della patologia riscontrata (5 febbraio 2003);
- la nota del 31 maggio 2002 con la quale non è stata rinvenuta la base giuridica affinché una struttura ospedaliera possa trasmettere ad un Vicariato, al fine di consentire ai parroci di assistere spiritualmente i parrocchiani malati, l'elenco dei degenti ricoverati presso la stessa struttura;
- la nota del 13 febbraio 2002 con la quale, su segnalazione di un medico, è stato esaminato il decreto del Ministero della sanità del 11 febbraio 1997, il quale prevede, fra l'altro, che ai fini dell'importazione in Italia di un farmaco, autorizzato in un paese estero, ma non ammesso alla commercializzazione nel territorio nazionale, il sanitario richiedente comunichi al Ministero (Ufficio di sanità marittima ed aerea) e all'Ufficio doganale i dati identificativi del paziente. In tal caso si è rilevato che tale decreto, precedente all'entrata in vigore della legge n. 675/1996, non dispone della necessaria forza giuridica richiesta dall'art. 22, commi 3 e 3-*bis* della legge. E' stata, pertanto, segnalata

la questione al Ministero della salute (Direzione generale della programmazione sanitaria- Gruppo di lavoro per la stesura del regolamento di cui all'art. 23, comma 1-*bis*, l. n. 675/1996), affinché ne tenga conto nella redazione dell'emanando regolamento ministeriale. In particolare, è stato ricordato che le operazioni su tali categorie di informazioni devono essere effettuate nel rispetto dei princìpi di cui agli artt. 3 e 4 del d.lg. n. 135/1999, fra i quali assume un rilievo precipuo la verifica dell'essenzialità e della indispensabilità dei dati rispetto al perseguimento delle finalità indicate dalle legge;
- la decisione, nell'ambito di un ricorso, con la quale l'Autorità, accogliendo il ricorso di un paziente che segnalava un riscontro inadeguato da parte dell'azienda ospedaliera cui si era rivolto per ottenere la comunicazione in forma intelligibile dei dati personali contenuti nella sua cartella clinica, ha stabilito che se la cartella clinica è illeggibile per la grafia di chi l'ha redatta, deve essere trascritta in modo che le informazioni in essa contenute risultino chiare per il malato (*Provv.* 30 settembre 2002).

21 Informazioni genetiche

Prosegue intensa nelle sedi comunitarie e internazionali, nonché in occasione di incontri e seminari, la rilevazione comparata di elementi utili per il rilascio della nuova autorizzazione del Garante in materia di dati genetici.

In base alle disposizioni contenute nella disciplina legislativa delegata del 1999 (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), il trattamento di dati genetici da parte di chiunque, può svolgersi solo in conformità alle prescrizioni e garanzie previste dal Garante con un'apposita e specifica autorizzazione.

L'Autorità ha a suo tempo avviato la 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*"). Nel frattempo, alla luce degli approfondimenti necessari, particolarmente complessi, e di indicazioni e suggerimenti ricevuti dagli esperti -nelle more di un approfondimento della materia- è stata transitoriamente prorogata 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)*), e riprodotta nell'autorizzazione n. 2/2002.

Allo stato, ferme restando alcune esclusioni soggettive e limitazioni nelle finalità, il trattamento dei dati genetici resta 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 è punita con sanzione penale (art. 37, l. n. 675/1996).

In questo quadro, l'Autorità ha avviato nel corso dei precedenti anni (cfr. Relazioni 2000 e 2001, rispettivamente pp. 32 e 42), avvalendosi dei poteri conferitigli dal legislatore (art. 32, comma 1, l. n. 675/1996), attività di monitoraggio e controllo di progetti di ricerca genetica sulle popolazioni della regione dell'Ogliastra, in Sardegna, e del Cilento.

Nel corso del 2002 un'analoga iniziativa di controllo ha riguardato un comune della provincia di Bergamo. Anche in questo caso la stampa ha dato notizia dell'imminente avvio di ricerche genetiche nella zona ed il Garante ha avviato accertamenti presso il Sindaco del comune coinvolto. Dalle risposte pervenute è emerso che, allo stato, l'iniziativa non è stata ancora avviata e che ulteriori elementi saranno forniti all'Autorità dal responsabile del progetto della ricerca.

Nell'ambito delle iniziative del Garante sul tema dei trattamenti di dati genetici, nei giorni 21-22 marzo 2002 si è 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. Sono stati inoltre rilevati grandi rischi, primo fra tutti quello di innescare pericolosi meccanismi sociali come l'"eugenetica di mercato e la concorrenza genetica" o di sottovalutare le insidie derivanti dalla commercializzazione dei dati genetici, considerandoli come una vera e propria merce.

Il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie ha pubblicato il 24 febbraio 2003 una dichiarazione nella quale segnala all'opinione pubblica ed a tutti i soggetti con responsabilità politiche i problemi legati alla pubblicità dei test genetici via *Internet*. Il documento evidenzia che la commercializzazione di massa dei test genetici pone molti e gravi problemi etici, sociali, giuridici e tende a trasformare uno strumento eminentemente diagnostico in una merce alla stregua di ogni altra, creando una domanda che può avere conseguenze potenzialmente laceranti per il tessuto sociale ed i rapporti interpersonali. In molti casi non ci sono sufficienti garanzie nella raccolta dei dati genetici inviati per i test e possono essere messe a rischio sia la salute delle persone sia la riservatezza dei dati sanitari.

Il predetto Gruppo -che ha il compito di offrire consulenza e indicazioni alla Commissione UE sugli aspetti etici dell'attività scientifica e delle nuove tecnologie, anche in rapporto a iniziative di legge- sottolinea che le informazioni fornite nei messaggi pubblicitari sono spesso fuorvianti e imprecise e che i test genetici possono avere conseguenze negative se non vengono accompagnati da un'adeguata consulenza.

Si stanno moltiplicando, infatti, le offerte via *Internet* di test genetici relativi soprattutto all'accertamento di paternità, ma anche alla predisposizione a diverse malattie (cardiache, diabete, ecc.). La pubblicità diventa sempre più aggressiva e capillare, anche in Europa: in alcuni Paesi compare, ad esempio, in popolari catene di negozi, nelle stazioni di servizio, negli autogrill lungo le autostrade, in televisione.

Rapporto di lavoro

22 Tutela dei dati personali dei lavoratori

L'Autorità si è pronunciata in più di un'occasione sul tema della protezione dei dati personali nel settore del lavoro, nel quale parte della disciplina integrativa è stata demandata all'autoregolamentazione dei datori di lavoro e degli altri soggetti coinvolti (si fa riferimento al codice di deontologia relativo ai trattamenti di dati personali necessari per finalità previdenziali o per la gestione del rapporto di lavoro, previsto dall'art. 20, comma 1, lett. *b)* del d.lg. n. 467/2001).

Tra gli ambiti più problematici affrontati occorre evidenziare il tema del controllo a distanza dei lavoratori effettuato con strumenti informatici e telematici, con particolare riferimento al controllo delle navigazioni in *Internet* e del traffico di posta elettronica sul luogo di lavoro, rispetto ai quali è in corso un vivace dibattito anche a livello internazionale.

La complessa tematica è stata affrontata dal Gruppo di lavoro istituito in applicazione dell'articolo 29 della direttiva 95/46/CE, il quale ha adottato il 29 maggio 2002 un importante documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro. Nell'atto è stata esamina la questione dei controlli e della vigilanza sulle comunicazioni elettroniche effettuate sul posto di lavoro, con particolare riferimento al controllo da parte del datore di lavoro della posta elettronica e dell'impiego di *Internet*. In relazione alla giurisprudenza della Corte europea dei diritti umani riguardante l'articolo 8 della Convenzione per la protezione dei diritti umani e delle libertà fondamentali, nonché di altri pertinenti testi di diritto internazionale e delle disposizioni della direttiva 95/46/CE, il documento offre precisi indirizzi interpretativi ed esempi concreti su ciò che può costituire attività legittima di controllo e circa i limiti giuridicamente configurabili di vigilanza sui dipendenti esercitata dal datore di lavoro.

Un'altra tematica di particolare interesse, per la quale sono stati presentati numerosi ricorsi e quesiti, concerne l'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).

Con particolare riferimento al 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, stante la 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 stato ribadito che è possibile presentare un'ampia richiesta di accesso al complesso dei dati, ivi compresi quelli riportati all'interno di valutazioni (*Provv.ti* 10 gennaio 2002, in *Bollettino* n. 24, p. 6 e 36).

Nell'esaminare il diverso caso in cui un lavoratore ha chiesto di accedere ai dati valutativi di altri colleghi contenuti in documenti amministrativi detenuti dal datore di lavoro,

l'Autorità ha ribadito che le disposizioni in materia di accesso ai documenti amministrativi rappresentano un'idonea fonte normativa, ai fini dell'applicazione dell'art. 27, comma 3, della legge n. 675/1996 e che spetta all'amministrazione destinataria della richiesta valutare la sussistenza dell'interesse giuridicamente rilevante e delle altre condizioni per accedere ai documenti amministrativi (*Provv.* 28 ottobre 2002).

Con specifico riferimento al caso in cui l'eventuale diniego dell'accesso trovi fondamento nei regolamenti di attuazione della legge n. 241/1990, il Garante ha poi ricordato (15 aprile 2003) che il Consiglio di Stato ha ritenuto illegittima la disposizione regolamentare di un comune che sottraeva all'accesso, per motivi di riservatezza dei terzi, la documentazione relativa al trattamento economico individuale del personale, precisando che l'amministrazione può semmai adottare la specifica cautela di limitare l'accesso del richiedente alla semplice visione degli atti, come prevede l'art. 24, lett. *d)*, della legge n. 241/1990 (Consiglio di Stato, sez. V, 10 febbraio 2000, n. 737).

Nell'ambito del procedimento contenzioso previsto dall'art. 29 della l. n. 675/1996, l'Autorità ha accolto il ricorso di un dipendente di un istituto di ricerca, con riferimento sia alle informazioni allo stesso relative contenute nel fascicolo personale detenuto presso gli uffici amministrativi dell'ente, sia ai dati personali comunque conservati in forma automatizzata nella memoria dei computer utilizzati dall'interessato medesimo presso le strutture di ricerca dell'istituto (*Provv.* 23 aprile 2002).

L'Autorità si è poi espressa sulla conoscibilità dei dati personali del lavoratore nell'ambito di una procedura di conciliazione obbligatoria, già prevista dagli artt. 69 e 69-bis del d.lg. n. 29/1993. In particolare, è stato ritenuto dall'Autorità che fosse stata illecitamente effettuata la comunicazione a persone non direttamente coinvolte dell'istanza di attivazione della procedura da parte del lavoratore; ciò in quanto non è stata individuata alcuna disposizione legislativa o regolamentare che potesse giustificare una tale comunicazione, ai sensi dell'art. 27, comma 3, della legge n. 675/1996 (*Provv.* 20 gennaio 2003).

In relazione ai dati contenuti nei fascicoli personali, sono poi pervenute al Garante numerose segnalazioni con le quali gli interessati sollevano questioni su alcune modalità con cui vengono gestiti i fascicoli del personale di Forze armate e di polizia, con specifico riferimento ai dati sulla salute. Da tali segnalazioni l'Autorità è venuta a conoscenza, in particolare, della procedura secondo la quale alcune amministrazioni esigerebbero dai dipendenti di allegare alle richieste di assenza al lavoro, per motivi di salute, certificati medici attestanti, oltre la prognosi, anche la diagnosi. Tale documentazione verrebbe poi conservata nel fascicolo personale del dipendente.

La procedura troverebbe solo in alcuni casi uno specifico fondamento normativo e verrebbe giustificata dall'esigenza dell'amministrazione di conoscere l'insorgenza nei propri dipendenti di quelle patologie che possono incidere sull'idoneità al servizio o, comunque, sull'utilizzo o porto di armi. Sul punto l'Autorità ha promosso preliminarmente un tavolo di lavoro con le amministrazioni interessate, al fine approfondire la tematica e fornire all'esito le necessarie indicazioni volte a rendere il trattamento di tali informazioni pienamente conforme alla normativa sui dati personali.

In conformità a precedenti pronunce, l'Autorità ha altresì posto nuovamente in evidenza il principio in base al quale il diritto tutelato dall'art. 13, comma 1, l. 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 di dati relativi a prestazioni lavorative: entrata e uscita in ufficio, registrazioni riguardanti le assenze e le carenze orarie, durata delle prestazioni lavorative rese in un determinato periodo) dei dati personali del richiedente (*Provv.* 29 gennaio 2003).

Con altra pronuncia si è, inoltre, nuovamente sottolineato che, sempre nell'esercizio del diritto di accesso a dati personali, il dipendente può chiedere di conoscere la logica, le finalità e le modalità del trattamento anche quando questo è relativo alla gestione del rapporto di lavoro e riguardi dati comunicati ad altri organi ed uffici con corrispondenza riservata (*Provv.* 29 gennaio 2003).

In una risposta (9 aprile 2002) al quesito di una commissione provinciale per le politiche del lavoro, circa il trattamento dei dati relativi a persone disabili iscritte negli elenchi per il collocamento obbligatorio, l'Ufficio ha precisato che la trasmissione dei dati in questione alle associazioni rappresentative di tali categorie, senza il preventivo consenso degli interessati, è consentita solo in presenza di una norma di legge o di regolamento che autorizzi espressamente tale comunicazione (art. 27, comma 3, legge n. 675/1996). Nel caso specifico è stato ricordato che l'art. 3 del d.P.R. n. 442/2000 consente ai competenti uffici provinciali del lavoro di comunicare solo ad alcuni soggetti (datori di lavoro, enti pubblici economici interessati all'assunzione, società di mediazione autorizzate, enti previdenziali, centri di formazione professionale ed altre pubbliche amministrazioni) i dati personali relativi alle persone presenti nelle banche dati, con l'esclusione di quelli sensibili di cui agli articoli 22 e 24 della legge n. 675/1996, al fine di promuovere l'occupazione, favorire l'inserimento al lavoro e l'accesso ad attività di orientamento e formazione professionale. Potendo venire in rilievo dati di carattere sensibile, si imponeva il rispetto dell'art. 22, commi 3 e 3-bis della legge 675/1996, nonché di quanto ribadito dagli art. 3 e 4 del d.lg. n. 135/1999 che consentono tale genere di trattamenti solo qualora gli stessi siano indispensabili all'espletamento delle funzioni istituzionali proprie dell'amministrazione titolare e non perché esso possa risultare utile all'eventuale destinatario dei dati. E', invece, da escludersi la possibilità che un componente della commissione provinciale, venuto in possesso di tali informazioni in ragione del proprio ufficio, potesse legittimamente diffondere tali dati ad altri soggetti, anche per ragioni attinenti al rispetto del segreto d'ufficio.

In relazione al quesito formulato da un curatore fallimentare a proposito delle modalità di accesso ai dati contenuti nelle cartelle sanitarie degli ex dipendenti di una società fallita, è stato ricordato che, ai fini dell'esercizio del diritto di accesso ai dati personali che lo riguardano, l'ex dipendente avrebbe potuto presentare, nei confronti della società ove prestava servizio, o per il tramite dei competenti organi del relativo fallimento, una richiesta per accedere in tutto o in parte ai dati riferiti alla propria persona (in tale ipotesi, è opportuno tenere conto delle disposizioni in materia di fallimento per quanto riguarda i poteri e gli obblighi dei diversi organi della procedura in tema di custodia e di apposizione e rimozione dei sigilli sui beni del fallito e quindi sugli eventuali supporti che possono contenere dati personali, anche dei dipendenti).

Si è, inoltre, ribadito anche in questo caso che la comunicazione all'interessato dei dati idonei a rivelare lo stato di salute contenuti nella "cartella sanitaria" può avvenire "solo per il tramite di un medico designato dall'interessato o dal titolare" (art. 23 della legge n. 675/1996). Pertanto, la comunicazione può essere effettuata, oltre che attraverso il medico dell'ex datore di lavoro, mediante trasmissione ad un medico di fiducia indicato dall'ex dipendente, il quale, ad esempio, potrebbe a tale scopo designare il medico competente in materia di igiene e sicurezza dei lavoratori presso il nuovo datore di lavoro (29 luglio 2002).

In un caso delicato un'insegnante elementare ha segnalato al Garante di non aver avuto idoneo riscontro ad una richiesta rivolta al competente provveditorato agli studi, con la quale chiedeva la cancellazione o la trasformazione in forma anonima della dicitura *"portatore di handicap"* che compariva accanto al proprio nome, in un elenco di lavoratori trasferiti presso altre sedi. La questione, affrontata nell'ambito di un ricorso, evidenziava, inoltre, come la diffusione del dato sanitario, avvenuta in violazione della legge n. 675/1996, avesse determinato nei confronti dell'insegnante una situazione di grave disagio a livello personale e di relazione con gli altri colleghi.

L'Autorità, accogliendo il ricorso, ha precisato che la divulgazione del dato sanitario dell'insegnante era illecita perché avvenuta in violazione della legge che vieta la diffusione di dati idonei a rivelare lo stato di salute delle persone. E' stato perciò vietato al Ministero di diffondere ulteriormente, anche presso altri uffici, accanto al nome dell'insegnante, la formula *"portatore di handicap"*, imponendo all'amministrazione la sostituzione con diciture generiche o codici numerici. Non è stata, invece, ritenuta idonea la soluzione di sostituire la dicitura con l'apposizione del riferimento normativo (legge 104/92). Ciò perché il riferimento ad una legge che tutela specificamente le persone handicappate finirebbe, anche se in via mediata, per rivelare comunque informazioni sulle condizioni di salute degli interessati (*Provv.* 27 febbraio 2002).

In un altro caso, riguardante l'accesso da parte dei dipendenti alle graduatorie relative all'ammissione ad alcuni corsi finalizzati all'avanzamento di carriera, è stato confermato che, in base alla legge n. 675/1996, la presa di conoscenza delle graduatorie da parte dei lavoratori avrebbe configurato un'ipotesi di comunicazione da parte del datore di lavoro dei dati relativi anche ad altri lavoratori, e che tale operazione sarebbe stata ammissibile qualora gli interessati vi avessero acconsentito, o in presenza di uno degli altri presupposti equipollenti previsti dalla predetta legge.

Nel caso di specie, la particolare procedura selettiva seguita è risultata essere specificamente prevista da alcuni accordi tra il datore di lavoro e le organizzazioni sindacali, attuativi di disposizioni del contratto collettivo nazionale di lavoro del settore. Tali accordi avevano previsto l'obbligo di formulare una graduatoria per l'ammissione ai corsi di formazione, che, come tale, deve essere resa nota ai partecipanti alla procedura. Occorre infatti permettere ai non ammessi, aventi comunque titolo per effetto delle obbligazioni assunte dal datore di lavoro in sede di contrattazione con le organizzazioni sindacali, una verifica della legittimità della stessa graduatoria e della correttezza delle operazioni seguite (ciò anche alla luce del principio di buona fede nell'adempimento delle obbligazioni più volte ribadito dalla giurisprudenza di legittimità in materia di copertura di qualifica superiore mediante selezioni o concorsi interni del personale).

In tale ipotesi, la comunicazione dei dati personali riportati nella graduatoria è stata quindi giudicata ammissibile in base alla legge n. 675/1996, in quanto necessaria per l'esecuzione di obblighi di natura contrattuale assunti dal datore di lavoro nei confronti dei lavoratori interessati (nella specie gli accordi sindacali attuativi del CCNL di settore: 5 agosto 2002).

Un altro caso esaminato ha riguardato una segnalazione relativa alle modalità di corresponsione dello stipendio, da parte di un'azienda, ad un dipendente che non intendeva indicare il proprio numero di conto corrente ai fini del bonifico. Come modalità alternativa di versamento dello stipendio, l'azienda aveva inizialmente previsto che il dipendente presentasse presso la banca indicata per il pagamento alcuni documenti, tra i quali la busta paga, il che era stato giudicato dal dipendente lesivo del proprio diritto alla riservatezza.

L'azienda ha infine convenuto sulla possibilità che il dipendente riscuota il proprio stipendio presentando presso la banca un documento di riconoscimento ed il telegramma inviato dalla società contenente l'importo del bonifico emesso a favore dell'interessato. Il Garante ha comunque richiamato l'attenzione sulla necessità di limitare la conoscenza dei dati personali dei dipendenti da parte dell'azienda ai soli dati strettamente necessari, ad esempio, ai fini della loro esatta identificazione, della verifica del titolo a riscuotere il bonifico emesso a loro favore e dell'eventuale adempimento da parte dell'istituto di credito ad altri obblighi di legge (ad esempio, relativamente alla normativa antiriciclaggio). L'esibizione allo sportello bancario di documenti ulteriori rispetto a quello di riconoscimento, come la "busta paga", senza l'adozione di opportuni accorgimenti per non permettere la visione di alcune parti non essenziali rispetto alle predette finalità, non può ritenersi giustificata, alla luce del principio di proporzionalità, considerato anche che tale documentazione può contenere indicazioni da cui è desumibile l'appartenenza sindacale del dipendente o informazioni sul suo stato di salute (5 febbraio 2003).

Nell'ambito delle diverse iniziative dell'Autorità sul tema dei trattamenti di dati personali nell'ambito del rapporto di lavoro sono da ricordare inoltre:

- l'iniziativa volta ad acquisire informazioni, in riferimento a notizie apparse sulla stampa, relative alla richiesta di alcuni dati personali di iscritti e di specifiche attività sindacali, che sarebbe stata rivolta dalle forze di polizia ad organismi sindacali nella zona di Benevento (8 agosto 2002);
- l'attività di accertamento per valutare se siano state violate le disposizioni legislative che tutelano la riservatezza e la dignità umana riguardo al caso, riportato dalla stampa, di un marittimo affetto da sindrome da *Hiv* licenziato dall'azienda per la quale lavorava (7 febbraio 2003);
- la decisione con la quale il Garante, nell'accogliere il ricorso di un laureato insoddisfatto dell'operato della ditta alla quale aveva chiesto invano l'aggiornamento dei dati relativi al titolo di studio appena conseguito e l'attestazione che la variazione fosse stata portata a conoscenza di tutti coloro ai quali i dati erano stati comunicati, ha stabilito che le aziende private e le pubbliche amministrazioni devono aggiornare i propri archivi con le qualifiche professionali ed i titoli di studio acquisiti dai lavoratori. Tale operazione deve essere tempestiva ed effettuata in ogni altro pertinente *data base* dell'azienda (*Provv.* 6 settembre 2002);

- la decisione, adottata anche in questo caso nell'ambito di un ricorso, con la quale si è stabilito che sul cedolino dello stipendio non deve essere riportata la dicitura "pignoramento", che deve essere sostituita da altre formule (ad es. "altre trattenute") o da codici identificativi che rendano ugualmente comprensibile la voce, ma non consentano a terzi di venire immediatamente a conoscenza di delicati aspetti relativi alla sfera privata del lavoratore. Con la medesima pronuncia è stato inoltre evidenziato che sul cedolino vanno riportate solo le notizie indispensabili a documentare al dipendente le diverse voci relative alle competenze e alle trattenute per consentire una verifica agevole dell'esatta corresponsione della retribuzione. Occorre, quindi, omettere, ad esempio, la specifica causale del pignoramento oppure, come in altri casi, l'indicazione del sindacato al quale il lavoratore iscritto versa la ritenuta sindacale. Il cedolino dello stipendio, infatti, può essere esibito sia in circostanze nelle quali interessa appurare solo il livello stipendiale, sia in altri casi nei quali è necessario siano specificate le causali delle varie voci, per identificare la porzione di retribuzione "disponibile" (ad es. in caso di richiesta di un finanziamento, "cessioni del quinto") (*Provv.* 19 febbraio 2002);
- il parere circa la possibilità per una persona, invalida civile, di conoscere il numero dei posti di lavoro e delle mansioni disponibili per i lavoratori disabili presso i singoli datori di lavoro, nonché, limitatamente ai datori di lavoro privati, il numero delle convenzioni in corso stipulate con le province ai fini dell'inserimento occupazionale dei disabili e del numero delle unità lavorative coinvolte (4 aprile 2003).

23 Controllo a distanza dei lavoratori

Altro profilo che assume particolare importanza nel settore del lavoro è quello del c.d. controllo a distanza dei lavoratori, connesso alla più ampia tematica della videosorveglianza.

In materia trova da tempo applicazione l'art. 4 della legge n. 300/1970 che, nel vietare "il controllo a distanza dell'attività dei lavoratori" (anche come mera possibilità di controllo ad insaputa del prestatore), disciplina distintamente le due ipotesi dell'impianto di apparecchiature finalizzate al controllo a distanza (primo comma) e di apparecchiature per fini produttivi, ma tali comunque da presentare la possibilità di fornire anche il controllo a distanza del dipendente (secondo comma).

Il Garante è intervenuto sul tema del controllo a distanza dei lavoratori in particolare in un caso concernente il Consiglio nazionale delle ricerche (CNR). Un lavoratore aveva segnalato all'Autorità l'esistenza, presso la sede dell'istituto, di un sistema di video sorveglianza dotato di una telecamera a circuito chiuso, idonea a sorvegliare l'attività dei lavoratori. A seguito della richiesta di chiarimenti, il CNR ha confermato la presenza di una telecamera con ampio angolo visuale, in grado di riprendere il passaggio delle persone che entrano nel relativo campo visivo ma non rivolta al controllo dell'attività dei dipendenti.

Le immagini, raccolte per motivi di sicurezza, non erano oggetto di registrazione e venivano trasmesse ad un *monitor* collocato nel posto di guardia. Sebbene si trattasse di una telecamera ben visibile, la sua presenza non era stata segnalata in alcun modo; all'Istituto è stata pertanto contestata la violazione della normativa sulla protezione dei dati personali per non aver preventivamente informato il pubblico e i lavoratori, attraverso cartelli o avvisi, della presenza della telecamera e per non aver inserito nelle notificazioni presentate al Garante la video sorveglianza e la video registrazione, quali modalità di trattamento dei dati (*Provv.* 1 ottobre 2002).

Su tale aspetto, e in generale sul problema delle procedure di informazione e di controllo a distanza del personale, l'Autorità è stata inoltre impegnata attivamente nel dibattito 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 si è concluso con l'approvazione del già richiamato documento adottato il 29 maggio 2002 riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro. In tale documento è stata esamina la questione dei controlli e della vigilanza sulle comunicazioni elettroniche effettuate dal posto di lavoro, con particolare riferimento al controllo da parte del datore di lavoro della posta elettronica e dell'impiego di *Internet* fatto dai dipendenti.

24 Annunci di lavoro, riforma del collocamento e del sistema informativo in materia di lavoro

Il Garante, già negli anni precedenti, ha avviato forme di collaborazione con enti, organismi ed associazioni del settore, per assicurare un più ampio rispetto della legge n. 675/1996 e un'omogeneità dei comportamenti degli operatori coinvolti. Ciò 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.

Già in passato questa Autorità aveva indicato alcuni criteri per la corretta applicazione della legge n. 675/1996 in relazione al trattamento di dati personali raccolti tramite *coupon* o mediante la diversa tipologia di richiesta dei dati rappresentata da annunci ed offerte di lavoro pubblicati su quotidiani e periodici con i quali viene sollecitato l'invio di *curricula* (v. *Provv.* 13 gennaio 2000, in *Bollettino* n. 11-12/2000, p. 39 e ss.).

In tale circostanza il Garante aveva riscontrato la mancanza delle necessarie idonee informative ai sensi dell'art. 10 l. n. 675/1996 e, conseguentemente, accertato l'invalidità del consenso al trattamento dei dati che si chiedeva di esprimere unitamente all'invio dei *curricula* (consenso che, secondo quanto precisato nel ricordato provvedimento, è peraltro superfluo ove i dati da inserire nel *curriculum* non abbiano natura sensibile o non siano comunicati a terzi).

Nel corso di un successivo monitoraggio effettuato su vari annunci più recenti pubblicati su quotidiani e periodici, concernenti offerte di lavoro curate da società di ricerca e selezione del personale, si è nuovamente constatato che, in diversi casi, era presente solo una sintetica richiesta ai candidati interessati di inviare i *curricula* e, contestualmente, di "autorizzare il trattamento dei dati personali ai sensi della legge n. 675/1996", peraltro priva delle informazioni prescritte dal predetto art. 10.

Oltre a quanto emerso dal menzionato monitoraggio, sono pervenute a questa Autorità segnalazioni, anche telefoniche, con le quali è stata lamentata l'assenza negli annunci di idonee indicazioni sulle modalità di trattamento dei dati contenuti nei *curricula* e circa i tempi della loro conservazione; sono state espresse preoccupazioni anche in ordine alla possibile divulgazione a terzi dei dati e al loro eventuale utilizzo per scopi ulteriori rispetto alla sola selezione del personale (ad esempio, per promuovere corsi di formazione a pagamento).

L'Autorità ha pertanto effettuato un'ulteriore verifica su un campione significativo di annunci pubblicati in alcuni quotidiani su iniziativa di società di selezione o di ricerca del personale, di società di lavoro temporaneo e di altri soggetti intermediari che offrono analoghi servizi. Con un nuovo provvedimento a carattere generale, ha poi segnalato alle società rispetto alle quali sono state accertate le violazioni menzionate, nonché agli organismi pubblici e pri-

vati 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 alcune 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).

Gli annunci di lavoro per i quali è stata contestata la violazione della legge n. 675/1996 non recavano, anzitutto, un'idonea informativa: oltre a non essere spesso indicata l'identità del titolare del trattamento, mancavano informazioni sulle modalità con le quali vengono utilizzati i dati e gli eventuali scopi ulteriori per i quali vengono raccolti. Non veniva inoltre chiarito se il conferimento dei dati era obbligatorio o facoltativo, né era specificato se i dati venivano divulgati o meno a terzi (non era quindi indicata nemmeno l'eventuale società per conto della quale venive svolta la selezione o la ricerca del personale). Mancavano poi indicazioni sui diritti di accesso ai dati o relativi al loro aggiornamento, rettifica, cancellazione e opposizione al loro successivo utilizzo per altri scopi, così come non era indicata la persona cui rivolgersi per esercitare tali diritti.

Gli annunci, nella maggioranza dei casi esaminati, contenevano solo un mero invito nei confronti dei candidati interessati a rilasciare, nel *curriculum* o nei documenti che intendevano inviare, un consenso generico al trattamento dei dati personali, oltretutto con formule improprie (come "autorizzazione ai sensi della legge n. 675/1996"). Consenso che, peraltro, non è affatto necessario se le società trattano dati personali comuni e non li mettono a disposizione di terzi (per scopi diversi dall'esecuzione di obblighi contrattuali) e che è, invece, obbligatorio se nei *curricula* sono contenute informazioni sensibili (ad esempio, relative all'appartenenza a particolari categorie protette).

Queste prassi non sono risultate conformi alla legge n. 675/1996. I principi di lealtà e correttezza del trattamento impongono che i candidati siano chiaramente informati, al momento della pubblicazione degli annunci, sulle modalità e sull'uso che viene fatto dei dati personali richiesti. Le società devono, in sostanza, consentire una scelta libera e consapevole da parte dei candidati e acquisire, quando necessario, un consenso specifico.

Per quanto riguarda i *curricula* inviati spontaneamente da soggetti in cerca di lavoro, il problema dell'informativa potrà essere risolto adeguatamente anche attraverso le disposizioni del codice di deontologia relativo alla gestione del rapporto di lavoro. Il Garante ha invitato nel frattempo le società a fornire l'informativa e a richiedere l'eventuale consenso in caso di successivo utilizzo dei dati contenuti nei *curricula* ricevuti. L'Autorità ha, infine, indicato alle categorie interessate un possibile schema di informativa (riproducibile nell'annuncio di lavoro, con l'indicazione anche di formule-tipo).

Con riferimento, invece, alla diversa ipotesi in cui i *curricula* siano inviati spontaneamente dagli interessati, i destinatari degli stessi, trovandosi di regola nell'impossibilità di fornire in via preventiva l'informativa, sono tenuti ad adempiere comunque, senza ritardo, a 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).

Nella precedente relazione annuale l'Autorità ha rilevato la confusa e carente tutela dei dati personali nei sistemi informativi in materia di lavoro, dovuta anche ad un quadro normativo stratificato e disomogeneo.

L'adozione di una disciplina più organica degli aspetti relativi ai flussi di dati nell'ambito del Sistema informativo lavoro ed una revisione delle modalità di redazione delle schede anagrafiche e professionali dei lavoratori era già prevista dal d.lg. n. 19 dicembre 2002, n. 297, recante disposizioni modificative e correttive del d. lg. 21 aprile 2000, n. 181. In virtù di tale decreto i Ministri del lavoro e delle politiche sociali e per l'innovazione e le tecnologie dovevano definire le modalità di trasferimento dei dati da parte dei servizi competenti, dei datori di lavoro e delle imprese fornitrici di lavoro temporaneo, nonché il modello di comunicazione, il formato di trasmissione ed il sistema di classificazione dei dati contenuti nella scheda anagrafica e nella scheda professionale dei lavoratori.

La promulgazione della l. 14 febbraio 2003, n. 30, recante *"Delega al Governo in materia di occupazione e mercato del lavoro"*, ha previsto la riforma della materia mediante la realizzazione di un sistema di strumenti intesi a garantire trasparenza ed efficienza al mercato del lavoro e a migliorare le capacità di inserimento professionale dei disoccupati e di quanti sono in cerca di una prima occupazione, nel rispetto delle competenze affidate alle regioni in materia di tutela e sicurezza del lavoro dalla legge costituzionale 18 ottobre 2001, n. 3, con particolare riferimento al sistema del collocamento, pubblico e privato. La nuova disciplina legislativa del 2003 prevede il mantenimento da parte dello Stato delle competenze in materia di conduzione coordinata ed integrata del sistema informativo lavoro e la ridefinizione del regime del trattamento dei dati relativi all'incontro tra domanda e offerta di lavoro, nel rispetto della l. n. 675/1996. Ciò anche al fine di favorire le esigenze di monitoraggio statistico, di prevenire forme di esclusione sociale e vigilanza sugli operatori, con previsione del divieto assoluto per gli operatori privati e pubblici di qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione dei lavoratori, anche con il loro consenso, in base all'affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale, o di famiglia, o di gravidanza, nonché ad eventuali controversie con i precedenti datori di lavoro. Viene inoltre vietata la raccolta, la memorizzazione o la diffusione di informazioni sui lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

Statistica e ricerca scientifica

25 Il codice deontologico per il trattamento dei dati a scopi statistici e di ricerca scientifica

Il 1° ottobre 2002 è stato pubblicato in *Gazzetta Ufficiale*, a cura del Garante, il Codice di deontologia e buona condotta per i trattamenti dei dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (SISTAN) (*Deliberazione* n. 13 del 31 luglio 2002).

Tale codice, previsto all'art. 10 del d.lg. 30 luglio 1999, n. 281, seguito dal Garante durante tutto l'*iter* preparatorio, è stato il frutto del lavoro che ha coinvolto numerosi soggetti pubblici e privati, tra cui rappresentanti dell'Istituto nazionale di statistica (Istat), dell'Istituto di studi ed analisi economica (ISAE), dell'Istituto per lo sviluppo della formazione professionale dei lavoratori (ISFOL) e della Presidenza del Consiglio dei ministri.

Le norme contenute nel codice, la cui osservanza costituisce condizione di liceità del trattamento dei dati, si applicano ai trattamenti effettuati da enti ed uffici statistica che, in relazione al loro ambito istituzionale, fanno parte o partecipano al SISTAN al fine di attuare il programma statistico nazionale.

Fra le caratteristiche più importanti del codice, si segnalano le forme di tutela introdotte per assicurare l'anonimato del cittadino, definendo i criteri per la valutazione del rischio di identificazione con l'associazione dei nominativi alle informazioni raccolte e attribuendo precise garanzie per il trattamento dei dati sensibili. I soggetti privati che partecipano al SISTAN e raccolgono tale categoria di dati devono farlo in forma anonima salvo casi di necessaria identificazione, anche temporanea, degli interessati, in cui sarà imprescindibile acquisire il consenso degli interessati e l'autorizzazione preventiva del Garante. Ulteriori disposizioni regolano l'informativa degli interessati, cui dovranno essere dettagliatamente resi noti gli scopi della ricerca, nonché la comunicazione e la diffusione dei dati, che a soggetti non facenti parte del SISTAN potranno pervenire, di regola, solo in forma aggregata. Inoltre, sono previste specifiche regole di condotta e misure di sicurezza soprattutto in relazione alla conservazione dei dati identificativi.

Un ruolo di controllo sulla corretta applicazione del codice è demandato anche alla Commissione per la garanzia dell'informazione statistica, istituita presso la presidenza del Consiglio, che provvederà a segnalare al Garante gli eventuali casi di inosservanza delle norme.

È, inoltre, di prossima adozione il codice deontologico che dovrà fornire indicazioni di dettaglio per la ricerca statistica effettuata da istituti universitari, enti di ricerca ed altri organismi non appartenenti al SISTAN.

Rinviando al paragrafo 9 "Banche dati di rilevanti dimensioni e censimento della popolazione" per le attività connesse al censimento della popolazione, devono qui evidenziarsi talune

problematiche emerse in sede locale a seguito della decisione di alcuni comuni di promuovere delle indagini conoscitive tra la popolazione.

Tali indagini, nei casi segnalati, benché fossero state definite come corollari del censimento della popolazione, avevano più i requisiti di sondaggi presso la popolazione che di vera e propria ricerca statistica e risultavano integralmente sottoposte alla disciplina della legge n. 675/1996 e del d.lg. n. 135/1999. È questo il caso, in particolare, della rilevazione progettata in un comune dove si intendeva svolgere un'indagine conoscitiva per conoscere le esigenze dei cittadini e coinvolgerli in una maggiore partecipazione alla vita politica e amministrativa del Paese.

Esaminando il progetto, è stato rilevato, tra l'altro, che con la rilevazione si intendevano perseguire diverse finalità non chiaramente illustrate al cittadino. Inoltre, molti dei quesiti posti apparivano estremamente dettagliati e, in alcuni casi, relativi anche ad informazioni di carattere sensibile. La nota esplicativa poi non evidenziava il carattere obbligatorio o facoltativo del conferimento di tali dati, cosa questa particolarmente importante, anche in relazione a talune finalità di carattere amministrativo che si intendeva perseguire con la progettata rilevazione (10 gennaio 2003).

Un altro comune ha avviato invece un sondaggio sulla condizione socio-economica degli utenti del servizio di assistenza domiciliare. Questa rilevazione, pur apparentemente non in grado di consentire l'individuazione delle persone coinvolte, in effetti -attraverso le modalità di consegna del questionario ed alcune informazioni ivi contenute- ha mostrato di poter consentire di risalire agli interessati. Anche in questo caso, la mancanza di chiarezza circa le finalità dell'indagine hanno reso difficile una valutazione in merito alla pertinenza e non eccedenza dei dati raccolti; in ogni caso, un'informativa carente e la mancata specificazione dell'obbligatorietà o facoltatività del conferimento dei dati, hanno indotto l'Ufficio a richiamare l'attenzione dell'ente sulla necessità di un attento rispetto della normativa vigente (25 ottobre 2002).

Associazioni, movimenti politici e partiti

26 Trattamento dei dati e realtà associative

All'inizio del 2002, il settore delle associazioni è stato interessato da alcune importanti novità sul piano normativo, di cui si è già dato anticipatamente conto anche nella *Relazione 2001* (p. 54).

Ci si riferisce alle 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- e che sono state oggetto di attenzione da parte del Garante in alcune delle autorizzazioni generali per il trattamento dei dati sensibili, ed in particolare nell'autorizzazione n. 3/2002.

Sulla base di tali novità, il trattamento di informazioni riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria non è più soggetto alla specifica disciplina indicata in materia di dati sensibili (consenso scritto dell'interessato e all'autorizzazione del Garante).

E' stata, inoltre, introdotta una semplificazione riguardo all'attività di associazioni, od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, i quali non devono più raccogliere necessariamente il consenso degli aderenti (o dei soggetti che, in relazione alle finalità statutarie perseguite, hanno contatti regolari con l'ente), per il trattamento dei loro dati sensibili, sempre che i dati non siano divulgati a terzi e l'associazione abbia adottato idonee misure per la tutela di tali dati (misure che, in sede di prima applicazione del d.lg. n. 467/2001, dovevano essere predisposte entro lo scorso 30 giugno).

Anche in questo caso, il d.lg. n. 467/2001 ha incoraggiato forme di maggiore responsabilizzazione dei soggetti che gestiscono i dati. Nel trattamento di eventuali dati sensibili di propri aderenti o sostenitori, gli enti *no profit* devono comunque rispettare le indicazioni fornite dal Garante con la citata autorizzazione generale n. 3/2002 circa i limiti e le modalità di trattamento, conservazione e comunicazione dei dati medesimi.

Tali aspetti sono stati confermati nelle risposte che l'Autorità ha fornito a diverse richieste di autorizzazione al trattamento di dati sensibili inviate da organismi associativi. In taluni casi, i richiedenti sono stati invitati a verificare se i trattamenti effettuati non rientrassero tra quelli già autorizzati dal Garante in via generale o, altrimenti, ad indicare le circostanze del tutto particolari o le situazioni eccezionali in base alle quali si sarebbe resa eventualmente necessaria un autorizzazione specifica.

Nell'ambito delle diverse iniziative dell'Autorità sul tema dei trattamenti di dati personali nell'ambito delle realtà associative sono da ricordare inoltre:

- il parere reso ad un'arciconfraternita in merito alla possibilità di affiggere al proprio

albo la notizia dei provvedimenti adottati nei confronti degli iscritti. In tal caso è stato rilevato che, stante la natura privata dell'ente, il trattamento dei dati personali degli iscritti doveva avvenire nel rispetto degli artt. 10, 11 e 20 della legge n. 675/1996 e, quindi, previo consenso degli iscritti. Allo scopo è stato ribadito che è sufficiente una formula concisa ma puntuale, da riportarsi nel modulo di adesione, che autorizzi l'arciconfraternita al trattamento dei dati nella misura necessaria per il perseguimento degli scopi statutari, sempre che tutte le operazioni di trattamento dei dati personali degli iscritti siano previste nello stesso statuto e che lo stesso sia stato previamente portato a conoscenza degli interessati. Con un consenso espresso nei termini sopra descritti può essere autorizzata anche l'eventuale pubblicazione sull'albo dell'ente. Ovviamente, nel caso in cui i dati soggetti a pubblicazione avessero riguardato anche informazioni di natura sensibile, fatto salvo il divieto di diffusione di dati sulla salute, occorre rispettare quanto previsto dall'autorizzazione generale del Garante n. 3 del 2002 (13 gennaio 2003);

- i diversi interventi seguiti alle segnalazioni inviate da parte di un gruppo cittadini disabili, i quali hanno lamentato di essere stati contattati dal segretario locale dell'AISTOM, una delle associazioni che riunisce i pazienti stomizzati, con l'invito a scrivere all'associazione stessa al fine di richiedere un'assemblea straordinaria per il rinnovo delle cariche sociali, utilizzando così dati personali per fini non previsti dallo statuto;

- decisione, nell'ambito di un ricorso, con la quale, a fronte di 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 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).

27 Confessioni religiose

Continuano a pervenire numerose segnalazioni di cittadini che, mutando il proprio orientamento religioso, hanno chiesto di modificare i dati personali contenuti nei registri dei battezzati e conservati presso gli archivi parrocchiali, motivando tale esigenza con le proprie convinzioni ateistiche.

Il Garante, già in passato (cfr. *Provv.* 19 settembre 1999, in *Bollettino* n. 9, p. 54), aveva evidenziato l'impossibilità di cancellare il nominativo dal registro dei battezzati, essendo l'annotazione relativa ad un fatto realmente avvenuto e in ragione del fatto che la cancellazione ai sensi dell'art. 13 della legge n. 675 può essere richiesta solo quando i dati sono trattati in violazione di legge oppure quando la loro conservazione non è necessaria agli scopi per i quali i dati sono stati raccolti e utilizzati. Nella medesima occasione l'Autorità aveva però precisato che l'interessato può però chiedere l'aggiornamento, la rettificazione ed eventualmente l'integrazione nell'ipotesi in cui si tratti di dati inesatti o incompleti; questa soluzione è stata confermata anche dalla giurisprudenza di merito (cfr. Trib. Padova, sez. ci n. 3531/99 RG del 26 maggio 2000).

Tali orientamenti sono stati ribaditi in occasione di alcune istanze esaminate nel corso del 2002, nell'ambito di decisioni riguardanti taluni ricorsi.

In due casi analoghi l'interessato aveva presentato ricorso all'Autorità dopo aver richiesto senza esito, alla parrocchia dove era stato battezzato, l'annotazione, accanto al proprio nome, di una postilla che specificasse la volontà di non voler essere più considerato membro della chiesa cattolica.

Il Garante ha ritenuto legittima "in entrambi i casi" l'aspirazione del ricorrente a veder correttamente rappresentata la propria immagine in relazione alle attuali convinzioni religiose: si trattava, infatti, di un'istanza volta ad aggiornare ed integrare i dati personali con specifico riferimento al "dato sensibile" relativo all'appartenenza religiosa, che può essere soddisfatta attraverso una semplice annotazione a margine del dato da rettificarsi.

Con la decisione sui ricorsi il Garante ha quindi invitato i parroci ad aggiornare il registro dei battezzati nel senso richiesto (*Provv.* 18 luglio e 30 settembre 2002).

In un'analoga vicenda il Garante ha parimenti accolto il ricorso dell'interessato ed ha ordinato al parroco -che non aveva provveduto ritenendo di non essere autorizzato dalla normativa canonica- di apporre l'annotazione sul registro parrocchiale dei battesimi (*Provv.* 10 ottobre 2002).

Infine, in un altro caso, riconoscendo il diritto dell'interessato a veder correttamente rappresentata la propria immagine in relazione alle proprie convinzioni originarie o sopravvenute, (mediante annotazione a margine del dato da rettificarsi ferma restando la documentazione del fatto storico dell'avvenuto battesimo), il Garante ha precisato che la sola, eventuale conservazione dell'istanza presentata dal ricorrente in allegato al registro dei battesimi non è sufficiente a far risultare in modo in equivoco e permanente, dal registro stesso, la volontà dell'interessato di non appartenere più alla Chiesa cattolica (*Provv.* 19 marzo 2003).

28 Condomini e multiproprietà

Diversi profili di protezione dei dati personali in ambito condominiale, approfonditi nel corso degli anni precedenti, sono stati ripresi nel corso dell'anno per rispondere al sempre rilevante numero di segnalazioni e quesiti pervenuti all'Autorità, che confermano la diffusa sensibilità dei cittadini circa i temi della tutela della riservatezza nella sfera condominiale.

Tra i filoni tematici che hanno visto maggiormente impegnato il Garante, si segnala, anzitutto, quello concernente la divulgazione dei dati personali all'interno del condominio, in relazione al quale l'Autorità ha nuovamente ribadito i limiti e le cautele da adottare nel mettere a disposizione dei condomini le reciproche informazioni di carattere personale, e segnatamente, i nominativi e i dati contenuti in bilanci e prospetti contabili.

Analogamente, sono stati posti numerosi quesiti tanto dagli interessati, quanto da amministratori di condominio, sul tema della diffusione di dati personali riguardanti eventuali situazioni di morosità di singoli condomini, allo scopo di appurare se le modalità di volta in volta in concreto utilizzate, in quanto potenzialmente idonee a rendere tali informazioni accessibili ad un numero indeterminato di soggetti esterni al condomino, fossero compatibili, ed in quali limiti, con le disposizioni contenute nella legge n. 675/1996. Su tale argomento, l'Autorità ha confermato la posizione già assunta nei provvedimenti e nelle decisioni adottate nel corso degli anni precedenti.

Altre richieste di parere o chiarimenti pervenute all'Autorità, hanno messo in luce interessanti profili tematici scaturenti dall'applicazione della legge n. 675/1996 in ambito condominiale, consentendo un approfondimento ulteriore di questioni già parzialmente esaminate negli scorsi anni.

Si segnala, al riguardo, un parere rilasciato all'inizio del 2003, con il quale l'Ufficio del Garante ha ritenuto ammissibile, per il condomino, la conoscenza dei dati disponibili presso l'amministratore relativi agli indirizzi degli altri condomini, considerati, alla stessa stregua dei nominativi, elementi essenziali per la regolare convocazione delle assemblee e per la comunicazione dei relativi avvisi, anche tenuto conto che si tratta di informazioni desumibili dai documenti o dagli atti notarili eventualmente esibiti dagli interessati o, comunque, acquisiti dal condominio.

Inoltre, ad integrazione di quanto già sostenuto in precedenti decisioni dell'Autorità in materia di divulgazione degli estremi identificativi delle utenze telefoniche, si è precisato che l'amministratore può comunicare il numero di telefono di un condomino, ad altro condomino che lo richieda, oltre che previa acquisizione del consenso dell'interessato, anche quando tale possibilità sia prevista nel regolamento condominiale, oppure nei casi particolari di necessità ed urgenza (es. per prevenire o limitare danni agli immobili in condominio).

Nello stesso parere (premessa, sulla base degli orientamenti giurisprudenziali e dottrinali in materia, l'applicabilità dei principi enunciati in materia di condominio anche nei confronti della gestione di edifici in multiproprietà a scopo residenziale), si è ritenuto che la normativa sulla riservatezza non impedisca l'accesso, da parte del proprietario di immobile in multiproprietà, ai dati disponibili presso l'amministratore riguardanti i nominativi e gli indirizzi di altri comproprietari (anche con residenza o domicilio diverso dall'immobile in multiproprietà), per le medesime finalità già delineate in ambito condominiale.

Attività forense, investigazione privata e liberi professionisti

29 Liberi professionisti e albi professionali

Il Garante si è occupato nuovamente dell'impatto della legge n. 675/1996 sull'attività svolta dai liberi professionisti, anche per quanto riguarda il regime di pubblicità degli albi professionali e degli atti connessi allo "status" d'iscritto all'albo.

La legge n. 675 non ha modificato la disciplina legislativa relativa agli albi professionali, che per loro natura sono destinati ad un regime di pubblicità, anche in funzione della tutela dei diritti di coloro che a vario titolo hanno rapporti con gli iscritti all'albo.

Le norme che regolano i vari albi permettono ai diversi ordini professionali, secondo le diverse modalità previste nei singoli casi, di comunicare e diffondere a soggetti pubblici e privati i dati personali contenuti nei rispettivi albi, compresi quelli relativi a provvedimenti di sospensione o interruzione dell'esercizio della professione.

L'Autorità, nel decidere su un ricorso presentato da un avvocato che lamentava, in particolare, che il numero della rivista trimestrale nel quale era inserito il provvedimento interdittivo adottato nei suoi confronti, fosse giunto agli iscritti quando il periodo di sospensione dall'attività si era esaurito e l'interessato aveva già ripreso ad esercitare, ha affermato che la notizia dell'esistenza di una grave sanzione disciplinare applicata da un ordine professionale non è "segreta" e il cittadino può conoscerla. E' stato così chiarito che l'inserimento nella rivista del Consiglio dell'ordine della notizia dell'esistenza di un provvedimento di sospensione o di radiazione dall'esercizio professionale non viola i diritti dell'avvocato interessato, purché i dati siano esatti e completi (*Provv.* 25 settembre 2002).

Analoga indicazione è stata fornita all'Ordine degli psicologi del Lazio, ritenendo legittima la pubblicazione sul notiziario dell'Ordine dell'elenco nominativo degli iscritti morosi. Ciò in quanto la specifica normativa contenuta nella l. n. 56/1989 disciplina il regime di pubblicità in materia. La lecita divulgabilità delle informazioni relative ai suddetti provvedimenti disciplinari tramite riviste, notiziari o altre pubblicazioni curate dal Consiglio dell'Ordine deve comunque garantire il diritto dell'interessato ad un'informazione corretta e completa anche in relazione al verificarsi di eventuali sviluppi favorevoli per quest'ultimo emergenti anche a seguito di contestazione (*Provv.* 10 dicembre 2002).

Merita infine di essere ricordato, con particolare riferimento ai cd. "dati sensibili", che il Garante ha reiterato l'autorizzazione n. 4/2002 in tema di trattamento di tali categorie di dati da parte dei liberi professionisti. Tale provvedimento tiene 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.

30 Raccolta di dati per finalità di difesa

La legge n. 675 ha inciso in modo particolare sulle attività di raccolta di informazioni svolte da investigatori privati, su incarico di terzi, al fine di raccogliere materiale probatorio da utilizzare per eventuali azioni legali o direttamente nell'ambito di procedimenti giudiziari e anche disciplinari.

La legge, che riconosce sotto diversi aspetti la liceità di queste forme di trattamento, collegate ad esigenze di tutela di diritti, ha rinviato al codice di deontologia per l'investigazione privata la disciplina in dettaglio del trattamento di dati sensibili nello svolgimento di indagini difensive o, comunque, in connessione alla difesa giudiziaria. In tale sede saranno individuati, tra l'altro, tempi ragionevoli di conservazione dei dati, la raccolta di determinati dati sensibili e i diversi doveri dei soggetti che a vario titolo collaborano al trattamento dei dati per le predette finalità. I lavori di tale codice, promossi dal Garante con provvedimento del 10 febbraio 2000, sono in fase di conclusione.

Il Garante ha altresì rilasciato l'autorizzazione generale n. 6/2002, relativa al trattamento di dati sensibili da parte degli investigatori privati, nella quale, tra i diversi aspetti disciplinati, si è richiamata l'esigenza che il trattamento dei dati raccolti sia strettamente indispensabile per eseguire specifici incarichi conferiti e che, una volta conclusa l'attività investigativa, il trattamento debba cessare in ogni sua forma (fatta salva, ovviamente, l'immediata comunicazione dei risultati al difensore o al soggetto che ha conferito l'incarico). Le prescrizioni di tale autorizzazione potranno essere in seguito integrate dal menzionato codice di deontologia.

Le questioni connesse alla raccolta dei dati per l'esercizio del diritto di difesa 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 relativa ad un procedimento di separazione personale (*Provv.* 28 febbraio 2002).

Con tre distinti provvedimenti, fondati su analoghe motivazioni (*Provv.* 19 febbraio 2002, in *Bollettino* n. 25, p. 17) concernenti 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 invece rilevato che alcuni dati personali erano stati acquisiti direttamente presso l'interessato, mediante indebito ascolto, registrazione o intercettazione effettuati a cura di un istituto investigativo, appurando che tali modalità di raccolta violavano anche 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 disposto sia nei confronti della agenzia investigativa, sia della società committente, il divieto di ogni ulteriore trattamento dei dati raccolti. Una comunicazione di reato è stata inviata alla competente autorità giudiziaria.

Il Tribunale di Bergamo, confermando l'intero impianto decisorio del Garante nell'ambito del procedimento di opposizione ai sopra citati provvedimenti adottati il 19 febbraio 2002, ha confermato l'illegittimità del trattamento dei dati personali contenuti nel rapporto investigativo in quanto acquisiti presso l'interessato (con mezzi tecnici di intercettazione a distanza e con mezzi di registrazione) senza la prevista obbligatoria informativa.

Settore del credito, finanziario ed assicurativo

31 Istituti di credito

Il settore in esame è stato al centro, anche nel 2002, dell'attenzione di consumatori e delle relative associazioni, nonché di imprenditori e professionisti, che spesso si sono rivolti all'Autorità per far chiarire delicati aspetti relativi alla raccolta, al trattamento e alla comunicazione dei dati che li riguardano, alla luce di un quadro normativo, quale quello bancario e finanziario, particolarmente complesso ed in fase di continua evoluzione, anche per le novità ed i servizi resi possibili dal rapido avanzarsi delle nuove tecnologie (cfr. *Relazione 2001*, p. 60).

Risulta anzitutto confermato il dato del progressivo aumento delle segnalazioni e delle istanze presentate da clienti degli istituti di credito avverso le violazioni delle norme poste a tutela della riservatezza nei rapporti bancari c.d. *on-line*, relativamente alla divulgazione a persone estranee di informazioni su proprie operazioni, conti od investimenti.

In proposito, è stato assunto un primo provvedimento in relazione al caso verificatosi nell'*e-banking*, riguardante il cliente di una banca *on-line* che, attraverso *Internet*, ha consultato non solo i dati del suo conto corrente, ma anche quelli di altri clienti della banca. L'interessato ha presentato ricorso al Garante che ha poi, nell'ambito di un distinto procedimento, svolto un accertamento sul sistema informatico della banca allo scopo di verificare i sistemi di sicurezza adottati dall'istituto di credito e il loro grado di affidabilità riguardo alla tutela della riservatezza dei dati personali della clientela (*Provv.* 11 novembre 2002). E' imminente l'adozione del provvedimento conclusivo del secondo procedimento.

Nel settore del credito si registra un aumento di reclami anche in riferimento a temi più tradizionali, quali quelli del rispetto del c.d. segreto bancario, dell'accesso da parte di eredi ai dati relativi a rapporti bancari e finanziari di defunti e della richiesta o dell'acquisizione di documenti di riconoscimento e di altre informazioni da parte delle banche, in correlazione alla presentazione di assegni per il pagamento, al cambio di valuta o all'esecuzione di altre operazioni.

In un caso il Garante è intervenuto ricordando che il diritto di accesso ai dati personali di un defunto può essere esercitato da chiunque vi abbia interesse (art. 13, l. n. 675/1996). Nel caso specifico della richiesta di accesso avanzata dall'erede, è stato riconosciuto il diritto ad ottenere tutte le informazioni di carattere personale relative al defunto, detenute da un istituto di credito, con particolare riferimento ai movimenti bancari compiuti dai cointestatari su alcuni depositi del parente deceduto, estinti dopo la sua morte (*Provv.* 3 aprile 2002)

Nell'ambito delle diverse iniziative dell'Autorità sul tema dei trattamenti di dati nel settore del credito sono da ricordare inoltre:

- la decisione, adottata nell'ambito di un ricorso, con la quale l'Autorità ha censurato il comportamento di una banca che inviava materiale pubblicitario nonostante la volontà

contraria del cliente. Nel caso in esame era emerso che il cliente, al momento della sottoscrizione dei modelli di informativa e consenso, aveva manifestato la propria contrarietà all'utilizzo dei dati personali per fini di informazione commerciale, ricerche di mercato ed offerte di prodotti o servizi, ed aveva poi ribadito tale richiesta. Il comportamento della banca, che non avrebbe dovuto inviare materiale promozionale, è risultato illegittimo e l'Autorità ha disposto che copia degli atti fosse inviata all'autorità giudiziaria per valutare se l'istituto di credito fosse incorso nel reato di trattamento illecito di dati personali (art. 35 legge n. 675/1996), punito con la reclusione fino ad un massimo di tre anni (*Provv.* 17 aprile 2002);

- la decisione con la quale l'Autorità, accogliendo il ricorso di un cittadino, ha statuito che alcune informazioni -contenute nella segnalazione di blocco della sua carta di credito trasmessa dalla banca ad una società- venissero rettificate, come richiesto, perché basate su motivazioni (morosità e rifiuto di riconsegnare la carta) non rispondenti al vero. Dopo l'invito del Garante ad aderire alle istanze del cliente, la banca aveva trasmesso a quest'ultimo la documentazione richiesta, ma aveva affermato di non poter rettificare i dati riferiti al blocco della carta di credito, in quanto tali annotazioni presupponevano una diversa valutazione di situazioni di fatto che erano oggetto di contenzioso presso l'autorità giudiziaria. Sosteneva anche che il ricorso dovesse essere dichiarato inammissibile proprio con riguardo ai procedimenti giudiziari pendenti. Nel decidere sul ricorso il Garante ha respinto tale l'eccezione di inammissibilità proposta dalla banca in quanto i procedimenti pendenti presso il giudice ordinario riguardavano una domanda su profili diversi (in particolare una controversia per risarcimento danni) e non vertevano, quindi, sul medesimo oggetto del ricorso avviato innanzi all'Autorità;

- la decisione sul ricorso di un cliente di una banca che si è opposto al trattamento dei propri dati personali nella parte riguardante l'eventuale ed ulteriore comunicazione illecita al coniuge ed utilizzate nel procedimento di separazione giudiziale. Con riferimento all'attuale utilizzo delle informazioni acquisite illecitamente dal coniuge del ricorrente nel procedimento di separazione giudiziale, è stato disposto l'invio della decisione del Garante al tribunale, per le valutazioni di competenza (*Provv.* 17 settembre 2002).

In merito, poi, alla questione relativa alla richiesta di documenti di riconoscimento da parte di banche, sono stati avviati, nel corso di quest'anno, accertamenti per specifici casi. In considerazione del rilevante numero di segnalazioni giunte all'Autorità su tale argomento, nei prossimi mesi l'Autorità intende completare una valutazione più approfondita per fornire precise indicazioni sulla corretta applicazione della legge n. 675/1996.

Ulteriore fonte di intensa attività è risultato l'esame delle numerose richieste di esonero dall'obbligo di informativa agli interessati in materia di cartolarizzazione dei crediti, formulate con riferimento al provvedimento di carattere generale adottato il 4 aprile 2001, che ha autorizzato le società che svolgono tali operazioni ad effettuare l'informativa in forma semplificata, attraverso le modalità alternative della sua pubblicazione in *G.U.* ed in alcuni giornali nazionali e, ove previsto, locali.

Sono, inoltre, pervenute di recente alcune segnalazioni nelle quali clienti di una banca hanno lamentato di essere venuti a conoscenza solo attraverso i mezzi di informazione che le agenzie presso le quali sono titolari di un rapporto di conto corrente bancario sono state

cedute ad un'altra banca. Le suddette segnalazioni, che riguardano il tema relativo alla cessione a banche di *rapporti giuridici individuali in blocco* (ai sensi dell'art. 58 del decreto legislativo n. 385/1993), saranno esaminate in relazione ai diversi profili di *privacy* che possono emergere in collegamento a questa tipologia di operazioni finanziarie.

In relazione alla semplificazione degli adempimenti nel settore bancario e finanziario, va da ultimo sottolineata l'importanza delle recenti modifiche introdotte dal decreto legislativo n. 467/2001, soprattutto per ciò che attiene alla previsione di nuovi casi che rendono superfluo il consenso anche per operazioni di comunicazione di dati personali strumentali all'esecuzione di obblighi contrattuali. Ciò dovrebbe comportare la 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.

32 Intermediazione finanziaria

In relazione al settore del credito e della finanza, meritano un cenno a parte le questioni relative alla tutela dei dati personali nell'ambito delle attività di intermediazione finanziaria, incentrate, per diversi aspetti, sulla raccolta, sul trattamento e sullo scambio di informazioni relative sia agli investitori, sia alle società che operano nei mercati finanziari. Tali attività stanno infatti subendo, nel corso di questi ultimi anni, una significativa trasformazione a causa della rapida diffusione anche in Italia delle reti telematiche e delle tecnologie della comunicazione e dell'informazione.

Sotto questo profilo, emerge evidente la preoccupazione dei clienti degli operatori e intermediari finanziari (banche, SIM, ecc.) per i delicati problemi della sicurezza e della riservatezza dei dati trasmessi, registrati o memorizzati elettronicamente, derivanti da servizi che permettono ai clienti di acquisire informazioni o effettuare investimenti tramite *Internet* (il c.d. *trading on-line*).

Oltre al descritto caso, nel paragrafo precedente, relativo al c.d. *e-banking*, il Garante ha esaminato una questione riguardante l'accesso del cliente di una banca ai dati contenuti nelle registrazioni delle telefonate, con le quali l'interessato aveva ordinato l'acquisto o la vendita di titoli e pacchetti azionari (*Provv.* 19 giugno 2002).

Nel caso sottoposto all'Autorità, il cliente aveva chiesto all'istituto di credito di accedere al contenuto delle registrazioni, laddove ancora conservate, di alcune telefonate effettuate nel corso del 1999, senza, tuttavia, ricevere da questa riscontro alla propria richiesta.

L'istituto bancario, su invito formulato dal Garante, ha fornito le informazioni richieste, dichiarando, però, che le registrazioni magnetiche degli ordini e delle autorizzazioni erano conservate, come previsto dalla vigente normativa, per almeno due anni. Pertanto, ogni registrazione attinente al periodo indicato dall'interessato non era più conservata presso l'istituto di credito, il quale aveva detenuto i dati per il solo periodo temporale previsto e non era più in possesso di tali informazioni.

Un argomento rilevante per il numero di casi segnalati al Garante riguarda il comportamento di promotori o intermediari finanziari per ciò che attiene al trattamento e alla divulgazione dei dati della clientela nell'ambito di servizi di distribuzione di prodotti finanziari bancari o assicurativi.

L'Ufficio del Garante terminerà prossimamente l'esame dei casi rappresentati da alcuni investitori i quali hanno segnalato di non aver ricevuto informazioni o di non aver autorizzato la cessione dei dati che li riguardano a consulenti di fiducia o collaboratori delle banche o delle società di intermediazione mobiliare cui si erano rivolti per i propri investimenti (ad esempio, nuovi promotori in sostituzione dei precedenti).

Va anche ricordato il parere rilasciato dal Garante in merito ad un quesito riguardante alcune proposte di modifiche regolamentari che la società di gestione della Borsa ha introdotto, sulla base delle determinazioni della Commissione di vigilanza, per assicurare una maggiore diffusione di informazioni concernenti operazioni mobiliari compiute da *manager* di società quotate, relative alle medesime società o a loro controllate. Il Garante ha evidenziato che la comunicazione di informazioni relative al controvalore e alle date degli scambi azionari e finanziari operati dagli amministratori, direttori generali o sindaci delle predette società non contrasta, in termini generali, con i principi stabiliti dalla legge n. 675, mentre spetta alla Consob verificare la loro conformità alla normativa italiana e comunitaria del settore e valutarne l'idoneità ad assicurare la trasparenza del mercato, l'ordinato svolgimento delle negoziazioni e la tutela degli investitori.

Le disposizioni sottoposte al vaglio del Garante prevedevano l'obbligo per le società quotate di comunicare periodicamente o, a seconda della rilevanza, tempestivamente le operazioni finanziarie eseguite da soggetti che, per i loro incarichi societari, hanno accesso a particolari informazioni (dette privilegiate o *"price sensitive"*), oppure effettuate da loro stretti familiari o per il tramite di fiduciari od interposte persone. Ogni società è tenuta, in proposito, ad adottare un codice di comportamento che identifichi le cosiddette "persone rilevanti" al proprio interno (coloro che le amministrano, dirigono o vigilano) e che richieda loro di comunicare le informazioni relative a tali operazioni, in modo da permettere alle società di divulgarle al pubblico dei risparmiatori attraverso gli strumenti informatici messi a disposizione dalla Borsa.

Le informazioni oggetto di diffusione si riferiscono nominativamente agli amministratori, ai direttori generali, ai sindaci, etc., e non agli eventuali terzi attraverso i quali vengono effettuate le operazioni (che non vengono identificati e che non hanno alcun diretto obbligo informativo nei confronti delle società emittenti). I trattamenti di dati personali che ne deriverebbero -ha chiarito il Garante- sono apparsi, quindi, conformi al principio di pertinenza e non eccedenza dei dati (art. 9 legge n. 675/1996), essendo riferiti soltanto ai dati anagrafici delle "persone rilevanti", nonché alla data, alla tipologia ed al controvalore delle operazioni mobiliari (*Provv.* 5 giugno 2002).

L' Autorità ha, inoltre, affrontato il delicato problema del ruolo che verranno a svolgere i codici di comportamento nei confronti degli esponenti delle società emittenti, avendo osservato che, qualora le regole di comportamento concretamente adottate non siano lasciate alla spontanea adesione ed osservanza da parte dei destinatari, ma siano per loro nella sostanza cogenti, in quanto rientranti nei più generali doveri, responsabilità ed impegni assunti nei rispettivi rapporti societari, i dati delle "persone rilevanti" potrebbero essere acquisiti e diffusi senza raccogliere il loro consenso, poiché questi trattamenti rientrerebbero tra quelli necessari per l'adempimento di obblighi informativi divenuti giuridicamente vincolanti anche per gli interessati (legge n. 675/1996).

33 Centrali rischi e società finanziarie

Nel 2002 si è registrato un ulteriore, significativo incremento di ricorsi, segnalazioni e reclami presentati da cittadini, imprese ed associazioni di consumatori, nei confronti di banche e società finanziarie, nonché delle c.d. "centrali rischi" private, ossia delle società che gestiscono sistemi informativi di rilevazione dei rischi creditizi, di cui nel corso di questi ultimi anni il Garante si è più volte occupato, come evidenziato nelle precedenti relazioni.

Al riguardo, l'Autorità è fra l'altro intervenuta (*Provv.* 6 giugno 2002) nell'ambito di un procedimento ai sensi dell'art. 29 della l. n. 675/1996, decidendo sul ricorso di un interessato che lamentava l'inerzia della società alla quale si era rivolto chiedendo di cancellare e di non diffondere ulteriormente, senza il proprio consenso, alcune informazioni che lo riguardavano, relative ad operazioni di finanziamento personale detenute nella banca dati della centrale rischi. Veniva infatti ritenuto dal ricorrente che la diffusione di queste informazioni fosse la causa del rifiuto, senza motivazione, della concessione di altri piccoli prestiti o fidi da parte di alcuni istituti bancari. Con la decisione l'Autorità ha affermato che la centrale rischi privata che conserva e diffonde nel circuito bancario e finanziario informazioni relative a prestiti richiesti e non concessi, oppure oggetto di rinuncia da parte dello stesso richiedente, agisce in violazione delle disposizioni in materia di protezione dei dati personali.

In considerazione della rilevanza assunta da tale tematica, il Garante aveva ritenuto necessario, alla fine del 2001 (*Relazione 2001* p. 67), avviare un'indagine approfondita anche attraverso richieste di informazioni ed incontri con gli operatori del settore e con le relative associazioni di categoria, così da poter fornire alcune indicazioni e chiarimenti per una corretta applicazione delle norme sulla tutela dei dati personali da parte dei soggetti che gestiscono le centrali rischi, eliminando larga parte del contenzioso esistente con gli interessati.

A conclusione della suddetta indagine il Garante ha adottato un provvedimento di carattere generale (*Provv.* 31 luglio 2002) che riassume l'orientamento già espresso in materia nei numerosi provvedimenti emessi da questa Autorità, ed individua alcune condizioni per la raccolta, la conservazione e l'uso delle informazioni presenti nei sistemi informativi di rilevazione dei rischi creditizi, anche in vista del codice deontologico la cui sottoscrizione è stata promossa dal Garante con deliberazione del 10 aprile 2002.

Le finanziarie e le banche si rivolgono alle "centrali rischi" per valutare le richieste di finanziamento presentate dai clienti, soprattutto nel settore del credito al consumo e alle famiglie (relativi ai beni di largo consumo, come, ad esempio, elettrodomestici, telefoni cellulari, computer, automobili, etc.), obbligandosi, anche sulla base di regolamenti consortili ed accordi associativi, a comunicare, con sistematicità, i dati relativi a coloro che li richiedono.

Le "centrali rischi" private possono essere connotate come banche dati "negative" (che registrano solo dati personali relativi a morosità, segnalazioni di sofferenze o esistenza di azioni

legali, procedure concorsuali o cessioni del credito a terzi), mentre la maggior parte delle "centrali rischi" operanti in Italia gestiscono banche dati di tipo positivo/negativo, cioè raccolgono informazioni sul rapporto di finanziamento a partire dalla richiesta dell'interessato, indipendentemente dall'esistenza di inadempimenti.

A differenza del servizio di centralizzazione dei rischi della Banca d'Italia o dell'archivio di recente istituzione a cura del medesimo Istituto relativo alla rilevazione dei rischi di importo contenuto, nel nostro ordinamento manca una specifica normativa di riferimento che disciplini le attività svolte dai soggetti privati che gestiscono i descritti sistemi informativi.

Al fine di giustificare la comunicazione dei dati relativi al finanziamento da parte dell'istituto bancario o finanziario alle "centrali rischi" private, e la successiva utilizzazione degli stessi dati da parte di queste ultime, gli operatori del settore hanno inserito nella modulistica contrattuale clausole di informativa agli interessati e di richiesta del consenso al trattamento di dati personali. Tuttavia, la questione relativa alla liceità delle prassi contrattuali finora seguite dagli operatori, non è stata affrontata nel predetto provvedimento del 31 luglio 2002, meritando un approfondimento in altra sede, alla luce del quadro normativo introdotto, mentre l'indagine era in corso, dal d.lg. n. 467/2001.

Nel provvedimento generale sono stati invece esaminati diversi profili relativi alle attività di raccolta, conservazione e trattamento di dati personali presenti nei circuiti privati di rilevazione dei rischi creditizi.

In particolare gli operatori sono stati richiamati a fornire ai clienti indicazioni precise sugli estremi identificativi delle "centrali rischi" alle quali i dati vengono trasmessi, nonché sugli scopi e sulle modalità di raccolta, registrazione e circolazione dei dati, in modo da garantire piena comprensione da parte degli interessati di questi diversi aspetti.

E' stato poi ricordato che i dati così raccolti possono essere trattati solo in stretta relazione con l'istruttoria di una richiesta di finanziamento e che, pertanto, è illecita l'utilizzazione da parte di banche e finanziarie delle informazioni presenti nelle "centrali rischi" per scopi ulteriori o comunque estranei all'attività di rilascio o gestione dei finanziamenti, ad esempio, per scopi collegati ad attività di *marketing*.

L'Autorità ha, altresì, ribadito l'esigenza di assicurare riscontro immediato e completo alle richieste di accesso, rettifica e cancellazione dei dati da parte degli interessati, in modo da garantire un maggiore rispetto dei relativi diritti, tenuto conto che alcuni comportamenti "scorretti" espongono sia le "centrali rischi", sia le banche e le finanziarie a responsabilità civile, anche sul piano dei danni non patrimoniali. Al riguardo è stata considerata opportuna la prassi, seguita da alcuni operatori, di sospendere la visualizzazione dei dati per il periodo necessario ad effettuare le verifiche con l'istituto bancario o finanziario al fine di fornire riscontro alle richieste degli interessati.

Riguardo ai problemi, più sentiti dai consumatori, della registrazione e della comunicazione dei dati relativi alle morosità nei pagamenti, il Garante ha chiesto di uniformare i criteri seguiti nei vari circuiti informativi per la segnalazione dei ritardi di pagamento delle rate sca-

dute, tenendo conto della reale gravità degli inadempimenti, in modo tale da non arrecare pregiudizi ingiustificati ai diritti degli interessati.

Le attuali modalità di gestione dei sistemi privati di rilevazione dei rischi creditizi, infatti, non sempre permettono di distinguere adeguatamente tra eventi da considerare fisiologici in un rapporto destinato a svolgersi nel tempo (ma che non incidono sull'affidabilità e solvibilità della clientela) e situazioni più critiche relative a inadempienze gravi e reiterate.

Per ciò che attiene, poi, alla segnalazione delle c.d. morosità alle "centrali rischi", l'Autorità ha segnalato di effettuarle *solo in caso di mancato pagamento di somme consistenti, di più rate o di gravi ritardi* (specialmente quando si tratta di finanziamenti di basso importo con rate di modesta entità) e a prevedere soglie temporali minime o di più rate cumulate (ad esempio per ritardi di almeno *quattro mesi* o di quattro rate, secondo la prassi già seguita da alcuni operatori), in modo da evitare che la comunicazione di mancati pagamenti avvenga quando ciò sia causato da anomalie o disguidi postali e bancari, non sempre imputabili agli interessati.

E' stato, inoltre, segnalato alle banche ed alle società finanziarie, prima di effettuare la segnalazione della morosità alla centrale rischi, di dare, comunque, un preavviso agli interessati affinché possano eventualmente intervenire.

Particolare attenzione è stata rivolta alla necessità di riconsiderare la congruità del tempo di conservazione delle informazioni di carattere negativo relative ai rapporti di finanziamento. In molti casi sottoposti all'attenzione del Garante tale termine è risultato eccedente rispetto alla finalità perseguita. L'obiettivo è, in sostanza, quello di evitare che l'ingiustificata presenza nelle banche dati delle "centrali rischi" di un'ampia quantità di dati non sempre o non più significativi (lievi morosità successivamente sanate, brevi ritardi nei pagamenti poi regolarmente effettuati ecc.) possa determinare effetti pregiudizievoli per gli interessati, anche in relazione alla possibilità di avere poi accesso a nuovi crediti.

L'Autorità non ha ritenuto poi giustificata la conservazione da parte delle "centrali rischi" dei dati di coloro ai quali non è stato concesso un finanziamento o che vi hanno rinunciato, in considerazione del fatto che il rapporto di finanziamento non si è instaurato o si è comunque interrotto ad uno stadio che non legittima una successiva utilizzazione dei dati, (spesso, peraltro, il rifiuto di concedere finanziamenti deriva da valutazioni discrezionali di banche e finanziarie o da politiche contrattuali piuttosto che dall'inaffidabilità del cliente).

Terminato il periodo necessario per l'istruttoria delle richieste di finanziamento (che può avere, comunque, una durata massima di sei mesi), i dati relativi alla richiesta non accolta o oggetto di rinuncia devono essere cancellati dalla "centrale rischi" *entro un mese* anziché essere conservati, come avveniva in alcuni casi, per un anno.

Sempre in merito ai tempi di conservazione, è stato, infine, rilevato che è sproporzionata la scelta, già in uso, di conservare per cinque anni tutti i dati acquisiti, anche nel caso in cui la sofferenza sia venuta meno o il finanziamento sia stato estinto, poiché deve essere garantita la piena tutela del cosiddetto "diritto all'oblio" degli interessati, anche in considerazione delle evoluzioni della recente normativa italiana, in tema di correttezza nei pagamenti e nell'adem-

pimento delle obbligazioni pecuniarie (relative, oltre alle esperienze applicative della "centrale rischi" della Banca d'Italia, ai registri informatici dei protesti cambiari ed all'archivio informatico degli assegni e delle carte di pagamento).

Il provvedimento adottato prevede, pertanto, che i dati relativi agli eventuali ritardi nei pagamenti, poi completamente sanati, devono essere cancellati *entro un anno* dalla data della loro regolarizzazione o comunque dalla data di estinzione del rapporto di finanziamento.

In applicazione, poi, del principio di proporzionalità rispetto alle finalità della raccolta e dell'ulteriore trattamento dei dati, ed in relazione alle conseguenze pregiudizievoli per gli interessati, il provvedimento segnala, anche, la necessità di ridurre in ogni caso i tempi di conservazione dei dati relativi ad inadempimenti o "sofferenze" ancora pendenti o solo parzialmente estinti, ritenendo congrua la loro conservazione per la durata del rapporto di finanziamento e, comunque, *non oltre tre anni* dalla data dell'ultimo aggiornamento in centrale rischi.

Il provvedimento è stato comunicato ai soggetti che gestiscono sistemi informativi di rilevazione dei rischi creditizi e alle società, banche o istituti finanziari che aderiscono ai relativi circuiti, ai quali è stato chiesto di fornire, entro il termine indicato (15 dicembre 2002) notizie sulle prime misure adottate per tutelare i consumatori in relazione anche al codice deontologico in fase di elaborazione.

Successivamente, sono stati avviati prontamente gli ulteriori lavori preparatori per il codice di deontologia in materia, considerato dall'Autorità prioritario nell'ambito del programma di lavoro per il 2003, con l'obiettivo di giungere ad uno schema consolidato di codice entro il mese di maggio del 2003.

34 Registro dei protesti

Le novità introdotte dalla normativa in materia di conservazione nel tempo dei dati sui protesti (legge n. 235/2000) tengono in qualche modo conto, con soluzioni specifiche, dei diritti delle persone protestate. Accanto, infatti, alla disposizione secondo la quale ogni protesto deve essere conservato per cinque anni nel registro informatico dal momento della sua iscrizione, sono stati disciplinati casi per i quali è invece prevista la cancellazione: si tratta di quelli in cui gli interessati hanno adempiuto ai propri obblighi o sono stati riabilitati, in base alle modalità stabilite dalla legge, o iscritti per errore nel registro.

La predetta legge del 2000 ha fissato le modalità di tenuta del registro informatico con l'obiettivo di assicurare un'informazione completa e tempestiva su tutto il territorio nazionale anche, ed in particolare, per quanto riguarda la durata temporale per la messa a disposizione delle informazioni al pubblico.

Il Garante, accogliendo il ricorso di un cittadino che lamentava di non aver avuto positivo riscontro alla richiesta di cancellazione di dati personali relativamente a un protesto, rivolta ad una società alla quale aveva chiesto un finanziamento, ha statuito che quando è stata sanata tempestivamente la posizione debitoria o è stata dimostrata l'illegittimità o l'erroneità del provvedimento, i dati devono essere cancellati dal registro informatico dei protesti e si deve essere considerati a tutti gli effetti come mai iscritti. Analoga procedura deve essere adottata per i soggetti riabilitati.

Nel caso esaminato, a causa della perdurante iscrizione in un archivio "parallelo", era stato negato al ricorrente il finanziamento. Il protesto, elevato per il mancato pagamento di alcuni effetti cambiari, pur non risultando da visura effettuata presso la camera di commercio, era annotato in un'altra banca dati privata consultata dalla finanziaria.

E' stato, pertanto, stabilito che i dati relativi al protesto devono essere cancellati non solo dal registro istituito dalla legge, ma da ogni banca dati parallela, anche privata, consultabile da terzi e in primo luogo dalle società che erogano finanziamenti.

Il ricorso esaminato si inserisce in questo contesto normativo che non può essere eluso immagazzinando i dati in altri archivi. Contesto che è anzi rafforzato dalla legge n. 675/1996, la quale dispone la cancellazione di informazioni, anche esatte, per le quali non è più giustificata la conservazione rispetto alle finalità perseguite. L'interessato ha potuto quindi beneficiare della cancellazione dei dati conservati presso la finanziaria. Una volta riabilitato, infatti, i dati erano stati cancellati dal bollettino dei protesti, ma erano ancora conservati da banche dati private. Banche dati che, peraltro, non avevano neanche indicato, come prescritto, a quale data fossero aggiornate le informazioni in loro possesso (*Provv.* 7 febbraio 2002).

35 Raccolte di dati in ambito assicurativo e banca dati Isvap

La novità più rilevante nel settore assicurativo, per i suoi effetti in materia di protezione dei dati personali, è costituita dalla recente adozione da parte dell'ISVAP del provvedimento di attuazione della disciplina delle procedure e delle modalità di funzionamento, nonché delle modalità e dei limiti di accesso alle informazioni raccolte dalla banca dati dei sinistri relativi all'assicurazione obbligatoria della responsabilità civile per i veicoli a motore immatricolati in Italia (*Provv.* n. 2179 del 10/3/2003, pubblicato sulla G.U. n. 63 del 17 marzo 2003).

Come ricordato nella relazione dello scorso anno (p. 64), in tale banca dati sono inseriti mensilmente, dalle imprese di assicurazioni, i dati relativi a ciascun sinistro avvenuto del quale le stesse ricevono denuncia o richiesta di risarcimento.

In considerazione dei rilevanti effetti che essa produce nella sfera privata e personale di ogni cittadino, la messa in opera della banca dati sinistri ha reso necessaria un'intensa attività di cooperazione istituzionale tra l'ISVAP ed il Garante, per individuare garanzie e soluzioni funzionali, organizzative, procedurali e tecniche idonee per contemperare l'esigenza di assicurare l'efficacia del sistema informativo in relazione al contrasto delle frodi assicurative con la necessità di mantenere un elevato livello di tutela dei diritti fondamentali delle persone coinvolte nei sinistri e le cui informazioni sono registrate in banca dati.

Grazie al positivo rapporto tra le due autorità sono state individuate e stabilite alcune importanti garanzie circa le informazioni che possono essere registrate nella banca dati e i soggetti che possono accedervi. Sono stati, inoltre, definiti alcuni principi relativi ai tempi di conservazione e visibilità dei dati, nonché i limiti, i presupposti e le forme per la consultazione dei dati stessi (con particolare attenzione a quelli sensibili). Sono state altresì disciplinate le attività di verifica da parte dell'ISVAP sulle imprese in relazione al rispetto delle prescrizioni impartite nel provvedimento, le misure di sicurezza e le modalità per assicurare il diritto di accesso agli interessati.

E' stato infine stabilito che l'ISVAP chieda il parere del Garante anche per le convenzioni che dovranno determinare le modalità tecniche di accesso alla banca dati da parte di organi giudiziari e forze di polizia per le finalità di giustizia penale.

Nel corso dell'anno sono stati evidenziati all'Autorità, anche da parte dell'ANIA, altri problemi riguardanti l'applicazione della disciplina sulla protezione dei dati personali nell'ambito del settore assicurativo, anche alla luce delle modifiche introdotte dal d.lg. n. 467/2001 e in prospettiva dell'elaborazione del testo unico.

In particolare, è emersa l'esigenza già sottolineata (v. *Relazione 2001*, p. 64), di predisporre per le assicurazioni un modello semplificato per l'informativa agli interessati e per la raccolta

del consenso, che tenga conto della molteplicità di trattamenti di dati personali, anche sanitari, posti in essere da società assicurative e da altre categorie di soggetti (agenti, periti legali, autofficine; società di servizi postali, informatici) partecipanti alla c.d. "catena" assicurativa.

L'esame complessivo del settore rende peraltro opportuno tener conto dello sviluppo di una realtà in continua crescita, relativa alle reti di distribuzione di servizi e prodotti assicurativi integrati a quelli bancari e finanziari, anche attraverso modalità di offerta fuori sede e uso di tecniche di comunicazione a distanza (in relazione ai quali dovrà essere recepita a breve in Italia la specifica direttiva 2002/65/CE del 23 settembre 2002 sulla commercializzazione a distanza dei servizi finanziari).

L'aspetto più problematico delle attività assicurative è collegato, comunque, al trattamento di dati sensibili, al quale il Garante ha sempre dedicato particolare attenzione, anche attraverso le autorizzazioni generali rinnovate il 31 gennaio 2002 (in particolare per le assicurazioni v. autorizzazioni nn. 2/2002, par. 1.2, lett. *e)*, e 5/2002, capo I).

Nel corso dell'anno sono poi pervenute al Garante alcune segnalazioni nelle quali si lamenta che le compagnie di assicurazioni, per procedere al risarcimento di danni o al rimborso di spese mediche, chiedono copia delle cartelle cliniche degli assicurati. Al riguardo è stato evidenziato che le autorizzazioni generali in tema di trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale e di trattamento dei dati sensibili da parte di diverse categorie di titolari, sono state rilasciate anche nei confronti delle società di assicurazioni per il trattamento dei soli dati ed operazioni realmente indispensabili per fornire specifici beni, prestazioni o servizi richiesti dall'interessato (cfr. paragrafo 1), punto 1.1, lett. *e)*, autorizzazione n. 2/2002, e capo I, punto 1), lett. *a)* e punto 3), autorizzazione n. 5/2002).

Alla luce di tale previsione, l'Autorità ha ritenuto, in passato, che possono risultare giustificati alcuni trattamenti di dati relativi alla salute degli assicurati effettuati da società di assicurazione al fine della gestione e dell'esecuzione di polizze infortuni e malattie. Tra questi trattamenti può rientrare anche la raccolta di dati contenuti nelle cartelle cliniche degli assicurati, quando tali dati sono effettivamente indispensabili in tutto o in parte per fornire le specifiche prestazioni richieste dagli interessati con questa tipologia di contratti (es. attività di accertamento dei sinistri denunciati e di rimborso delle spese mediche sostenute dall'assicurato).

Questo tema sarà, tuttavia, oggetto di un necessario ulteriore approfondimento da parte dell'Autorità al fine di fornire alcune indicazioni più specifiche su presupposti, finalità e modalità della raccolta e del trattamento dei dati sanitari contenuti nelle cartelle cliniche, ed in altri documenti e certificazioni, richieste da compagnie di assicurazioni per il risarcimento di sinistri o il rimborso di spese mediche, ed evitare l'impropria richiesta a tappeto di dati e documenti esuberanti rispetto alle finalità da perseguire.

Nell'ambito del settore delle assicurazioni, rimangono sul tappeto altri 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).

Il delicato rapporto tra la protezione dei dati personali e le finalità assicurative delle imprese è stato infine oggetto di una raccomandazione del Consiglio d'Europa approvata il 18 settembre 2002 sulla protezione dei dati personali raccolti e trattati per scopi assicurativi. E' un documento al quale gli esperti del Consiglio hanno lavorato per quasi 12 anni, a partire dal novembre 1990, e che rappresenta un importante contributo in un settore di grande complessità che tocca direttamente gli interessi della quasi totalità dei cittadini. La Raccomandazione si fonda sui principi fissati dalla Convenzione n. 108/1981 del Consiglio d'Europa, relativa alla protezione delle persone fisiche rispetto al trattamento di dati personali, ma tiene conto anche degli sviluppi nel frattempo intercorsi ed, in particolare, dei principi sanciti dalla direttiva europea in materia di protezione dei dati personali (95/46/CE). La Raccomandazione non riguarda i trattamenti effettuati per scopi di previdenza sociale, oggetto di una specifica raccomandazione che il Consiglio d'Europa aveva elaborato nel 1986 (Raccomandazione R(86) 1); tuttavia, lascia gli Stati membri liberi di decidere se estendere l'applicazione dei principi di questa più recente raccomandazione anche a tali trattamenti.

I principi contenuti nella Raccomandazione non hanno un carattere direttamente vincolante, ma, potrebbero essere oggetto di opportuna considerazione per le future iniziative del legislatore e del Garante, come già avvenuto per le altre Raccomandazioni del Consiglio d'Europa.

36 Perizie medico-legali

Nell'ultimo anno di attività sono stati presentati solo alcuni ricorsi in relazione allo specifico trattamento dei dati personali nel settore assicurativo; si è quindi confermata quella tendenza ad un diverso atteggiamento da parte dei destinatari di tali richieste, 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). A tale diverso atteggiamento sembrano aver contribuito anche gli approfondimenti che l'Autorità ha sviluppato e sta sviluppando sulla definizione di "dato personale" e la Raccomandazione sui dati valutativi dei dipendenti predisposta del Gruppo dei Garanti europei il 22 marzo 2001.

Nelle cd. perizie medico-legali predisposte dal medico fiduciario delle diverse compagnie di assicurazioni, compaiono accanto ai dati personali più "comuni" quali quelli anagrafici, altri dati personali inerenti allo stato di salute e a lesioni riportate che figurano all'interno di valutazioni e giudizi formulati più spesso da un professionista che ha visitato l'interessato o che ha esaminato la relativa documentazione. La posizione espressa dall'Autorità in diverse occasioni riconosce 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. Al termine di questa prima fase di applicazione dei principi in materia, nella quale non sono mancati fisiologici contrasti anche nella sede giudiziaria ordinaria investita con alcune opposizioni a decisioni del Garante, l'Autorità è impegnata nell'approfondire gli sviluppi che questa esperienza può avere sul piano normativo, per individuare ad esempio eventuali soglie temporali per l'accesso o chiarire il rapporto tra dati di origine valutativa e diritto alla correzione, all'aggiornamento o all'integrazione.

Accade ancora, tuttavia, che il soggetto coinvolto in un sinistro, o comunque interessato ad un risarcimento di danni fisici, adisce l'Autorità per poter accedere ai dati personali che lo riguardano contenuti nella perizia medico-legale redatta dal medico fiduciario della società di assicurazione cui è stata richiesta la liquidazione del danno. Se nel corso del precedente anno le modalità di presentazione e il contenuto delle richieste avanzate al titolare del trattamento e del ricorso successivamente presentato all'Autorità potevano risentire di una conoscenza ancora superficiale dei contenuti della legge, tali problematiche sono nettamente diminuite nel corso del 2002.

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.

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 in casi particolari 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 in concreto e realmente l'effettiva esistenza del pregiudizio, con una valutazione da condurre caso per caso (*Provv.* 19 giugno 2002, in Bollettino n. 29; *Provv.* ti 16 ottobre 2002 e 11 dicembre 2002).

Nell'accogliere il ricorso di una persona che aveva segnalato di non aver ricevuto riscontro ad una richiesta di accesso ai propri dati personali, tra i quali vi erano anche dati sanitari contenuti in una perizia redatta dal medico di una società di assicurazioni, il Garante ha ribadito il principio in base al quale le informazioni sulle condizioni di salute contenute in una perizia medica devono essere comunicate, all'interessato che lo richieda, tramite un medico.

La società assicuratrice, chiamata dal Garante a fornire chiarimenti, aveva affermato di voler aderire alle richieste del ricorrente, mettendo a disposizione per la consultazione tutta la documentazione (composta dagli esiti di una visita medica e da un successivo certificato redatto da un medico supervisore), depositata presso il proprio centro liquidazione sinistri, situato in un'altra città.

Entrambe le modalità di adempimento sono state ritenute dal Garante non aderenti alla normativa vigente.

Secondo il principio generale previsto (in particolare, l'art. 23, comma 2, della l. n. 675/1996), l'interessato può accedere ai dati sanitari che lo riguardano solo per il tramite di un medico, designato dall'interessato oppure dalla società che tratta i dati. Altre modalità, quali la semplice messa a disposizione di materiale non selezionato, peraltro presso gli uffici della società che ha raccolto ed utilizzato i dati, siti in altra città, non sono conformi alle norme.

Per i dati personali "comuni", invece, resta ferma la procedura secondo cui il titolare del trattamento deve confermare l'esistenza dei dati richiesti e comunicarli all'interessato, senza ritardo, in forma intelligibile, estrapolandoli, se necessario dai documenti dove sono contenuti. Solo nel caso in cui l'estrazione risulti particolarmente difficoltosa, la documentazione può essere esibita, o se ne può consegnare una copia (*Provv.* 19 febbraio 2002).

In un altro caso, è stata contestata una sanzione amministrativa ad una società di assicurazioni per aver violato le disposizioni in tema di comunicazioni di dati sullo stato di salute. L'assicurazione è stata "multata" per aver consegnato direttamente ad un suo assistito, che ne aveva fatto richiesta, copia di una perizia medica senza rispettare la disposizione che prevede la comunicazione di dati sanitari solo tramite il medico di fiducia dell'interessato o designato da chi detiene ed usa i dati, cioè da quello che la legge chiama "il titolare del trattamento" (*Provv.* 15 novembre 2002).

Attività giornalistiche e mezzi di informazione

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

Particolarmente delicata continua a rivelarsi l'opera del Garante volta a perseguire un giusto equilibrio tra il diritto/dovere dei mezzi di comunicazione di informare la collettività su fatti di rilevanza pubblica e il diritto alla riservatezza delle persone coinvolte.

Anche nel 2002 sono state numerose le segnalazioni relative a possibili violazioni delle norme dettate dalla legge 31 dicembre 1996, n. 675 e dal codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (provvedimento del 29 luglio 1998, in G.U. n. 179 del 3 agosto 1998) con riferimento ai trattamenti svolti nell'esercizio della professione giornalistica o, più in generale, del diritto di libera manifestazione del pensiero.

Occorre, d'altra parte, evidenziare anche un'accresciuta attenzione su tali temi da parte degli operatori dell'informazione. Conferma di ciò è anche l'aumento dei casi in cui sono gli stessi organi di informazione e -in particolare- i singoli cronisti ad interpellare il Garante, ponendo quesiti o chiedendo chiarimenti in ordine al corretto utilizzo delle informazioni nel quadro delle vigenti norme in materia di protezione dei dati.

Nel fornire risposte alle segnalazioni dei cittadini e alle richieste di parere provenienti dai diversi interessati, il Garante ha così cercato di contribuire a specificare e integrare alcuni parametri -talvolta di incerti confini- posti dalla legge 31 dicembre 1996, n. 675 e dal predetto codice deontologico a garanzia del lecito e corretto trattamento dei dati.

Ci si riferisce in particolare al principio di essenzialità dell'informazione a cui il giornalista -e chiunque tratta dati per scopi affini- deve attenersi nel raccogliere e diffondere dati personali relativi ad episodi di cronaca di pubblico rilievo (artt. 12, lett. *e)*, 20, lett. *d)* e 25, l. n. 675/1996; artt. 5 e 6 del codice). Ci si riferisce, inoltre, ai limiti particolari dettati con riguardo ai trattamenti concernenti soggetti "deboli", meritevoli di speciale protezione (ad esempio i minori - cfr. art. 7 del codice) ovvero relativi a determinate categorie di dati (ad esempio, quelli idonei a rivelare lo stato di salute -cfr.art. 10 del codice- o attinenti alla sfera sessuale -cfr. art. 11 del codice- o, ancora relativi a persone coinvolte in vicende giudiziarie- cfr. art. 12 del codice).

38 Tutela dei minori

Limitare le intrusioni nella vita privata dei minori è certamente un'esigenza molto sentita dalla collettività. Costante è l'attenzione del Garante nei riguardi dei trattamenti dei dati relativi ai minori, sempre più spesso esposti a rischi legati alla diffusione non controllata delle informazioni che li riguardano nell'ambito dell'attività giornalistica.

Il codice deontologico prevede com'è noto speciali garanzie a tutela dei minori (art. 7) richiamando anche i principi contenuti nella Carta di Treviso. Tali garanzie si traducono in particolare nel divieto di diffondere dati idonei ad identificare anche indirettamente minori coinvolti in episodi di cronaca (e non solo in reati). Ciò in ragione del fatto che la diffusione delle informazioni che li riguardano può segnare profondamente il loro sviluppo e provocare danni ben più ingenti di quelli che possono essere prodotti in una persona matura.

Tale particolare disciplina è stata oggetto di richiamo con riguardo al trattamento di dati effettuati nel corso di due puntate della trasmissione *"Al posto tuo"* (curata dalla RAI) nella quale è stato intervistato un minore di 11 anni. In tale circostanza, oltre ad informazioni di carattere personale del bambino, sono emersi episodi della vita familiare e sono state divulgate delicate informazioni non note al minore.

Il Garante, ribadendo la ferma esigenza di evitare intrusioni nella vita privata dei minori ed inutili spettacolarizzazioni di vicende familiari, ha segnalato alla RAI di non mandare più in onda le due puntate e di evitare in futuro il ripetersi di tali episodi. Il trattamento effettuato nella citata trasmissione è stato ritenuto in contrasto con la disciplina sulla *privacy*, con il codice deontologico dei giornalisti e con lo stesso codice di autoregolamentazione su tv e minori, la cui nuova versione è stata proprio di recente sottoscritta (29 novembre 2002).

Nella sua decisione, l'Autorità ha ricordato che la normativa da ultimo citata prevede che la protezione della vita privata e della personalità del minore è da considerarsi primaria rispetto al diritto-dovere del giornalista di informare su fatti di interesse pubblico. Le interviste televisive -quali quelle cui è stato sottoposto il protagonista della trasmissione citata- possono porre il minore in una condizione che non gli consente di determinare appieno gli effetti dei propri comportamenti, sia in ragione dell'età, sia del particolare contesto dello studio televisivo. Il fatto, poi, che la partecipazione del minore a trasmissioni televisive come quella citata sia avvenuta con il consenso dei genitori non bastava a giustificare l'intervista del giornalista, il quale aveva comunque il dovere di valutarne i possibili effetti pregiudizievoli sullo sviluppo della personalità del minore.

Il Garante ha evidenziato come tali principi trovino conferma nella Carta di Treviso, la quale stabilisce che "il bambino non va intervistato o impegnato in trasmissioni televisive o radiofoniche che possano ledere la sua dignità, né turbato nella sua *privacy* o coinvolto in una

pubblicità che possa ledere l'armonico sviluppo della sua personalità e ciò, a prescindere dall'eventuale consenso dei genitori" (*Provv.* 11 dicembre 2002).

La tutela accordata ai minori non viene necessariamente meno in caso di morte di questi ultimi. È quanto ha affermato, ancora, l'Autorità occupandosi della denunciata violazione delle norme in materia di tutela della riservatezza con riferimento alla pubblicazione, sulla copertina di una rivista, delle fotografie che ritraggono il viso dei bambini deceduti nel crollo della scuola di S. Giuliano, a seguito del sisma che il 31 ottobre 2002 ha colpito l'omonima località. Fotografie, queste, acquisite dal settimanale senza il consenso dei genitori, riproducendo immagini apposte, ancora precariamente, nei luoghi in cui i bambini erano stati tumulati.

Al riguardo il Garante ha precisato come la raccolta delle fotografie sia avvenuta in violazione dei principi di liceità e correttezza e di compatibilità degli scopi perseguiti (art. 9, legge n. 675/1996). La loro esposizione in un luogo, pure aperto al pubblico, era infatti finalizzata unicamente al ricordo, alla memoria e alla pietà dei defunti; tale circostanza non rendeva, perciò stessa, legittima la riproduzione *in loco* delle immagini dei bambini e l'ulteriore sfruttamento delle stesse per finalità di informazione al pubblico. Ciò, anche in considerazione del legittimo interesse al decoro e al riserbo personale delle famiglie interessate dalle dolorose perdite. Alla luce di tali considerazioni, il Garante ha disposto che le fotografie venissero eliminate dagli archivi redazionali (*Provv.* 19 dicembre 2002).

39 Cronache giudiziarie

Anche nell'odierno periodo di riferimento sono state esaminate numerose segnalazioni relative a presunte violazioni della normativa in materia di protezione dei dati nell'ambito delle "cronache giudiziarie".

L'art. 25 della legge n. 675/1996 ed il menzionato codice deontologico prevedono la possibilità di trattare dati personali relativi ai procedimenti penali e ai provvedimenti giudiziari di cui all'art. 686, commi 1, lett. a) e d), 2 e 3, c.p.p., senza il consenso dell'interessato e senza una preventiva autorizzazione del Garante, subordinando, però, ciascun trattamento al rispetto dei diversi limiti previsti dallo stesso codice deontologico, tra i quali, in particolare, quello dell'essenzialità dell'informazione (cfr. art. 12 del codice).

Alla luce dei predetti principi, l'Autorità ha più volte ricordato agli organi di informazione come la giusta esigenza di informare l'opinione pubblica su vicende giudiziarie non debba entrare in conflitto con il rispetto della vita privata delle persone.

Tale assunto è stato ribadito di recente, nell'esaminare le segnalazioni relative ad una possibile violazione della *privacy* con riguardo alla pubblicazione, da parte di alcuni giornali, dei nomi delle persone coinvolte nell'inchiesta su un giro di prostituzione nella Capitale. In tale circostanza il Garante ha richiamato l'attenzione degli organi di informazione sulla necessità di non diffondere informazioni non indispensabili, specie se legate ad aspetti particolarmente riservati come la vita sessuale delle persone e attinenti, quindi, alla loro sfera più strettamente privata. Ciò anche allo scopo di evitare ingiustificate spettacolarizzazioni o eventuali strumentalizzazioni di scelte personali. Tali norme -come ha chiarito l'Autorità- devono trovare applicazione anche quando, come nel caso oggetto dell'inchiesta suindicata, si tratti di persone che rivestono posizioni di particolare rilevanza sociale o pubblica (artt. 5, 6 e 11 del codice deontologico).

Con riferimento all'episodio di cronaca segnalato il Garante ha precisato, altresì, che il rispetto della dignità personale e l'obbligo di trattare i dati in conformità al canone dell'essenzialità dell'informazione devono valere sia per i clienti, beneficiari dell'ipotizzato giro di prostituzione, sia per le ragazze alle quali gli stessi si sarebbero rivolti. Ciò, tanto più in considerazione del fatto che i dati e le fotografie diffusi potrebbero comunque riguardare anche persone totalmente estranee alla vicenda (*Comunicato* 10 ottobre 2002).

In generale, numerose sono state le segnalazioni riguardanti la diffusione, da parte degli organi di stampa, dei dati di persone sottoposte ad indagini, imputate o condannate nell'ambito di un procedimento penale.

Al riguardo, il Garante ha ribadito che la possibilità di diffondere tale tipo di informazione non è preclusa, anche in mancanza del consenso dell'interessato, purché avvenga nel rispetto

dei limiti previsti per l'esercizio del diritto di cronaca, tra i quali quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 25 l. n. 675/1996 e 12 del codice deontologico), oltre che in osservanza delle disposizioni che prevedono specifici limiti alla pubblicità degli atti del procedimento e eventualmente anche del loro contenuto.

L'Autorità ha altresì ricordato che le disposizioni in materia di tutela della riservatezza qui richiamate, d'altra parte, non possono essere utilmente invocate rispetto alla diffusione di informazioni puramente denigratorie o diffamatorie (profili su cui spesso si concentrano le segnalazioni degli interessati) per le quali, invece, il codice civile e il codice penale prevedono altre forme di tutela da esercitare nei confronti dell'Autorità giudiziaria.

Diverse sono state anche le segnalazioni con le quali è stata lamentata l'illecita acquisizione di dati personali da parte degli organi di informazione e il fenomeno delle cosiddette "fughe di notizie". In relazione a tale profilo, va ricordato che assurgono a parametro di valutazione del trattamento, oltre ai principi della legge n. 675/1996, le norme a garanzia del segreto sugli atti d'ufficio e sull'attività di indagine o che prevedono un regime di tendenziale pubblicità degli atti processuali, delle udienze e dei provvedimenti del giudice.

Nell'esaminare alcuni casi di diffusione, da parte degli organi di stampa, dei dati relativi a persone vittime di furto a domicilio, l'Autorità ha constatato che, fermo restando l'interesse pubblico alla conoscenza di tali fenomeni delittuosi, l'identificazione delle relative vittime può porsi in vari casi in contrasto con il principio di essenzialità dell'informazione sopra richiamato, nonché con quello di pertinenza e non eccedenza dei dati diffusi rispetto alle finalità del trattamento (art. 9, comma 1, lett. *d)*. Con riferimento a tale fattispecie, l'indicazione delle sole iniziali e l'omissione dell'indirizzo non sottraggono comunque valore all'efficacia informativa della notizia (*Provv.* 11 luglio 2002).

40 Foto segnaletiche o di persone arrestate

A circa quattro anni dalle direttive impartite in materia dal Ministero dell'interno, il Garante ha nuovamente esaminato la tematica in relazione ad alcuni casi recenti in cui sono state nuovamente diffuse immagini e fotografie di persone sottoposte a misure restrittive della libertà personale (presentate con ferri o manette ai polsi) o foto segnaletiche di persone interessate ad indagini, in violazione di specifici divieti di legge previsti anche a tutela della dignità degli interessati (codice di procedura penale, ordinamento penitenziario e legge sul diritto d'autore) e ribaditi dal codice deontologico per l'attività giornalistica.

Con un provvedimento del 19 marzo 2003 l'Autorità ha ribadito le regole che presiedono ad una corretta informazione in materia, nel rispetto dei diritti e della dignità degli interessati e tenendo conto delle finalità di accertamento, prevenzione e repressione dei reati.

E' stato così ricordato il principio che non è consentito pubblicare su giornali o trasmettere in tv immagini di persone arrestate in manette. La diffusione delle foto segnaletiche è vietata, anche nell'ambito di conferenze stampa, a meno che ricorrano fini di giustizia e di polizia o motivi di interesse pubblico che ne rendano necessaria la diffusione (circostanze che sono state ritenute esistenti per le immagini relative ad appartenenti a formazioni terroristiche, diffuse a seguito del grave episodio accaduto il 2 marzo 2003 sul treno Roma-Firenze).

L'intervento dell'Autorità ha disposto il divieto dell'ulteriore diffusione delle immagini, pubblicate in sei casi, nonché la trasmissione di copia del provvedimento (oltre che alle testate giornalistiche e radiotelevisive interessate e all'Ordine dei giornalisti), ai vertici delle forze dell'ordine, al Dipartimento dell'amministrazione penitenziaria e all'autorità giudiziaria che procedeva in un caso, per le opportune valutazioni di competenza, anche di ordine disciplinare.

41 Diffusione di informazioni raccolte mediante l'uso di telecamere nascoste

Sulla base di una segnalazione, l'Autorità ha avviato accertamenti in relazione alla vicenda riguardante il servizio televisivo diffuso dalla trasmissione *Striscia la notizia* il 9 gennaio 2003. Come si è potuto evincere dallo stesso servizio, i responsabili della trasmissione avrebbero utilizzato telecamere nascoste per smascherare una possibile truffa ai propri danni, messa in atto da presunti giornalisti. Questi ultimi, infatti, si spacciavano per operatori appartenenti alla redazione di *Striscia la notizia* al fine ottenere denaro dai sindaci di due comuni interessati a fare pubblicità su alcune vicende accadute nelle loro amministrazioni, in cambio della realizzazione di un servizio televisivo sull'argomento. Il filmato relativo agli incontri tra i diversi protagonisti della vicenda e la registrazione delle conversazioni tra i medesimi sono stati quindi oggetto della puntata televisiva sopra citata.

Gli accertamenti avviati presso l'emittente televisiva e i sindaci interessati avevano lo scopo di valutare il rispetto, da parte dei medesimi, dei principi di finalità, liceità e correttezza nella raccolta delle informazioni, anche alla luce del fatto che il materiale raccolto attraverso le telecamere sarebbe stato utilizzato dai predetti responsabili, in prima battuta, per realizzare uno *scoop* televisivo. Il procedimento di controllo avviato è pressoché ultimato.

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

Particolare attenzione continua ad essere rivolta dal Garante alle segnalazioni concernenti la diffusione, da parte degli organi di informazione, dei dati idonei a rivelare lo stato di salute. Ciò, alla luce degli articoli 5 e 10 del citato codice deontologico, i quali prevedono specifiche garanzie affinché l'eventuale trattamento di tali delicatissime informazioni avvenga nel rispetto della dignità e del diritto alla riservatezza dell'interessato.

In un caso è stato ad esempio avviato un accertamento per verificare quanto segnalato dalla dipendente di un comune circa la diffusione -da parte dell'assessore al personale, nel corso di un'intervista televisiva- di alcuni dati idonei ad identificarla, nonché informazioni relative alle sue condizioni di salute, ivi compresa la circostanza che la stessa avesse subito un aborto.

In altra occasione 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).

A proposito dell'essenzialità dell'informazione e del rispetto della dignità della persona, l'Autorità è intervenuta in relazione alla pubblicazione, su un quotidiano, della notizia 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 al contrario indurre l'autore dell'articolo e il direttore responsabile del quotidiano ad operare un rigoroso vaglio 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 fotogrammi delle videoregistrazioni dei predetti incontri.

Fermo restando il rilievo pubblico assunto dalla vicenda -connesso, peraltro, al fatto che sull'accaduto sono state avviate 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 evidenziato, 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).

43 Esercizio dei diritti nei confronti degli organi di informazione

Ingente è stato, nel periodo di riferimento, il numero di segnalazioni con cui è stata denunciata la difficoltà, per gli interessati, di accedere ai dati personali trattati dagli organi di informazione e di ottenere, ad esempio, copia della registrazione di un programma televisivo al quale gli interessati stessi avevano preso parte o nel quale, comunque, erano state trattate informazioni ad essi relative.

Nel rispondere a tali istanze il Garante ha riaffermato il principio in base al quale i diritti di cui all'art. 13 della legge n. 675/1996 possono essere fatti valere anche nei confronti degli editori e dei direttori responsabili delle testate giornalistiche, relativamente ai trattamenti di dati personali da loro effettuati (*Provv.ti* 25 settembre e 8 novembre 2002). Fatte salve le norme sul segreto professionale dei giornalisti per quanto concerne la fonte della notizia, l'interessato può rivolgersi a tali soggetti per ottenere conferma dell'esistenza del trattamento ed avere comunicazione in forma intelligibile dei dati trattati (anche mediante la trasmissione di un duplicato della registrazione che li contiene). Inoltre può chiederne la cancellazione, la trasformazione in forma anonima o il blocco, nel caso in cui i dati medesimi siano trattati in violazione di legge, ovvero non sia necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati. Anche nell'ipotesi in cui i dati siano stati raccolti e utilizzati in conformità alla legge, l'interessato ha comunque diritto di opporsi, per motivi legittimi, al loro trattamento.

Sorveglianza e sistemi biometrici

44 Videosorveglianza

Negli ultimi anni, gli organismi pubblici e privati in Europa hanno fatto sempre maggior ricorso a sistemi di acquisizione di immagini. Tale circostanza ha suscitato un acceso dibattito tanto a livello comunitario, quanto a quello dei singoli Stati membri, al fine di identificare presupposti e restrizioni applicabili all'installazione di attrezzature di videosorveglianza, nonché le necessarie garanzie per le persone interessate.

Dall'esperienza acquisita negli ultimi anni, anche a seguito del recepimento, a livello nazionale, della direttiva n. 95/46/CE, si constata un'enorme proliferazione di sistemi a circuito chiuso, videocamere e altri strumenti più sofisticati utilizzati nei settori più diversi.

Inoltre, lo sviluppo delle tecnologie disponibili, digitalizzazione e miniaturizzazione, aumentano notevolmente le possibilità offerte dai dispositivi di registrazione di immagini e suoni, anche in relazione con la loro utilizzazione in intranet e *Internet*.

Il Garante ha continuato ad occuparsi delle tematiche relative alla videosorveglianza, confermando l'ampia diffusione del fenomeno e una costante crescita di attenzione al problema da parte di molti cittadini.

Com'è stato più volte rilevato, la normativa italiana, seguendo l'indirizzo europeo in materia, considera come "dato personale" qualunque informazione che permetta l'identificazione, anche in via indiretta, di un individuo, compresi i suoni e le immagini.

L'Autorità ha proseguito nella fattiva collaborazione con 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.

Da un'analisi effettuata, diverse sono le finalità che si intendono raggiungere in tale ambito con l'utilizzo dei predetti strumenti: *a)* prevenzione di reati, illeciti amministrativi e rilevazione di infrazioni del codice della strada; *b)* sicurezza pubblica (es. protezione civile); *c)* controllo degli accessi a zone a traffico limitato; *d)* monitoraggio del traffico; *e)* tutela del patrimonio artistico (es. atti di vandalismo); *f)* tutela del patrimonio dell'ente (immobili, parco auto, ecc.); *g)* controllo degli accessi agli edifici pubblici; *h)* controllo di zone utilizzate come discariche abusive; *i)* controllo delle disposizioni in tema di smaltimento dei rifiuti (ad es. abbandono di sacchetti fuori degli appositi contenitori o in orari e giorni diversi da quelli prestabiliti).

Non tutte queste finalità risultano compatibili con i princìpi sanciti dalla legge n. 675. In ragione di ciò agli enti richiedenti è stata più volte segnalata la necessità del rispetto di quanto

sintetizzato nel primo "decalogo" adottato dall'Autorità nel 2000 e sono state fornite, volta per volta, puntuali indicazioni.

Tali indicazioni, nel frattempo arricchite da varie specificazioni concernenti casi particolari o derivanti dal confronto a livello comunitario o internazionale, conservano validità ma hanno però natura "transitoria", in attesa di quanto disporrà il previsto testo unico e il codice deontologico previsto dal d.lg. n. 467/2001.

Tra i casi più significativi relativi all'utilizzo di strumenti di rilevazione di immagini in ambito pubblico, è stata esaminata la segnalazione di una compagnia di trasporto comunale i cui addetti sarebbero stati dotati di *"scanner"* per l'acquisizione ottica dei documenti delle persone sprovviste di titolo di viaggio e di fotocamere digitali con le quali riprendere i medesimi soggetti privi anche di documento di identità. Al riguardo l'Autorità ha rilevato (20 novembre 2002) la non proporzionalità dello strumento utilizzato (ed anche la sua dubbia utilità con riguardo alle fotografie di persone sconosciute).

In un altro caso è stato avviato un accertamento in relazione alla notizia apparsa su un quotidiano locale circa l'avvenuta installazione da parte di un comune di alcuni sistemi video per il monitoraggio del flusso veicolare, le cui immagini erano accessibili a chiunque e in tempo reale attraverso il collegamento al sito *web* del comune stesso.

Sempre in tema di accertamenti e controlli volti alla verifica dell'osservanza, da parte di operatori pubblici e privati, delle disposizioni in materia di trattamento di dati personali nell'effettuazione di trattamenti a mezzo di impianti di videosorveglianza, vanno segnalate anche in questa sede le sanzioni amministrative, per un importo complessivo di € 18.564,00, applicate al Consiglio nazionale delle ricerche ed al Comune di Bari. In particolare, come già accennato, l'ente di ricerca aveva istallato presso la propria sede una telecamera a circuito chiuso, con ampio angolo visuale, senza aver fornito alcuna informativa alle persone riprese. Relativamente al Comune di Bari, su segnalazione di un abitante erano state invece richieste informazioni in merito all'istallazione di telecamere nelle auto della polizia municipale finalizzate al controllo delle infrazioni; a tale richiesta di informazioni, però, il comune non ha fornito riscontro entro i termini previsti, costringendo l'Autorità ad applicare la prevista sanzione amministrativa (*Provv.* 5 novembre 2002).

L'Autorità ha anche contestato ad un supermercato in Roma la mancanza di un'idonea informativa alla clientela, prescritta dall'articolo 10 della legge 675/1996, circa la presenza di un sistema di videosorveglianza, istallato per motivi di sicurezza, attivo nell'arco delle ventiquattro ore. L'Autorità, avendo accertato che la capacità delle telecamere consentiva la piena riconoscibilità delle persone inquadrate e che nel fabbricato non erano presenti cartelli e avvisi circa la loro presenza e dei diritti attribuiti dalla legge ai soggetti ripresi, ha sanzionato l'ipermercato, per il solo aspetto relativo all'informativa, con una somma di € 3.098,74. (*Provv.* 2 aprile 2002).

Va anche ricordato che il Garante ha fornito chiarimenti in relazione alla notizia diffusa dai *media* secondo cui alcune telecamere erano state istallate in un istituto di credito in maniera tale da riprendere esclusivamente i piedi dei rapinatori a causa della normativa sulla *privacy*. In

proposito, è stato precisato che nessuna norma della legge n. 675 vieta di installare telecamere che non siano in grado di individuare il volto di una persona presente nella filiale di una banca. La normativa vigente non ostacola l'installazione di telecamere a fini di sicurezza, come dimostra anche il cospicuo numero di sistemi di videosorveglianza in uso presso banche, esercizi commerciali, enti pubblici, aziende, semplici privati e come emerge dalle diverse pronunce con le quali l'Autorità ha indicato i criteri per contemperare il diritto alla riservatezza delle persone con le esigenze di sicurezza della collettività (*Comunicato* 27 dicembre 2002).

In un altro caso, concernente l'installazione di un sistema di video controllo all'interno dei mezzi di trasporto urbano di una società di autoservizi al fine di verificare e prevenire atti di vandalismo e furti di carburante, è stata sottolineata la necessità di rispettare il principio di proporzionalità fra i mezzi impiegati e i fini perseguiti. E' stato escluso, peraltro, che l'installazione di detti impianti potesse essere direttamente rivolta a scopi più generali (di competenza di autorità o organismi pubblici), come quelli di assicurare una maggiore sicurezza ai passeggeri o contenere il fenomeno della criminalità.

Sulla base, poi, della segnalazione di un cittadino che denunciava la presenza di un impianto di videoregistrazione nei locali di un cinema, sono state avviate nei confronti del titolare le procedure per l'applicazione della sanzione amministrativa relativamente all'assenza di informativa agli interessati: in particolare, anche se nel caso concreto l'esercente aveva informato oralmente l'interessato della presenza di telecamere, mancava tuttavia un'informativa rivolta alla generalità degli avventori del locale. È parso inoltre necessario richiamare l'attenzione dell'esercente sulla necessità, ai fini del rispetto della legge n. 675/1996, di prestare puntuale osservanza sotto diversi profili alle indicazioni già fornite dal Garante con il citato "decalogo" del 2000.

Infine, una banca ha posto alcuni quesiti relativamente alla gestione degli impianti di videosorveglianza all'interno e all'esterno dei propri locali. La banca ha evidenziato l'asserita esigenza da un lato di conservare le registrazioni per un periodo piuttosto lungo (40/50 giorni), e di permettere agli incaricati del trattamento (nonché ai direttori delle filiali) di accedervi al fine di verificare eventuali movimenti *bancomat* anomali lamentati dai clienti, dall'altro di ampliare l'angolo visuale delle riprese per inquadrare anche la zona relativa alla postazione di lavoro antistante alla cassa, con possibilità, quindi, di riprendere gli impiegati bancari addetti allo sportello, in relazione alla verifica di eventuali anomalie nella fase di chiusura di cassa.

Al riguardo, il Garante ha ritenuto che tali modalità di trattamento e tempi di conservazione dei dati fossero sproporzionati in relazione alla finalità perseguita. L'installazione di telecamere che riprendevano la zona adiacente agli sportelli *bancomat*, e la conservazione delle relative immagini per un ristretto periodo di tempo (alcuni giorni o, al massimo, una settimana) potevano essere giustificate in base allo scopo di prevenire e perseguire eventuali illeciti (ad esempio, rapine o furti di denaro). Come emerge anche dal citato decalogo, l'ulteriore conservazione delle immagini e la loro successiva consultazione da parte di incaricati del trattamento nominati dalla banca, sarebbero risultati ammissibili solo in relazione ad illeciti che verificatisi o ad indagini dell'autorità giudiziaria o di polizia, ma non anche automaticamente, in relazione alle sole esigenze di accertamento di eventuali segnalazioni di clienti di movimenti *bancomat* anomali, prodromiche all'eventuale attivazione di azioni legali o giudiziarie.

Circa la possibilità di ampliare l'angolo visuale delle riprese all'interno dei locali della banca, l'Autorità ha confermato che l'art. 4 della legge n. 300/1970, fatto espressamente salvo dalla legge n. 675/1996, consente l'installazione di impianti e apparecchiature di controllo a distanza richieste da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, previo accordo con le rappresentanze sindacali aziendali. In ogni caso, l'allargamento dell'angolo visuale delle riprese delle immagini avrebbe dovuto essere limitato e rendere del tutto occasionale la registrazione di immagini dell'addetto allo sportello. Si è poi indicato che ulteriori aspetti (ad esempio, relativi all'informativa ai dipendenti interessati, alle modalità di accesso ai dati, agli incaricati del loro trattamento e ai tempi di conservazione) potevano essere in parte disciplinati direttamente nell'accordo con le organizzazioni sindacali.

Numerose sono state infine le istanze presentate da singoli cittadini circa l'utilizzazione di detti sistemi a fini esclusivamente personali (ad esempio, installazione a fini di sicurezza di videocamere nei condomini o in spazi antistanti le porte delle proprie abitazioni private). In linea con quanto già indicato con il citato decalogo in materia di videosorveglianza, è stato più volte precisato che tali trattamenti possono essere considerati in alcuni casi come effettuati a fini esclusivamente personali, e quindi sottratti all'ambito di integrale applicazione della legge n. 675/1996 (ad eccezione delle disposizioni in materia di sicurezza dei dati). Si è ricordato comunque che è necessario che le riprese siano strettamente limitate allo spazio antistante tali accessi, senza forme di videosorveglianza su aree circostanti e senza limitazioni delle libertà altrui, che possono comportare anche un'eventuale responsabilità penale per il reato di interferenze illecite nella vita privata altrui. Occorre inoltre che le informazioni raccolte non siano in alcun modo comunicate o diffuse. Altrimenti si rientra nell'ambito di applicazione generale della legge 675/1996 e devono, quindi, essere rispettate tutte le indicazioni analiticamente stabilite nel citato decalogo.

45 Rilevazioni biometriche

L'Autorità ha seguito con attenzione i lavori parlamentari della legge 30 luglio 2002, n. 189, di riforma della normativa in materia di immigrazione ed asilo, che contiene disposizioni in base alle quali ogni straniero che richieda il permesso di soggiorno o lo rinnovi è sottoposto a rilievi fotodattiloscopici (artt. 5 e 7).

Sull'argomento della raccolta delle impronte digitali il Garante ha inoltrato in data 27 giugno 2002 ai Presidenti delle Camere e agli organismi parlamentari più direttamente interessati una nota con la quale, nel richiamare il quadro di garanzie previsto a livello internazionale, ha segnalato la necessità del rispetto, in tale delicata materia, dei principi in materia di protezione dei dati personali, specie per quanto attiene alla raccolta, alla conservazione e alla successiva utilizzazione di tali dati. In materia di immigrazione e di asilo ha poi curato collegialmente, per i profili di sua competenza, un primo esame delle previsioni sulla raccolta delle impronte digitali.

Queste ultime, al pari di altri dati biometrici, comportano infatti un "trattamento" di dati personali soggetto alle disposizioni comunitarie e nazionali in materia e, in specie, alla legge 31 dicembre 1996, n. 675.

Come ogni altro trattamento di dati, quello concernente le impronte digitali presuppone anch'esso un rapporto di proporzionalità rispetto alle finalità perseguite, finalità che nelle norme in fase di approvazione sembravano essere quelle di identificazione degli interessati.

La valutazione da effettuare al riguardo richiedeva a sua volta una previa considerazione di vari aspetti che, allo stato, non emergevano dalle disposizioni in fase di approvazione, nelle quali non comparivano indicazioni su diversi aspetti applicativi.

Ci si riferisce, in particolare, alle modalità di utilizzazione e di conservazione dei dati, alla specificazione delle finalità, alla durata del trattamento anche in relazione ad eventi di vario tipo che possono riguardare gli interessati, alle persone che soggiornano nel Paese solo per brevi periodi, ai soggetti aventi eventuali accesso alle informazioni raccolte, alle regole di sicurezza per assicurare l'integrità delle informazioni e per prevenire ipotetici accessi o usi abusivi.

Questi profili richiedono un attento esame in quanto, a differenza di altri dati biometrici quale ad esempio l'iride, le impronte digitali costituiscono anche (oltre che uno strumento per l'identificazione), una traccia del passaggio di un soggetto in determinati luoghi. Ciò richiede particolari cautele per garantirne la genuinità, l'inalterabilità e le gravi conseguenze per gli interessati in caso di eventuale "furto d'identità".

Nella *Relazione 2001* il presidente del Garante sottolineava che *"se questo tipo di furto si con-*

creta, come nella maggior parte dei casi, nell'utilizzazione abusiva di una carta di credito o di uno dei tanti codici d'identificazione personale, le conseguenze possono essere assai sgradevoli, le dimensioni del fenomeno possono avere contraccolpi negativi sulla diffusione del commercio elettronico, ma esiste tuttavia rimedio, che consiste nel cambiare il numero della carta di credito o il codice d'identificazione. Non è così, invece, quando ci si appropria di un dato identificativo personale permanente e non modificabile, qual è ad esempio l'impronta digitale. In questo caso, il "furto" produrrebbe effetti pesantemente negativi per l'interessato, che verrebbe escluso da tutti i circuiti che condizionano l'accesso a quel particolare sistema di identificazione. Vi sono dunque ragioni assai concrete che impongono di valutare con estremo rigore la legittimità dell'utilizzazione dei dati biometrici e, in ogni caso, di prevedere per le loro raccolte severe misure di sicurezza".

Non a caso in vari Paesi la raccolta generalizzata delle impronte non è ammessa, oppure è prevista in termini selettivi o è basata su specifiche garanzie che prevengono, ad esempio, la costituzione di banche dati centralizzate (peraltro di difficile gestione, anche per l'inadeguatezza di *software* in grado di gestire sistemi di riconoscimento di milioni di impronte) e si basano soltanto sul raffronto immediato tra un'impronta rilevata all'atto di un controllo e quella riprodotta su un supporto identificativo della persona.

Andrebbe quindi prevenuto il rischio che le nuove disposizioni in materia, riferite ai richiedenti il permesso di soggiorno o a tutti i cittadini, non rechino esplicite garanzie analoghe a quelle che il citato regolamento comunitario prevede pure per i richiedenti asilo e in relazione alle persone che effettuano un ingresso irregolare alle frontiere.

Successivamente – come riportato più ampiamente in altra parte della relazione (par. 2, lett. *g)* – nel corso dei lavori di conversione del decreto-legge 9 settembre 2002, n. 195, con il quale il Governo ha ampliato gli interventi di legalizzazione del lavoro irregolare di cui alla predetta legge n. 189/2002, l'Autorità ha segnalato al Governo l'opportunità di interventi emendativi a due disposizioni di particolare interesse sempre in materia di rilevazione di impronte digitali. I chiarimenti forniti dall'ufficio del Garante hanno consentito di ricondurre in parte le due previsioni nel quadro dei principi previsti dalla legge n. 675 del 1996. L'Autorità, nell'ambito delle più ampie indicazioni fornite, ha comunque confermato la disponibilità a cooperare per l'individuazione delle modalità tecniche per la raccolta e la gestione delle impronte digitali, in attuazione delle due disposizioni normative approvate.

Marketing

46 *Marketing* e diritti dell'interessato

La protezione dei dati personali acquisiti e utilizzati dai soggetti operanti a vario titolo nel settore del *direct marketing* (in attività di invio di materiale pubblicitario, ricerche di mercato, comunicazione commerciale interattiva e vendita diretta) ha rappresentato, anche nel 2002 e nei primi mesi del 2003, una tematica di notevole rilievo per il Garante.

Nel più ampio contesto dell'attività di autoregolamentazione promossa dall'Autorità dovrà essere profuso il massimo impegno nello svolgimento dei lavori finalizzati all'adozione del codice di condotta previsto per questo settore.

Diversi principi di tutela dei dati personali in tale ambito, già approfonditi nel corso degli anni precedenti, sono stati ripresi nel periodo di riferimento per fronteggiare il cospicuo numero di istanze e quesiti pervenuti all'Autorità, i quali dimostrano la particolare sensibilità degli utenti e dei consumatori italiani rispetto alle intrusioni nella vita privata derivanti dall'adozione di nuovi strumenti e strategie per commercializzare prodotti o servizi, nonché di tecniche e metodologie di comunicazione più aggressive.

Numerose segnalazioni hanno riguardato ad esempio il problema della raccolta e del trattamento dei dati personali nell'ambito della distribuzione nei supermercati di carte per promuovere operazioni a premi nell'ambito dei propri programmi di fidelizzazione della clientela.

Al riguardo, il Garante ha svolto presso le società accertamenti tesi a ricostruire le modalità dei trattamenti effettuati, in modo da verificarne la conformità alla legge n. 675/1996. In particolare sono state acquisite notizie sulla tipologia e sull'essenzialità dei dati richiesti per l'iscrizione ai programmi e raccolti successivamente in relazione allo stesso servizio o ad altri attivati dagli utenti, nonché sull'ambito soggettivo di divulgazione dei dati stessi.

L' Autorità ha poi svolto alcune verifiche preliminari circa la raccolta presso le stazioni ferroviarie italiane di dati di alcuni passeggeri in partenza, effettuata da una società incaricata di una ricerca di mercato per conto della società ferroviaria.

Dalle verifiche è emerso che i dati identificativi dei passeggeri dei treni erano stati acquisiti ai fini dell'esecuzione e della verifica delle interviste telefoniche necessarie per l'elaborazione della ricerca di mercato commissionata, e venivano cancellati dopo una settimana dalla loro raccolta, con conseguente utilizzazione delle restanti informazioni acquisite e loro comunicazione alla società ferroviaria in forma anonima ed aggregata.

Il Garante si è pertanto limitato a richiamare l'attenzione delle società coinvolte nell'iniziativa sulla necessità, ai fini del rispetto della legge n. 675/1996, di riformulare i modelli di informativa agli interessati e di richiesta del loro consenso, se ancora utilizzati in futuro, in

modo da far chiarezza sulla circostanza che il personale incaricato della raccolta dei dati presso i passeggeri non fa parte di quello ferroviario, ma pertiene unicamente alla società incaricata della ricerca, fornendo così agli interessati un'univoca prospettazione della possibilità di una parziale compilazione del modulo, con l'indicazione delle informazioni (es. recapito telefonico e firma) che è necessario rilasciare affinché il modulo stesso venga preso in considerazione per la successiva intervista telefonica (ed, infine, da precisare che i dati identificativi dei passeggeri intervistati venivano eliminati dopo una settimana dalla loro acquisizione).

A fronte dell'attenzione dimostrata da utenti e consumatori per l'uso dei dati personali nell'ambito di operazioni commerciali e pubblicitarie, e dei diversi interventi che, al riguardo, questa Autorità ha effettuato in questi anni, occorre registrare un incremento dei casi di richieste preventive di parere e informazioni da parte delle società e degli operatori di *direct marketing.*

All'interno di questa casistica, il Garante si è espresso in merito ad una richiesta di parere relativa alla possibilità, da parte di alcune società appartenenti allo stesso gruppo societario, di scambiarsi alcuni dati non sensibili dei rispettivi clienti, al fine di promuovere e sviluppare nuove iniziative di carattere commerciale. In tale occasione, l'Autorità ha constatato la necessità di verificare l'esistenza del preventivo consenso dei clienti alla circolazione e al trattamento dei dati, all'interno del gruppo, per finalità di *marketing.* Al riguardo, è stata inoltre evidenziata la necessità per il futuro di evitare, nella richiesta del consenso, il ricorso a complicati rinvii a precedenti lettere o paragrafi del modulo di informativa. Sulla base di tali presupposti, il Garante ha accolto favorevolmente la soluzione prevista di limitare, comunque, i flussi dei dati nell'ambito del gruppo attraverso l'individuazione di alcune strutture "responsabili" del loro trattamento.

In un altro caso, l'Ufficio del Garante si è pronunciato favorevolmente in merito ad una richiesta di parere sulla possibilità per una società italiana di avvalersi della collaborazione di altre imprese, aventi sede in Paesi dell'Ue, per consulenze relative al sistema informativo di *marketing* del gruppo d'appartenenza. Ancora una volta, il Garante ha ricordato la necessità della corretta attuazione della normativa della legge 675/1996, con particolare riferimento all'eventuale designazione di società di consulenza europee come "responsabili del trattamento", nonché all'esigenza del rispetto delle disposizioni sulla protezione dei dati personali in vigore nei loro rispettivi Paesi, ai sensi della direttiva comunitaria vigente in materia.

Telefonia e reti di comunicazione

47 Profili generali

Il settore della comunicazione telematica è caratterizzato da uno sviluppo continuo, che favorisce la nascita 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, sia con riguardo al mondo della rete *Internet*.

Di questo inarrestabile sviluppo, che determina una crescita esponenziale del numero di dati personali trasmessi e scambiati, tiene conto anche la recente direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (G.U.C.E., n. L 201 del 31 luglio 2002), che ha modificato la direttiva 97/66/CE.

Innumerevoli segnalazioni e richieste di parere sono pervenute all'Autorità, sia da parte di singoli interessati, che chiedono tutela in relazione all'uso fatto dai fornitori di servizi di telecomunicazione dei propri dati personali, sia in via preventiva da parte degli operatori del settore. Questi ultimi sempre più spesso chiedono chiarimenti in merito alla corretta applicazione della normativa sulla protezione dei dati personali prima di procedere al trattamento dei dati medesimi, ad esempio in occasione dell'offerta di nuovi servizi ai loro clienti.

Ciò a testimonianza, da un lato, della maggiore importanza attribuita dagli utenti alle problematiche legate all'utilizzo dei dati personali nell'ambito delle reti telematiche e, dall'altro, dell'accresciuta consapevolezza degli stessi fornitori di servizi riguardo alla centralità di tali problematiche. L'adozione di adeguate misure a tutela della vita privata è considerata sempre più frequentemente non soltanto come un obbligo di legge, ma anche e soprattutto, come uno strumento per istaurare un durevole rapporto di fiducia con i propri clienti ed utenti.

Tali preventive richieste degli operatori, peraltro, consentono all'Autorità di intervenire prima che possano verificarsi eventuali lesioni, nonché di incidere sul trattamento di dati riguardanti un numero maggiore di interessati, in quanto le relative decisioni riguardano anche i soggetti che non si sono ancora rivolti al Garante.

Sempre più frequenti sono stati, pertanto, gli incontri con numerosi operatori, anche in vista della prossima adozione del codice deontologico sui trattamenti di dati personali effettuati dai fornitori di servizi di comunicazione e informazione, previsto dal d.lg. 467/2001. A tal fine, l'Autorità ha dato avvio all'istruttoria relativa all'individuazione dei principali elementi da inserire nel suddetto codice.

Tra i problemi affrontati si evidenzia anche quello relativo alla *"carrier preselection"*, ossia il sistema mediante il quale l'abbonato può instradare il proprio traffico telefonico verso un operatore preselezionato.

In base a quanto previsto dalla direttiva 2002/58/CE, infatti, *"i dati relativi al traffico possono tra l'altro consistere in dati che si riferiscono all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo usato, all'ubicazione dell'apparecchio terminale di chi invia o riceve, alla rete sulla quale la comunicazione si origina o termina, all'inizio, alla fine o alla durata di un collegamento"*.

48 Accesso ai dati di traffico telefonico e altre questioni

Fatturazione dettagliata

Anche nel corso dell'anno 2002 questa Autorità si è trovata più volte a dover affrontare le problematiche sottese alla tutela della riservatezza -in particolare degli utenti, diversi dall'abbonato, che effettuano chiamate dal terminale di quest'ultimo- nell'ambito delle fatturazioni inviate agli abbonati.

Tali profili sono già stati analizzati nelle precedenti relazioni annuali successive all'emanazione del d.lg. 13 maggio 1998, n. 171 alle quali pertanto si rinvia soprattutto con riferimento all'oscuramento delle ultime tre cifre dei numeri telefonici chiamati.

Il persistere di alcuni nodi problematici nell'applicazione della disciplina, evidenziati anche dal gran numero di segnalazioni e reclami pervenuti all'Autorità, nonché le novità normative sopravvenute, hanno reso necessario un nuovo intervento del Garante sull'argomento.

In particolare, dalla maggior parte degli abbonati è stato segnalato che l'oscuramento delle ultime tre cifre nelle fatture non consente loro di controllare l'esattezza degli addebiti, soprattutto all'interno del medesimo distretto telefonico, nel quale i numeri degli abbonati differiscono solo per le ultime cifre.

Per tali motivi, è in corso di adozione un provvedimento di carattere generale che tiene conto, in particolare, della possibilità che le chiamate effettuate da qualsiasi terminale vengano pagate con modalità alternative alla fatturazione, anche in grado di mantenere l'anonimato del chiamante, ad esempio, attraverso l'uso di carte prepagate (cfr. art. 5, comma 1, d.lg. n. 171/1998).

Con riferimento a tali profili, va rilevato che la maggior parte dei fornitori di servizi telefonici ha fatto pervenire a questa Autorità, entro la prevista scadenza del 30 giugno 2002 (cfr. art. 5, comma 1-*bis*, del citato decreto, introdotto dal d.lg. n. 467/2001), la documentazione –di cui è stato completato il vaglio- relativa all'effettiva predisposizione delle suindicate modalità alternative.

Al riguardo, il Garante ha ribadito l'importanza -per la tutela della sfera privata degli utenti chiamanti, diversi dall'abbonato- dell'effettiva operatività di tali servizi, in quanto gli stessi consentono all'utente di addebitare sulle schede di pagamento o prepagate il costo delle chiamate effettuate, in modo tale che le stesse non compaiano nella fatturazione inviata agli abbonati.

Inoltre, fermi restando gli specifici obblighi a garanzia degli interessati, già segnalati ai fornitori dei servizi telefonici nel provvedimento del 5 ottobre 1998 (in *Bollettino* n. 6, p. 101),

il Garante ha sottolineato nuovamente la piena applicabilità dell'art. 13 della legge n. 675/1996 alle informazioni incluse nella fatturazione, trattandosi, come già chiarito, di dati personali (art. 1, comma 1, lett. *c)* legge citata).

Questa Autorità si è pronunciata in tal senso anche in occasione di un nuovo ricorso relativo ad una richiesta di accesso ai propri dati personali concernenti il traffico in uscita, rivolta da un interessato ad un noto operatore telefonico (*Decisione* del 30 settembre 2002).

Chiamate in entrata e chiamate di disturbo

In relazione alle chiamate in entrata l'Autorità è in procinto di adottare un provvedimento generale che tiene conto di diverse previsioni normative che richiedono una lettura congiunta. Da un lato, infatti, occorre considerare la previsione dell'art. 14, comma 1, lett. *e-bis)*, l. n. 675/1996 (anch'essa introdotta dal richiamato d.lg. n. 467/2001), che limita l'accesso ai dati identificativi delle chiamate in entrata ai soli casi in cui dal mancato accesso può derivare un pregiudizio allo svolgimento delle investigazioni difensive di cui alla legge n. 397/2000. Dall'altro lato, non si può prescindere dalla possibilità riconosciuta all'abbonato di ottenere dall'operatore, con la procedura prevista dall'art. 7, comma 1, d.lg. n. 171/1998, la selezione dei dati relativi alle chiamate ricevute, qualora le stesse siano di disturbo.

Il Garante è infine impegnato nell'esame delle questioni attinenti alla tematica relativa all'identificazione della linea chiamante, di cui all'art. 6, d.lg. n. 171/1998, anche in relazione al servizio in tal senso offerto da alcuni fornitori telefonici. Al fine della predisposizione di un provvedimento in materia, sono in fase di completamento, tra l'altro, consultazioni con i principali fornitori telefonici, volte ad approfondire lo stato di attuazione della normativa in argomento.

Elenco telefonico generale

L'Autorità ha continuato ad esaminare le problematiche connesse all'inserimento dei dati personali nell'ambito degli elenchi telefonici. Tali attività hanno condotto all'adozione della delibera del 23 maggio 2002, nella quale sono stati chiariti tutti gli aspetti più rilevanti in relazione alla prossima realizzazione dell'elenco telefonico generale, che conterrà i dati degli abbonati ai servizi degli operatori di telefonia fissa e mobile.

La formazione di tale elenco era stata già prevista dal d.P.R. 11 gennaio 2001, n. 77, sulla cui predisposizione, realizzata senza la necessaria, preventiva consultazione del Garante, ci si è soffermati nella relazione dello scorso anno (v. *Relazione 2001*, p. 85). Tale decreto, all'art. 20, subordina in ogni caso, 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. 3 maggio 1998, n. 171).

Nella citata deliberazione del 23 maggio 2002 il Garante ha individuato le modalità e le forme con cui devono essere realizzati i trattamenti connessi alla predisposizione dell'elenco

telefonico generale. Ciò, con particolare riguardo alla possibilità, per gli abbonati, di limitare i dati inseriti negli elenchi a quelli necessari per la loro identificazione, nonché alla possibilità, per gli stessi, di chiedere gratuitamente di non essere inclusi negli elenchi, di ottenere che il proprio indirizzo sia in parte omesso e, qualora ciò sia fattibile dal punto di vista linguistico, di non essere contraddistinto da riferimenti che rivelino il sesso (cfr. art. 9 del d.lg. n. 171/1998).

Queste garanzie sono state rafforzate dalla richiamata direttiva 2002/58/CE, in particolare per ciò che concerne gli obblighi di informativa dei fornitori di servizi nei confronti degli abbonati, nonché la possibilità per gli stessi abbonati di decidere se i loro dati personali -e, in caso positivo, quali- debbano essere *"riportati in un elenco pubblico, sempreché tali dati siano pertinenti per gli scopi dell'elenco dichiarati dal suo fornitore"*. È inoltre previsto che agli abbonati debba essere garantita la possibilità di *"verificare, rettificare o ritirare tali dati"* (cfr. art. 12 della direttiva 2002/58/CE).

L'esame di tali problematiche è avvenuto nel quadro di una proficua collaborazione tra il Garante e l'Autorità per le garanzie nelle comunicazioni, le quali, nell'ambito delle rispettive competenze, hanno individuato -anche in un comunicato congiunto del 13 giugno 2002- le garanzie da adottare per inserire le informazioni personali nel suddetto elenco generale che interessa milioni di cittadini italiani.

D'intesa tra le due Autorità, è stato in particolare stabilito che gli abbonati hanno il diritto di essere preventivamente informati sull'utilizzo e le finalità degli elenchi, di scegliere se essere inseriti o meno nell'elenco e quali dati devono essere presenti nello stesso. Ai medesimi abbonati è stato altresì riconosciuto il diritto di esprimere un consenso specifico e differenziato per l'eventuale utilizzo dei dati inseriti nell'elenco per scopi pubblicitari. Consenso, questo, che sarà evidenziato nell'elenco attraverso l'apposizione di uno specifico simbolo.

A tal riguardo, si fa presente che sono all'esame del Garante le prime bozze di moduli redatti dai fornitori di servizi telefonici volte a fornire agli abbonati l'informativa di cui sopra. L'Autorità, nel valutare i moduli predisposti, ha sottolineato la necessità di evitare il rischio che gli abbonati siano indotti a sottoscrivere, in modo inconsapevole, le formule di consenso presenti negli stessi, specie se tale consenso è richiesto per scopi pubblicitari (*comunicato* 25 gennaio 2003).

Sempre nell'ambito delle procedure per la realizzazione del suddetto elenco telefonico generale, il Garante, in cooperazione con l'Autorità per le garanzie nelle comunicazioni, ha preso parte a una serie di incontri e riunioni con i fornitori di servizi di telefonia fissa e mobile, volti alla definizione degli accordi-quadro previsti dalle decisioni adottate in materia (cfr. il citato provvedimento del Garante del 23 maggio 2002 nonché le delibere dell'AGCOM nn. 36/02/CONS, 180/02/CONS).

Il tema degli elenchi è in conclusione seguito con particolare attenzione dall'Autorità, anche in ragione dei delicati effetti che si determinano nei confronti di milioni di persone interessate.

49 Servizi non richiesti e consenso dell'interessato

In merito all'attivazione di contratti e servizi di telefonia mobile e fissa, senza il preventivo consenso degli interessati, il Garante ha continuato a ricevere numerose segnalazioni ed ha avviato un'indagine conoscitiva (*Provv.* 10 gennaio 2002, in *Bollettino* n. 24, p. 3) presso i fornitori di servizi di telecomunicazione, nonché presso taluni esercizi commerciali abilitati all'attivazione dei contratti telefonici (v. anche *Relazione 2001*, p. 84).

Sulla base delle informazioni acquisite, il Garante ha concluso l'esame e sta per emanare un provvedimento generale diretto, oltre che a risolvere i singoli casi segnalati, anche a formulare indicazioni generali sulla materia.

L' Autorità, nel ribadire la necessità che l'attivazione di qualunque contratto o servizio telefonico sia preceduta da un'idonea informativa all'abbonato sul trattamento dei dati personali che verrà effettuato (*ex* art. 10, legge n. 675/1996), ha ricordato anche che, per la realizzazione di alcuni trattamenti, è necessario richiedere il consenso agli interessati, specificamente ed in forma differenziata, specie in relazione all'attivazione di servizi aggiuntivi rispetto a quello principale oggetto del contratto.

50 Comunicazioni indesiderate dirette a utenze telefoniche mobili

Hanno formato oggetto di esame anche numerose istanze e segnalazioni di abbonati, utenti e associazioni di consumatori, relative alle possibili violazioni della normativa in materia di protezione dei dati personali in occasione della ricezione, sulle utenze di telefonia mobile, di brevi messaggi di testo di diverse tipologie (*sms* pubblicitari, istituzionali e anonimi).

Oltre alle suddette tipologie, si è venuti a conoscenza di altre, in fase di progettazione o di sperimentazione, riguardanti la possibilità, per talune amministrazioni pubbliche, 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.

La possibile utilità di nuovi servizi non deve far sottovalutare la particolare forza invasiva che caratterizza le comunicazioni realizzate attraverso l'invio di sms, che si avvalgono del numero del telefono cellulare, generalmente considerato come personale e riservato. Pertanto, si è ritenuto necessario formulare alcune prescrizioni in materia. L'Autorità è in procinto di definire a breve 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.

Sms pubblicitari

Il Garante ha concluso l'esame delle problematiche concernenti gli *sms* utilizzati per scopi di informazione commerciale o di vendita diretta, relativamente a prodotti offerti dal fornitore di servizi telefonici o da altri fornitori (al di fuori del settore delle telecomunicazioni), in riferimento ai quali l'operatore telefonico si limitava a trasmettere il contenuto del messaggio. E' pertanto di prossima adozione il relativo provvedimento.

Nell'ambito dei vari profili esaminati, hanno trovato espresso richiamo le garanzie contenute nell'art. 10, comma 1 del d.lg. n. 171/1998. Tale disposizione, nel disciplinare il fenomeno delle chiamate indesiderate, ha stabilito che l'utilizzo di sistemi automatizzati di chiamata senza intervento di un operatore per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva è consentito esclusivamente *"con il consenso espresso dell'abbonato"*.

Le garanzie ora richiamate con riferimento al fenomeno degli *sms* a scopi pubblicitari, sul quale si è appuntata a più riprese l'attenzione del Garante (cfr. le decisioni del 18 luglio e del 6 settembre 2002) trovano conferma nella direttiva 2002/58/CE (cfr. considerando n. 40 e art. 13 relativo alle Comunicazioni indesiderate). Esse, inoltre, vengono ad aggiungersi a quelle previste per i casi in cui le finalità commerciali sono perseguite attraverso mezzi diversi da quelli appena indicati (ad esempio, quelli in cui la comunicazione è instaurata mediante l'intervento di un operatore). In tali ipotesi, trovano applicazione le disposizioni dettate in generale per il consenso al trattamento dei dati personali e, quindi, anche alcune specifiche esenzioni da tale obbligo (cfr., in particolare, gli artt. 11 e 12 l. n. 675/1996).

In tale ambito, sono state individuate le misure che i diversi titolari devono adottare al fine di assicurare il rispetto degli obblighi posti dalla normativa sulla protezione dei dati personali, in relazione alle differenti, possibili modalità di invio dei messaggi, quali sono emerse dalle segnalazioni pervenute.

I principi qui riassunti sono stati affermati anche in occasione di un provvedimento riguardante la ricezione indesiderata sulle utenze di telefonia mobile o tramite la posta elettronica di messaggi pubblicizzanti i servizi offerti tramite le numerazioni "899". Il fenomeno, diffusosi in Italia in modo dirompente soprattutto negli ultimi tempi, ha richiesto, da parte del Garante, indagini complesse, che hanno comportato anche frequenti contatti con altre istituzioni interessate alla vicenda (Autorità per le garanzie nelle comunicazioni; Autorità garante per la concorrenza e il mercato; Ministero delle comunicazioni; Polizia postale).

Tali indagini hanno portato ad individuare alcuni soggetti, italiani e stranieri, nei confronti dei quali -direttamente, o attraverso la collaborazione degli altri Garanti europei- sono stati avviati accertamenti ai sensi dell'art. 32, comma 1, della legge n. 675/1996.

Sms istituzionali

Nel 2002 il Garante ha effettuato alcuni accertamenti con riguardo all'invio ad abbonati e/o ad altri soggetti detentori di carte telefoniche, da parte di alcuni enti pubblici, di *sms* contenenti informazioni di pubblica utilità, attinenti all'attività istituzionale degli enti stessi (ad esempio, comunicazione di provvedimenti di blocco del traffico adottati a tutela della salute pubblica o informazioni sugli avvenimenti culturali in corso). Ciò al fine di verificare la rispondenza di tali trattamenti alle vigenti norme in materia di protezione dei dati personali.

Pur nella consapevolezza che l'invio di tali *sms* può soddisfare in alcuni casi finalità di interesse collettivo, l'Autorità ha chiarito in un provvedimento di carattere generale le misure e gli accorgimenti idonei ad evitare che il connesso trattamento di dati personali determini un'ingiustificata lesione della riservatezza dei soggetti cui i dati stessi si riferiscono.

È stata distinta l'ipotesi in cui i suddetti *sms* siano inviati, per conto di enti pubblici, da parte di un operatore telefonico, attraverso l'utilizzo della banca dati dei propri abbonati, rispetto a quella in cui sia invece lo stesso ente pubblico ad inviarli, utilizzando una propria banca dati. A seconda che si versi in una delle suddette ipotesi -e fatte salve eventuali deroghe

alla disciplina vigente in caso di messaggi che trovino fondamento in provvedimenti contingibili e urgenti adottati in conformità alle leggi- trovano quindi applicazione le diverse disposizioni concernenti le condizioni di liceità del trattamento dei dati personali (cfr., rispettivamente artt. 11 e 27 della legge). Ciò, ferma restando, in ogni caso, la necessità che gli abbonati siano informati preventivamente e adeguatamente della possibilità di ricevere, sulla propria utenza, tali messaggi (art. 10 della legge n. 675/1996).

Sms anonimi

Il Garante ha concluso l'esame ed è in procinto di adottare un provvedimento che individua le garanzie necessarie volte a salvaguardare le esigenze di riservatezza degli utenti in relazione alla possibilità, offerta da talune società di telefonia mobile, di inviare (e quindi ricevere) messaggi *sms* anonimi, senza l'identificazione del numero del mittente. L'Autorità ha precisato che tale servizio non fa venir meno il diritto dei destinatari di siffatti messaggi di tutelarsi contro possibili pregiudizi che tale forma di comunicazione può arrecare loro e, quindi, di avvalersi degli strumenti che la legge n. 675/1996 offre a loro protezione.

51 Messaggi multimediali (*Mms*)

Hanno formato oggetto di esame anche le numerose segnalazioni sulle possibili violazioni della normativa in materia di protezione dei dati personali con riguardo alle nuove tecnologie che consentono a chiunque, mediante l'utilizzo di telefoni mobili che abbiano determinate caratteristiche tecniche, di effettuare, registrare ed inviare fotografie e suoni, tramite *Gprs*, nonché filmati, attraverso il sistema *Umts* (*Mms*). Attraverso l'utilizzo di tali sistemi, è infatti possibile riprendere e far circolare immagini, raccolte in luoghi pubblici, aperti al pubblico o privati, relative ad altre persone anche a loro insaputa, con conseguente invasione dell'altrui sfera privata.

L'Autorità è intervenuta con un provvedimento del 12 marzo 2003, con il quale ha chiarito che anche chi scatta le fotografie o effettua riprese con il proprio telefono mobile, esclusivamente per soddisfare esigenze di carattere strettamente personale (culturali, di svago o di altro genere), e beneficiando, in tal modo, dell'esenzione di cui all'art. 3 della legge n. 675/1996, deve rispettare in ogni caso alcune disposizioni applicabili anche a tale fattispecie, in particolare riguardo alla sicurezza delle informazioni trattate (art. 15) e alla responsabilità per i danni cagionati per effetto del trattamento (art. 18).

Il Garante ha poi precisato che, allorquando si tratti di fotografie o filmati comunicati in via sistematica ad una pluralità di destinatari, oppure diffusi (ad esempio mediante pubblicazione su un sito *Internet*), devono ritenersi applicabili tutte le disposizioni della suddetta legge.

Un discorso diverso deve ritenersi praticabile con riferimento all'attività giornalistica. In riferimento a tale caso, il Garante ha ribadito che non sussiste alcun obbligo per il giornalista di chiedere il consenso dell'interessato, fermo restando il rispetto delle cautele e dei limiti posti dalla legge e dal pertinente codice deontologico. Resta fermo, in ogni caso, il necessario rispetto dei principi di correttezza e di tutela della dignità della persona. La concretizzazione di tali principi comporta la necessità, per chi procede al trattamento delle informazioni personali, di effettuare un attento vaglio circa la pertinenza e la non eccedenza delle informazioni raccolte e trattate, rispetto alle finalità di natura personale perseguite.

L'Autorità ha altresì ricordato che sia in caso di invio episodico, sia di diffusione sistematica di immagini, si devono comunque rispettare ulteriori obblighi previsti da altre norme civilistiche e penalistiche, nonché dalla legge n. 633/1941 sul diritto d'autore.

52 Localizzazione

Nel corso dell'anno, in vista del recepimento della direttiva 2002/58/CE, l'Autorità ha intrapreso un primo studio relativo alla conservazione dei dati relativi alle chiamate effettuate da apparecchi mobili, con specifico riguardo ai dati personali concernenti la localizzazione degli apparecchi medesimi, anche per ciò che concerne la distinzione operata dalla direttiva 2002/58/CE tra i dati relativi al traffico e quelli relativi all'ubicazione (cfr. considerando 35, nonché art. 9 della direttiva).

53 Attività di cooperazione con l'Autorità per le garanzie nelle comunicazioni

Il 20 febbraio 2003 si è tenuta una riunione congiunta tra il collegio del Garante e quello dell'Autorità per le garanzie nelle comunicazioni, nel corso della quale sono state messe a punto alcune linee di intervento comune, anche al fine di intensificare, nell'ambito delle rispettive aree di competenza, le forme di cooperazione istituzionale già avviate in precedenza (v. comunicato stampa del 20 febbraio 2003).

Nel corso dei lavori sono state sottolineate l'importanza e la novità istituzionale rappresentate dalla proficua collaborazione già realizzatasi su questioni di interesse comune (elenchi telefonici, servizi di telecomunicazione non richiesti etc.) e la necessità di procedere a forme ancor più strette di cooperazione.

In vista di questo obiettivo le due Autorità hanno convenuto di rendere sistematico lo scambio di informazioni e di documentazione tra gli uffici, nonché di approfondire, a breve termine, un protocollo che dia attuazione alle linee generali tratteggiate nell'incontro e alle ipotesi di collaborazione proposte.

Nell'ambito di tale collaborazione, l'Ufficio del Garante ha avuto modo di svolgere una prima valutazione, del tutto preliminare, sulla possibile realizzazione in Italia del progetto noto come *"e-number"* o *"Enum"*, con riferimento ad una consultazione pubblica promossa dall'Autorità per le garanzie nelle comunicazioni. Tale sistema permette di creare connessioni fra indirizzi *Internet* e numeri telefonici, al fine di realizzare un numero identificativo universale che consente di instradare il traffico verso i diversi recapiti dell'interessato (telefono fisso, mobile, indirizzo di posta elettronica, ecc.).

Il sistema Enum, già allo studio in altri Paesi europei, ha suscitato notevoli perplessità in ordine alle possibili implicazioni che la sua introduzione potrebbe avere in relazione alla sfera di riservatezza degli interessati.

L'Autorità per le garanzie nelle comunicazioni ha così avviato una consultazione pubblica sull'introduzione del protocollo *Enum* rivolgendo particolare attenzione anche agli aspetti riguardanti la sicurezza e la protezione dei dati personali (v. *Comunicato* pubblicato nella G.U. n. 95 del 24 aprile 2003).

Trattamento di dati personali in Internet

54 Profili generali

Gli sviluppi relativi alla protezione dei dati personali in materia di reti telematiche sono strettamente connessi alla continua evoluzione del settore, come testimoniano le diverse e sempre crescenti segnalazioni, richieste di chiarimenti e quesiti che provengono giornalmente a questa Autorità.

Nel corso del 2002, il Garante ha proseguito nell'opera di costante monitoraggio dell'evoluzione tecnica del settore, stabilendo, in particolare, forme opportune di consultazione con i diversi operatori, in modo da poter promuovere l'adozione di garanzie adeguate sia sul piano della prassi operativa, sia su quello normativo, anche provvedendo a sollecitare l'adozione delle misure necessarie alle autorità pubbliche competenti.

D'altronde, le numerose problematiche esaminate hanno confermato come un'altra caratteristica peculiare della maggior parte dei trattamenti realizzati in tale ambito sia quella di poter prescindere, in larga misura, dai confini nazionali e, quindi, dalla legislazione sulla protezione dei dati applicabile all'interno di essi.

Proprio in ragione di tali peculiarità, sono destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici previsti dal d.lg. n. 467/2001, nonché l'emanando testo unico più volte richiamato.

Sono stati avviati i lavori preliminari per la redazione del codice deontologico relativo ai trattamenti di dati personali *"effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica"*.

In questo quadro, è utile ricordare che la direttiva 2002/58/CE (da recepirsi entro il 31 ottobre p.v.), relativa al *"trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche"*, nel modificare la direttiva 97/66/CE, si pone l'obiettivo di adeguare la disciplina sulla tutela dei dati personali agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica. Ciò, adottando un approccio "tecnologicamente neutro", mirante, cioè, a predisporre una normativa valida ed applicabile a tutte le forme di comunicazione elettronica realizzate per via telefonica, su *Internet* o su altri mezzi.

Nelle more dell'adozione del testo unico e del codice sopra richiamati, nonché della trasposizione in Italia della direttiva citata, l'Autorità ha comunque già fornito alcuni chiarimenti in ordine a diverse problematiche sottese alla materia.

Oltre a offrire alcune prime precisazioni in merito al possibile esercizio, sulla rete *Internet*, dei diritti di cui all'art. 13 della legge 675/1996, il Garante ha concluso l'esame e sta per adottare un provvedimento di carattere generale che fornisce alcuni suggerimenti ed indicazioni agli operatori del settore ed agli utilizzatori della rete in materia di invio di posta elettronica indesiderata (c.d. "*spamming*").

55 Comunicazioni indesiderate

Spamming su Internet

Il Garante si è più volte occupato della problematica relativa all'invio di messaggi di posta elettronica non sollecitati di natura prevalentemente pubblicitaria.

Come già evidenziato in passato (v. *Relazione 2001*, p. 88), la direttiva 2002/58/CE ha recepito, quale sistema di regolamentazione del problema, il principio secondo cui l'invio di messaggi di posta elettronica di carattere pubblicitario è subordinato all'espresso consenso dell'interessato ("*opt-in*").

Il Garante ha espresso un positivo avviso in ordine alla predetta opzione (v. Newsletter, 12 - 18 febbraio 2001). D'altronde, come chiarito dal Garante nel corso del 2002, la legge 675/1996 (art. 11), il d.lg. 171/1998 (art. 10) ed il d.lg. 185/1999 (art. 10, comma 1) già riconducono la fattispecie in esame alla regola del consenso preventivo ed esplicito.

In tal senso, il Garante si è espresso anche in occasione delle decisioni adottate in merito ai ricorsi presentati da alcuni utenti, ai sensi dell'art. 29 della legge 675/1996 (*Provv.* 25 giugno, 25 luglio e 30 settembre 2002). Accertata la fondatezza delle pretese dei ricorrenti, l'Autorità ha provveduto a bloccare le banche dati delle relative società che avevano inviato numerose *e-mail* pubblicitarie e promozionali senza aver acquisito, in via preventiva, il consenso informato degli interessati.

Il blocco dei trattamenti connessi alle predette banche dati si è reso necessario anche per impedire che il trattamento illecito e non corretto dei dati personali potesse estendersi ad un elevato numero di cittadini i cui indirizzi di posta elettronica erano presenti negli archivi delle società medesime.

Svariati altri provvedimenti di blocco sono stati adottati in altre successive circostanze.

In questo quadro, il Garante è altresì in procinto di adottare un provvedimento di carattere generale volto ad offrire altre indicazioni in materia.

L'Autorità ha, già più volte ricordato che nei casi di specie non può essere invocato l'art. 12, comma 1, lett. *c)*, della legge 675/1996, il quale esonera il titolare dal richiedere il consenso dell'interessato ove i dati relativi a quest'ultimo siano provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Infatti, questa disposizione si riferisce esclusivamente agli elenchi o ai registri per i quali è previsto uno specifico regime giuridico di piena conoscibilità da parte di chiunque, e non è, quindi, applicabile ai casi in cui un determinato dato possa essere consultato dal pubblico per mere circostanze di fatto (ad esempio: raccolta su siti *web* o presso *newsgroup* ove erano disponibili per diverse finalità).

Quanto, poi, al consenso all'invio di messaggi pubblicitari e al connesso obbligo di informativa nei confronti dei destinatari, il Garante ha sottolineato che il consenso, oltre a dover essere manifestato liberamente e documentato per iscritto, secondo le previsioni del già citato art. 11 della legge, deve essere preventivo, esplicito ed espresso in forma differenziata rispetto alle varie categorie di prodotti offerti.

La circostanza, poi, che l'indirizzo di posta elettronica sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti, non lo rende liberamente utilizzabile e non autorizza, comunque, l'invio di informazioni di qualunque genere, anche se non specificamente a carattere commerciale o promozionale senza un preventivo consenso.

Ed ancora, con riguardo al diritto degli interessati di richiedere la cessazione dell'invio di messaggi pubblicitari indesiderati, il Garante ha più volte sottolineato che, indipendentemente dal rapporto esistente tra i mittenti ed i destinatari dei messaggi pubblicitari, deve essere data sempre a questi ultimi la possibilità di far valere il proprio diritto di opporsi, in tutto o in parte, al trattamento dei dati medesimi ai fini di informazione commerciale. La richiesta per l'esercizio di tale diritto può essere avanzata senza formalità, ad esempio tramite posta elettronica o anche verbalmente (art. 17, comma 1, d.P.R. n. 501/1998). In ogni caso, tali diritti devono poter essere esercitati gratuitamente ed in maniera agevole.

Nel caso di esercizio dei diritti di cui al richiamato art. 13, i titolari o i responsabili dagli stessi designati, sono tenuti a fornire all'interessato una risposta completa ed esaustiva, con riferimento a tutti gli elementi richiesti.

Nomi a dominio

Durante il periodo di riferimento sono inoltre pervenute a questa Autorità diverse segnalazioni in ordine alla protezione dei nomi a dominio, con specifico riguardo ai dati relativi ai soggetti che registrano siti *web* ("*registrant*") nonché alla pubblicazione di alcuni dati personali sulla rete.

Al riguardo, il Garante ha svolto alcune indagini conoscitive in merito alle modalità ed alle regole di registrazione dei nomi a dominio in Italia, al fine di predisporre un provvedimento generale.

56 Il codice deontologico

Come accennato nel paragrafo relativo ai profili generali, nonché nella *Relazione 2001* (p. 89), è prossima l'adozione del codice sui trattamenti dei dati personali *"effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica"*.

Ed infatti, sulla base di quanto stabilito dal d.lg. 467/2001, il Garante ha promosso, nell'ambito di una generale attività collaborativa con i diversi operatori del settore, la sottoscrizione del predetto codice di deontologia e buona condotta, con il dichiarato scopo di fornire *"i 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"*, nell'ottica di *"una più 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"*.

A tal riguardo, è utile sottolineare che, al pari di quanto previsto per i codici sui trattamenti realizzati a fini storici o statistici, tale codice assumerà il ruolo di fonte dell'ordinamento, come, d'altronde, dispone l'art. 20 del d.lg. 467 cit., il quale testualmente recita: *"il rispetto delle disposizioni in essi contenute costituisce condizione essenziale per la liceità del trattamento dei dati"*.

57 Pubblicazione di fotografie sui siti *web*

Sono pervenute, nel 2002, segnalazioni concernenti la liceità della pubblicazione -anche su siti *web*- di fotografie e immagini che ritraggono persone.

Sul punto merita ricordare un provvedimento del Garante nel quale, tra i vari aspetti esaminati, sono stati forniti chiarimenti in ordine agli adempimenti gravanti sui fotonegozianti e sulle società (che di regola operano sulla base di specifici accordi negoziali con i primi) i quali offrano al cliente, oltre al tradizionale servizio di sviluppo e stampa dei rullini, anche la visione delle proprie fotografie su un apposito sito *web* (*Provv.* 16 maggio 2002, in *Bollettino* n. 28).

In tale occasione il Garante, oltre a ribadire il principio in base al quale le fotografie possono contenere immagini e informazioni qualificabili alla stregua di dati personali (art. 1, comma 2, lett. c), l. n. 675/1996, ha richiamato l'obbligo, per i titolari di siffatto trattamento, di fornire al cliente un'idonea informativa, anche oralmente (art. 10, comma 1, l. n. 675/1996), sin dal momento della richiesta della prestazione e, quindi, della consegna del rullino. Ciò al fine di porre l'interessato in condizione di scegliere in modo consapevole la particolare modalità del servizio di sviluppo desiderato e di conoscere in anticipo le modalità del peculiare trattamento. Tale esigenza non può ritenersi sufficientemente soddisfatta -ha precisato il Garante- tramite la mera esibizione o consegna di materiale promozionale ai clienti. Né l'informativa sui dati personali può considerarsi implicita nel mero pagamento di un prezzo diverso rispetto a servizi tradizionali.

Il Garante ha altresì richiamato l'attenzione sulla necessità che in tali casi siano adottate le specifiche misure di sicurezza volte a prevenire taluni rischi, tra i quali quelli di distruzione o perdita dei dati personali trattati o di accesso non autorizzato (art. 15 l. n. 675/1996 e d.P.R. 28 luglio 1999, n. 318); obblighi che, con riferimento al peculiare trattamento in questione, assumono rilievo in relazione alle diverse fasi del processo di realizzazione del servizio, nonché ai diversi soggetti in esso coinvolti (i negozianti e gli altri addetti allo sviluppo delle fotografie; il gestore del *server* nel quale viene conservato il *file* contenente le fotografie; la società titolare del sito su cui queste ultime vengono pubblicate).

58 Fotografie e immagini su cataloghi pubblicitari, giornali, riviste o altri strumenti di diffusione

I principi sopra ricordati sono stati riaffermati dall'Autorità in risposta ai numerosi quesiti concernenti, più in generale, la possibilità di pubblicare fotografie o immagini costituenti dati personali su cataloghi, giornali, riviste o altri analoghi strumenti di diffusione, ivi compresa la rete *Internet.*

In varie occasioni, pertanto, l'Autorità ha ricordato che le suddette immagini possono essere trattate solo con il consenso espresso, specifico e documentato per iscritto (art.11, l. n. 675/1996). Ciò, fatta salva l'eventuale sussistenza degli altri presupposti equipollenti del consenso indicati agli artt. 12 e 20 della legge citata.

Tra i casi in cui è consentito ad un soggetto privato trattare fotografie e immagini prescindendo dal consenso dell'interessato -ma non dalla previa informativa, ai sensi dell'art.10 della legge n. 675/1996- rileva, in particolare, l'ipotesi in cui la raccolta e la diffusione dei predetti dati siano necessarie per l'esecuzione degli obblighi derivanti da un contratto del quale è parte la persona ritratta (ad esempio, come nel caso evidenziato nel paragrafo precedente nel contesto di un servizio fotografico richiesto dall'interessato), ovvero per l'esecuzione di misure precontrattuali adottate su richiesta della stessa (artt. 12 lett. *b)*, e 20 lett. *a-bis)*, l. n. 675/1996).

Analogamente, è possibile prescindere dal consenso nel caso in cui il trattamento sia effettuato nell'esercizio del diritto di cronaca e, in generale, della libertà di manifestare il proprio pensiero (artt. 12, lett. *e)* 20, lett. *d)* e 25). In tale caso trovano applicazione le disposizioni contenute nel codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica.

Il Garante ha inoltre precisato che la legge n. 675/1996 non ha inciso sulle garanzie contenute nella legge sul diritto d'autore (artt. da 87 a 97 l. 22 aprile 1941, n. 633) le quali prevedono, fra l'altro, che l'esposizione, la riproduzione e la messa in commercio del ritratto di una persona presuppongono il consenso della persona ritrattata, a meno che la riproduzione dell'immagine sia giustificata *"dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico"* e che vietano, comunque, l'esposizione o la messa in commercio qualora rechi *"pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata"* (v. art.10 c.c.).

L'Autorità ha infine ricordato che -fermo restando quanto previsto per i trattamenti effettuati nell'esercizio del diritto di cronaca e di libera manifestazione del pensiero (art. 25, l. n. 675/1996 citata)- le specifiche disposizioni concernenti i dati c.d. "sensibili" (in particolare gli artt. 22 e 24 e le autorizzazioni generali per il 2002) trovano applicazione anche con riferimento alle immagini idonee a rivelare tale tipo di informazione.

Sicurezza dei dati e dei sistemi

59 Misure di sicurezza: novità normative e casi applicativi

La sicurezza costituisce una priorità nella normativa concernente la protezione dei dati personali e pertanto specifiche norme si rinvengono sia in atti sopranazionali, sia nella normativa nazionale.

Importanza primaria riveste la direttiva 95/46/CE che, come è noto, è stata recepita in Italia in larga misura con la legge n. 675/1996. In particolare, l'art. 15 si occupa della sicurezza dei dati, prevedendo due livelli di misure di sicurezza: le misure idonee e le misure minime.

Le prime sono rivolte a ridurre al minimo il rischio di distruzione, di perdita accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme, mentre le seconde sono quelle indicate nel regolamento emanato ai sensi dell'art. 15, comma 2, della legge n. 675/1996 (d.P.R. n. 318/1999). Questo regolamento doveva essere già adeguato in passato, essendo previsto al comma 3 che l'aggiornamento avvenga con cadenza almeno biennale.

La mancata adozione delle misure adeguate espone il destinatario della norma ad una responsabilità di tipo civile ai sensi dell'art. 18 della legge n. 675, mentre all'inosservanza delle prescrizioni indicate nel d.P.R. n. 318/1999 sono collegate le sanzioni penali previste all'art. 36 della medesima legge n. 675/1996, come modificato dal decreto legislativo n. 467/2001.

Le modifiche operate sugli aspetti sanzionatori penali per la mancata osservanza delle misure minime, entrate in vigore il 1° febbraio 2002, operano principalmente su due versanti: da un lato l'esclusione dal penale del trattamento effettuato per fini personali (art. 2, d.lg. n. 467/2001), dall'altro la rivisitazione della fattispecie criminosa (art. 14, d.lg. n. 467/2001).

In merito al primo punto l'esclusione della sanzione penale indicata all'art. 36 della legge n. 675/1996 non esonera le persone fisiche che trattano i dati per fini esclusivamente personali dall'adottare le misure di sicurezza di cui all'art. 15 comma 1, restando pertanto operanti le conseguenze civili previste al successivo articolo 18, e il conseguente obbligo al risarcimento dei danni cagionati ai sensi dell'art. 2050 del codice civile.

Con riguardo invece al secondo profilo il legislatore ha mantenuto, anche nella nuova formulazione dell'art. 36, la figura del reato, seppure diversamente configurato da delitto in contravvenzione e punito, pertanto, con l'arresto o con l'ammenda.

La novità più rilevante è data tuttavia dall'introduzione di una procedura estintiva del reato (cd. ravvedimento operoso) espressamente mutuata dalla normativa in materia di sicurezza e igiene sul lavoro prevista nel decreto legislativo n. 758/1994 (art. 20, d.lg. n. 467/2001).

Il tema della sicurezza ha un carattere poliedrico e si riverbera su numerosi settori di intervento della normativa sulla riservatezza.

È utile ricordare anche in questo paragrafo che nel 2002 è stato adottato il codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (cfr. paragrafo 25), pubblicato nella *Gazzetta Ufficiale* n. 230 del 1 ottobre 2002. Il codice contiene specifiche indicazioni in ordine all'adozione delle misure di sicurezza. Sono previste numerose misure volte a proteggere i dati. I rilevatori devono garantire la sicurezza delle informazioni e rispettare le norme poste dal codice a tutela dei cittadini. La comunicazione dei dati tra soggetti del Sistema statistico nazionale deve avvenire nel rispetto delle misure di sicurezza previste dall'art. 15 della legge. E' necessario determinare differenti livelli di accesso ai dati personali con riferimento alla natura dei dati e alle funzioni dei soggetti coinvolti nei trattamenti, nonché adottare le cautele previste dagli articoli 3 e 4 del d. lg. n. 135/1999 in riferimento ai dati sensibili.

Tra gli atti normativi del 2002 che contengono apposite previsioni in ordine alle misure di sicurezza, assume particolare rilievo la direttiva 2002/58/CE sulla tutela della vita privata nelle comunicazioni elettroniche. L'importanza di tale direttiva è evidenziata dal fatto che il legislatore, per consentire il suo recepimento con lo strumento della legge comunitaria (legge 3 febbraio 2003, n.14), ha disposto uno slittamento di sei mesi del termine entro cui adottare il previsto testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

La direttiva prevede l'obbligo per il fornitore del servizio di predisporre appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi congiuntamente con il fornitore della rete pubblica di comunicazione.

La nuova direttiva fa gravare in capo al fornitore del servizio l'obbligo di informare gli abbonati quando sussiste un particolare rischio di violazione della sicurezza della rete, indicando i relativi costi e rimedi o situazioni che consentano di apprendere in modo non intenzionale il contenuto delle conversazioni o delle comunicazioni.

Sullo stesso tema è intervenuta anche la risoluzione del 28 gennaio del 2002 del Consiglio dell'Ue, tesa a fornire un approccio comune e azioni specifiche nel settore della sicurezza delle reti (2002/C43/02), la quale precisa che la sicurezza delle reti e dell'informazione presuppone che sia assicurata la disponibilità di dati e servizi. Ciò impedendo interruzioni o intercettazioni abusive delle comunicazioni, confermando che i dati trasmessi, ricevuti o archiviati sono completi e invariati, assicurando la riservatezza dei dati, proteggendo i sistemi da accessi non autorizzati e *software* maligni e garantendo, infine, l'affidabilità dell'autenticazione.

Anche l'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), nel corso del 2002, si è attivato nel settore delle misure di sicurezza tracciando alcune Linee guida approvate il 25 luglio, che prendono il posto di quelle elaborate nel 1992. Lo sviluppo esponenziale di *Internet* nei settori pubblico e privato ha imposto la necessità di indicare nuovi principi in materia di sicurezza dei sistemi informativi e delle reti. Esse, come espressamente raccomandato dall'OCSE, andranno riesaminate ogni cinque anni per l'esplicitato fine di promuovere una cooperazione internazionale sulle questioni connesse al sistema di sicurezza delle reti e dei sistemi informativi.

Le Linee guida si propongono di sviluppare una "cultura della sicurezza" fra i governi, le imprese e gli utenti, con l'invito a tutti gli utilizzatori di tecnologie dell'informazione a rispettare ed applicare nove principi base, fra cui la sensibilizzazione e la responsabilità in materia di sicurezza e il rispetto di valori etici e democratici, con particolare riguardo alla tutela dei dati personali.

Anche l'Autorità, nel corso del 2002, si è pronunciata numerose volte in materia di sicurezza, in seguito a ricorsi presentati ai sensi dell'art. 29, a segnalazioni o a procedimenti ispettivi.

Con alcuni ricorsi si è lamentato che il titolare, nell'effettuare il trattamento dei dati, non avesse osservato le specifiche disposizioni previste dalla legge n. 675/1996 anche con riferimento alla mancata adozione delle misure di sicurezza. In tali circostanze il Garante ha però ribadito che il procedimento disciplinato dall'art. 29 ha caratteri peculiari in quanto il ricorso che lo introduce può essere presentato solo per la tutela di precise richieste formulate in riferimento agli specifici diritti tutelati dall'art. 13, comma 1, della medesima legge e non si può rappresentare senza un collegamento a tale articolo qualsiasi violazione della disciplina del trattamento dei dati personali, compresa la mancata adozione delle misure minime di sicurezza (2 maggio 2002 - *Bollettino* n. 28).

In un altro caso il Garante, dopo aver esaminato il ricorso di un cittadino, ha disposto un'ispezione del sistema informatico di una importante banca *on line* per verificare i sistemi di sicurezza adottati dall'istituto di credito e il loro grado di affidabilità riguardo alla tutela della riservatezza dei dati personali della clientela. La decisione è stata assunta in quanto il ricorrente, cliente della stessa banca, è riuscito attraverso *Internet* a consultare non solo i dati del suo conto corrente, ma anche quelli di altri clienti della banca.

Sono da ricordare anche le segnalazioni di consumatori che lamentavano la violazione della normativa sulla *privacy* da parte di una società che, dopo aver sviluppato fotografie, le pubblicava come ulteriore servizio su un sito *web* dove, attraverso un codice personale, erano accessibili ai clienti i quali potevano così stamparle, raccoglierle in album virtuali o spedirle via *e-mail*. Nelle segnalazioni, oltre a sottolineare la mancanza della dovuta informativa preventiva sul tipo di servizio che veniva offerto, si evidenziava la carenza dell'adozione di idonee misure di sicurezza, in quanto il codice personale fornito dalla società era collocato all'esterno della busta che contiene le foto ritirate dal cliente, visibile anche da terzi non autorizzati a visionare il materiale fotografico.

Nella conseguente pronuncia il Garante ha disposto che la società attuasse i necessari accorgimenti volti a prevenire taluni rischi, tra i quali quelli di distruzione o perdita dei dati personali trattati o di accesso non autorizzato. Le misure da adottare assumono rilievo sia nelle diverse fasi del processo di realizzazione del servizio *"photosìonline"*, sia con riguardo ai diversi soggetti in esso coinvolti (i negozianti e gli altri addetti allo sviluppo delle fotografie; il gestore del *server* nel quale viene conservato il *file* contenente le fotografie; la società titolare del sito su cui queste ultime vengono pubblicate) (*Provv.* 16 maggio 2002, in *Bollettino* n. 28).

I trasferimenti all'estero dei dati

60 Paesi che offrono una protezione adeguata

A seguito del primo recepimento in Italia -con le autorizzazioni del Garante (v. *Relazione 2001*, pag. 91)- delle decisioni della Commissione europea in materia di trasferimento di dati personali all'estero, e in considerazione delle modifiche apportate dal d.lg. n. 467/2001 all'articolo 28 della legge 675/1996, l'Autorità ha iniziato a svolgere un attento monitoraggio in relazione ad operazioni ed attività di esportazione di dati da parte di operatori italiani e al tipo di garanzie e strumenti adottati per tutelare i diritti degli interessati.

Nell'aprile 2002 sono state formulate nei confronti di alcune importanti società, che avevano inviato comunicazioni o notificazioni sul trasferimento di dati all'estero e, in particolare, negli Usa, richieste di informazioni circa il rispetto delle disposizioni nazionali e comunitarie sui presupposti di liceità delle operazioni di trasferimento, con particolare riguardo, da un lato, alle relative finalità e modalità, alle categorie di dati e di persone interessate, nonché agli estremi dei soggetti importatori, e, dall'altro, all'eventuale adesione di questi ultimi al *Safe Harbor* o all'utilizzazione di clausole contrattuali tipo.

Dagli elementi acquisiti è risultato che, nella maggior parte dei casi, i dati personali oggetto di trasferimento all'estero riguardavano dipendenti e altre società e imprese (clienti, concorrenti, fornitori, ecc.) e che i flussi di dati erano stati effettuati previa acquisizione di specifico consenso degli interessati o avvalendosi di uno degli altri presupposti di liceità previsti dal citato art. 28 (esecuzione di obblighi contrattuali, ecc.)

In alcune ipotesi in cui la gestione del personale all'estero viene effettuata negli U.S.A., gli importatori dei dati (società capogruppo o comunque collegate o controllate) hanno aderito all'accordo sui principi dell'approdo sicuro, dichiarandosi disponibili a cooperare con le Autorità di vigilanza degli altri Paesi europei.

In nessuno di questi primi casi esaminati dal Garante è emerso che le società interpellate abbiano utilizzato le clausole contrattuali standard indicate dalla Commissione europea, trattandosi peraltro di strumenti introdotti solo recentemente.

Nell'ambito della stessa indagine, è stato infine evidenziato che, accanto alla proposta di una società di predisporre un apposito contratto per i propri flussi di dati all'estero da sottoporre al Garante al fine di ottenere una specifica autorizzazione, il gruppo societario di appartenenza stava sviluppando un contratto "multilaterale" per tutte le consociate da sottoporre anch'esso al parere preventivo delle Autorità Garanti europee.

Nel mese di marzo 2003 l'Autorità ha disposto un'ampia verifica preliminare, tuttora in atto, circa le modalità di applicazione da parte delle principali società industriali e di servizi delle disposizioni comunitarie e nazionali in materia di trasferimento dei dati personali all'e-

stero. Tale verifica è risultata necessaria al fine di valutare lo stato di attuazione delle disposizioni sui flussi di dati all'estero, prima d avviare specifici accertamenti relativi a singole società.

Oggetto dell'indagine è, in particolare, l'analisi dei presupposti, delle finalità e modalità del trasferimento di dati all'estero, anche in relazione ad operazioni effettuate da eventuali società collegate o controllate, delle categorie di dati trasferiti e delle persone interessate, degli estremi e delle attività dei soggetti importatori, nonché delle garanzie assunte per la tutela dei dati personali nei confronti di ciascuna tipologia di trasferimento. E' stato inoltre richiesto di indicare in termini percentuali, l'incidenza dell'utilizzo di clausole contrattuali tipo, dell'adesione ai principi di approdo sicuro e di uno dei casi indicati dall'art. 28, comma 4, della citata legge n. 675 (consenso degli interessati, esecuzione di obblighi contrattuali, ecc.), rispetto al volume complessivo dei trasferimenti di dati all'estero.

Il Garante ha, da ultimo, dato attuazione (*Deliberazione* n. 6 del 30 aprile 2003) alla decisione comunitaria del 20 dicembre 2001 con cui la Commissione europea ha riconosciuto anche il Canada tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali. (v. *Relazione 2001*). Tale deliberazione, al momento in cui il presente testo viene redatto, è in fase di pubblicazione nella *G.U.*

61 *"Safe Harbor"*

La Commissione europea ha riconosciuto in passato che i principi internazionali di riservatezza del *Safe Harbor*, 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 (decisione n. 2000/520/CE).

Il Garante, con l'autorizzazione del 10 Ottobre 2001 (pubblicata in G.U. 26 novembre 2001), ha attuato la suddetta decisione riservandosi di controllare la legittimità dei trasferimenti e di adottare i provvedimenti ad essa eventualmente conseguenti.

La stessa Commissione europea ha effettuato un primo rapporto (in data 13 febbraio 2002) sull'applicazione della decisione 2000/520/CE, 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 (v. *Relazione 2001*, p. 93).

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. Vari spunti di riflessione sono giunti al riguardo dal Gruppo dell'art. 29 della direttiva 95/46/CE.

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 al riguardo. In tal senso, va ricordata la visita negli Usa il 13 e 14 marzo 2002 di una delegazione di rappresentanti delle autorità di protezione dati europee, 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 è derivato un nuovo pronunciamento del Gruppo europeo in data 2 luglio 2002.

In tale documento è stata evidenziata la necessità di collaborazione di tutte le autorità competenti a dare piena esecuzione all'accordo.

In particolare, conformemente alla richiesta fatta dal Parlamento europeo nella sua risoluzione del 5 luglio 2000, si richiamano le autorità, le organizzazioni e le associazioni coinvolte a collaborare per raccogliere -in particolare attraverso le autorità nazionali per la protezione dei dati e la Commissione europea- informazioni aggiornate, con particolare attenzione:

- ad accordi per l'aumento della trasparenza nei confronti delle organizzazioni firmatarie, in particolare se una dichiarazione di adesione non è accompagnata da adeguate politiche per la *privacy*;
- alla possibilità di fornire meccanismi di controllo addizionali nei confronti della procedura d'adesione all'accordo, la conformità di condotta degli aderenti allo stesso con le proprie politiche di *privacy* e l'eventuale perdita dei benefici dell'Approdo sicuro;
- alle iniziative da adottare al fine di aumentare la conoscenza dei prerequisiti per l'adesione all'Approdo sicuro, anche attraverso di documenti brevi, facilmente comprensibili e l'eventuale integrazione nel *Safe Harbor Workbook*;
- ai provvedimenti da adottare per mettere a punto meccanismi di risoluzione delle controversie, aumentare l'uniformità e la conoscenza dei criteri salienti, aumentare la trasparenza circa l'esito delle controversie e semplificarne i meccanismi di pubblicazione;
- alle eventuali difficoltà derivanti dall'esistenza di molteplici politiche di *privacy* dichiarate dal medesimo operatore;
- ai criteri di priorità ed alle possibili ulteriori iniziative intraprese dalle competenti autorità statunitensi ed agli accordi per una rinnovata cooperazione tra il comitato europeo per la protezione dei dati, gli organi di risoluzione delle controversie e la Federal Trade Commission.

Il Garante

PAGINA BIANCA

La trattazione dei ricorsi

62 Principali problemi esaminati

Il primo dato caratterizzante la trattazione dei ricorsi nel corso del 2002 e nei primi mesi del corrente anno è un dato statistico: l'aumento consistente di tali atti proposti ai sensi dell'art. 29 della legge n. 675. Nell'anno solare 2002 sono stati infatti esaminati dal Collegio del Garante 390 ricorsi, un numero più che doppio rispetto all'anno precedente (erano stati, infatti, 169 i ricorsi decisi nel corso del 2001). Nel periodo del 1 gennaio -15 aprile 2003 sono stati decisi 110 ricorsi.

L'impressione è che il ricorso al Garante per la tutela delle posizioni giuridiche di cui all'art. 13, comma 1, della legge n. 675 sia uno strumento ormai entrato nella diffusa conoscenza non solo di professionisti, ma anche di un ampio numero di persone che dimostrano di saperlo utilizzare con efficacia.

Velocità della procedura, economicità dello strumento, facilità di utilizzo dello stesso giustificano il rapido diffondersi di questo meccanismo di tutela.

La ragione vera dell'affermarsi dei ricorsi consiste però, probabilmente, nell'estrema duttilità di questo strumento di tutela e nella vastità del suo campo d'azione a tutela dei diritti previsti dal citato art. 13.

L'ampia nozione di "dato personale" accolta dalla legge n. 675, oggetto in questi anni di precisazioni sempre più puntuali da parte del Garante, amplia infatti la latitudine del diritto di accesso ai dati personali previsto dal predetto art. 13 e, di conseguenza, estende l'applicabilità anche delle altre posizioni giuridiche tutelate dal medesimo articolo (diritto di integrazione e/o di correzione dei dati, opposizione al trattamento per motivi legittimi...). L'esperienza di questi mesi dimostra, anzi, come in molteplici settori della vita economica e sociale si affaccino sempre nuove situazioni rispetto alle quali i diritti tutelati dalla legge sulla protezione dei dati personali possono aprire prospettive innovative di tutela. Naturalmente ciò comporta un rilevante e continuo sforzo interpretativo da parte dell'Autorità per individuare correttamente l'ambito di applicazione della legge, difendere le legittime aspirazioni dei cittadini che se ne avvalgono, e prevenire, al tempo stesso, un uso strumentale e improprio della legge medesima.

Indubbiamente l'accesso ai dati personali ha reso più concreta quell'autodeterminazione informativa del singolo individuo tante volte segnalata come uno degli obiettivi della legge n. 675. Qualche volta, però, non è mancato da parte dei ricorrenti il tentativo di passare da richieste volte ad accedere ad informazioni relative all'interessato medesimo (così come richiesto dalle norme citate) ad istanze riferite in realtà a terzi. Né sono mancati tentativi di utilizzare certi strumenti (cancellazione dei dati, blocco degli stessi, opposizione al trattamento) non per motivi legittimi, o come reazione a dimostrate violazioni della legge, ma come tentativi di impedire legittimi utilizzi di informazioni da parte di soggetti pubblici e privati.

A dimostrazione della varietà di situazioni che sono state sottoposte all'attenzione del Garante sono qui tratteggiati una serie di settori in riferimento ai quali è stata proposta una pluralità di ricorsi, rinviando l'approfondimento delle specifiche questioni alle singole parti della presente Relazione.

"Centrali rischi" private

Il trattamento di dati personali (essenzialmente riferito ad operazioni di finanziamento, con particolare riguardo al credito al consumo) svolto dalle cd. "centrali rischi" ha da sempre costituito oggetto di numerose pronunce del Garante in riferimento a ricorsi proposti ai sensi dell'art. 29. Nel corso del 2002 la casistica si è moltiplicata e l'Autorità ha adottato numerose decisioni con le quali ha focalizzato l'attenzione su questi particolari tipi di trattamenti, fissando alcuni significativi principi di riferimento.

L'importanza dei diritti e degli interessi coinvolti ed il rilevante numero di ricorsi e segnalazioni pervenute ha indotto il Garante a svolgere un'approfondita istruttoria e ad adottare in data 31 luglio 2002 anche un provvedimento di carattere generale su tale tema (sul punto vedi il paragrafo 33).

Modalità del rilascio del consenso informato da parte dell'interessato, tempi di conservazione dei dati riferiti allo svolgimento dei rapporti di finanziamento negli archivi delle "centrali rischi", posizione dei soggetti che rivestono il ruolo di garanti di finanziamenti erogati a terzi sono solo alcuni degli aspetti in ordine ai quali il Garante, nelle motivazioni delle decisioni sui ricorsi, è più volte intervenuto in riferimento ai fondamentali principi di esattezza, aggiornamento, completezza e proporzionalità nel trattamento dei dati di cui all'art. 9 della legge n. 675. Tutti principi che nel citato provvedimento del 31 luglio 2002 hanno trovato un più sistematico tracciamento.

Dati relativi allo stato di salute e dati conservati nelle perizie medico legali redatte in campo assicurativo

In diverse occasioni il Garante si è pronunciato su richieste di accesso a dati di questo tipo, normalmente con riferimento a informazioni contenute in cartelle cliniche o riferite ad accertamenti diagnostici. In qualche caso (vedi ad esempio decisione del 30 settembre 2002) è stato nuovamente precisato che i dati, oltre che in modo esatto e completo, devono essere anche messi a disposizione in forma intelligibile. In tali ipotesi il titolare del trattamento deve trascrivere il contenuto dei referti diagnostici non comprensibili e rendere intelligibili i risultati di esami ed altri accertamenti eventualmente espressi attraverso codici o altri riferimenti di non immediata comprensibilità. Si tratta, anche in questo caso, di prescrizioni che mirano a rendere effettiva la piena conoscenza dei dati personali dell'interessato che, nel campo dei dati riferiti allo stato di salute, trova un'ulteriore tutela nella disposizione dell'art. 23, comma 2, della citata legge n. 675/1996 (per il quale, come si è detto, tali dati possono essere resi noti all'interessato stesso solo per il tramite di un medico).

Fra i dati relativi allo stato di salute rientrano anche quelli contenuti nelle perizie medico legali redatte in ambito assicurativo. È questo un tema sempre vivo e per alcuni aspetti controverso, anche se i principi più volte fissati al riguardo dal Garante (vedi Relazioni degli anni precedenti) sembrano ora meglio conosciuti dagli interessati e dagli operatori del settore. Ciò sia in riferimento alla possibilità di esercitare al riguardo il diritto di accesso previsto dall'art. 13 della legge n. 675, sia in ordine alla possibilità per i titolari del trattamento di eccepire, in caso di pregiudizio, il differimento del diritto stesso ai sensi dell'art. 14, comma 1, lettera e), della legge n. 675.

Trattamento di dati da parte di operatori telefonici e problematiche relative ai trattamenti in rete

È il settore che ha registrato nel corso del 2002 il più alto numero di ricorsi pervenuti, a dimostrazione di una sensibilità diffusa fra gli interessati, ma anche della necessità di un chiarimento da parte dell'Autorità in ordine al quadro normativo di riferimento.

Si inseriscono in quest'ambito i molti provvedimenti di accoglimento di ricorsi proposti con riguardo all'invio di messaggi di posta elettronica aventi contenuto promozionale e pubblicitario, senza che risultasse acquisito il previo consenso dell'interessato od operante uno dei presupposti del trattamento di cui all'art. 12 della legge n. 675/1996, all'art. 10 del d.lg. 13 maggio 1998 n. 171 (in materia di tutela della vita privata nel settore delle telecomunicazioni) all'art. 10 del d.lg. 22 maggio 1999, n. 185 in materia di contratti a distanza.

Con tali provvedimenti il Garante ha in particolare ribadito l'illiceità della raccolta (a volte effettuata anche con l'ausilio di particolari *software*) di indirizzi di posta elettronica reperiti in rete in assenza dei requisiti di legge sopra citati.

Ugualmente illecito è risultato poi il trattamento svolto anche da singoli utenti della rete che inviano a terzi messaggi e-*mail* contenenti l'invito ad inserirsi in un meccanismo per l'invio sistematico di messaggi di posta elettronica al fine di conseguire benefici economici.

In tale ipotesi (il caso più diffuso ha riguardato l'invio di *e-mail* collegate al sistema "*Mlm*") il trattamento ricade nell'ambito di applicazione della legge n. 675. Infatti lo stesso attiva, per sua natura, una comunicazione sistematica di dati personali a scopo di possibile lucro e, pur vedendo coinvolte persone fisiche, anziché imprese, non può essere qualificato alla stregua di un trattamento a "fini esclusivamente personali" ai sensi dell'art. 3 della legge n. 675/1996 (vedi, fra gli altri, provvedimento del 21 novembre 2002).

Per quanto concerne poi il trattamento di dati svolto da società telefoniche, vanno segnalati alcuni ricorsi che hanno portato all'attenzione dell'Autorità illeciti trattamenti di dati svolti da rivenditori autorizzati attraverso l'attivazione di schede telefoniche o di altri servizi, associati al nome di interessati ignari ed estranei al reale utilizzo del servizio in questione o, addirittura, defunti. Sul grave fenomeno è stata richiamata l'attenzione dei gestori dei servizi e si è proceduto anche ad ulteriori accertamenti attraverso interventi ispettivi e successive denunce di reato all'autorità giudiziaria.

Alcuni ricorsi hanno riguardato poi il problema del diritto di accesso ai dati personali relativi al traffico telefonico "in entrata". Al riguardo il Garante ha richiamato il disposto dell'art. 14, comma 1, lettera *e) bis*, della legge n. 675, che esclude l'esercizio del diritto di accesso a tali particolari tipi di dati *"salvo che possa derivarne pregiudizio per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n. 397"*. Nell'esame delle singole fattispecie (vedi ad esempio provvedimento del 16 ottobre 2002) l'Autorità ha verificato in concreto l'effettiva esistenza degli specifici presupposti richiesti dalla norma citata, per consentire, in via di eccezione, l'accesso da parte dell'interessato. Nei casi finora esaminati tali presupposti non ricorrevano e pertanto le richieste di accesso a tali dati sono state rigettate.

Dati relativi ai dipendenti

Si tratta di una problematica ricorrente in quanto logicamente connessa allo svolgimento del rapporto di lavoro, spesso propedeutica o contestuale alla proposizione di ulteriori istanze dinanzi al giudice ordinario. I casi sottoposti all'esame del Garante hanno generalmente riguardato problemi relativi al completo accesso dell'interessato ai dati personali relativi alla propria esperienza professionale, anche con riguardo alla eventuale formulazione di schede di valutazione, note caratteristiche, ecc. In due significativi provvedimenti del 30 settembre 2002 è stata sottolineata la possibilità di accedere altresì a informazioni personali conservate in documenti sottratti al diritto di accesso agli atti e documenti amministrativi tutelato dalla legge n. 241/1990 (nel caso di specie si trattava di procedimenti di tipo disciplinare), rimarcando l'autonoma disciplina che regola diversamente il diritto di accesso ai dati personali dell'interessato rispetto al diritto tutelato dalla citata legge n. 241.

Trattamenti svolti da pubbliche amministrazioni

Sono numerosi i casi di richieste rivolte ai sensi dell'art. 13 nei confronti di pubbliche amministrazioni. Quasi sempre gli interessati chiedono di accedere a complessi più o meno ampi di dati, spesso accompagnando tale richiesta con ulteriori istanze volte ad ottenere l'integrazione o l'aggiornamento dei dati o ad opporsi all'ulteriore utilizzo dei dati stessi sulla base di asserite violazioni di legge compiute dal titolare del trattamento (vedi ad esempio provvedimento del 25 novembre 2002 relativo ad istanze formulate nei confronti dell'INPS).

Un caso significativo ha riguardato una richiesta di aggiornamento dei dati personali di un interessato proposta ai sensi dell'art. 13 nei confronti dell'Automobile Club d'Italia in qualità di conservatore del Pubblico registro automobilistico (PRA). In tale occasione il Garante ha ritenuto infondato il ricorso (vedi provvedimento dell'8 novembre 2002), in quanto l'operazione di trattamento richiesta risulta specificamente disciplinata da apposita disposizione normativa non abrogata dalla legge n. 675. Tale disposizione subordina la modifica dei dati personali in questione (nel caso di specie il cambio del nome dell'interessato) ad una specifica procedura (che prevede altresì il versamento di somme a titolo di imposte e diritti di segreteria) la quale non può essere aggirata invocando in altra sede, ovvero sul piano del trattamento dei dati, la gratuità di alcuni diritti previsti dall'art. 13 della legge n. 675/1996.

Con tre provvedimenti adottati in data 30 dicembre 2002 e 9 gennaio 2003 il Garante ha poi esaminato, in relazione ad altrettante istanze di opposizione al trattamento, il sistema di videosorveglianza recentemente attivato nel centro storico della città di Brescia. Al riguardo, dai pochi atti acquisiti, non risultava accertato che i trattamenti in questione eccedessero i limiti richiamati dal provvedimento di carattere generale in materia di videosorveglianza del 29 novembre 2000. L'Autorità ha pertanto deciso di verificare nell'ambito di un autonomo procedimento l'idoneità e la completezza dell'informativa rilasciata ai sensi dell'art. 10 e le più specifiche modalità di funzionamento del sistema di videosorveglianza in questione, con particolare riguardo al rispetto del principio di proporzionalità e alla non eccedenza dei tempi di conservazione dei dati personali raccolti.

In altro ambito, con provvedimento del 6 settembre 2002, il Garante ha poi ritenuto infondata la richiesta degli interessati volta ad ottenere la cancellazione totale dai registri immobiliari di iscrizioni ipotecarie a suo tempo apposte. Al riguardo, l'Autorità ha confermato la legittimità dei trattamenti svolti da un ufficio provinciale dell'Agenzia del territorio che aveva negato la cancellazione dei dati richiesti dagli interessati ai sensi dell'art. 13 della legge n. 675 rilevando, nel caso di specie, le specifiche disposizioni del codice civile che regolano le modalità di tenuta dei registri immobiliari e le formalità per la cancellazione delle ipoteche.

Trattamenti svolti in ambito bancario

È un settore dove la legge sulla protezione dei dati personali ha trovato ampia applicazione. Nel periodo più recente l'Autorità ha avuto modo di affrontare, decidendo su alcuni ricorsi profili specifici di particolare rilievo. Con la decisione del 3 aprile 2002 è stato affermato il diritto di un erede testamentario ad accedere ad informazioni relative ai rapporti bancari precedentemente intrattenuti dal defunto, anche con riferimento ad alcuni dati, sempre relativi a rapporti bancari, riferiti a terzi. Ciò in quanto, nel caso di specie, alcune informazioni relative ai contestatari che avevano effettuato operazioni rilevanti nel comune rapporto erano indispensabili per rendere intelligibili i dati del richiedente.

In un altro caso, deciso in data 8 novembre 2002, è stato accolto un ricorso in riferimento alla richiesta di rettifica dei dati personali dell'interessato comunicati da un istituto di credito ad una società di emissione di carte di credito. Ciò in relazione ad una complessa controversia in atto fra l'interessato e la banca, vicenda che non legittimava, però, quest'ultima a comunicare a terzi la posizione dell'interessato indicando lo stesso come "insolvente" senza dare correttamente conto del contenzioso in essere.

Trattamenti svolti da professionisti e da investigatori privati

I trattamenti svolti da avvocati nell'esercizio del mandato difensivo o da investigatori privati sono stati al centro di alcune significative pronunce che hanno messo in luce il complesso rapporto fra legittimo esercizio del diritto di difesa e tutela della riservatezza. Vanno in particolare ricordate due pronunce (entrambe del 17 settembre 2002) che hanno in parte accolto due ricorsi con i quali gli interessati avevano chiesto di conoscere l'origine dei dati personali

che li riguardano, oggetto di trattamento da parte dei legali di controparte nell'ambito dei complessi contenziosi in essere. In entrambe le situazioni (diverse fra loro) non sono stati rappresentati elementi idonei volti a far ritenere che dalla rivelazione dell'origine dei dati potesse derivarne un concreto pregiudizio per l'esercizio di un diritto in sede giudiziaria. Per quanto concerne gli investigatori privati, gli spazi per l'esercizio della relativa attività e i limiti che la stessa incontra sono stati precisati in alcuni provvedimenti (vedi, ad esempio, quello del 30 settembre 2002) che hanno ribadito le specifiche prescrizioni fissate al riguardo dall'autorizzazione generale n. 6/2000.

Trattamenti in ambito giornalistico

La diffusa sensibilità degli interessati fatti oggetto di cronache giornalistiche ha portato all'attenzione dell'Autorità diverse vicende nelle quali, attraverso gli strumenti di tutela propri della legge n. 675, gli stessi hanno proposto istanze volte a conoscere l'origine dei dati che li riguardano, ad opporsi al loro ulteriore trattamento e, più in generale, a denunciare l'asserita violazione dei limiti posti al diritto di cronaca in relazione alla tutela della riservatezza personale (limiti enunciati nell'art. 25 della legge n. 675 e specificati nel relativo codice deontologico pubblicato sulla Gazzetta Ufficiale del 3 agosto 1998). Come in passato, le vicende portate all'attenzione dell'Autorità hanno riguardato sia trattamenti svolti a mezzo di pubblicazioni a stampa, sia trasmissioni radio-televisive.

Quanto agli specifici diritti fatti valere si segnala in particolare la pronuncia dell'11 luglio 2002 con la quale il Garante -nell'accogliere parzialmente un ricorso proposto nei confronti di alcune testate giornalistiche in relazione ad alcuni articoli di cronaca che fornivano numerosi dettagli sugli interessati- ha messo in luce il mancato rispetto dei principi dell'essenzialità rispetto a fatti di interesse pubblico, con particolare riferimento alla pubblicazione delle generalità complete dei ricorrenti e del loro domicilio che, nel caso di specie, non erano indispensabili ai fini dell'intelligibilità e dell'efficacia informativa della notizia.

Significativa è stata anche la decisione del 19 dicembre 2002 con la quale il Garante, accogliendo un ricorso proposto in via d'urgenza da un'associazione costituita per tutelare i diritti delle vittime del terremoto verificatosi il 31 ottobre 2002 a San Giuliano di Puglia, ha riconosciuto l'illiceità dell'acquisizione e della successiva pubblicazione delle immagini dei bambini deceduti nel crollo della scuola del paese, immagini che risultavano raccolte, senza il consenso dei genitori, presso le tombe ove le quali le famiglie le avevano esposte, tra l'altro in modo ancora provvisorio.

Con decisione del 31 luglio 2002 è stato poi precisato che anche il trattamento di dati personali svolto tramite un sito *Internet* rientra nella sfera di applicazione della legge n. 675/1996 e ricade nella fattispecie disciplinata dall'art. 25, comma 4 *bis*, della medesima legge.

63 Profili procedurali, impugnazione dei provvedimenti dell'Autorità

Messi a fuoco negli anni scorsi i principali problemi interpretativi connessi alle disposizioni procedurali in materia di ricorsi di cui al d.P.R. n. 501/1998, sono emersi nel periodo più recente profili nuovi e specifici sui quali il Garante nel corso del 2002 ha preso posizione con interventi significativi.

Con decisione del 4 luglio 2002 l'Autorità ha dichiarato inammissibile un ricorso munito di sottoscrizione non autenticata apposta da una persona che risultava iscritta nel registro speciale dei laureati in giurisprudenza che svolgono pratica nei termini previsti dal r.d.l. n. 1578 del 1933.

Al riguardo è stata sottolineata la necessità, ai sensi dell'art. 18, comma 1, del citato d.P.R. n. 501/1998, che il ricorso rechi la sottoscrizione del ricorrente o del procuratore speciale autenticata nelle forma di legge o che, ai sensi del comma 2 del medesimo articolo, la sottoscrizione sia apposta presso l'Ufficio *"da un procuratore speciale iscritto all'albo degli avvocati e al quale la procura sia stata conferita ai sensi dell'art. 83 del codice di procedura civile"*.

Con la decisione adottata il 22 ottobre 2002 è stato poi ricordato che, ai sensi dell'art. 17 del d.P.R. n. 501/1998 la persona che agisce su incarico dell'interessato -in sede di esercizio dei diritti di cui all'art. 13 della legge n. 675- deve esibire o allegare copia della procura o della delega recante sottoscrizione autenticata nelle forme di legge.

Nel caso di specie non risultava che, all'epoca della proposizione dell'istanza *ex* art. 13, tali atti fossero stati allegati, né, pur in presenza di specifica istanza del resistente, tale delega o procura anteriore all'istanza medesima era stata prodotta in atti con il ricorso o durante il procedimento.

Anche nel corso del 2002 è stato molto contenuto il numero delle decisioni dell'Autorità che sono state oggetto di opposizione in tribunale secondo la procedura delineata dai commi 6 e 7 dell'art. 29 della legge n. 675. In proposito va ricordata la sentenza n. 7341/2002 della prima sezione civile della Corte di cassazione. Con tale pronuncia la Suprema Corte -sciogliendo autorevolmente un dubbio che aveva dato luogo a contrastanti decisioni a livello di merito- ha precisato che *"il ricorso al giudice ordinario in opposizione al provvedimento del Garante non può essere inteso che come primo rimedio giurisdizionale a disposizione del soggetto che si pretende leso dall'atto del Garante"*. Pertanto l'Autorità può partecipare al giudizio di impugnativa di un proprio atto quale che sia stato il procedimento che lo ha preceduto per far valere davanti al giudice lo stesso interesse pubblico a tutela del quale l'Autorità agisce. Coerentemente con questa impostazione l'Autorità si è costituita in giudizio a difesa dei provvedimenti oggetto di opposizione in tribunale mirando sempre alla corretta interpretazione della legge sulla protezione dei dati personali e sottolineando altresì la valenza generale di molti dei problemi oggetto dei giudizi in questione.

Vanno altresì rimarcate due decisioni, adottate a seguito di opposizioni in tribunale, con le quali sono stati confermati precedenti provvedimenti del Garante adottati in relazione a ricorsi proposti ai sensi dell'art. 29 della legge n. 675/1996.

In particolare con decreto del 2 luglio 2002 il Tribunale di Bologna -in relazione alla richiesta di accesso al complesso dei dati personali proposta da un dipendente nei confronti del proprio datore di lavoro- ha confermato la precedente decisione del Garante specificando che i dati devono essere messi a disposizione in modo completo e intelligibile mediante estrapolazione degli stessi dai supporti sia cartacei sia informatizzati nei quali gli stessi sono conservati, *"o mediante consegna di copia integrale dei dati stessi"*. Nella stessa decisione il tribunale ha poi concluso nel senso che anche i giudizi valutativi riferiti ai dipendenti costituiscono dati personali agli stessi riferiti.

Con decisione del 31 luglio 2002 il Tribunale di Bergamo ha invece confermato tre decisioni del Garante del 19 febbraio 2002 che avevano affrontato ambiti e limiti dell'attività svolta dagli investigatori privati (sul punto v. *Relazione 2001*, pp. 58 e 101 e il paragrafo 30 della presente *Relazione*).

Attività ispettive e applicazioni di sanzioni amministrative

64 Tipologia degli accertamenti ispettivi e criteri adottati

Tra i compiti del Garante previsti dall'art. 31 della legge 31 dicembre 1996, n. 675, vi è anche quello di controllare se i trattamenti sono effettuati nel rispetto delle norme di legge e di regolamento e in conformità alla notificazione.

A questa attività provvede in particolare il Dipartimento vigilanza e controllo il cui personale riveste, nell'esercizio dei poteri di accertamento previsti dalla legge, la qualifica di ufficiale/agente di polizia giudiziaria.

Le *attività ispettive* sono costituite da accertamenti effettuati, direttamente dall'Ufficio ovvero, su suo incarico da altri organi dello Stato, nei luoghi dove si svolgono i trattamenti utilizzando i poteri previsti dall'art. 32 della legge 31 dicembre 1996, n. 675.

La scelta dello strumento potestativo da utilizzare per l'esercizio dell'attività di controllo, continua ad essere informata a principi di *proporzionalità, adeguatezza e gradualità*, tenendo presente, di volta in volta, il contesto operativo di riferimento (rischio di dispersione o alterazione degli elementi di prova) ed il profilo soggettivo del controllato in termini di collaborativitá.

I controlli possono essere pertanto effettuati mediante: richieste, anche *in loco*, di informazioni ed esibizioni di documenti; 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.

Le richieste di informazioni *in loco* vengono effettuate sulla base del disposto dell'art. 32, comma 1, della legge, hanno natura collaborativa e si svolgono con la presenza di funzionari 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 sia quando sono necessarie descrizioni analitiche alle quali titolare e responsabile potrebbero avere difficoltà a rispondere in modo esaustivo, sia quando è necessario effettuare controlli incrociati rispetto a trattamenti di dati personali cui siano interessati più titolari. Considerata la natura "collaborativa" di queste attività esse vengono di regola effettuate mediante preavviso.

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"*. I funzionari incaricati possono pertanto procedere a rilievi e ad operazioni tecniche e possono estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Questi tipi di controlli sono di regola disposti quando, per acquisire gli elementi

necessari per la compiuta definizione del contesto, non è ritenuto opportuno procedere alla richiesta di informazioni o di esibizione di documenti, ovvero nei casi in cui non sono pervenute le informazioni o i documenti richiesti o, se pervenuti, sono ritenuti incompleti o non veritieri. A differenza del potere di cui al comma 1 dell'art. 32 della legge, quella prevista dal comma 2 del medesimo articolo è una potestà di tipo marcatamente inquisitoria ed *"i soggetti interessati agli accertamenti sono tenuti a farli eseguire"* (art. 32, comma 4 della legge 31 dicembre 1996, n. 675). L'accertamento, come previsto dall'art. 15, comma 5 del d.P.R. 31 marzo 1998, n. 501, è eseguito anche in caso di rifiuto e le spese in tal caso occorrenti sono poste a carico del titolare. Durante l'accertamento il titolare o il responsabile possono farsi assistere da persone di loro fiducia. Dell'accesso è redatto sommario processo verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

L'esercizio del potere di accesso di cui all'art. 32, comma 2, è subordinato dalla legge alla previa autorizzazione del presidente del tribunale territorialmente competente (art. 32, comma 3, della legge), ma è esercitato anche in assenza di tale autorizzazione, qualora sia acquisito il preventivo assenso scritto e informato dei titolari o dei responsabili dei trattamenti (art. 15, comma 1, d.P.R. n. 501/1998).

Le ispezioni sono collegate a procedimenti amministrativi di controllo al termine dei quali l'Autorità:

- segnala, ai titolari o responsabili del trattamento dei dati, le modificazioni *necessarie o opportune* al fine di rendere il trattamento conforme alle disposizioni vigenti;
- contesta le sanzioni amministrative eventualmente rilevate;
- invia, nei casi più gravi previsti dalla legge, una comunicazione di notizia di reato all'autorità giudiziaria per l'accertamento delle violazioni costituenti reato.

65 La collaborazione con organi dello Stato. Il protocollo d'intesa con la Guardia di finanza

Nello svolgimento dell'attività ispettiva il Garante può avvalersi, ove necessario, della collaborazione di altri organi dello Stato e di fatto già da tempo si sono avute molteplici occasioni di collaborazione con le forze di polizia ed in particolare con la Guardia di finanza, (in ragione delle peculiari competenze nel campo delle attività di controllo in campo amministrativo proprie del Corpo) e con la con la Polizia postale e delle comunicazioni, (per quanto riguarda attività in ambito telematico).

Nell'ottica del potenziamento dell'attività di vigilanza e controllo pertanto, il 26 ottobre 2002 il Garante e la Guardia di finanza hanno siglato un protocollo d'intesa attraverso il quale è stata potenziata l'attività di collaborazione tra le due istituzioni.

Il protocollo prevede che la Guardia di finanza collabori alle attività ispettive del Garante in particolare attraverso:

- il reperimento di dati e informazioni sui soggetti da controllare;
- la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- l'assistenza nei rapporti con l'autorità giudiziaria;
- lo sviluppo di attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale e amministrativa;
- l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori.

Il reparto competente a ricevere le richieste di collaborazione è il Comando unità speciali con sede a Roma il quale, in ragione della natura della richiesta, può procedere direttamente o interessare i reparti del Corpo territorialmente competenti.

Successivamente al perfezionamento del protocollo di intesa, nel mese di gennaio del 2003, è stata effettuata un'intensa attività di formazione del personale del Corpo destinato a svolgere in via continuativa l'attività di collaborazione (venti unità circa tra ufficiali, ispettori e sovrintendenti). La formazione ha riguardato tutti i principali campi di applicazione della legge ed è stata concepita per consentire, sin da subito, nonostante l'elevato grado di tecnicismo che caratterizza la materia della tutela dei dati personali, il più efficace impiego delle risorse nelle attività ispettive ed agevolare le sinergie informative tra il Garante ed il Corpo.

La collaborazione con la Guardia di finanza si è dimostrata immediatamente proficua sia nella fase preparatoria degli interventi più delicati, grazie alle capacità investigative proprie del Corpo, sia nella fase esecutiva con l'esecuzione, pure in un arco limitato di tempo, di 8 interventi di cui 4 in collaborazione.

Proficua è stata anche la collaborazione avviata con la Polizia postale, per quanto riguarda gli accertamenti effettuati nei confronti di titolari di trattamenti di dati personali che utilizzano *Internet* come dimostra la prima operazione, effettuata nel mese di luglio del 2002, in cui si è proceduto alla notifica di provvedimenti di blocco del trattamento dei dati personali contenuti nei *data-base* di sette società responsabili di *"spamming"* (pratica di inviare via *e-mail* informazioni pubblicitarie e commerciali indesiderate utilizzando indirizzi di posta elettronica senza il consenso degli interessati).

Assai significative sono risultate anche le collaborazioni e i flussi informativi ricevuti dall'Arma dei carabinieri.

La collaborazione con le forze di polizia, che sarà ulteriormente intensificata nel prossimo anno, ha così costituito un importante elemento di rafforzamento dell'efficacia dell'azione di tutela dei diritti dei cittadini che passa anche attraverso una più intensa attività di vigilanza e controllo.

66 La programmazione delle ispezioni e i risultati

L'attività ispettiva effettuata nel periodo di riferimento è stata pari a 40 controlli effettuati nei confronti di soggetti pubblici (9) e privati (31) ed è stata effettuata con i poteri previsti dall'art. 32, comma 2, in 5 casi e con quelli di cui al 32, comma 1, nei restanti 35 casi.

Le ispezioni hanno riguardato:

- il riscontro di segnalazioni pervenute all'Ufficio (17 controlli);
- autonomi accertamenti a seguito di ricorsi presentati al Garante sulla base dell'art. 29 della legge (12 controlli);
- il riscontro dell'avvenuto adempimento di deliberazioni del Garante in seguito a ricorsi ex art. 29 della legge (1 controllo);
- l'esecuzione di due *indagini conoscitive*, per verificare lo stato di attuazione della legge, con riferimento all'utilizzazione di impianti di video sorveglianza (5 controlli) e ai trattamenti di dati personali sensibili da parte dei comuni (5 controlli). Per quanto riguarda i controlli effettuati nell'ambito di queste indagini i soggetti controllati sono stati individuati tramite segnalazioni ricevute dall'Ufficio oppure, come nel caso dei comuni, 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).

Il complesso di attività sopra descritto ha comportato l'avvio di diversi procedimenti amministrativi di controllo, alcuni dei quali ancora in corso, nei confronti dei soggetti ispezionati, con l'applicazione di numerose sanzioni amministrative, di due provvedimenti di blocco del trattamento di dati personali, nonché, in cinque casi, l'invio di segnalazioni all'autorità giudiziaria per le valutazioni in ordine alla sussistenza di violazioni costituenti reato relativamente alle ipotesi previste dall'art. 35, trattamento illecito di dati personali, dall'art. 36, omessa adozione di misure di sicurezza e dall'art. 37, inosservanza dei provvedimenti del Garante.

Tra le attività più significative realizzate si evidenzia quella che ha consentito di accertare l'illecito trattamento di dati personali effettuato da una società concessionaria del marchio relativo ai servizi di una *"veggente"* che adottava il sistema dell'acquisizione di dati personali attraverso la pubblicazione di *coupon*, privi di qualsiasi informativa e di richiesta di consenso, su giornali a grande diffusione.

L'ingente quantità di dati personali illegittimamente acquisita era stata poi oggetto di cessione all'estero nei confronti di società operanti anche al di fuori dell'Unione europea. Al riguardo il Garante oltre a disporre il blocco dei trattamenti dei dati illecitamente acquisiti, ha trasmesso copia del provvedimento anche all'omologa autorità australiana e tedesca, oltre che alla *Federal trade commission* degli Stati Uniti, per le iniziative di competenza nei confronti delle società cessionarie.

67 L'attività sanzionatoria del Garante

Nella precedente Relazione erano state evidenziate, per quanto attiene alla potestà sanzionatoria del Garante, le principali modifiche apportate all'impianto della normativa sulla protezione dei dati personali dal decreto legislativo del 28 dicembre 2001, n. 467 (v. *Relazione 2001*, p. 107).

L'attività operativa effettuata in materia di sanzioni amministrative nel corso del 2002 è stata caratterizzata da un utilizzo di tale strumento più incisivo ed esteso.

Le attività di controllo e le indagini conoscitive effettuate d'ufficio, le segnalazioni inviate dagli interessati, i riscontri effettuati nell'ambito delle procedure attinenti ai ricorsi *ex* art. 29 della legge, hanno portato all'applicazione di alcune decine di sanzioni amministrative (per le quali per completezza si rimanda al prospetto analitico contenuto nel paragrafo "Dati statistici" della presente *Relazione*) nei confronti di altrettanti titolari del trattamento.

Esaminando nel dettaglio gli articoli di legge assistiti dalla previsione di una sanzione amministrativa -e per i quali è stata predisposta la preliminare contestazione- il più ricorrente è stato sicuramente quello che riguarda l'obbligo di fornire le preventive, necessarie, idonee informazioni all'interessato (art. 10, l. n. 675/1996) in ordine al quale sono stati emessi e notificate ventotto contestazioni a seguito di procedimenti di controllo avviati nei confronti di titolari del trattamento a seguito sia di segnalazioni inviate da interessati, sia all'esito di attività ispettive o indagini conoscitive promosse d'ufficio dal Garante.

A seguire, l'inadempimento a richieste di informazioni formulate dall'Ufficio (art. 32, comma 1, della medesima legge) è stato oggetto di tredici contestazioni mentre, per quanto concerne la comunicazione di dati attinenti allo stato di salute (art. 23, comma 2, l. cit.), a seguito della conclusione di due procedimenti ex art. 29 della legge, è stato accertato un trattamento effettuato in modo difforme dalla previsione normativa e, di conseguenza, si è proceduto alla contestazione della violazione medesima.

Infine, a seguito di due procedimenti amministrativi di controllo effettuati in conseguenza di una segnalazione e di un accertamento ispettivo, in materia di videosorveglianza, sono stati redatti due verbali di contestazione per notificazione incompleta (art. 34, l. cit) essendosi accertato, all'esito della verifica presso il registro generale dei trattamenti sulla notificazione inviata all'Ufficio ai sensi dell'art. 7 della legge, che il titolare aveva omesso di indicare tra le modalità di trattamento quella realizzata per mezzo appunto di sistemi di videosorveglianza.

Più contenuto rispetto alle contestazioni è stato il numero dei provvedimenti motivati di ordinanza-ingiunzione pagamento adottati (ai sensi dell'art. 18 della legge n. 689/1981), con deliberazione dell'Autorità. Anche questo dato può essere considerato particolarmente indicativo dell'atteggiamento dei titolari che, nella stragrande maggioranza dei casi, una volta fatti

oggetto di preliminare accertamento e contestazione da parte dell'Ufficio, hanno preferito avvalersi della facoltà di effettuare il pagamento in misura ridotta e conseguentemente rendere conforme alle disposizioni di legge e di regolamento il trattamento di dati personali effettuato nell'ambito delle loro attività istituzionali.

Al riguardo, in occasione di controlli amministrativi effettuati nell'ambito di proprie attività istituzionali, altri organi dello Stato (Carabinieri, Guardia di finanza e Polizia di Stato), hanno preliminarmente rilevato e provveduto a contestare ai trasgressori violazioni della normativa sulla protezione dei dati personali, inviando all'Autorità il rapporto (ai sensi dell'art. 17 della legge n. 689/1981) necessario all'adozione del provvedimento di ordinanza-ingiunzione. In ordine a ciò preme sottolineare il maggiore livello qualitativo delle attività poste in essere in materia dagli organi sopra citati, che testimonia l'attenzione e la sensibilità istituzionale posta riguardo alla normativa sulla protezione dei dati personali.

Con riguardo alle risultanze di detta attività, a prescindere dai procedimenti che sono in corso a quelli attivati nei primi mesi del 2003, si rileva che i trasgressori destinatari delle contestazioni, in oltre il settanta per cento dei casi, si sono avvalsi della facoltà di effettuare il pagamento in misura ridotta (art. 16 della legge n. 689/1981). L'ammontare delle somme pagate a titolo di contestazioni di sanzioni amministrative nell'anno 2002 è pari a € 73.336,94.

Per quanto riguarda i provvedimenti di ordinanza-ingiunzione adottati, si rileva che in un solo caso è stata proposta un'infondata impugnazione (ai sensi dell'art. 22-*bis* della legge n. 689/1981) innanzi ad un giudice di pace che si è all'esito dichiarato incompetente per territorio. L'Autorità, presentando memoria di costituzione ha esercitato la facoltà di stare in giudizio personalmente ai sensi dell'art. 23 della citata legge.

Per quanto attiene invece gli altri provvedimenti di ordinanza-ingiunzione, che non sono stati impugnati, si sta predisponendo quanto necessario per il recupero forzato delle somme ai sensi dell'art. 27 della legge n. 689/1981.

Attività di informazione e comunicazione

68 Profili generali

In linea con l'obiettivo di promuovere una sempre più estesa cultura del rispetto e di rendere, al contempo, quanto più trasparente l'attività svolta, l'Autorità ha mantenuto un elevato livello di produzione di informazione, fornendo a cittadini, imprese, istituzioni un costante flusso di informazioni riguardo alle tematiche sulle quali si incentra l'azione del Garante (prime fra tutte, la salvaguardia della libertà e della dignità della persona, la gestione trasparente delle banche dati, l'uso non discriminatorio delle informazioni personali, specie di quelle più delicate) e gli strumenti attuativi delle norme.

Particolare significato ha assunto l'impegno costante dell'Autorità volto alla definizione di regole e cautele per l'utilizzo sempre più diffuso delle tecnologie di sorveglianza e dei nuovi sistemi di comunicazione, sia da parte di privati cittadini, sia da parte di imprese e pubbliche amministrazioni, così come l'attenzione posta ai rischi che possono derivare per la liberà delle persone dalle indagini genetiche, dalla raccolta dei dati *on line,* dalla localizzazione.

La ricerca di un corretto ed equilibrato rapporto tra sicurezza collettiva e tutela della riservatezza dell'individuo, anzitutto alla luce dei cambiamenti sociali intervenuti dopo l'11 settembre, ha connotato anche nel 2002 l'azione dell'Autorità, sia in ambito nazionale, sia in sede internazionale.

Con l'obiettivo di "comunicare" la *privacy*, l'Autorità ha mantenuto la scelta di affidare la sua informazione ad un linguaggio rigoroso ed insieme attento ad una funzione divulgativa, teso a ricordare a pubbliche amministrazioni e mondo dell'impresa, da una parte gli obblighi imposti dalla legge n.675/1996 e, dall'altra, la necessità di considerare la *privacy* più una risorsa che un ostacolo allo sviluppo di un più proficuo e corretto rapporto con cittadini, utenti, consumatori.

Gli aspetti ai quali i *mass media* hanno dedicato più spazio sono stati quelli relativi alle violazioni della *privacy* in rete e nel settore delle telecomunicazioni (in particolare lo spamming) e alle tutele messe in campo dalla disciplina sulla protezione dei dati personali, ai rapporti tra diritto di cronaca e dignità delle persone, alla protezione dei minori sia *on line* che *off-line*, alla tutela dei consumatori (specie per il credito al consumo), ai *test* genetici, alla videosorveglianza, ai previsti codici deontologici (primo fra tutti quello per *Internet*).

Nel periodo dal gennaio 2002 al marzo 2003, sulla base della rassegna stampa prodotta dall'Ufficio, le pagine dedicate alle tematiche della *privacy* dai maggiori quotidiani e periodici nazionali sono state circa 5000, delle quali oltre 1900 (compresi quotidiani internazionali) dedicate specificamente all'attività del Garante. Le prime pagine dedicate ai temi della *privacy* sono state circa 750. Numerose sono state le interviste pubblicate sulla carta stampata, su tv e radio, nazionali e locali, e diverse su pubblicazioni *on line*.

La tipologia dei prodotti informativi è stata ampia e differenziata.

La *Newsletter* settimanale è al suo quarto anno di pubblicazione. Affiancando la comunicazione tradizionale, realizzata attraverso comunicati stampa, con un'informazione di tipo più ampio e approfondito, la *Newsletter* si è rivelata, oltre che uno strumento di comunicazione, 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 2002 e il 30 aprile 2003 sono state 60, mentre i comunicati stampa 46.

Nel 2002, è giunto alla sua settima edizione l'archivio digitale ipertestuale *"Cittadini e Società dell'informazione"*, che contiene in forma integrale e nell'originale veste editoriale, la documentazione relativa all'attività del Garante, alla normativa nazionale ed internazionale di riferimento, alle pubblicazioni realizzate. Il CD-Rom, che consente una consultazione con funzioni di ricerca *"full-text"*, è stato inviato gratuitamente in questa prima fase e rappresenta uno strumento ormai conosciuto e costantemente richiesto da parte di amministrazioni pubbliche, imprese, liberi professionisti e semplici cittadini. Le copie pubblicate sono state 8000. Le recenti edizioni presentano, oltre che una nuova impostazione grafica in linea con la corporate identity studiata appositamente per il Garante, anche miglioramenti tecnici che ne rendono ancora più funzionale l'uso e un "glossario" esplicativo delle voci principali e delle definizioni presenti nella l. n. 675/1996.

Tra le attività di comunicazione il *Bollettino* che ha raggiunto il numero 28 e raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa ed altra documentazione.

La necessità di sviluppare una quanto più diffusa conoscenza delle norme sulla *privacy* e dei diritti oggi riconosciuti ai cittadini, ha spinto l'Autorità a sviluppare sempre nuove modalità di informazione: oltre all'uso degli strumenti di comunicazione già realizzati -da quelle tradizionali (comunicati stampa, *newsletter*, conferenze stampa) a quelle multimediali ed interattive- l'Autorità ha dato vita ad un bimestrale, *"Garanteprivacy.it"*, destinato a personalità del mondo imprenditoriale ed istituzionale, caratterizzato da una comunicazione agile ed essenziale, in grado di sottolineare l'attività dell'Autorità nei diversi settori di intervento.

Inoltre, allo scopo di contribuire in maniera fattiva all'approfondimento dei temi legati alla *privacy* e ai principi posti dalla normativa nazionale e comunitaria, il Garante ha deciso di dar vita ad una collana di pubblicazioni che ospiteranno contributi dedicati di volta in volta ad un argomento legato alla propria attività. Sono in preparazione già alcuni volumi, tra i quali quello dedicato ai rapporti tra diritto di cronaca e tutela della riservatezza, ed un massimario relativo ai provvedimenti adottati dal Garante nel primo quadriennio di attività.

Un'attività di massimazione è stata avviata ed esplicata, in chiave tecnico-giuridica sebbene in forma non ufficiale, per i molti provvedimenti emessi nel corso degli anni, 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 arricchirà il panorama delle pubblicazioni e la cui edizione, anche su supporto informatico, è imminente, si indirizza in particolar modo ad una platea di utenti costituita da giuristi, operatori del diritto, ordini professionali, imprese, istituzioni pubbliche e private, fornendo un punto di riferimento anche per la consultazione del testo ufficiale e integrale delle decisioni.

Il rapporto diretto con la società riveste un'importanza fondamentale per l'Autorità che, fin dall'inizio della sua attività, ha inteso presentarsi come un'istituzione vicina ai cittadini, presidio dei nuovi diritti della persona, ed attenta alle nuove frontiere della protezione dei dati personali. La messa a disposizione sul sito di una notevole quantità di documentazione, con continui aggiornamenti in tempo reale, ha avuto, comunque, un parziale effetto deflattivo sul numero dei contatti telefonici giornalieri. In questo senso, il recente avvio dell'Urp ha consentito di offrire al pubblico, in collegamento con un *call center*, non solo un contributo di chiarificazione e supporto, ma anche 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.

L'impegno per una comunicazione efficace e quanto più capillare ha trovato concreta attuazione nella realizzazione della campagna di informazione istituzionale, attraverso la produzione di uno *spot* televisivo e radiofonico, trasmesso dalle tre reti Rai nel marzo 2003, e da altre emittenti televisivi nei mesi successivi, incentrato sul concetto di dato personale in quanto "valore" da proteggere e sul diritto attribuito al cittadino di decidere liberamente e consapevolmente la circolazione delle informazioni che lo riguardano.

Il progetto di comunicazione istituzionale, realizzato in proprio dall'Autorità, nasce dall'esigenza di realizzare una campagna di comunicazione istituzionale allo scopo di promuovere presso i cittadini la conoscenza dei nuovi diritti riconosciuti dalla normativa sulla *privacy*. Questo obiettivo rientra specificamente tra i compiti affidati al Garante dalla stessa l. n. 675/1996. La scelta del mezzo televisivo, in particolare, accoglie l'indicazione fornita da un'indagine, a suo tempo svolta dal Garante in collaborazione con una società specializzata, dalla quale era emerso che il grande pubblico privilegia nell'approccio alle problematiche della *privacy* il mezzo televisivo.

L' iniziativa pone le sue basi su una duplice esigenza: a) raggiungere, senza mediazione giornalistica e con un messaggio diretto, semplice ed incisivo, l'opinione pubblica; b) rendere chiare le novità, in termini di diritti e crescita sociale, della legge sulla protezione dei dati personali.

69 Seminari, convegni ed altre iniziative

L'attività dell'Autorità collegata ai seminari, convegni e altre iniziative ha visto, nel corso del 2002 e nei primi mesi del 2003, una serie di importanti occasioni di confronto e approfondimento. 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 con il proprio stand e con la partecipazione dei rappresentanti a dibattiti e convegni.

Il *Forum P.A.* edizione 2002, svoltosi a Roma dal 6 al 10 maggio, ha visto la partecipazione del vicepresidente Giuseppe Santaniello al convegno su "Lo sviluppo della società dell'informazione in Italia" e del Segretario generale, Giovanni Buttarelli, a quello dedicato a sicurezza e tutela della *privacy*. Lo stesso Buttarelli ha tenuto un corso di formazione per amministratori pubblici dedicato a protezione dei dati personali e pubblica amministrazione.

L'Autorità è stata anche presente al Com-P.A., Salone della comunicazione pubblica, svoltosi a Bologna dal 18 al 20 settembre 2002. Gaetano Rasi ha preso parte al dibattito su *"E-government: la nuova frontiera della P.A."*, mentre Mauro Paissan è intervenuto al convegno su *"Innovazione tecnologia e innovazione culturale nei new media:verso la e-society"*. Giovanni Buttarelli ha preso parte alla tavola rotonda su *"Carta di identità elettronica e firma digitale: dalla sperimentazione ai servizi"*.

Il *Com–P.A. 2002* ha offerto l'occasione per illustrare l'attività del Garante ed il suo ruolo nella realizzazione dell'*e-society*. Ha permesso, inoltre, di fare il punto sullo stato di attuazione della legge sulla protezione dei dati personali dopo introduzione del decreto legislativo 467/2001 e di affrontare alcune tematiche legate ai settori delle telecomunicazioni e di *Internet* a pochi mesi dall'entrata in vigore, il 31 luglio, della nuova direttiva 2002/58/CE sulla *privacy* nelle comunicazioni elettroniche.

Da sottolineare che al Garante per la protezione dei dati personali è stato assegnato dalla giuria del premio Diritto all'informazione, il Premio Qualità Com–P.A. 2002 "per gli interventi di promozione e diffusione del *valore privacy*". Il riconoscimento viene assegnato alle amministrazioni e alle aziende che nell'ambito del Salone di Bologna si distinguono per progetti e presentazioni di qualità nel campo dell'innovazione e della comunicazione pubblica. La cerimonia di premiazione si è svolta venerdì 20 settembre a conclusione dell'evento.

Nell'ambito di *Smau 2002*, svoltosi a Milano dal 24 al 28 ottobre, Mauro Paissan ha partecipato al convegno su *"Internet e il cittadino"*. La partecipazione a Smau ha consentito di affrontare le problematiche connesse alla protezione dei dati personali e ai nuovi diritti nella *e-society*.

Per quanto riguarda l'attività internazionale, va ricordata innanzitutto la partecipazione alla Conferenza di primavera delle Autorità europee per la *privacy*, svoltasi a Bonn il 25 e 26 aprile (v. par. 89). Per il Garante italiano erano presenti il presidente Stefano Rodotà, i componenti Gaetano Rasi e Mauro Paissan e il segretario generale Giovanni Buttarelli. La sessione d'apertura è stata dedicata alle conseguenze dei tragici eventi dell'11 settembre 2001: nuove norme sulla sicurezza e diritti dei cittadini alla protezione dei dati personali, un rapporto delicato. Altri temi trattati, le procedure di identificazione biometrica, la collaborazione con i paesi dell'Est: i programmi di informatizzazione della pubblica amministrazione, i processi di certificazione della politica della *privacy* di imprese e altri soggetti.

Sempre ad aprile si è svolta a S.Francisco la XII Conferenza internazionale su *"Computers, Freedom & Privacy"*. La *CFP Conference* rappresenta da tempo un appuntamento importante per la comunità degli studiosi e degli operatori della *privacy* di tutto il mondo. Per l'Autorità italiana ha partecipato quest'anno alla *CFP Conference* Gaetano Rasi. Riallacciandosi ai temi riguardanti i nuovi diritti e le nuove libertà nella rete, il ruolo dei consumatori, lo sviluppo del commercio elettronico, e il ritardo da parte di imprese e organizzazioni in generale nel costruire programmi di protezione dei dati personali, Rasi ha affermato come la *privacy* si caratterizza sempre di più come criterio di qualità per le imprese.

Dal 9 all'11 settembre del 2002 l'Autorità ha partecipato alla XXIV Conferenza internazionale delle Autorità garanti, svoltasi a *Cardiff* con oltre 25 Paesi provenienti dai diversi continenti per discutere su temi cruciali quali l'uso delle nuove tecnologie, l'*e-government* le misure per bilanciare la sicurezza sociale e *privacy*. Aprendo la sessione finale, Rodotà ha posto l'accento sul ruolo imprescindibile svolto dalle autorità indipendenti nell'assicurare la tutela dei diritti fondamentali in una realtà dominata dai rischi derivanti dal massiccio uso delle tecnologie dell'informazione e della comunicazione e dalla costruzione di grandi banche dati. L'Autorità era rappresentata dal presidente Stefano Rodotà, dai componenti Gaetano Rasi e Mauro Paissan e dal segretario generale, Giovanni Buttarelli.

Il vice presidente dell'Autorità, Giuseppe Santaniello, ha tenuto il 7 ottobre all'Istituto italiano di cultura di Berlino una conferenza dedicata al sistema di garanzie a tutela della *privacy* introdotto nel nostro Paese dalla legge n. 675 del 1996. L'iniziativa si inserisce nel ciclo di conferenze sulla tutela della riservatezza dei dati personali presso i più importanti istituti di cultura italiani all'estero (la precedente conferenza si era svolta a Madrid) e rientra nei compiti di promozione della conoscenza, presso i cittadini, delle norme sulla *privacy* che il Garante è chiamato a svolgere, ma che assume, come in questo caso, un particolare rilievo per i suoi aspetti culturali e sociali.

Nel marzo 2002, Stefano Rodotà ha guidato una delegazione formata da rappresentanti delle autorità di protezione dati europee in visita ufficiale a *Washington*. Scopo della visita era quello di favorire la cooperazione fra USA ed Europa anche alla luce dell'accordo di *Safe Harbor* ("porto sicuro"), raggiunto nel 2000, e di raccogliere informazioni e spunti per l'attività futura del Gruppo che riunisce tutte le autorità per la protezione dei dati personali nell'Ue ed è presieduto dallo stesso Rodotà. Della delegazione italiana hanno fatto parte anche il componente dell'Autorità, Mauro Paissan, e il segretario generale, Giovanni Buttarelli.

Tra i diversi convegni nazionali ai quali l'Autorità ha preso parte vanno ricordati il convegno su "Etica in *Internet*" (Roma, 28 febbraio 2003, al quale ha partecipato il Presidente Stefano Rodotà; il convegno organizzato dal Ministro dell'innovazione e le tecnologie "Chi ha paura della rete? Per un uso consapevole di *Internet*" (Roma, 29 maggio 2002) al quale ha partecipato Gaetano Rasi; il convegno organizzato dalla Federazione Nazionale della Stampa (Gubbio, 18 al 20 ottobre 2002), dedicato a "Il riassetto del sistema radiotelevisivo italiano. Pluralismo, concorrenza, incroci editoriali. Quale garanzia per l'informazione?", al quale ha partecipato Mauro Paissan.

Nel quadro dell'attenzione rivolta al mondo dei media, il Garante ha organizzato il 30 ottobre un incontro con tutti direttori della maggiori testate nazionali, della carta stampata della radio e delle televisioni, allo scopo di un confronto costruttivo sulle esigenze di rispetto delle persone poste al mondo dell'informazione dalle norme sulla tutela della riservatezza.

Il 5 e 6 dicembre 2002 si è tenuta, poi, a Roma, organizzata dal Garante, la Conferenza internazionale *"Privacy, Cost to Resource – Privacy, da costo a risorsa"*. La Conferenza ha rappresentato un'occasione di proficuo confronto relativamente all'impatto che le norme sulla *privacy* hanno avuto sul mondo delle imprese. Oltre 40 relazioni e più di 200 partecipanti (fra i quali molti esponenti del mondo imprenditoriale) hanno esaminato le opportunità che la tutela della *privacy* offre al settore economico. La Conferenza ha sottolineato che la protezione dei dati personali costituisce la chiave di volta per coniugare rispetto di diritti fondamentali e sviluppo economico attraverso un rapporto corretto fra imprese e cittadini.

70 Il nuovo sito *Internet* dell'Autorità

Il 24 marzo 2003 è stato messo *on line* il nuovo sito dell'Autorità all'indirizzo *www.garanteprivacy.it* o *www.dataprotection.org*. La precedente versione, essendo in corso il trasferimento della base dati documentale, è ancora consultabile all'indirizzo *www2.garanteprivacy.it*.

La presentazione del sito è coincisa con la messa in onda della prima campagna informativa istituzionale del Garante: lo *spot* televisivo e radiofonico "LA NOSTRA FIRMA, NON È UNA FIRMETTA!".

La filosofia progettuale del sito si fonda sulla radicale modifica dell'attuale modalità di navigazione e si caratterizza per la presenza di un diverso motore di ricerca e per i criteri di usabilità (anche in modalità "solo testo", con *browser* diversi anche non recenti e multi-piattaforma), non utilizzando immagini in movimento e *frame*.

L'uso di tali accorgimenti rende fruibili le informazioni del sito agli utenti ipovedenti e non vedenti.

Sino a ieri i provvedimenti erano suddivisi per tipologia di atto; oggi, grazie ad una più ampia marcatura tecnico-giuridica del documento ed all'adozione di uno schema di classificazione per materia, la navigazione "a vista" è intuitiva ed efficace. I provvedimenti sono presentati in ordine cronologico e visualizzati in una nuova finestra, accompagnati dalla consueta massima giornalistica, dal collegamento ipertestuale con documenti correlati, dall'indicazione bibliografica di pubblicazione nel Bollettino e dall'eventuale richiamo al comunicato stampa o *Newsletter*.

Il reperimento dei documenti è affidato ad una funzione di "ricerca semplice" per parole in modalità *full text*, attivabile direttamente dalla *Home Page*, mentre la ricerca avanzata presenta una maschera articolata che consente la ricerca attraverso l'incrocio di più canali che disegnano le caratteristiche specifiche della base dati: *full text* in *and/or/not* –anche circoscritta al solo titolo o alla massima–, per estremi di pubblicazione, secondo lo schema di classificazione per materia, per tipologia di atto, per range di data, oppure per numero di documento (*ID*).

Un'altra importante novità è rappresentata dall'assegnazione a ciascun documento di un *ID* numerico, univoco e permanente che ne renderà più agevole il reperimento e consentirà una piena adesione al progetto NormeinRete (*www.normeinrete.it*), punto di accesso unitario alla normativa italiana ed europea pubblicata nei siti web istituzionali.

Le funzionalità del motore di ricerca sono esaltate dalla presenza del *Thesaurus* giuridico che –sempre attivo nei canali *full text*– valuterà il testo inserito dall'utente secondo la catena sintagmatica e la relazione logica tra le parole (sinonimi, termini collegati ecc.), proponendo

come risultato della ricerca tutti i provvedimenti collegati (ad esempio, digitando la parola "telefonino" si possono ottenere le informazioni in tema di *Sms* (*Short message service*) e *Mms* (*Multimedia messaging service*). La costruzione ed implementazione del Thesaurus, sarà curata giorno per giorno dalla redazione del sito seguendo l'evoluzione linguistica, dei costumi, della tecnologia, della tecnica di normazione, mantenendo costante il rigore tecnico-giuridico proprio della base documentale.

Tra i principali servizi che sono già disponibili nel nuovo sito, spicca la possibilità di utilizzare un protocollo di transazione sicura con carta di credito. Il Garante, prima amministrazione ad aver sottoscritto tale accordo, attiverà fra breve la riscossione dei diritti di segreteria per ricorsi e notificazioni e l'iscrizione a congressi o convegni.

Le altre novità del nuovo progetto sono la costruzione di una specifica area "Pubblicazioni" dove troveranno posto anche contributi giuridico-divulgativi in formato audio/video sulle principali tematiche affrontate dal Garante, distribuiti attraverso uno specifico video *server*; il servizio di inoltro della *Newsletter* settimanale via *e-mail* che consentirà una tempestiva informazione sulle attività e decisione dell'Autorità.

Di particolare rilievo è la pagina relativa alla *"Privacy policy"* del sito (*ID*=36573), in cui si rende l'informativa generale sulle modalità, logica e finalità del trattamento dei dati di navigazione, dei dati conferiti volontariamente dagli utenti, specificando e sulle modalità di uso dei *"cookies"*. Specifiche informative vengono, poi, rese in ogni pagina di avvio dei distinti servizi o *"form"* di registrazione.

L'infrastruttura tecnologica sottostante al sito è altresì utilizzata come *Intranet* aziendale. La piattaforma di amministrazione è il punto di gestione di varie basi di dati strutturate. Ogni dipartimento/servizio, attraverso un sofisticato sistema di privilegi di accesso e l'applicazione di specifici *workflow*, può contribuire direttamente al "popolamento" di tali banche dati inserendo i contenuti attraverso una semplice interfaccia *web oriented*, ovvero rendendo disponibili i *files* grazie ad una veloce ed efficiente rete locale.

La redazione del sito -che verrà a breve potenziata- cura l'intero ciclo di lavorazione tecnico-giuridica sino alla messa *on line* nell'*Intranet* aziendale e alla pubblicazione nel sito *Internet*; provvede inoltre ad allestire le pubblicazioni istituzionali dell'Ufficio licenziando la versione tipografica del *Bollettino* e delle relazioni annuali.

La gestione amministrativa dell'Ufficio

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

L'attuazione del disegno organizzativo delineato dal regolamento n. 1/2000 sul funzionamento e l'organizzazione dell'Ufficio del Garante ha permesso una più efficiente ed efficace azione istituzionale ed il raggiungimento di positivi risultati. Il processo di consolidamento della struttura organizzativa dell'Autorità, avviato negli anni precedenti, è proseguito nel 2002 con il miglioramento delle condizioni di operatività delle unità organizzative di primo livello (dipartimenti e servizi) e la progressiva assegnazione ad esse delle risorse umane che via via si sono rese disponibili all'esito delle diverse procedure concorsuali e selettive indette dall'Autorità.

Parallelamente a tale processo è emersa l'esigenza di una riflessione finalizzata al potenziamento della struttura organizzativa dell'Ufficio, che ha tratto spunto anche dai documentati studi di due società di consulenza le quali hanno offerto un valido contributo conoscitivo oggetto di attenta analisi da parte dell'Autorità.

Ha preso così forma un disegno di consolidamento che, sulla base dell'esperienza maturata in sede di prima applicazione del regolamento n. 1/2000, ridelinea in termini innovativi alcuni aspetti dell'organizzazione dell'Ufficio del Garante, anche in vista dei nuovi compiti demandati all'Autorità dal d.lg. n. 467/2001.

Il progetto di *reengineering* si articola in due interventi: a) completamento di un ampio processo di ricognizione e di delega di funzioni e poteri amministrativi ai dirigenti in servizio e definizione delle rispettive sfere di autonomia e responsabilità, anche sulla base di una direttiva del segretario generale per la gestione amministrativa e contabile intesa ad indirizzare ed uniformare i comportamenti amministrativi; ciò in conformità alle disposizioni regolamentari contenute nei regolamenti n. 1/2000 (concernente il funzionamento e l'organizzazione) e n. 3/2000 (sull'amministrazione e la contabilità); b) individuazione di un nucleo funzionale di coordinamento amministrativo presso la segreteria generale al quale saranno assegnate due nuove figure dirigenziali ("direttore di gestione" e "direttore del supporto") cui saranno delegati compiti di coordinamento di individuati settori di attività e l'attuazione di progetti di particolare interesse per l'Autorità.

Con tali limitati, ma significativi interventi organizzativi l'Autorità si propone di sperimentare una più equilibrata articolazione e distribuzione delle competenze operative e decisionali e un più incisivo coordinamento, lasciando inalterata la peculiarità di un modulo organizzativo caratterizzato da elevata flessibilità, come evidenziato nella *Relazione 2001*.

L'attuazione delle scelte organizzative prima illustrate è in via di completamento. In particolare sono stati conferiti i previsti poteri decisionali alle unità organizzative esistenti ed è stata definita la menzionata direttiva sull'amministrazione e la gestione delle spese; si è inoltre con-

clusa la selezione pubblica (indetta con avviso pubblico pubblicato sulla *G.U.* – 4a serie speciale – n. 91 del 19 novembre 2002) per il reclutamento del direttore di gestione con l'individuazione del candidato a tale incarico.

L'individuazione della figura di direttore del supporto all'attività giuridica è stata, invece, preceduta da un interpello dei dirigenti in servizio presso l'Ufficio e le relative procedure sono in corso di svolgimento.

Nel quadro delle iniziative per migliorare efficienza, efficacia ed economicità dell'azione amministrativa, contestualmente all'approvazione del bilancio di previsione il Garante ha definito, avvalendosi dei contributi delle unità organizzative, i principali obiettivi e risultati che esse saranno chiamate a realizzare, i progetti di miglioramento e le priorità per il 2003, in conformità alle disposizioni regolamentari.

La direttiva del Garante è seguita da ulteriori atti di indirizzo del segretario generale per specificare tempi e modalità di attuazione dei programmi di lavoro di ciascun dipartimento e servizio.

Per un efficace monitoraggio del raggiungimento dei risultati e per la definizione di parametri di valutazione e di indicatori per la verifica dei risultati dell'attività dell'Ufficio, oltre che per un controllo di regolarità della gestione contabile, è stato istituito un servizio di controllo interno del quale sono stati chiamati a farne parte un magistrato contabile e due dirigenti di provata esperienza e competenza.

E' stato inoltre rafforzato, mediante l'assegnazione di nuovo e qualificato personale, l'ufficio relazioni con il pubblico (Urp) ed è stato potenziato il servizio di centralino, dando avvio nel contempo ad una sperimentazione per la creazione di un *call center* che, nel rispetto di rigorose misure di riservatezza, fornisca un più efficiente servizio di accoglienza e prima informazione agli utenti.

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

Il bilancio di previsione del 2002, come quello del 2001, è stato elaborato secondo le direttive del regolamento del Garante n. 3/2000, concernente la gestione amministrativa e la contabilità. Esso è riferito al sesto anno di attività dell'Autorità ed è stato elaborato sulla base delle esigenze funzionali delle unità organizzative (dipartimenti e servizi) e degli obiettivi e dei programmi definiti dal Garante.

Il bilancio di previsione del 2002 è stato predisposto tenendo conto anche dei maggiori oneri derivanti da nuove immissioni di personale con diverse tipologie lavorative (fuori ruolo, contratto di specializzazione a tempo determinato, *stage*), delle più generali esigenze di rafforzamento dell'Ufficio, nonché delle spese derivanti dall'organizzazione della conferenza internazionale su: *"Privacy: da costo a risorsa"*, tenutasi nella sala conferenze presso la sede dell'Autorità il 5 e 6 dicembre 2002.

Il 23 dicembre 2002 si sono conclusi i concorsi pubblici a complessivi ventuno posti di varie qualifiche banditi dall'Autorità e la selezione, bandita nell'agosto del 2002, per il reclutamento di quattro giovani laureati con contratto di specializzazione a tempo determinato.

L'intensa attività del 2002 trova riscontro nelle spese liquidate e pagate -sia in conto competenza, sia in conto residui- che si sono mantenute superiori a □ 11.500.000,00 in linea con il precedente esercizio, e soprattutto nelle spese per il personale, comprese le indennità spettanti ai componenti il collegio, che sono passate da □ 6.068.500,00 a € 6.674.500,00.

Le risorse a disposizione del Garante per il 2002 sono state pari a € 12.187.000,00, provenienti dal contributo dello Stato per € 10.849.996,00. Le restanti risorse finanziarie accertate e riscosse dall'Autorità si riferiscono ai diritti di segreteria per le notificazioni, per i ricorsi e le autorizzazioni, ai rimborsi spese provenienti dal Consiglio d'Europa e dalle istituzioni comunitarie per la partecipazioni di rappresentanti del Garante a riunioni da esse indette, agli interessi maturati sui fondi relativi agli avanzi pregressi, alle entrate derivanti dalla sublocazione di parte dei locali della sede dell'Autorità, alle quote di iscrizione alla suddetta conferenza internazionale.

Da segnalare che il contributo dello Stato per il 2002 è stato ridotto rispetto al 2001 di oltre € 500.000. Inoltre, a fine anno, in attuazione delle disposizioni del d.m. 29 novembre 2002 (con il quale il Ministro dell'economia e delle finanze ha disposto la riduzione del 15 per cento delle spese di funzionamento per acquisti di beni e servizi degli enti ed organismi pubblici non territoriali), il Garante, pur ritenendo di non essere destinatario della citata norma, con apposita delibera ha apportato una riduzione degli stanziamenti del 2002 per le spese di funzionamento per € 125.400,00, in considerazione degli obiettivi di contenimento della spesa pubblica.

Tali riduzioni comporteranno un ridimensionamento dei programmi di attività del 2003, tenuto conto dell'esiguità dell'avanzo di amministrazione e dell'ulteriore riduzione del contributo dello Stato, fissato in € 10.252.000,00. Di contro, le spese lieviteranno per effetto della immissione in servizio dei nuovi assunti, sia per gli oneri retributivi, sia per le spese di funzionamento connesse alla maggiore attività dell'ufficio.

La spesa per il personale, contenuta nel 2002 al di sotto del 60 per cento delle risorse disponibili, nel 2003 si avvicinerà al 70 per cento comprimendo le risorse disponibili.

Nel documento programmatico del 2002 era indicato come prioritario il potenziamento delle strutture informatiche. Nel corso dell'anno per il raggiungimento di tale obiettivo sono state impegnate risorse per oltre € 1.100.000,00 (di cui € 800.000,00 per contratti conclusi con la liquidazione e il pagamento ai fornitori, e € 300.000,00 per obbligazioni contrattuali giuridicamente perfezionate, che risultano impegnati sui fondi di competenza dell'esercizio 2002). Parte delle risorse per l'informatizzazione dell'Ufficio sono state finalizzate a dotare la biblioteca del Garante della tecnologia indispensabile per la gestione della stessa da parte del personale addetto e per la migliore fruizione da parte degli studiosi che vi accederanno. Inoltre la biblioteca è stata arricchita, nel corso del 2002, di acquisizioni librarie per oltre € 106.000,00.

L'Autorità si è avvalsa delle convenzioni stipulate dalla CONSIP s.p.a., con risultati soddisfacenti e con sensibili risparmi, per l'acquisto di beni di facile consumo, *computer* anche portatili, nonché per la locazione di fotocopiatrici e *computer*.

La fornitura di beni e servizi occorrenti per realizzare gli ambiziosi obiettivi posti dal documento programmatico e per assicurare il funzionamento dell'Autorità ha comportato una intensa attività contrattuale concretizzatasi in circa 40 procedure.

L'importo complessivo dei contratti stipulati ammonta a circa € 2.500.000,00, la maggior parte dei quali destinati al potenziamento delle strutture tecnologiche.

L'Autorità ha infatti dato priorità al progetto di sviluppo del sistema informativo dell'Autorità previa l'acquisizione, anche tramite la convenzione CONSIP, di ulteriori sistemi *server* e postazioni di lavoro.

Sono stati acquisiti alcuni *software*, tra i quali quello per la di gestione della biblioteca idoneo a consentire anche il collegamento alla rete *sbm* (sistema bibliotecario nazionale), ed è stata affidata ad una società specializzata la realizzazione di un sistema amministrativo-contabile finalizzato alla gestione automatizzata del bilancio, del relativo *software* di base e dei servizi di *setup*, installazione, manutenzione ed assistenza. Sono stati, altresì, attivati appositi corsi di istruzione sull'utilizzo dei nuovi strumenti per i funzionari dei dipartimenti interessati alle innovazioni.

Su richiesta del dipartimento risorse tecnologiche e della redazione del sito *web* sono state avviate, in conseguenza dell'accresciuta utilizzazione del sito *web* del Garante, le procedure per il suo potenziamento tramite l'aggiornamento *software*, l'espansione del *server*, la migliore organizzazione del *data-base*, l'innovazione della parte grafica e del sistema di ricerca ipertestuale.

La sala delle conferenze è stata dotata di un moderno impianto audio ed è stata implementata la rete per i servizi di videoconferenza; sono state avviate le procedure negoziali per dotare il dipartimento registro generale dei trattamenti, nel quadro delle iniziative tese ad automatizzare le lavorazioni e rendere più veloce l'accesso alle notificazioni da parte degli utenti, del servizio di scansione ottica delle notificazioni (circa 5.000.000 di fogli) e di memorizzazione dei *file* contenuti nei *floppy disk* (circa 64.000). Il bando di gara della licitazione privata (ai sensi del d.lg. 17 marzo 1995, n. 157, come modificato dal d.lg. 25 febbraio 2000, n. 65), con importo a base d'asta di € 270.000 i.v.a. esclusa, è stato pubblicato sulla *G.U.C.E.* n. S231 del 28 novembre 2002 e sulla *G.U.R.I.* n. 280 del 29 novembre 2002.

L'attività contrattuale relativa al servizio relazioni con i mezzi d'informazione ha riguardato l'affidamento della realizzazione di uno spot pubblicitario radio-televisivo –in onda sulla reti pubbliche dal 24 marzo 2003- e la stipula di un accordo con una delle maggiori agenzie di stampa italiane per la produzione e la trasmissione di servizi radiofonici e televisivi informativi sull'attività del Garante.

Tra le attività contrattuali ulteriori si può citare quella che ha riguardato l'allestimento di uno stand fieristico e dei relativi servizi presso il *Forum.P.A.* di Roma, il *Com-P.A.* di Bologna e lo *Smau* di Milano. Sono stati, inoltre, curati gli atti amministrativi per la realizzazione di una nuova iniziativa editoriale curata dal servizio relazioni con i mezzi d'informazione: la pubblicazione bimestrale *"Garanteprivacy.it"*.

73 Lo sviluppo del sistema informativo

Nel 2002 è proseguita l'attività di sviluppo avviata nel 2001, caratterizzata dall'implementazione delle principali procedure componenti il sistema informativo dell'Autorità, sulla base dell'infrastruttura di supporto tecnologico realizzata lo scorso anno.

Tra i progetti più significativi portati a compimento e messi in produzione si citano qui di seguito i principali componenti del sistema informativo e alcune realizzazioni sistemistiche:

- sistema informatico amministrativo-contabile: il sistema, sviluppato sulla base di un'attenta analisi delle esigenze dell'Ufficio, in collaborazione con il dipartimento di amministrazione e contabilità, è basato su un avanzato *software* di gestione delle risorse (*Oracle E-Business Suite*) che, opportunamente configurato, consentirà al personale del dipartimento di amministrazione e contabilità il controllo dei capitoli di spesa e delle funzioni, e permetterà ai dirigenti dell'Ufficio l'accesso alle posizioni di propria competenza. L'accesso alle funzionalità del sistema avviene, previa autenticazione, tramite un comune browser, rendendo interscambiabili le postazioni di lavoro;
- sistema di gestione del contenzioso amministrativo: è un'applicazione *web-oriented* sviluppata interamente nell'ambito del dipartimento risorse tecnologiche, programmata in linguaggio PHP in ambiente *Linux* e basata su un database relazionale di tipo *MySQL*. Offre funzionalità di creazione, di consultazione, di aggiornamento, di generazione di rapporti, di ricerca e di statistica relative alle pratiche di contenzioso amministrativo;
- sistema di consultazione *web* del registro generale dei trattamenti: è costituito da una serie di pagine *html* con codice programmativo PHP che consentono di interrogare la base di dati del registro generale dei trattamenti, connettendosi al *database Oracle* che la ospita. La consultazione avviene al momento in modalità *Intranet*, ma il sistema è predisposto per la consultazione da parte di utenti esterni tramite *Internet*;
- sistema di notificazione *on line* del trattamento dei dati personali: è sviluppato come evoluzione del sistema di consultazione precedentemente descritto, di cui condivide gli strumenti programmativi, e consente ai titolari di trattamenti di dati personali di effettuare la compilazione *on line* della notificazione al Garante, evitando il ricorso al supporto magnetico, il cui uso negli anni passati ha causato inconvenienti dovuti alla sua fragilità magnetica e alla frequente perdita di dati. Con il nuovo sistema, sviluppato in collaborazione con il dipartimento registro generale dei trattamenti, viene superata la complessa ed onerosa fase di d*ata entry* manuale basato sulla documentazione cartacea e sui *floppy-disk*, avvicinando così ulteriormente l'Autorità ai cittadini;
- nuovo sito *web* ufficiale del Garante: di particolare rilievo lo sviluppo del nuovo sito *web* dell'Autorità, che consente una più efficiente gestione dei contenuti e facilita il processo redazionale, permettendo la gestione coordinata e partecipativa del processo di pubblicazione. Il dipartimento risorse tecnologiche ha curato gli aspetti sistemistici del progetto e la sua implementazione nelle varie fasi, effettuata utilizzando il sistema *Oracle Internet Application Server* in ambiente operativo *Linux*. Tali componenti *software* di

base e l'architettura sistemistica prescelta garantiscono una buona tolleranza ai guasti e un notevole livello di continuità del servizio, con notevole incremento delle prestazioni effettive e di quelle percepite dai visitatori, pur con un modesto investimento iniziale sull'hardware. Oltre agli aspetti tecnici sistemistici, sono state privilegiate le caratteristiche di usabilità del sito, con capacità di presentare i contenuti su tre diversi livelli di dettaglio grafico (alta risoluzione, alta leggibilità, solo testo) e con il supporto per la consultazione da parte dei non vedenti. Lo sviluppo del sito è stato condotto in collaborazione con la redazione del sito, che ha partecipato all'analisi delle esigenze, alla formulazione delle specifiche funzionali e ha seguito la fase di realizzazione;

- sistema di videoconferenza in rete: è stato realizzato un impianto professionale per videoconferenza che consente l'interazione tra postazioni di sala, postazioni individuali e interlocutori esterni. I collegamenti possono avvenire secondo gli *standard ITU H.320* (tramite linee ISDN dedicate) o *ITU H.323* (tramite protocolli IP). L'impianto consente di effettuare connessioni punto-punto e multipunto, con un sofisticato sistema di regia integrato. Gli stessi apparati consentono al personale dell'Ufficio di approntare postazioni esterne di videoconferenza per venire incontro alle esigenze di collegamenti esterni;

- sistema di *unified messaging* integrato con funzioni di *call center*: è stato introdotto, nell'ambito del nuovo servizio di gestione delle chiamate entranti, un sistema di *unified messaging* che consente il trattamento uniforme dei messaggi vocali (segreteria telefonica), dei *fax* in entrata e uscita, degli *sms* e della posta elettronica. Il sistema consente di centralizzare i flussi di comunicazione, garantendo una migliore efficienza ed economia. Inoltre, l'uso della posta elettronica come strumento di unificazione consente di pervenire a un notevole risparmio nei costi telefonici e aumenta considerevolmente l'efficienza del lavoro, laddove sia necessario mantenere, anche da postazioni remote, il contatto informativo con l'Ufficio;

- sistema di protezione della rete e di rilevamento di intrusioni: sono stati introdotti a protezione della rete dei sistemi *firewall* aggiuntivi a tecnologia diversa da quelli precedentemente installati. E' stato inoltre installato nella rete un sistema avanzato di rilevamento di intrusioni, nell'ambito di un più generale intervento volto ad accrescere l'affidabilità dell'infrastruttura LAN interna.

Tra le altre attività svolte, va ricordato il complemento della migrazione verso la piattaforma *Oracle* dei principali sistemi di *database* precedentemente utilizzanti diverse tecnologie, nonché l'ampliamento della dotazione informatica con l'introduzione di nuovi *server Windows* e *Linux*, l'espansione dei server *Sun Solaris* utilizzati per applicazioni gestionali e l'incremento delle postazioni di lavoro individuali per far fronte alla crescita numerica del personale in servizio.

E' stato inoltre sviluppato, il sito *web* del convegno *"Privacy: from cost to resource"*, tenutosi nel dicembre dello scorso anno, con il contributo grafico dei consulenti dell'Ufficio e la collaborazione della redazione del sito.

Tra i numerosi progetti in corso, si evidenzia quello riguardante l'acquisizione del nuovo sistema di gestione del protocollo, a tecnologia *web*, con funzioni di firma digitale, di protocollo federato, di protocollazione automatica della posta elettronica con segnature conformi

alle normative italiane e comunitarie, di archiviazione ottica, di instradamento della corrispondenza

E' stata, inoltre, progettata un'infrastruttura di *storage area network* a tecnologia *fiber channel*, che integrerà un moderno sistema di gestione condivisa di *file systems multi standard* dinamicamente ridimensionabili e allocabili alle diverse piattaforme in dotazione e un sistema robotizzato di gestione dei *backup* su supporto magnetico. La tecnologia *fiber channel*, unita alla disponibilità in Ufficio di una moderna rete di cablaggio strutturato con tratte dorsali in fibra ottica multimodale, consentirà di installare le unità di *backup* in posizioni remote rispetto al locale tecnico informatico, aumentando le capacità di sopravvivenza in caso di disastro.

E' stato progettato, ed è in corso di realizzazione, il sistema di gestione delle risorse umane, che integrerà funzionalità di rilevamento presenze, di gestione delle missioni del personale, di controllo degli accessi. Il sistema si avvale della rete locale per l'interconnessione delle unità di lettura, dei concentratori e dei sistemi *server* e delle postazioni di controllo.

E' stato perfezionato il 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.

E' stato ulteriormente sviluppato, con l'attivazione di nuove funzionalità, il sistema *software* Sebina per la gestione bibliotecaria, che consente la gestione del catalogo da parte del personale bibliotecario, la consultazione sul *web* dell'*OPAC*, la generazione di rapporti e ricerche bibliografiche.

E' stato altresì delineato il sistema di *management* integrato *Unicenter TNG*, che consente al personale tecnico del Dipartimento risorse tecnologiche di effettuare il monitoraggio degli apparati di rete, dei *server* e dei *personal computer*.

E' stato progettato un *autonomous system IP* che consentirà la gestione paritaria di flussi di traffico *Internet* senza dipendenza da un particolare provider. Il progetto prevede una fase di formazione, una di acquisizione delle tecnologie necessarie e di contemporanea gestione delle procedure tecniche di assegnazione e di registrazione dell'AS presso gli enti europei di coordinamento. La transizione verso un a*utonomous systems* della rete *IP* del Garante consentirà di stipulare contratti indipendenti con diversi *provider Internet*, allo scopo di accrescere l'affidabilità dei servizi *extranet* dell'Ufficio, di assicurare ancora migliori prestazioni alla rete, e consentirà di utilizzare indirizzi di rete *IP* indipendenti dal *provider*, facendo venir meno la dipendenza tecnica da un solo *provider* introdotta dall'assenza del concetto di *number portability* ormai consolidato nell'ambito delle reti telefoniche.

74 Il personale e i collaboratori esterni

Il 2002 si è caratterizzato per una intensa attività finalizzata al rafforzamento dell'organico dell'Autorità.

Sono stati, infatti, espletati i quattro concorsi pubblici per titoli ed esami (pubblicati nella *G.U.* -4ª serie speciale- n. 47 del 15 giugno 2001) banditi dal Garante per la copertura di complessivi 21 posti, di cui n. 2 per dirigente, n. 1 per dirigente informatico, n. 10 per funzionario e n. 8 per impiegato operativo.

Le commissioni esaminatrici, ciascuna presieduta da un magistrato amministrativo designato dal Consiglio di presidenza della giustizia amministrativa, composte da tre docenti universitari e dal segretario generale del Garante, si sono insediate nel mese di ottobre 2002 (ad eccezione di quella del concorso per funzionario insediatasi nel mese di settembre).

I lavori, nonostante la complessità delle procedure e la difficoltà della valutazione prevista dai bandi di concorso, si sono conclusi in appena due mesi.

Il 30 dicembre sono stati sottoscritti i contratti individuali di lavoro con i vincitori di concorso i quali il 15 gennaio 2003 sono stati immessi in servizio presso l'Autorità. I posti complessivamente assegnati sono stati 19, due in meno rispetto a quelli banditi.

I concorsi si sono svolti con la massima regolarità ed i candidati, considerate la difficoltà delle prove e la severità della valutazione, sono stati sottoposti ad una rigorosa selezione. Si può, quindi, affermare che i concorsi espletati dal Garante costituiscono una concreta attuazione dei principi di imparzialità, celerità ed economicità delle procedure concorsuali previsti dall'art. 35 del d.lg. n. 165/2001 ("*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*").

Con l'immissione dei vincitori di concorso si è determinato un rafforzamento dell'organico dell'Ufficio il quale può ora contare su 91 unità per il contemporaneo inserimento di altre 4 unità con contratto di specializzazione a tempo determinato, selezionate con una procedura che si è svolta parallelamente a quelle concorsuali, bandita nell'agosto del 2002 (*G.U.* - 4ª serie speciale – n. 66 del 20 agosto 2002).

Un'analoga selezione si era conclusa nell'aprile del 2002 con l'assunzione di 6 unità. Complessivamente sono 10 i giovani che, all'esito di una rigorosa selezione effettuata mediamente su circa 450 domande in ciascuna delle due selezioni, hanno avuto l'opportunità di un inserimento nell'Ufficio del Garante per specializzarsi in materia di trattamento dei dati personali o perfezionare la propria preparazione nella medesima materia.

Il 5 luglio del 2002 si è conclusa anche la selezione, rivolta a giovani laureati di età non superiore a 28 anni, per l'effettuazione di periodi di tirocinio presso l'Autorità. Sulla base della graduatoria formata da una qualificata commissione di selezione agli inizi di settembre 2002 un primo gruppo di 5 *stagiare* ha iniziato presso l'Ufficio un periodo di tirocinio della durata di sei mesi, prorogabile sino ad anno, e nel maggio del 2003 analoga opportunità è stata offerta ad un altro gruppo di 6 giovani laureati.

Nel corso del 2002 sono proseguite le iniziative di formazione e perfezionamento nelle lingue straniere di uso corrente nell'attività d'ufficio e sono state promossi alcuni momenti di aggiornamento di carattere seminariale su tematiche ed ambiti disciplinari di immediato interesse per le attività istituzionali dell'Autorità.

Come accennato, l'organico a disposizione dell'Ufficio è di 91 unità, di cui n. 15 con contratto a tempo determinato e n. 17 in posizioni di fuori ruolo o comando da altre amministrazioni ed enti pubblici, come da prospetto allegato:

SITUAZIONE DEL PERSONALE E TIPOLOGIA LAVORATIVA

PERSONALE IN SERVIZIO

Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	Personale a contratto	TOTALE
Dirigenti	26	18	5		23
Funzionari	40	26	7		33
Operativi	25	15	5		20
Esecutivi	9				0
Personale a contratto	20			15	15
TOTALE	120	59	17	15	91

L'Autorità, allo stato, si avvale della collaborazione di cinque consulenti per i necessari approfondimenti nelle tematiche giuridiche e della comunicazione istituzionale. 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, nonché per la preparazione della conferenza internazionale promossa dal Garante *"Privacy: da costo a risorsa"* e per la redazione del bilancio di previsione e consuntivo.

Le commissioni di selezione dei contratti di specializzazione e per il tirocinio e le commissioni esaminatrici dei concorsi pubblici hanno esaurito i loro compiti nel 2002.

Il registro dei trattamenti

75 Organizzazione e sviluppi futuri

L'istituto della notificazione del trattamento dei dati personali, previsto dagli artt. 7, 16 e 28, legge n. 675/1996 è stato rivisitato a fondo dal d.lg. 28 dicembre 2001, n. 467. Alcune modifiche sono già entrate in vigore e riguardano:

- l'obbligo di designazione (e di indicazione nella notificazione) 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 (artt. 1, comma 2, e 3, comma 3);
- l'indicazione nella notificazione 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).

Le novità più consistenti riguardano però l'individuazione dei casi e dei contenuti della notificazione -che attualmente sono stabiliti direttamente dalla legge n. 675/1996- mediante norme da inserire nell'emanando testo unico delle disposizioni in materia di protezione dei dati personali.

L'obbligo di notificazione sarà limitato alle sole ipotesi in cui 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"* (art. 3 d.lg. n. 467/2001). Un gruppo di lavoro interno ha già effettuato alcuni primi approfondimenti sui casi di notificazione, ponendo particolare attenzione a due aspetti fondamentali: rendere l'adempimento della notificazione pienamente rispondente alle finalità dell'istituto e circoscrivere le notizie che il titolare deve fornire agli elementi significativi.

In attesa del testo unico, la disciplina della notificazione, salvo quanto detto circa le novità entrate già in vigore, rimane sostanzialmente immutata.

Le notificazioni confluiscono nel registro generale dei trattamenti previsto dall'art. 31, comma 1, lett. *a)* della l. n. 675/1996 e sono consultabili tramite la Intranet del Garante. Nel 2002 sono state definitivamente superate le difficoltà evidenziate nella relazione precedente in ordine allo sviluppo del *software* per l'accesso ai dati, mediante l'affidamento del servizio ad un'altra ditta che ha operato efficacemente e con tempestività. Il programma, molto complesso, oltre alla possibilità di effettuare ricerche e produrre *report* statistici, permette di rilevare automaticamente le incompletezze e gli errori (purtroppo frequenti) contenuti nelle notificazioni. E' cura poi dell'Ufficio, con procedure automatizzate, invitare i notificanti a regolarizzare le irregolarità.

Le notificazioni tuttora vengono redatte su un modello *standard* o, in alternativa su *floppy disk*. Il modello e il programma attualmente possono essere prelevati dal sito *Internet* del

Garante o richiesti direttamente all'Ufficio e comunque per tutto l'anno 2002 è stata assicurata la distribuzione capillare e gratuita presso tutti gli uffici postali. Essendo nel frattempo cessata la convenzione con Poste italiane s.p.a. si è preferito non rinnovarla sia a motivo della sua onerosità, sia per la constatazione che gli utenti ritengono più comodo scaricare direttamente da *Internet* il modello di notificazione. Esiste comunque la possibilità di reperire il modello tramite negozi specializzati per uffici o di utilizzare fotocopie.

L'Ufficio ha bandito una gara europea per la scansione ottica di tutte le notificazioni e connessa documentazione pervenuta in questi anni, finanziando in parte il progetto con i risparmi derivanti dalla cessata convenzione con Poste italiane. Allo stato attuale, la commissione appositamente nominata sta concludendo l'esame delle numerose offerte pervenute. con la previsione di stipulare il contratto entro breve termine.

In tale maniera sarà possibile procedere a controlli più accurati sul contenuto delle notificazioni, verificare l'esatta corrispondenza dei dati immessi ed eliminare l'enorme massa di documentazione cartacea e su *floppy disk* che occupa ampi spazi.

Permane l'orientamento di ridurre sensibilmente i costi, migliorando e ottimizzando il servizio. In tale ottica è stata riposta attenzione sulla modalità di trasmissione telematica della notificazione con utilizzo della firma elettronica e pagamento *on line* dei diritti di segreteria (attualmente fissati in € 7,75 per le notificazioni su *floppy disk* e € 12,91 per quelle su modello cartaceo) stipulando convenzioni con organismi pubblici e privati per agevolare le operazioni di notificazione da parte di utenti eventualmente sforniti di firma elettronica.

E' stata incrementata, anche rispetto all'anno precedente, l'attività di assistenza diretta e telefonica svolta dal dipartimento registro generale dei trattamenti, che cura tutti gli adempimenti relativi alla notificazione, e dall'ufficio relazioni con il pubblico. Risposte ai quesiti più frequenti (FAQ) sono consultabili direttamente dall'utente sul sito del Garante.

A seguito di varie lettere di regolarizzazione delle notificazioni che presentano errori od incompletezze inviate dall'Ufficio (destinate a ridursi drasticamente con l'introduzione del nuovo modello telematico di notificazione, più "leggero", comprensibile e con controlli automatizzati già nella fase di immissione dei dati), le richieste di accesso al registro e di copia delle notificazioni già presentate si sono incrementate sensibilmente.

Accanto all'attività di regolarizzazione di cui si è già detto, sono inoltre proseguite le attività consistenti essenzialmente nella memorizzazione delle notificazioni pervenute tramite il personale messo a disposizione dalla società che ha curato il programma di gestione del registro. Inoltre il dipartimento registro generale dei trattamenti collabora attivamente con l'attività ispettiva fornendo notizie, materiali e dati utili per il controllo.

La novità introdotta dal d.lg. n. 467/2001 circa l'obbligo di comunicare al Garante almeno un responsabile del trattamento ha ridotto sensibilmente il numero di notificazioni pervenute nell'anno, anche se in seguito a controlli e richieste di regolarizzazione si è registrata nei mesi scorsi una nuova impennata nell'invio dei modelli.

Un notevole impegno è stato profuso nell'attività di recupero dei diritti di segreteria non versati con risultati decisamente positivi.

L'anno in corso impegnerà l'Ufficio nella predisposizione del "nuovo registro dei trattamenti", nello sviluppo *software* e nella stipula di convenzioni per effettuare la notificazione per via telematica.

Dati statistici

76 Prospetto analitico

ATTI E PROVVEDIMENTI/ATTIVITÀ GARANTE

Richieste di informazione e quesiti telefonici	12.800
Segnalazioni e reclami pervenuti	7.550
Quesiti pervenuti	1.725
Richieste di parere pervenute (parere ex art. 31, comma 2)	12
Richieste di autorizzazione pervenute	33
Assistenza telefonica relativa alle notificazioni	6.400
Notificazioni dei trattamenti previste dagli articoli 7, 16 e 28	12.227
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	1
Risposte a richieste di autorizzazione (art. 22)	32
Atti e provvedimenti a seguito di segnalazioni e reclami	3.689
Risposte a quesiti	1.003
Pareri rilasciati in base all'art. 31, comma 2	9
Altri provvedimenti di segnalazione del Garante	37
Provvedimenti istruttori ai sensi dell'art. 32, comma 1	165
Procedimenti contenziosi definiti sulla base di ricorsi (art. 29)	500
Elementi forniti per la risposta del Governo a interrogazioni parlamentari	5
Comunicati stampa	46
Notiziari settimanali pubblicati dall'Ufficio Stampa	58
Richieste di accesso e/o di verifica di dati esistenti nel Sistema Informativo Schengen	273
Procedimenti relativi alle richieste di accesso e/o di verifica di dati esistenti nel Sistema Informativo Schengen già definiti	175
Procedimenti ispettivi	40
Segnalazioni all'autorità giudiziaria	6
Ordinanze di ingiunzione	5

Periodo di riferimento della statistica: 1 gennaio 2002 - 30 aprile 2003

Ispezioni effettuate:	
Sopralluoghi ex art. 32, comma 1	35
Accessi alle banche dati con decreto dell'A.G.	4
Accessi alle banche dati con assenso	1
Collaborazioni con autorità giudiziarie	
Ispezioni effettuate nei confronti di:	
Soggetti privati	31
Soggetti pubblici	9
Segnalazioni inviate all'autorità giudiziaria:	
Per trattamento illecito (art. 35)	3
Per omessa adozione misure minime di sicurezza (art. 36)	1
Per inosservanza dei provvedimenti del Garante (art. 37)	1

SERVIZI ISPETTIVI

Periodo di riferimento della statistica: 1 gennaio 2002 - 30 aprile 2003

SERVIZIO RICORSI

Decisi	500

Tipo di decisioni adottate:	
Non luogo a provvedere	195
Inammissibilità	87
Accoglimento	124
Parziale accoglimento	52
Infondati	42

Statistica dei ricorsi decisi dal 1 gennaio 2002 - 15 aprile 2003

UFFICIO CONTENZIOSO

Verbali redatti	45
Ordinanze	5

Articoli di cui si è accertata la violazione:	
Art. 10 (omessa informativa agli interessati)	28
Art. 23, comma 2 (comunicazione di dati attinenti allo stato di salute)	2
Art. 32, comma 1 (omessa risposta a richiesta di informazioni)	13
Art. 34 (notificazione incompleta)	2

Opposizioni e ordinanze di ingiunzione	1

Periodo di riferimento della statistica: 1 gennaio - 31 dicembre 2002

DIPARTIMENTO REGISTRO GENERALE DEI TRATTAMENTI

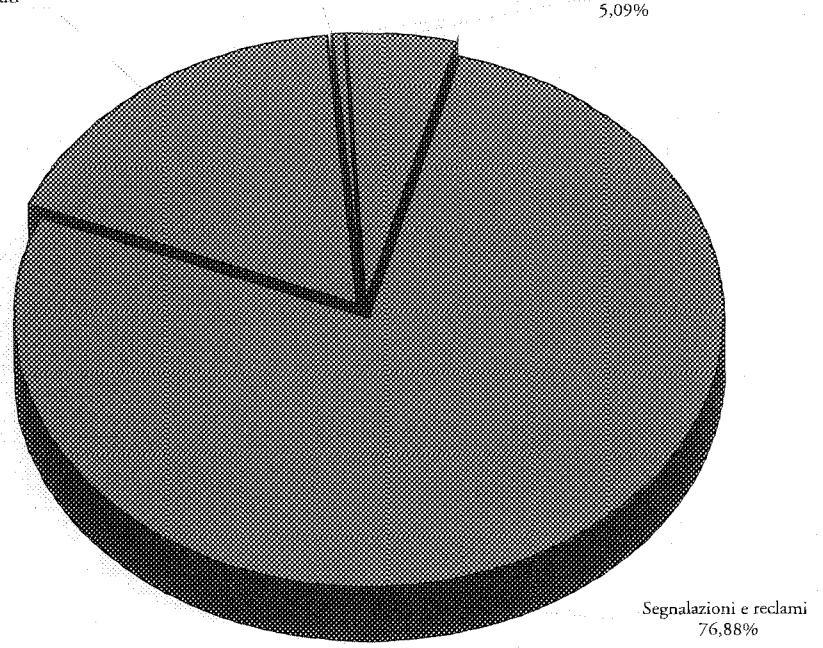
numero notificazioni presenti nel registro (circa)	315.000
numero lettere inviate per la regolarizzazione dei conti correnti (circa)	16400
numero richieste di accesso al registro	100
numero richieste di copie della notificazione (da 2002 a febbraio 2003)	485
somma relativa ai diritti di segreteria recuperati (da gennaio 2002 ad aprile 2003)	Euro 62.670,00

Alcuni dati statistici significativi estratti dalla consultazione del registro:

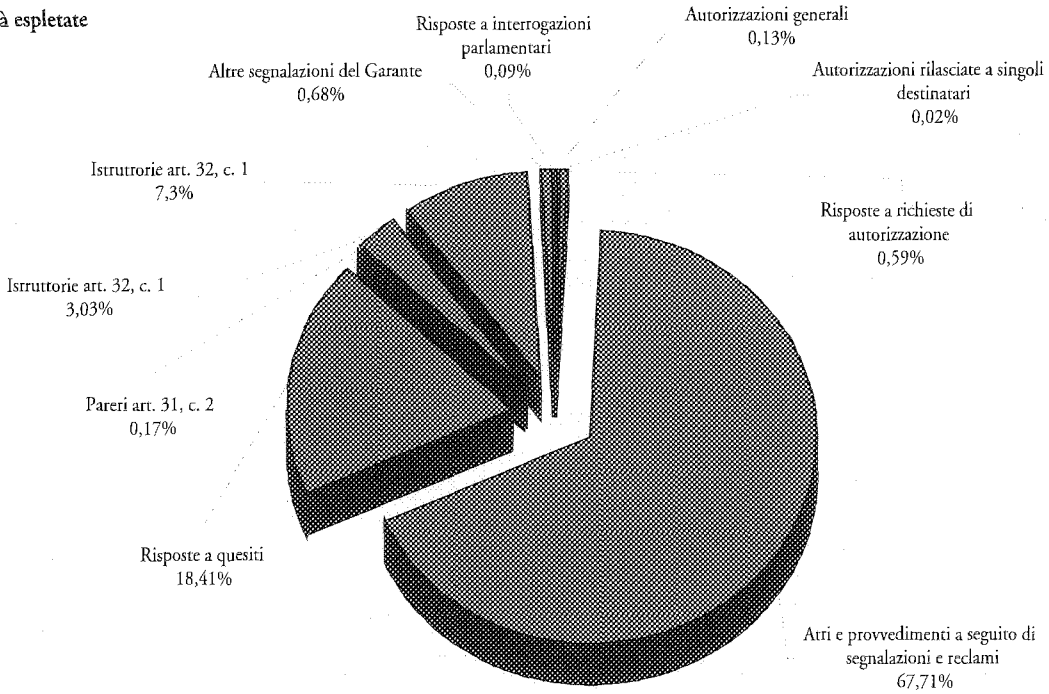
numero di notificazioni che riguardano il trasferimento di dati all'estero in ambito comunitario	172
numero di notificazioni che riguardano il trasferimento di dati in paesi extraeuropei	502
numero di notificazioni che contemplano tra le modalità di trattamento impianti di videosorveglianza	124
numero di notificazioni che contemplano tra le modalità di trattamento la costruzione di profili dei clienti	258

Periodo di riferimento della statistica: 1 gennaio - 30 aprile 2003

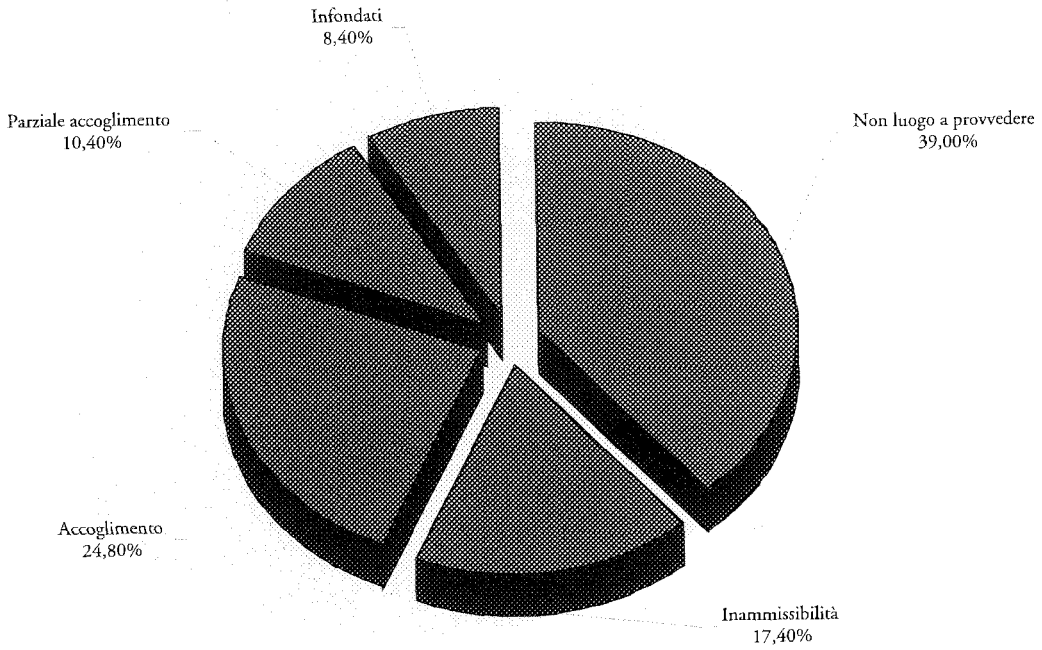
Atti e Provvedimenti richiesti
(esclusa assistenza telefonica e notificazioni)



Attività espletate



Statistica dei ricorsi



Attività comunitarie e internazionali

PAGINA BIANCA

Il recepimento delle direttive comunitarie

77 Le direttive sulla protezioni dei dati

La direttiva generale in materia di protezione dei dati personali è stata recepita con la legge n. 675/1996. Successivi, ulteriori interventi legislativi hanno apportato modificazioni ed integrazioni alla citata legge anche per renderla più aderente al testo della direttiva.

Come già riferito nella precedente Relazione annuale, il più recente di tali interventi si è avuto con il d.lg. 28 dicembre 2001, n. 467 che ha introdotto il principio del bilanciamento degli interessi in attuazione di quanto previsto dalla direttiva all'art. 7, lett. f, ed ha attribuito al Garante il compito di individuare gli ulteriori casi in cui il titolare può effettuare il trattamento dei dati personali in mancanza del consenso dell'interessato. Il decreto ha inoltre introdotto nell'ordinamento italiano, attribuendo al Garante la necessaria competenza, l'istituto del controllo preliminare (*prior checking*) sui trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone. Le verifiche sono svolte dall'Autorità di controllo prima dell'inizio del trattamento dei dati "sulla base di un eventuale interpello del titolare". Altre disposizioni del decreto hanno precisato il campo di applicazione della normativa ed il diritto applicabile, richiedendo, in presenza di una stabile organizzazione, l'indicazione del rappresentante in Italia del titolare del trattamento stabilito al di fuori dei Paesi dell'UE.

La direttiva sulla protezione dei dati nelle telecomunicazioni (97/66/CE) è stata sostanzialmente trasposta con il d.lg. n. 171/1998, recante *"Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni"*.

Con il citato d.lg. n. 467/2001 sono state apportate al decreto alcune modifiche per consentire, in linea con quanto previsto dalla direttiva, il pieno utilizzo di modalità di pagamento alternative alla fatturazione e l'informazione al pubblico sull'identificazione della linea chiamante e collegata, nonché per garantire, nel caso in cui l'abbonato si sia avvalso del diritto di eliminare l'identificazione della linea chiamante, l'annullamento di tale soppressione da parte dei servizi abilitati a ricevere chiamate di emergenza.

78 Stato di recepimento delle direttive 95/46/CE e 97/66/CE negli Stati membri

Direttiva 95/46/CE

Nel 2002, il Lussemburgo ha provveduto a promulgare la legge di recepimento della direttiva 95/46 (*Loi du 2 août 2002 – Protection des personnes à l'égard du traitement des données à caractère personnel*). La legge, entrata in vigore definitivamente il 1 dicembre 2002, ha abrogato la precedente normativa in materia di "protezione dei dati personali nei trattamenti informatizzati" del 31 marzo 1979.

Fra le caratteristiche salienti della legge lussemburghese, che è modellata da vicino sul testo della direttiva comunitaria, oltre l'ampliamento del campo di applicazione ai trattamenti automatizzati ed alle persone giuridiche, si segnala l'espressa inclusione dei trattamenti effettuati per scopi di sorveglianza: tali trattamenti, soggetti all'applicazione della legge *"qualora consentano di identificare una persona fisica o una persona giuridica"*, sono ammessi soltanto sulla base del consenso dell'interessato, ovvero qualora concernano luoghi pubblici o accessibili al pubblico purché tali luoghi *"presentino un rischio che renda necessario il trattamento per garantire la sicurezza degli utenti e prevenire possibili incidenti"*.

In particolare, per i trattamenti per scopi di sorveglianza sul luogo di lavoro, è previsto che il consenso dell'interessato non sia elemento sufficiente per legittimare il trattamento da parte del datore di lavoro.

Si segnala, inoltre, l'inclusione espressa dei dati genetici fra le categorie di dati "particolari" (dati sensibili) e l'ammissibilità del loro trattamento per fini giudiziari o di indagine penale soltanto al fine di accertare l'esistenza di "un legame genetico" nell'ambito del regime probatorio o per identificare una persona, oppure per la prevenzione o la repressione di specifici illeciti penali; l'obbligo del *"prior checking"* (controllo preliminare) da parte dell'autorità di controllo (particolarmente rispetto ai trattamenti sopra indicati).

La legge, introduce la previsione dell'esistenza di un "incaricato per la protezione dei dati", ai sensi dell'art. 18 della direttiva, con la conseguente esenzione dall'obbligo di notifica dei trattamenti; consente, inoltre, di presentare una notificazione semplificata secondo i modelli che saranno predisposti dall'autorità di controllo.

All'autorità di controllo prevista dalla legge (Commissione nazionale per la protezione dei dati) sono attribuiti i poteri di applicare sanzioni amministrative e di svolgere attività investigativa ai fini dell'accertamento di eventuali infrazioni, attività quest'ultima esercitabile previa richiesta anzichè d'ufficio.

Il 10 aprile 2003 è stato approvato in Irlanda il testo della legge che modifica il Data Protection Act del 1988, recependo la direttiva 95/46/CE. Le modifiche entreranno in vigore

(tranne quelle concernenti il sistema di notificazione ed i poteri ispettivi dell'autorità di protezione dati) dopo il 1 luglio 2003, sulla base del regolamento di attuazione che il Governo è incaricato di emanare.

Tra le innovazioni più importanti della legge irlandese si segnalano:

- l'estensione dell'ambito di applicazione ai dati sottoposti a trattamento non automatizzato ed il conseguente riconoscimento del diritto di accesso degli interessati, che è esercitabile anche rispetto a "pareri" o "opinioni" relativi all'interessato e che possono essere comunicati senza necessità di chiedere autorizzazione al soggetto che ha predisposto il parere o l'opinione;
- l'introduzione di una definizione specifica di "dati sensibili", attraverso un elenco modellato su quello della direttiva, che include anche i dati "relativi alla commissione o presunta commissione di reati da parte dell'interessato";
- la definizione dei requisiti di legittimità del trattamento in modo da meglio corrispondere alle disposizioni della direttiva (consenso dell'interessato, oppure necessità del trattamento per obblighi di legge, ecc.). Le nuove norme prevedono che, qualora dati personali siano accessibili a chiunque sulla base di disposizioni di legge (è il caso, ad esempio, dei registri elettorali), sia necessario comunque chiedere il consenso dell'interessato prima di fornirli a terzi per scopi di *marketing* diretto;
- l'introduzione dell'obbligo generale di notificazione dei trattamenti e la previsione delle esenzioni, che saranno specificate in un successivo regolamento. Attualmente in Irlanda vige il principio opposto: la notificazione non deve essere presentata, a meno che il titolare non appartenga alle categorie citate nell'art. 16 della legge del 1988: soggetti pubblici, società e imprese nel settore finanziario o del *marketing* diretto, soggetti che trattano dati "sensibili";
- l'ampliamento dei poteri del Data Protection Commissioner, soprattutto per quanto riguarda la possibilità di condurre ispezioni d'ufficio ed emanare codici deontologici validi come linee-guida per l'applicazione della normativa in materia di protezione dati rispetto a singoli settori.

Direttiva 97/66/CE

Per quanto concerne il recepimento della direttiva 97/66/CE, ed in attesa delle misure legislative che gli Stati dovranno adottare in linea con la nuova direttiva 2002/58, occorre segnalare che l'Irlanda ha provveduto ad emanare il regolamento in materia di protezione dati e *privacy* nel settore delle telecomunicazioni, entrato in vigore l'8 maggio 2002. Il Regolamento prevede, in particolare, la conservazione dei dati di traffico telefonico per scopi di fatturazione fino ad un massimo di sei mesi; le norme relative all'identificazione della linea chiamante; la possibilità per l'utente di non essere inserito in elenchi telefonici pubblici, su richiesta, e di limitare i dati riportati a quanto necessario per l'identificazione; l'istituzione di un registro nazionale di *"opt-out"* nel quale potranno farsi inserire tutti gli utenti (anche persone giuridiche) che non desiderino ricevere chiamate telefoniche indesiderate (per scopi di *marketing* diretto); la cooperazione fra autorità per la protezione dei dati e l'Ufficio del *Director of Telecommunications Regulations* ai fini dell'attuazione del regolamento – in particolare, il Data Protection Commissioner sarà responsabile degli aspetti di protezione dati e

potrà intervenire d'ufficio per garantire l'osservanza del regolamento da parte delle società di telecomunicazione.

TABELLA DI RECEPIMENTO DELLA DIRETTIVA 95/46/CE – aprile 2003

STATO	Legge nazionale di recepimento	Entrata in vigore
AUSTRIA	*Datenschutzgesetz 2000* (Legge sulla tutela dei dati 2000) del 17 agosto 1999	1 gennaio 2000
BELGIO	Legge dell'8 dicembre 1992 sulla tutela della *privacy* nel trattamento di dati personali, così come modificata dalla Legge 11 dicembre 1998, di trasposizione della direttiva 95/46/CE	1 settembre 2001
DANIMARCA	Legge n. 429 del 31 maggio 2000	1 luglio 2001
FINLANDIA	Legge n. 523/99	1 giugno 1999
GERMANIA	*Bundesdatenschutzgesetz* (Legge federale sulla protezione dei dati) del 23 maggio 2001, e successive modificazioni	23 maggio 2001
FRANCIA	Legge "informatica e libertà" del 6 gennaio 1978 (e successive modificazioni) Sono previsti emendamenti per recepire integralmente la Direttiva	Progetto di legge (*Petite Loi*) di recepimento approvato dall'Assemblea Nazionale il 30 gennaio 2002, modificato dal Senato il 1 aprile 2003
GRECIA	Legge n. 2472 del 10 aprile 1997 (Protezione delle persone rispetto al trattamento di dati personali)	10 novembre 1997
IRLANDA	*Data Protection (Amendment) Act* 2003, del 10.04.2003, che modifica il *Data Protection Act* (Legge sulla protezione dei dati) del 13 luglio 1988.	- 1 luglio 2003 (alcune norme entreranno in vigore successivamente) - Gli articoli 4, 17, 25 e 26 della direttiva erano stati attuati con Regolamento approvato il 19 dicembre 2001, entrato in vigore il 1 aprile 2002
ITALIA	Legge 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali" (e successive modificazioni)	8 maggio 1997
LUSSEMBURGO	*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*	1 dicembre 2002
PAESI BASSI	*Wet bescherming persoonsgegevens* (Legge per la tutela dei dati personali) del 6 luglio 2000	1 marzo 2001
PORTOGALLO	Legge sulla protezione dei dati, n. 67/98, del 26 ottobre 1998	27 ottobre 1998
SPAGNA	*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (Legge organica 15/1999, del 13 dicembre, sulla protezione dei dati personali)	14 gennaio 2000
SVEZIA	*Personuppgiftslagen* (1998:204) (Legge sui dati personali) del 29 aprile 1998 (integrata dall'Ordinanza sui dati personali (1998:1991) del 3 settembre 1998)	24 ottobre 1998
UK	*Data Protection Act* 1998 (Legge sulla protezione dei dati 1998) + legislazione secondaria (regolamenti di attuazione)	1 marzo 2000

La non completa trasposizione della direttiva 95/46/CE in tutti i Paesi dell'Unione e la recente entrata in vigore di diverse normative nazionali di attuazione dei principi della stessa, da cui scaturisce necessariamente la consapevolezza di una conseguente ancora scarsa esperienza applicativa, ha consigliato alla Commissione di non farsi promotrice al momento di alcuna iniziativa tendente ad una revisione del testo della direttiva.

La Commissione ha infatti intrapreso, prima con una consultazione pubblica, poi con la sottoposizione di questionari rivolti ai governi degli Stati membri ed alle autorità di protezione dei dati, culminate con una conferenza svoltasi a Bruxelles il 30 settembre - 1 ottobre 2002, una attività tendente a valutare -secondo quanto richiestole dall'articolo 33 della direttiva- lo stato di applicazione di questa.

Secondo quanto affermato dal Commissario F. Bolkestein, in esito ai lavori della Conferenza, sembra prematuro che un primo rapporto sull'applicazione di una direttiva che ha richiesto cinque anni di negoziati contenga radicali proposte di modifiche sulla base di una così scarsa esperienza applicativa. Ciò in quanto andava infatti considerato che molti Paesi hanno trasposto in ritardo la direttiva e gran parte delle disposizioni nazionali adottate sono entrate in vigore solo nel 2000 e 2001, che la nuova legge del Lussemburgo entra in vigore nel 2003 e che due Paesi a far tempo alla data della Conferenza non avevano ancora completato le necessarie procedure legislative. La Commissione, in base alle dichiarazioni del Commissario, avrebbe pertanto deciso di concentrare la sua azione sulla ricerca di soluzioni pragmatiche, tendenti ad assicurare una uniforme e piena applicazione ed interpretazione della direttiva tra i quindici Paesi dell'Unione. Da un lato un'attività del genere potrebbe dover comportare cambiamenti in alcune legislazioni nazionali; dall'altro potrebbero essere individuati alcuni aspetti della direttiva che richiedono ulteriori azioni a livello comunitario, vuoi a fini di semplificazione dell'applicazione, vuoi a fini di ulteriore, puntuale armonizzazione. In questi casi un ruolo fortemente innovativo dovrebbe essere assegnato al Gruppo dei garanti europei.

Alcuni aspetti da approfondire a livello comunitario sono già stati individuati. Si tratta, in particolare:

- della semplificazione degli obblighi di notificazione dei trattamenti;
- della riduzione delle divergenze applicative che si registrano tra gli Stati membri,
- di uno sforzo maggiore per promuovere l'uso delle tecnologie di protezione della *privacy*;
- di una più chiara ed uniforme interpretazione delle norme della direttiva e di accordi per rendere più agile il trasferimento
- della promozione di codici di autoregolamentazione ed in particolare di codici di condotta, anche attraverso una maggiore cooperazione tra le autorità di protezione dei dati.

79 *Privacy* nelle telecomunicazioni

Come già riferito nella precedente Relazione, fin dalla metà del 2000 la Commissione aveva presentato diverse proposte di direttive tendenti a modificare quelle esistenti in materia di telecomunicazioni.

Uno dei principi informatori dell'intervento della Commissione consisteva nella necessità di tener conto del rapido sviluppo tecnologico e, pertanto, del mutato quadro dei servizi di comunicazione elettronica.

Anche la direttiva 97/66/CE doveva essere adeguata agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, per fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate.

Con la nuova proposta di direttiva la Commissione ha inteso promuovere regole neutrali rispetto alla tecnologia, che non impongano, né discriminino il ricorso ad un particolare tipo di tecnologia (da qui anche il mutamento della terminologia da *"telecomunicazioni"* a *"comunicazioni elettroniche"*). L'obiettivo ricercato era di garantire a consumatori e utenti lo stesso elevato livello di tutela indipendentemente dalla tecnologia con la quale viene fornito un determinato servizio.

La proposta di direttiva è stata discussa nel gruppo "Telecomunicazioni" del Consiglio, anche con la partecipazione attiva di rappresentanti del Garante.

Dopo l'adozione della posizione comune raggiunta dal Consiglio affari generali dell'UE il 28 gennaio 2002 ed il dialogo apertosi con il Parlamento europeo, quest'ultimo, nella sessione plenaria del 29-30 maggio, ha adottato una serie di emendamenti che riflettevano largamente una proposta di compromesso formulata dalla presidenza spagnola, in particolare in relazione all'invio di comunicazioni elettroniche non sollecitate.

Il testo è stato successivamente approvato senza discussione dal Consiglio il 25 giugno e dopo le verifiche di ordine linguistico è stato pubblicato sulla *G.U.C.E.* come direttiva 12 luglio 2002, n. 58 (2002/58/CE). Gli Stati membri dovranno trasporla entro il 31 ottobre 2003.

Tra i contenuti più importanti della direttiva, che si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica su reti pubbliche di comunicazione nella Comunità, si segnalano:

- le definizioni dei termini *chiamata, comunicazione, dati relativi al traffico, dati relativi all'ubicazione (localizzazione), servizio a valore aggiunto, posta elettronica*;
- l'introduzione delle definizioni e delle regole da rispettare in relazione all'utilizzo di

cookies ed altri dispositivi simili;
- la riaffermazione dell'obbligo di cancellare o rendere anonimi i dati relativi al traffico non più necessari ai fini della trasmissione di una comunicazione e l'autorizzazione della loro memorizzazione solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione.
- l'introduzione della nozione di *dati relativi all'ubicazione diversi dai dati relativi al traffico* e la definizione delle condizioni che ne possono legittimare il trattamento. Si tratta di dati che le reti mobili digitali possono avere la capacità di trattare e che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni. Questi dati vengono utilizzati per fornire servizi a valore aggiunto, come ad esempio i servizi di informazioni individuali sul traffico e di radioguida.

In particolare, due scelte contenute originariamente nella proposta della Commissione sono state confermate dal Consiglio: si tratta della scelta del consenso preliminare ai fini dell'inserimento dei dati personali in elenchi telefonici (art.12) che comporta, per gli abbonati, il diritto di determinare se i loro dati personali possano essere pubblicati in un elenco e, in caso affermativo, quali debbano figurarvi. La ragione della scelta si basa sulla considerazione che per i nuovi servizi di comunicazione elettronica come il *Gsm* e la posta elettronica non risulta più opportuno dare per scontato che gli utenti di tali servizi devono figurare negli elenchi pubblici in modo automatico, cioè in assenza di ulteriore loro determinazione.

La seconda scelta condivisa concerne la protezione contro le comunicazioni indesiderate effettuate, anche a mezzo della posta elettronica (inclusi *Sms* e *Mms*) a fini di *"direct marketing"*.

Questo comporta il divieto di inviare messaggi elettronici non richiesti tranne nei confronti degli abbonati che abbiano dichiarato di voler ricevere tali messaggi elettronici (art.13).

La direttiva 2002/58/CE in questo caso armonizza a livello dei quindici Stati membri il criterio del consenso preventivo (*opt in*) già introdotto in alcuni Stati, tra cui l'Italia, come criterio che legittima il trattamento. Come chiarito nella direttiva, infatti, tali forme di comunicazioni commerciali indesiderate possono da un lato essere relativamente facili ed economiche da inviare e dall'altro imporre un onere e/o un costo al destinatario. Inoltre, in taluni casi il loro volume può causare difficoltà per le reti di comunicazione elettronica e le apparecchiature terminali. Per tali forme è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi.

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

80 Profili generali

Nel confermare quanto già segnalato nella precedente Relazione riguardo al venir meno, in ambito europeo, delle occasioni di dibattito e discussione istituzionali nel settore della protezione dei dati, nel 2002 si è notata, più in generale, una disattenzione a tale tema da ricollegarsi in gran parte agli effetti dei tragici eventi dell'11 settembre, che hanno posto all'attenzione di tutte le istituzioni comunitarie il tema del terrorismo e, quindi, della lotta alla criminalità ed alla *cybercriminalità*, richiedendo alle stesse la concentrazione di gran parte delle risorse nello studio ed elaborazione di strumenti efficaci a contrastare il fenomeno. Ciò in contrasto con l'introduzione di uno specifico articolo nella Carta dei diritti fondamentali (art. 8) ed il conseguente pieno riconoscimento del ruolo che la protezione dei dati personali assume nella realizzazione e sviluppo dell'integrazione europea attraverso l'inserimento del diritto alla protezione dei dati personali nel testo di trattato che la Convenzione europea sta elaborando.

Come si è già evidenziato, non vi sono più state convocazioni del gruppo di lavoro protezione dati del Consiglio dell'UE, mentre il gruppo c.d. di *"terzo pilastro"*, denominato "Sistemi di informazione e protezione dei dati", è stato soppresso a seguito di una generale revisione dei gruppi operanti nel citato pilastro, pur essendovi stato il tempestivo intervento del Garante volto a rappresentare al Rappresentante permanente d'Italia presso l'UE la necessità che l'attività di revisione tenesse doverosamente conto -anche nel contesto della creazione di uno spazio di libertà, sicurezza e giustizia- del riconoscimento dell'importanza e della specificità della protezione dai dati personali, in quanto strettamente attinente ai diritti fondamentali della persona umana.

In questo quadro, necessariamente sono aumentati il ruolo e le competenze del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 della direttiva 95/46/CE, ed il lavoro da esso svolto per interpretare, segnalare e indirizzare, attraverso l'adozione di pareri, raccomandazioni ad altre iniziative, l'attività della Commissione europea (e, di riflesso, degli Stati membri) in relazione all'applicazione dei principi della direttiva generale in materia di protezione dei dati personali e delle specifiche ulteriori disposizioni per il settore delle comunicazioni elettroniche.

E' aumentata quindi -come meglio si vedrà nel paragrafo successivo- la visibilità del Gruppo stesso il quale, sotto la presidenza del Presidente del Garante italiano, è stato più volte richiesto di partecipare ad audizioni ed a pubblici incontri promossi dal Parlamento europeo per discutere ed approfondire temi di particolare rilevanza (l'Accordo sul *Safe Harbor* con gli Stati Uniti e, più di recente, i trattamenti di dati effettuati nell'ambito delle cooperazioni di polizia e giudiziaria, nonché i riflessi che l'introduzione di norme di ordine pubblico a seguito degli eventi dell'11 settembre da parte degli USA determina sulla protezione dei dati in Europa – caso APIS-PNR).

Il Gruppo, già in un parere adottato alla fine del 2001, aveva ribadito l'esigenza di un approccio equilibrato nella lotta al terrorismo, in particolare dopo gli eventi dell'11 settembre 2001, per far sì che il diritto alla sicurezza e il diritto alla *privacy* coesistano in maniera equilibrata, suggerendo pertanto di abbandonare l'equazione *"più sicurezza meno privacy"*, di evitare forme generalizzate di sorveglianza, di valutare le conseguenze delle misure antiterrorismo sulle libertà delle persone. Nel parere si sottolineava come la lotta al terrorismo non dovesse ridurre il livello di tutela dei diritti fondamentali che caratterizza ogni società democratica, ma che occorresse sempre rispettare determinate condizioni che costituiscono anche il fondamento delle società democratiche in cui viviamo: da questo punto di vista le numerose iniziative legislative e di altra natura approvate o in discussione a livello comunitario e nazionale in molti casi sembrano destinate ad avere un ambito di applicazione molto più ampio della lotta contro il terrorismo. Come esempio, nel parere del Gruppo viene citata la proliferazione di strumenti per il riconoscimento dell'identità, anche attraverso dispositivi biometrici, o la previsione dei reati di *"criminalità informatica"*, la cui definizione -a giudizio del Gruppo- è molto ampia e lascia spazio a interpretazioni non rispettose del principio di legalità.

L'introduzione di misure legislative negli USA volte ad imporre sanzioni alla compagnie aeree che operano voli da e per gli Stati Uniti qualora non forniscano in anticipo alle autorità statunitensi una serie di dati relativi ai passeggeri ed ai membri dell'equipaggio, anche attraverso l'accesso diretto ai dati trattati nei sistemi di prenotazione e controllo delle partenze (che non si limitano ai dati relativi ai tragitti da o verso gli USA, ma includono anche preferenze personali dei passeggeri abituali iscritti a programmi *"frequent flyer"* tra cui informazioni di tipo sanitario), ha nuovamente e specificamente determinato l'intervento del Gruppo che, nell'ottobre 2002, ha adottato un parere (n. 6/2002) nel quale ha ritenuto che, pur nel rispetto della sovranità degli Stati, una previsione normativa di tal genere (ed i conseguenti obblighi per i destinatari) ingenera difficoltà nell'applicazione della direttiva 95/46/CE cui le compagnie aeree che operano sul territorio comunitario sono soggette.

Successivamente, dopo un intervento della Commissione europea che ha ritenuto di poter negoziare una sorta di sostanziale accordo "ponte" con autorità amministrative USA, si è avuto un ampio dibattito nel Parlamento europeo, che ha chiesto un fermo ripensamento ed un vero negoziato su basi giuridiche solide ed appropriate. Il 25 marzo la Commissione *"Libertà pubbliche"* del Parlamento europeo ha organizzato un seminario per dibattere ulteriormente il tema con i diversi soggetti: Commissione europea, autorità americane, compagnie aeree, organizzazioni rappresentative dei consumatori/utenti. Al seminario sono intervenuti, anche in considerazione del ruolo rivestito di Presidente del Gruppo, il Presidente del Garante e, in qualità di Presidente dell'Autorità di controllo *Schengen*, il segretario generale del Garante.

Alla luce di quanto evidenziato ed anche in considerazione delle proposte finora maturate nel corso del lavori della Convenzione europea, che portano alla previsione di un nuovo articolo specificamente rivolto alla protezione dei dati personali, superando quindi la divisione tra materie di primo e terzo pilastro, potrebbe allora porsi la questione di una diversa e migliore collocazione del Gruppo stesso all'interno del quadro delle competenze comunitarie.

Per quanto concerne gli ulteriori aspetti di novità legati al diritto comunitario, si segnala poi la presentazione, nel giugno del 2002, da parte della Commissione europea di una propo-

sta di direttiva relativa al riutilizzo dei documenti del settore pubblico e al loro sfruttamento a fini commerciali.

La proposta di direttiva è stata esaminata dal gruppo di lavoro del consiglio *"Telecomunicazioni"* ed alle discussioni ha preso parte attiva, nell'ambito della delegazione italiana, l'Ufficio del Garante. Nel corso del Consiglio dei Ministri delle telecomunicazioni del 27-28 marzo 2003 sul testo della proposta è stato raggiunto un accordo politico.

L'intento alla base della direttiva è quello di agevolare il riutilizzo delle informazioni del settore pubblico al fine di favorire la crescita di un mercato di servizi informativi a valore aggiunto estesi in maniera omogenea a tutti gli stati membri dell'Unione, anche nella prospettiva della diffusione di nuove piattaforme di comunicazione. Secondo la Commissione, la realizzazione di servizi informativi a livello europeo è di fatto ostacolata dall'esistenza di norme e prassi diverse negli Stati membri in materia di tariffe, tempi di risposta, accordi di esclusiva e disponibilità generale dei dati ai fini del riutilizzo. Per favorire lo sviluppo di prodotti informativi a valore aggiunto e limitare le distorsioni della concorrenza sul mercato europeo, la Commissione si propone di definire attraverso la direttiva un quadro di garanzie, relative alla definizione di condizioni di mercato eque e trasparenti, tariffazione, tempi e modalità di risposta, compatibile con le normative nazionali, senza interferire sulle previsioni nazionali riguardanti il diritto di accesso e nel pieno rispetto delle disposizioni in materia di protezione dei dati personali.

Un'altra iniziativa legislativa promossa dalla Commissione, sulla quale è iniziata la discussione in seno al Consiglio e riguardo la quale il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ha espresso, il 2 luglio 2002, un parere preliminare, riguarda l'armonizzazione delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di credito al consumo.

Si tratta di una proposta di notevole ampiezza ed impatto, che prevede la creazione e gestione di banche dati ed introduce talune disposizioni per il trattamento dei dati, pur nella generale salvaguardia e richiamo delle disposizioni della direttiva 95/46/CE. L'Ufficio ne segue attentamente l'*iter*, anche al fine di formulare proposte emendative e soppressive di talune parti del testo proposto che potrebbero avere riflessi su emanandi provvedimenti interni (codici di deontologia).

Nel settore giustizia ed affari interni si segnala inoltre l'effettiva costituzione ed entrata in funzione di *Eurojust* e si registrano diverse richieste, dibattute nel gruppi di lavoro di terzo pilastro ed in ambito del Consiglio GAI, volte a consentire l'accesso al sistema informativo *Schengen* da parte di *Europol* e di consentire allo stesso di accedere ai dati della banca dati *Eurodac*. Sono anche allo studio i sistemi per rendere *Eurojust* parte di questi sistemi.

La cooperazione tra Autorità garanti in Europa

81 Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

Come anticipato nel precedente paragrafo, molto ampia ed attenta è stata l'attività svolta dal Gruppo, di cui il Presidente del Garante è stato riconfermato all'unanimità Presidente.

La conferma rappresenta un riconoscimento al lavoro svolto nei due anni del primo mandato, che ha visto, tra l'altro, la chiusura del negoziato tra USA ed UE riguardo alla tutela della *privacy* da assicurare ai cittadini europei i cui dati personali devono essere trasferiti oltreoceano, l'elaborazione delle linee guida sulla *privacy* in *Internet*, la presa di posizione sulla necessità di un approccio equilibrato nella lotta al terrorismo, l'emanazione di vari pareri sul genoma umano, sulle comunicazioni elettroniche, sul *cybercrime*, sul trattamento dei dati nel rapporto di lavoro.

L'attività del Gruppo nel corso del 2002 ha affrontato, in particolare, il rapporto tra sicurezza e *privacy*, l'uso dei dati genetici, l'espandersi delle nuove tecnologie a fini di controllo e sorveglianza, l'impatto della società elettronica e la tutela dei diritti fondamentali dei cittadini europei, il trasferimento di dati verso Paesi terzi, l'uso delle clausole contrattuali standard e l'approfondimento delle esigenze rappresentate dall'industria e dalle società multinazionali per avere un quadro di riferimento il più possibile uniforme rispetto ai principi ed ai criteri per effettuare il trasferimento stesso. Nella definizione del calendario dei lavori e nella definizione dei temi da approfondire si è tenuto in particolare conto del lavoro di "controllo" sullo stato d'applicazione della direttiva da parte della Commissione, cui si è fatto cenno nel par. 76.

Una parte rilevante dell'attività è stata concentrata sull'attenta valutazione delle sfide poste dalle nuove tecnologie, dallo sviluppo della società dell'informazione e in particolare di *Internet*. Si segnalano i pareri sulla "standardizzazione" della *privacy* in Europa (parere 1/2002 WP 57 del 30 maggio 2002), sull'uso di un identificativo unico negli apparecchi terminali di telecomunicazioni (parere 2/2002 WP 58 del 30 maggio 2002) ed i documenti di lavoro riguardanti: la determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento di dati personali su *Internet* da parte di siti non stabiliti nell'UE (WP 56 del 30 maggio 2002); primi orientamenti del Gruppo in merito ai servizi d'autenticazione *on line* (tema sul quale i lavori del Gruppo sono continuati ed hanno portato all'adozione di un più corposo documento di lavoro il 20 gennaio 2003 WP 68); la vigilanza sulle comunicazioni elettroniche sul posto di lavoro (WP 55 del 29 maggio 2002); il trattamento di dati personali tramite videosorveglianza, promosso dai componenti italiani del Gruppo, documento che, una volta adottato, è stato aperto alla pubblica consultazione sul sito della Commissione dedicati ai lavori del Gruppo (WP 67 del 25 novembre 2002).

Altri pareri hanno riguardato la proposta di direttiva in materia di credito al consumo (parere 3/2002 WP 60 del 2 luglio 2002, già richiamato), l'adeguatezza della protezione dei dati in Argentina (parere 4/2002 WP63 del 3 ottobre 2002), la determinazione adottata dai

Garanti europei della protezione dei dati nel corso della conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni (parere 5/2002 WP 64 dell'11 ottobre 2002). Il parere si riferisce alle richieste formulate dalle forze di polizia tendenti ad una preliminare, generalizzata, conservazione di tali dati e richiama al rispetto dei principi sanciti in materia, da ultimo, dall'articolo 15 della direttiva 2002 /58/Ce.

Nei primi mesi del 2003 il Gruppo ha adottato un parere sulla conservazione dei dati di traffico a fini di tariffazione (parere 1/2003 WP 69 del 29 gennaio 2003), proprio per chiarire gli ambiti che la citata direttiva offre alla possibilità di derogare al principio generale fissato all'articolo 6 in base al quale i dati relativi al traffico devono essere cancellati o resi anonimi al termine della comunicazione (chiamata o connessione).

Il Gruppo ha continuato ad occuparsi ed a seguire con grande attenzione l'applicazione ed il funzionamento dell'accordo con gli Stati Uniti (cd. *Safe Harbor*). Una prima, provvisoria valutazione, effettuata dalla Commissione nei primissimi mesi del 2002, aveva dato risultati non soddisfacenti e, in una successiva visita negli USA i rappresentanti del Gruppo avevano confermato la necessità che l'accordo fosse applicato con serietà.

Il rapporto della Commissione offriva diversi spunti di riflessione, evidenziando come, pur essendo presenti tutti. i requisiti necessari per darvi applicazione vi fosse in realtà, da parte delle non numerose imprese che avevano aderito su base volontaria al *Safe Harbor*, un deficit di trasparenza sia riguardo alle informazioni messe a disposizione dei cittadini sia riguardo alla completezza delle informazioni stesse (ad esempio, per quanto riguarda il diritto di accedere ai dati e di farli cancellare in determinati casi). Inoltre, i sei organismi per la risoluzione delle controversie (tra gli altri, *BBBOnline*, *TRUSTe*, *DMA*), ai quali le imprese USA possono demandare la gestione degli eventuali ricorsi presentati da cittadini UE, non risultavano fornire informazioni complete su come istruire i ricorsi ed autocertificare l'adesione ai meccanismi previsti dal *Safe Harbor*. Questo nonostante l'impegno profuso dalla Federal Trade Commission e dal Dipartimento per il commercio degli USA per diffondere la conoscenza dell'accordo e promuoverne la corretta applicazione.

I Garanti europei, hanno deciso lo scorso 2 luglio a *Bruxelles* di condurre un'analisi approfondita sull'attuazione dell'accordo.

Il Gruppo ha ritenuto, infatti, necessario disporre di informazioni più approfondite e aggiornate per meglio assolvere il proprio ruolo rispetto alle questioni attinenti alla protezione dei dati personali. L'obiettivo di quest'attività informativa è soprattutto quello di valutare, in uno spirito costruttivo, come superare eventuali divergenze rispetto all'attuazione di alcune disposizioni del *Safe Harbor* e colmare le lacune esistenti in termini di prassi applicative. Ciò risulta tanto più necessario se si vuole estendere l'ambito di applicazione dell'accordo ad altre tipologie di trattamento, o magari ad altri Paesi.

Il Gruppo ha richiamato, in tale situazione, la risoluzione adottata dal Parlamento europeo il 5 luglio 2000 a proposito dell'accordo di *Safe Harbor*, ed ha invitato tutte le autorità, gli enti e le associazioni interessate a collaborare per fornire informazioni aggiornate e specifiche su:

- misure per aumentare la trasparenza del funzionamento dell'Accordo;
- possibilità di definire strumenti di verifica ulteriori per quanto riguarda l'adesione all'Accordo e l'eventuale perdita dei benefici da esso derivanti (in caso di comportamenti non conseguenti);
- iniziative per migliorare fra le imprese la conoscenza dei requisiti da soddisfare per rimanere nel *Safe Harbor*;
- misure necessarie per perfezionare i meccanismi di risoluzione delle controversie, favorirne la conoscenza su entrambe le sponde dell'Atlantico e armonizzare le modalità di informazione rispetto agli esiti di tali controversie;
- iniziative da intraprendere per potenziare la cooperazione fra il *"panel"* costituito dalle autorità europee con il compito di esaminare eventuali controversie (al quale possono decidere di rivolgersi anche le imprese USA), gli organismi USA di risoluzione delle controversie previsti dall'Accordo e la *Federal Trade Commission*.

Sulla base delle informazioni raccolte il Gruppo si è riservato di adottare in tempi rapidi un parere con il quale indicare alla Commissione profili utili ai fini della valutazione complessiva del funzionamento del *Safe Harbor*. Nel prendere atto che ancora non sono stati compiutamente forniti gli elementi richiesti, il Gruppo ha dovuto riconoscere che al momento non dispone di informazioni tali da far ritenere ottimale il funzionamento dell'accordo, poi successivamente sollecitate.

Un altro tema di grande interesse sul quale i Garanti si sono pronunciati nell'autunno del 2002 ha riguardato la trasmissione da parte delle compagnie aeree di informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti (parere 6/2002 WP 66 del 24 ottobre 2002).

L'obbligo per le compagnie operanti voli da, verso ed in transito gli Stati Uniti è stato introdotto nella legislazione americana a seguito degli attentati dell'11 settembre 2001. L'imposizione di un tale vincolo, accompagnato inoltre da sanzioni che possono giungere al divieto di sorvolo ed alla perdita dei diritti di atterraggio, oltre a quelle di natura pecuniaria, ha determinato seri riflessi riguardo all'applicazione della direttiva europea in materia di protezione dei dati personali.

Il parere del Gruppo ha evidenziato i rischi della normativa statunitense ed ha richiamato al rispetto delle normative europee.

Per evitare l'entrata in vigore del sistema sanzionatorio, alcuni mesi più tardi, rappresentanti della Commissione europea e delle Dogane USA hanno iniziato un negoziato per definire le condizioni da rispettare a tal fine. Le immediate, forti reazioni del Parlamento europeo e del Gruppo hanno imposto che l'eventuale fornitura dei dati fosse il frutto di un accordo formale. Il Gruppo sta attualmente lavorando alla definizione dei tempi e modi per discutere in ordine alle soluzioni ipotizzabili.

In materia di videosorveglianza, come si è ricordato, i Garanti europei, lo scorso 2 ottobre, hanno approvato in via preliminare un importante documento in cui sono state affermate alcune regole fondamentali che tutti i titolari di trattamenti pubblici e privati effettuati attraverso sistemi di videosorveglianza dovrebbero adottare. Il documento è stato pubblicato sul

sito del Garante e su quello dell'UE ed è stato messo a disposizione per raccogliere suggerimenti ed osservazioni nell'ambito di una ampia consultazione pubblica.

Scopi leciti e chiaramente definiti, raccolta dei dati personali ridotta al minimo, adeguata informazione dei cittadini europei. Questi alcuni dei pilastri del "decalogo" messo a punto dal Gruppo per un uso delle telecamere nel pieno rispetto della riservatezza degli individui.

Il "decalogo" europeo nasce dall'esigenza di definire un quadro di riferimento uniforme ed armonico a livello comunitario riguardo all'installazione di tali sistemi, e contiene indicazioni generali (da specificare ulteriormente nei singoli settori di applicazione) che rappresentano un denominatore comune minimo al quale fare riferimento.

Le indicazioni riguardano in parte anche i trattamenti di dati che non ricadono sotto le disposizioni della direttiva sulla protezione dei dati, come ad esempio, i trattamenti effettuati per scopi di sicurezza pubblica o per il perseguimento di reati, oppure trattamenti effettuati da una persona fisica per scopi esclusivamente privati o familiari.

Come nel decalogo italiano (*Provv.* 29 novembre 2000) e in quello in adozione presso il Consiglio d'Europa, le regole messe a punto riguardano aspetti fondamentali quali l'effettiva necessità del ricorso ai sistemi di videosorveglianza, la definizione di precisi scopi in base ai quali raccogliere le immagini, la necessità di informare i cittadini circa l'installazione delle telecamere, l'adozione di misure di sicurezza.

82 La partecipazione ad altri comitati e gruppi di lavoro

Sempre nell'ambito della definizione di forme di collaborazione e scambio tra le autorità di protezione dei dati, va ricordato l'*International Working group on data protection in telecommunications* (cd. Gruppo di Berlino), che si propone come luogo di discussione ed approfondimento, non solo a livello europeo, tra esperti in materia di tecnologie ed informazione su temi quali *Internet*, crittografia, comunicazioni elettroniche.

Il gruppo nel periodo considerato ha tenuto due riunioni: la prima a *Berlino* e la seconda a *Zurigo*.

In tali incontri, oltre ai consueti aggiornamenti sullo stato di attuazione e sul completamento della disciplina inerente alla tutela dei dati personali, sono stati affrontati alcuni temi, tra cui quello delle frodi poste in essere *on line*, su cui si è soffermato il rappresentante della *Federal Trade Commission* (FTC) statunitense, che ha sollecitato lo sviluppo di forme di cooperazione transfrontaliere, caratterizzate da celerità ed efficacia e basate su una ampia conservazione dei dati di traffico e la loro *disclosure* (a prescindere dal consenso dell'interessato) in caso di richiesta da parte dei soggetti incaricati di svolgere le indagini. Da parte europea sono stati rappresentati gli ostacoli alla realizzazione di questa attività dal punto di vista della tutela della *privacy* individuale, con particolare riguardo alla *data retention* (pur nell'ambito di un bilanciamento con le esigenze di *enforcement*).

Altri temi hanno riguardato la diffusione di dati personali via *Internet*, l'invio di *Mms* (tema sul quale il Garante si è recentemente pronunciato e che ha fornito lo spunto per un intervento del rappresentante dell'Autorità presente all'incontro, l'invio di comunicazioni commerciali non sollecitate, sul quale le Autorità di protezione dei dati belga e francese hanno richiesto al pubblico di inviare segnalazioni e denunce (è in corso di completamento l'analisi di quelle ricevute).

Nel 2002 sono proseguiti gli incontri organizzati con cadenza semestrale ai fini dello scambio di informazioni e della definizione di un *modus operandi* comune per la trattazione dei ricorsi e delle segnalazioni presentati alle autorità nazionali per la protezione dei dati, con particolare riguardo ai casi che, per la loro rilevanza o per la natura delle parti interessate, travalichino l'ambito nazionale. I due seminari si sono tenuti rispettivamente a *Dublino* il 14-15 marzo 2002 ed a *Berlino* il 25-26 novembre 2002 ("*Complaints Handling Workshops*").

Nel seminario di *Dublino* è stata dedicata particolare attenzione al tema dei flussi transfrontalieri di dati, con un approfondimento in merito ai poteri ispettivi e di controllo delle autorità nazionali. In particolare, sono stati presentati i risultati di un questionario sull'argomento fatto circolare fra tutte le autorità dell'UE. Ne è emerso un quadro piuttosto variegato, soprattutto per quanto concerne i criteri di effettuazione delle indagini ispettive in loco ed i poteri sanzionatori delle Autorità. Una tabella comparativa dei risultati è stata resa disponibile attraverso CIRCA ed è stata anche presentata alla *Spring Conference* di *Bonn* delle Autorità europee di protezione dei dati.

Il tema ha avuto ulteriori approfondimenti nel successivo incontro tenutosi a *Berlino* nel mese di novembre 2002, con un'analisi dei risultati del questionario. E' stata anche presentata la procedura seguita in Germania, in coordinamento tra le autorità dei singoli *Laender*, ai fini della valutazione di codici di condotta per il trasferimento di dati da parte di multinazionali.

Al seminario, che ha visto la partecipazione di un numero elevato di delegazioni (circa 24) in rappresentanza di tutte le Autorità garanti dell'UE e dei Paesi candidati all'adesione, sono stati anche oggetto di confronto altri temi, quali:

- la videosorveglianza, con una rassegna dei principali casi nei vari Paesi (il Garante ha illustrato i princìpi indicati del c.d. "decalogo");
- la procedura di trattazione dei ricorsi da parte dell'Autorità inglese, incentrata sull'obbligatoria compilazione di un modello per la presentazione di tali atti e sulla risoluzione preventiva dei problemi segnalati, in modo da evitare il contenzioso o l'applicazione di sanzioni, ed il trasferimento di dati all'estero.

Particolare interesse ha suscitato la trattazione del tema relativo alle cosiddette "centrali dei rischi creditizi": la Francia ha illustrato la situazione normativa esistente in Usa, Germania e UK, mentre il Garante ha presentato il provvedimento adottato in materia nel mese di novembre 2001.

Nel marzo del 2003, si è tenuto a *Varsavia* il VII seminario, cui hanno partecipato anche rappresentanti dei futuri Paesi membri dell'UE. Ad essi sono state fornite alcune indicazioni di metodo basate sull'esperienza sinora raccolta ed è stata condotta un'analisi delle modalità di trattazione di ricorsi e segnalazioni a livello nazionale, evidenziando le tipologie dei principali problemi incontrati e le soluzioni messe in atto.

Fra i temi esaminati in modo più specifico, occorre menzionare le cosiddette *"black lists"*, rispetto alle quali sono state evidenziate alcune importanti discrepanze anche nella normativa dei singoli Paesi UE. In parte connesso a tale tematica è il funzionamento delle cosiddette "centrali rischi": le delegazioni hanno sottolineato l'opportunità di elaborare una serie di indicazioni a livello comunitario, eventualmente attraverso il coinvolgimento del Gruppo per la tutela delle persone con riguardo ai dati personali.

Un terzo punto affrontato riguarda i trasferimenti di dati personali all'estero, anche alla luce degli sviluppi più recenti a livello comunitario. La delegazione italiana ha sintetizzato quattro casi emblematici relativi ad importanti società multinazionali alle quali erano stati chiesti chiarimenti in merito alle metodologie adottate; ne è emerso che i molteplici strumenti già oggi disponibili sembrano consentire di rispondere in modo adeguato alle esigenze di circolazione dei dati prospettate da aziende anche di grandi dimensioni. Si è concordato sull'esigenza di individuare un approccio uniforme, soprattutto onde evitare il rischio di un *authority shopping* da parte delle aziende; a tale scopo, si è proposto di potenziare l'uso degli strumenti offerti dallo spazio *web* di discussione CIRCA. Questo ed altri temi (trattamento di dati biometrici, bilanciamento di interessi, iniziative di sensibilizzazione) saranno approfonditi nel corso del prossimo *workshop*, che si terrà a Roma.

L'Autorità di controllo comune Schengen

83 L'attività dell'Autorità

L'Autorità comune di controllo (Acc), attualmente presieduta dal segretario generale del Garante, ha proseguito la sua attività di verifica e controllo del funzionamento della parte centrale del Sistema di informazione Schengen, nel perseguimento delle finalità che la Convenzione le attribuisce.

Una parte importante delle riunioni dell'Autorità è stata rivolta ad approfondire e discutere i progetti di sviluppo del sistema consistenti nell'introduzione di nuove funzioni, in particolare al fine di combattere il terrorismo, le quali dovrebbero prevedere l'accesso e l'uso dei dati contenuti nel SIS da parte di altri organismi, quali Europol ed Eurojust.

L'Autorità in due pareri, del 1 ottobre e del 3 dicembre, ha ribadito le sue perplessità riguardo a tali progetti ed ha segnalato per alcuni aspetti la carenza di idonee motivazioni e basi legali per poter esaminare nel merito la richiesta, attese le precise disposizioni della Convenzione relative all'accesso ed all'uso dei dati.

E' stato adottato inoltre un parere, nel giugno 2002, concernente le segnalazioni nel SIS delle persone la cui identità è stata usurpata ed il modo per evitare che le stesse subiscano conseguenze negative dall'abuso perpetrato da altri. Questo parere è stato richiamato in occasione del parere sul cd. *"SIS II"* proprio per sottolineare come la previsione di un ampliamento delle categorie di dati cui accedere e dei soggetti ai quali tale accesso ed uso è consentito non deve provocare una limitazione dei diritti delle persone che hanno subito il furto dei documenti di identità.

La disamina relativa ai problemi nascenti dal previsto passaggio al nuovo Sistema d'informazione Schengen, è stata compiuta dall'Autorità anche con riferimento ad altri aspetti quali il fatto che lo stesso sarà basato su nuove piattaforme informatiche, che conterrà ulteriori categorie di informazioni e sarà costruito in vista del futuro ampliamento ed allargamento dell'Unione europea: sarà quindi compito dell'autorità sorvegliare il processo e ricordare che, in parallelo, deve esservi una corrispondente estensione delle garanzie previste dall'originaria Convenzione.

Un altro importante parere adottato dall'Autorità riafferma che la valutazione in merito alla durata della conservazione delle segnalazioni concernenti dati personali inserite nel Sistema debba essere effettuata con esclusivo riferimento all'articolo 112 della Convenzione.

L'Autorità ha inoltre deciso di rendere biennale la redazione e la conseguente pubblicazione del rapporto di attività.

Il mantenimento del dialogo aperto con il Parlamento europeo (in particolare con la

Commissione "diritti e libertà pubbliche" che ha invitato il Presidente dell'Acc ad un'audizione pubblica l'8 ottobre 2002 ed ha recepito in dicembre le proposte dell'Acc sul SIS II), ed anche con il Comitato parlamentare cui è affidato in Italia il controllo sull'attuazione delle Convenzioni Schengen ed Europol, ha consentito al Presidente dell'Autorità Schengen di essere ascoltato riguardo alle questioni emergenti.

È stato inoltre approvato l'avvio dell'istituzione di una *newsletter* dell'Acc ed il rinnovo del sito *web* su impulso della presidenza italiana.

Nel periodo considerato è proseguita l'opera di controllo svolta dal Garante sul funzionamento dell'archivio della sezione nazionale del Sistema d'informazione, anche attraverso le numerose segnalazioni pervenute da privati.

Europol

84 L'attività dell'Autorità comune di controllo e i primi casi di contenzioso

L'Autorità comune di controllo, prevista dall'art. 24 della Convenzione di applicazione dell'Accordo di Schengen, ha continuato la sua attività di verifica e controllo sulla gestione degli archivi Europol, che dal luglio 1999 comprendono gli archivi di analisi.

L'Autorità ha seguito con attenzione i progetti di negoziato sottoposti dal Direttore dell'Europol per ottenere il consenso ad iniziare le trattative ai fini di effettuare lo scambio di dati con alcuni Paesi terzi. Particolare impegno è stato posto nel seguire il negoziato per pervenire ad un accordo formale che disciplinasse, nel rispetto dei principi in materia di protezione dei dati personali sanciti nella Convenzione stessa, la fornitura di dati da Europol agli Stati Uniti.

L'Autorità, interessata da Europol in attuazione della decisione di fornire dati agli USA a seguito degli attentati dell'11 settembre, aveva infatti rappresentato la necessità di stipulare con le competenti autorità americane un accordo formale, contenente le garanzie necessarie per poter operare in piena legittimità ed aveva espresso la volontà di essere interessata al relativo negoziato. L'attività dell'Autorità è testimoniata, in particolare, dalla nota verbale aggiuntiva all'accordo per lo scambio di dati.

Sono stati inoltre espressi pareri in relazione all'apertura di *file* di analisi, alla modifica dell'Atto che definisce la trasmissione di dati da Europol a Stati ed organismi terzi, nonché in relazione alle proposte di modifica della Convenzione presentate dal regno di Danimarca.

È stata compiuta una ulteriore ispezione alla sede dell'Europol che, in particolare, si è incentrata sugli archivi di analisi e sugli sviluppi tecnologici del sistema.

È stata approvata la prima relazione di attività e sono in corso contatti per la stampa e la presentazione della stessa.

Si sta lavorando per l'apertura di una pagina dedicata all'interno del sito di Europol.

Il Comitato di appello ha ricevuto i primi ricorsi, di cui uno attualmente in trattazione.

Il controllo sul Sistema informativo doganale

85 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'articolo K3 del Trattato sull'Unione europea del 26 luglio 1995.

La convenzione mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'UE, particolarmente attraverso lo scambio di dati personali.

A tal fine è stata prevista la creazione di un sistema informativo automatizzato comune (Sistema informativo doganale-SID) che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La convenzione istituisce una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

L'Autorità ha iniziato i suoi lavori nel corso della primavera del 2002 ed ha provveduto alla nomina del Presidente e del vice presidente (quest'ultimo nella persona di un dirigente dell'Ufficio del Garante). Ha poi adottato il regolamento interno ed un parere sull'istituzione di un archivio di identificazione dei fascicoli a fini doganali.

Eurodac

86 Collaborazione tra Stati membri e garanzie per gli interessati

L'autorità comune di controllo Eurodac per il confronto delle impronte digitali dei richiedenti asilo è stata istituita ed ha tenuto la sua prima riunione nel dicembre 2002, pervenendo alla nomina del Presidente ed all'adozione del regolamento interno.

La funzionalità dell'organismo è però ben lungi dall'essere effettiva in quanto, all'atto dell'ormai imminente istituzione dell'organo di controllo indipendente di cui all'art. 286, par. 2 del Trattato di Amsterdam i compiti di supervisione e controllo provvisoriamente svolti da tale organo, saranno attribuiti al Garante europeo.

All'autorità di controllo indipendente, in attuazione appunto dell'art. 286 del Trattato di Amsterdam, il regolamento n. 45/2001 conferisce il compito di controllare la correttezza dei trattamenti di dati effettuati dalle istituzioni e dagli organismi dell'UE.

Consiglio d'Europa

87 La convenzione sul *cybercrime*

La Convenzione del Consiglio d'Europa sul *cybercrime*, sottoscritta da 30 Paesi il 23 novembre 2001, è stata finora ratificata da soli due Stati (Albania e Croazia); pertanto non è ancora entrata in vigore non essendo stato raggiunto il numero minimo richiesto di 5 ratifiche, di cui almeno 3 di Stati membri del Consiglio d'Europa.

Si ricorda che tra i firmatari figurano Paesi non membri del Consiglio d'Europa (Stati Uniti, Canada, Giappone e Sud Africa).

Successivamente è stato negoziato, ad aperto alla firma il 21 gennaio 2003, un Protocollo aggiuntivo che prevede l'estensione del campo d'applicazione della Convenzione, incluse tutte le disposizioni sostanziali e procedurali, nonché quelle che disciplinano la cooperazione internazionale, agli atti di natura razzista o xenofoba commessi per mezzo di strumenti informatici.

A cagione, e successivamente agli attentati dell'11 settembre 2001, anche il Consiglio d'Europa ha iniziato una intensa attività rivolta a rendere più efficace la reazione internazionale contro il terrorismo ed, in questo quadro, a sviluppare strumenti legali per combattere lo stesso.

Il Consiglio d'Europa aveva già, fin dal 1977, adottato una specifica Convenzione sull'eliminazione del terrorismo.

Dopo gli attentati dell'11 settembre, il Comitato dei ministri aveva richiesto uno sforzo più incisivo. Tutti i 44 Stati membri hanno firmato la citata Convenzione ed è stato conferito un formale incarico di rivedere gli strumenti adottati dal Consiglio d'Europa in materia di lotta al terrorismo ad un Gruppo -il GMT o Gruppo multidisciplinare per un'azione internazionale contro il terrorismo- di cui fanno parte, oltre ai rappresentanti degli Stati membri del Consiglio d'Europa, anche Stati Uniti, Canada, Giappone, Messico e Santa Sede.

Il Gruppo ha presentato il rapporto finale delle attività formulando una proposta di protocollo emendativo della Convenzione del 1977. Nel gennaio 2003 l'Assemblea parlamentare ha adottato un parere sul testo ed il Comitato dei ministri ha formalmente approvato la proposta il 13 febbraio 2003. L'apertura alla firma è prefissata per il 15 maggio 2003.

Le proposte emendative riguardano sostanzialmente la de-politicizzazione di alcuni atti criminosi, che divengono quindi oggetto di estradizioni, oltre ad una semplificazione delle procedure per ampliare la lista dei crimini estradabili.

Il Consiglio d'Europa, ha nel contempo incaricato il Comitato diritti umani di studiare e proporre delle linee guida sulla lotta al terrorismo ed i diritti umani. Le linee-guida, che sono state adottate dal Comitato dei Ministri nel luglio 2002, costituiscono certamente il primo testo internazionale in questo campo, anche se non direttamente vincolante per gli Stati.

In esse è riaffermato l'obbligo degli Stati di proteggere chiunque nei confronti del terrorismo, di evitare arbitrarietà, di adottare misure di contrasto solo nel pieno rispetto dei principi di legalità e legittimità, ed è ribadito il divieto assoluto di sottoporre chiunque a tortura e/o trattamenti inumani e degradanti. Il quadro legale disegnato dalle linee guida -che comprende regole riguardo all'arresto, fermo e custodia da parte della polizia, detenzione preventiva, estradizione- attribuisce particolare attenzione alla raccolta e all'elaborazione di dati personali, alle misure che interferiscono con la riservatezza (come le perquisizioni, l'intercettazione di comunicazioni, ecc).

Di seguito si riporta il testo delle linee guida V e VI che riguardano più specificamente il trattamento dei dati personali e la tutela della riservatezza, segnalando che il testo completo, in francese ed in inglese, è pubblicato sul sito web del Consiglio d'Europa *www.coe.int.*

V. Collection and processing of personal data by any competent authority in the field of State security

Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular:

(i) are governed by appropriate provisions of domestic law;

(ii) are proportionate to the aim for which the collection and the processing were foreseen;

(iii) may be subject to supervision by an external independent authority.

VI. Measures which interfere with privacy

1. Measures used in the fight against terrorism that interfere with privacy (in particular body searches, house searches, bugging, telephone tapping, surveillance of correspondence and use of undercover agents) must be provided for by law. It must be possible to challenge the lawfulness of these measures before a court.

2. Measures taken to fight terrorism must be planned and controlled by the authorities so as to minimise, to the greatest extent possible, recourse to lethal force and, within this framework, the use of arms by the security forces must be strictly proportionate to the aim of protecting persons against unlawful violence or to the necessity of carrying out a lawful arrest.

88 L'attività dei gruppi di esperti

Il Protocollo addizionale alla Convenzione n. 108 del 1991, che prevede l'istituzione con compiti di verifica e controllo dei trattamenti ad autorità di controllo indipendenti e disciplina i flussi transfrontalieri di dati, aperto alla firma l'8 novembre 2001, è stato finora ratificato da tre Stati (Germania, Slovacchia, Svezia) e non è ancora entrato in vigore essendo necessarie almeno cinque ratifiche.

L'Italia è tra i Paesi firmatari, ma non ancora presentato in Parlamento il disegno di legge di ratifica.

Per quanto riguarda le modifiche alla Convenzione per consentire l'adesione alla stessa da parte delle Comunità europee, l'Italia non risulta aver firmato il relativo Protocollo emendativo.

A seguito della celebrazione del ventesimo anniversario della Convenzione, che ha fornito occasione per una verifica dell'attualità e della tenuta dei principi ivi fissati, si è deciso di concentrare maggiormente i lavori dei gruppi specializzati, il CJ-PD ed, in qualche misura anche il T-PD, o comitato "convenzionale", nell'individuazione ed adozione degli strumenti, vincolanti o meno in relazione alle materie trattate, resisi necessari per adeguare e specificare i principi della Convenzione rispetto, in particolare, agli sviluppi tecnologici ed all'uso crescente delle tecnologie elettroniche.

Il CJ-PD -il comitato che ha lavorato alla predisposizione della Convenzione n. 108 e, in seguito, all'elaborazione delle Raccomandazioni dirette a disciplinare i singoli settori in cui garantire l'applicazione della normativa in materia di tutela dei dati- ha concluso definitivamente i suoi lavori riguardo la proposta di Raccomandazione sul trattamento dei dati personali raccolti e trattati a fini assicurativi. Il testo della Raccomandazione, adottato dal Comitato dei Ministri il 18 settembre 2002 (*Racc.* 2002/9) specifica e dettaglia, con riferimento ai delicati aspetti sollevati da quel tipo di trattamento, i principi della Convenzione. Il lungo negoziato che ha portato all'adozione del testo, ed in un certo senso il progressivo alleggerimento di alcuni degli obblighi previsti, testimoniano appunto dell'importanza di affermare dei principi specifici cui riferire l'attività svolta in materia.

Nella riunione dell'ottobre 2002, il CJ-PD ha anche approvato il progetto di linee guida in materia di video sorveglianza con modificazioni di minore rilievo rispetto al testo già contenuto nella precedente Relazione. Il testo dovrà quindi essere approvato definitivamente dal Comitato dei Ministri.

Si sono inoltre conclusi, con la presentazione di un corposo rapporto, i lavori di un gruppo specializzato cui era stato affidato il non semplice compito di effettuare la terza ed ultima valutazione dell'applicazione della Raccomandazione n. 87 (15) concernente il trattamento dei

dati personali nell'attività svolta a fini di polizia e di affrontare il tema dell'applicazione dei principi della Convenzione rispetto all'attività svolta per finalità giudiziarie in materia penale.

Infatti, a differenza della direttiva comunitaria, la Convenzione del Consiglio d'Europa non esclude dal campo d'applicazione tali trattamenti, rimasti di fatto finora esclusi sulla base di una "restrittiva" interpretazione che limitava ai trattamenti automatizzati il rispetto di quei principi (ad eccezione di quei Paesi che, come l'Italia, avessero fin dalla firma predicato di volerne estendere l'applicazione anche ai trattamenti manuali o cartacei) o proprio perché all'epoca non automatizzati.

Il Gruppo ha pertanto lavorato al fine di valutare se e come le regole del processo penale vigenti nei diversi Paesi potessero essere considerate in qualche misura rispondenti ai principi della Convenzione ed ha redatto una sorta di decalogo con cui richiama l'attenzione sugli aspetti fondamentali della tutela dei dati personali.

Una parte specifica è stata dedicata ai trasferimenti di dati ed a tal fine sono stati presi in esami gli obblighi scaturenti dalle convenzioni relative all'assistenza giudiziaria in materia penale ed alla convenzione per la lotta al *cybercrime*.

Temi attualmente in trattazione concernono l'uso delle *smart card* e della biometria.

Il T-PD si è lungamente dedicato all'approfondimento del sistema legato alla definizione di clausole contrattuali tese a facilitare gli scambi di dati con Paesi non legati alla convenzione e che non dispongono di una legislazione che garantisca il richiesto livello di protezione (equivalente nel testo originario, adeguato nella dizione usata dal Protocollo aggiuntivo).

Il T-PD nelle priorità del 2003 ha inserito un approfondimento in ordine ai seguenti temi:

- i diritti della persona interessata, con possibile eventuale redazione di una sorta di guida ai diritti e doveri;
- l'applicazione dei principi della Convenzione in relazione agli sviluppi tecnologici: il gruppo si propone -ad esempio- di esaminare, alla luce della definizione data dalla Convenzione, se un indirizzo di posta elettronica o il numero di un telefono cellulare sia da considerare "dato personale" e di valutare i rischi che derivano dalla diffusione di nuove tecnologie (molteplicità dei fini, conservazione dei dati da parte dei "nuovi" media) come pure le opportunità (PETs, tecnologie non invasive ecc);
- i flussi transfrontalieri;
- l'applicazione dei principi di protezione dei dati ad *Internet*.

Prosegue inoltre l'esame delle modalità da intraprendere per razionalizzare i lavori del Consiglio d'Europa in materia di protezione dei dati personali, eventualmente anche attraverso la fusione degli stessi comitati in un'unica struttura.

89 Linee-guida in materia di sorveglianza

In particolare per le attività di videosorveglianza, che presentano specifiche problematiche per la protezione dati, il Consiglio d'Europa ha adottato, sulla base del rapporto predisposto dal segretario generale del Garante cui era stato conferito apposito incarico, un documento che individua e descrive le regole di base da rispettare da parte di qualunque soggetto, pubblico o privato, che intenda porre in essere tale attività.

Le linee-guida del documento, ampiamente illustrate nella Relazione 2001 (v. p. 145), nel richiamare il principio secondo cui l'attività di videosorveglianza deve svolgersi su base legale per fini leciti, espliciti e legittimi, afferma l'esigenza che siano adottate tutte le misure volte ad assicurare che tale attività sia conforme alla normativa in materia di protezione dei dati personali e che il ricorso alla stessa possa darsi solo quando non sia possibile utilizzare sistemi meno invasivi ed intrusivi della *privacy*.

L'attività di videosorveglianza deve, poi, conformarsi ai principi di selettività e proporzionalità rispetto agli scopi perseguiti nei singoli casi, nonché a quelli di pertinenza e non eccedenza rispetto a immagini, suoni e dati biometrici raccolti, con particolare riguardo alle modalità di raccolta e ai tempi di conservazione dei dati.

Tra le altre linee-guida individuate dal documento, figura anche il divieto di diffusione e di comunicazione dei dati a soggetti non interessati all'attività di videosorveglianza.

Di particolare rilievo sono, inoltre, le prescrizioni volte ad evitare che l'attività di videosorveglianza possa determinare discriminazioni, basate sulle opinioni, convinzioni o comportamentio di tipo sessuale, ovvero possa configurare un controllo a distanza dei lavoratori interessati. La tutela delle posizioni soggettive coinvolte può essere validamente perseguita, sulla base delle indicazioni del documento, con un'adeguata informativa ai lavoratori interessati (ed una eventuale intesa con le organizzazioni sindacali che contemperi i diritti dei lavoratori con le esigenze organizzativo-produttive o le ragioni di sicurezza sottese all'introduzione della videosorveglianza) e con una regolamentazione del diritto di accesso ai dati personali e degli altri diritti dei soggetti interessati.

O. C. S. E.

90 I risultati conseguiti nel 2002

Il Garante per la protezione dei dati personali ha partecipato anche nel 2002 ai lavori del *Working Party on Information Security and Privacy* (WPISP) all'interno del *Committee for Information, Computer and Communication Policy* (ICCP).

Il gruppo nei primi sei mesi del 2002 ha concentrato i propri sforzi per portare a termine il lavoro sulle linee-guida per la sicurezza dei sistemi informativi e delle reti, poi approvate dal Consiglio dell'O.C.S.E. il 25 luglio 2002. Il testo si propone di sensibilizzare i governi, le imprese e gli utenti rispetto ad una nuova cultura della sicurezza partendo dal riconoscimento del fatto che i sistemi informativi e le reti hanno un ruolo sempre più rilevante rispetto alla stabilità e all'efficienza delle economie nazionali e del commercio internazionale, nonché della vita sociale, culturale e politica.

L'aumento delle opportunità e delle modalità di interconnessione comporta però maggiori rischi e una maggiore vulnerabilità di tutti coloro che partecipano "alla nuova società dell'informazione". Per tale ragione è opportuno e necessario un impegno particolare al fine di tutelare la vita privata e promuovere la fiducia nei confronti dei sistemi informativi e delle reti, anche attraverso una crescente consapevolezza dei rischi e dunque una maggiore attenzione alle politiche, alle misure e alle procedure per far fronte a questi rischi.

Le linee-guida sono composte da nove principi cardine cui si dovranno ispirare, nell'elaborazione di future politiche, misure e programmi in tema di sicurezza *on-line*, tutti i governi dei paesi membri dell'O.C.S.E.. L'elenco si apre con i principi di sensibilizzazione, responsabilità e capacità di reazione rispetto ai rischi che tutti gli utilizzatori dei sistemi informativi e delle reti dovrebbero aver sempre presenti soprattutto in relazione ai danni derivanti da *deficit* di sicurezza, anche nei confronti di terzi. Si prosegue, poi, con il principio dell'etica (le parti dovrebbero rispettare i legittimi interessi di terzi), e quello di democrazia, nel quale si afferma che la sicurezza dovrebbe essere compatibile con i valori riconosciuti dalle società democratiche, e in particolare, con la libertà di manifestazione del pensiero, la libera circolazione delle informazioni, la riservatezza delle informazioni e delle comunicazioni, la protezione adeguata dei dati personali, l'apertura e la trasparenza. Seguono, infine, i principi sull'analisi dei rischi, sulla progettazione e la gestione dei sistemi informativi e delle reti in un'ottica di sicurezza, e sulla necessità di riesaminare, rivedere e modificare gli aspetti legati alla sicurezza costantemente, in modo da poter fronteggiare le nuove vulnerabilità.

Immediatamente dopo l'approvazione, il Garante ha provveduto a tradurre il documento in italiano e a pubblicarlo nel sito *web* dell'Autorità.

Nel periodo autunnale il gruppo ha lavorato per individuare le misure più efficaci a livello nazionale per diffondere e dare attuazione ai principi contenuti nelle linee-guida. A questo

proposito sembra opportuno sottolineare che all'interno dell'O.C.S.E. è stato avviato un dibattito su una possibile riforma dell'organizzazione internazionale, volta soprattutto ad aumentare il peso dei lavori prodotti in quella sede sulle politiche di sviluppo nazionali. Alla qualità dei lavori prodotti, infatti, non sembra corrispondere una effettiva incisività sulle politiche nazionali, oltre ad essere stata evidenziata la necessità di ridurre e razionalizzare un certo numero di comitati. E' stata inoltre resa nota l'intenzione della Cina di candidarsi all'adesione.

Per quanto riguarda gli argomenti più strettamente relativi alla *privacy*, sono stati elaborati due documenti dal titolo *Privacy on-line: policy and practical guidance* e *Report on compliance with, and enforcement of, privacy protection on-line.*

Il primo documento fa un inventario di tutti i lavori promossi dopo la Conferenza ministeriale di *Ottawa* del 1998 al fine di adempiere al mandato di applicare i principi contenuti nelle linee-guida del 1980 anche alle reti mondiali di comunicazioni. In particolare, si sofferma sulla necessità di a) incrementare politiche di sensibilizzazione alla *privacy on-line*; b) garantire la disponibilità in rete di adeguati rimedi giuridici in caso di inosservanza dei principi (attraverso il ricorso a sistemi alternativi rispetto al ricorso giurisdizionale cd. ADR); c) incoraggiare l'uso delle PETs (*privacy enhancing technologies*); d) incoraggiare il ricorso a soluzioni contrattuali per i trasferimenti di dati all'estero *on-line.*

Nella parte finale si invitano gli Stati a ribadire l'importanza della cooperazione internazionale e della collaborazione con il settore privato per incrementare la fiducia degli utilizzatori nelle reti; le imprese a sviluppare *privacy policies* sulla base delle linee-guida del 1980, a valutare quali strumenti di autoregolamentazione siano idonei alle loro attività, a collaborare con i governi perché l'approccio normativo e autoregolamentativo induca a nuovi modelli flessibili di implementazione in grado di coniugare il libero flusso di informazioni con la protezione dei dati personali.

Il secondo documento presenta e analizza i meccanismi di attuazione previsti nei paesi O.C.S.E. sia in caso di mancata osservanza dei principi e delle politiche in materia di *privacy*, sia per garantire l'accesso a forme di risarcimento. Esso costituirà il fondamento della valutazione concernente l'applicazione pratica degli strumenti disponibili per garantire l'osservanza e l'attuazione di tali principi e politiche in ambito telematico, nonché la loro rispondenza agli obiettivi fissati nelle linee-guida del 1980.

Per quanto riguarda il programma di lavoro per il prossimo biennio sono state avanzate numerose proposte tutte attinenti alla *trust-economy*, con riferimento alle aspettative di *privacy* non tutelate dal mercato, alle azioni congiunte da parte dei settori pubblico e privato per accrescere la fiducia dei consumatori e al circolo virtuoso generato dall'incremento di fiducia dovuto all'applicazione di adeguate misure volte a tutelare la *privacy.*

91 Ulteriori iniziative

Il Garante ha costantemente partecipato a numerose conferenze europee e di rilievo mondiale nelle quali sono stati trattate importanti tematiche di rilevante attualità per il nostro Paese.

Il 25 e 26 aprile 2002 si è svolta a *Bonn* la Conferenza di primavera delle Autorità europee per la protezione dei dati personali, cui hanno preso parte 20 paesi. La prima sessione di lavori si è occupata del rapporto fra le disposizioni in materia di sicurezza – emanate in seguito agli eventi dell'11 settembre 2001 – e la tutela del diritto alla riservatezza. E' stato ribadito, ancora una volta, che l'esigenza di maggiore sicurezza non confligge con un elevato livello di garanzie per i diritti fondamentali dei cittadini, e in particolare con il diritto alla *privacy*. Si è poi discusso del tema della biometria, soprattutto con riferimento alle procedure di identificazione che, grazie al progresso tecnologico, consentono di individuare l'identità personale a partire dalle impronte digitali, dai punti di riferimento facciali, dagli occhi, dal portamento etc., a costi sempre minori. La raccolta di dati personali attraverso queste tecniche, e la loro conservazione, è un problema emergente in tutti gli ordinamenti nazionali. Fra gli altri temi trattati, meritano una menzione i programmi di *e-government*, la certificazione delle politiche *privacy* portate avanti dalle imprese e la collaborazione con i paesi dell'est.

Dal 9 all'11 settembre 2002 si è tenuta a *Cardiff* la 24° Conferenza mondiale sulla *privacy*. Nell'incontro sono stati affrontati numerosi argomenti di particolare interesse, fra i quali devono essere menzionati l'impatto della *privacy* come leva per una maggiore efficienza del settore pubblico e privato, il ruolo della tecnologia al fine di proteggere la *privacy* nella diffusione delle informazioni, il trattamento di dati svolto al fine di valutare la solvibilità rispetto al credito e la difficoltà di preservare l'anonimato nell'era della globalizzazione, dell'informazione e del terrorismo internazionale. La sessione finale è stata dedicata al ruolo delle Autorità indipendenti come organismi che, pur mantenendo nella sfera pubblica decisioni socialmente ed economicamente rilevanti, si pongono fuori dalla tradizionale divisione dei poteri, e contribuiscono così ad incrementare il sistema di pesi e contrappesi fondamentale per la democraticità dei sistemi. E' stato rilevato, inoltre, che il modello dell'Autorità indipendente non è una prerogativa solo dei sistemi europei, ma si è imposto anche in Canada, in America Latina, in Asia e perfino negli Stati Uniti sono state avanzate proposte in questo senso. La protezione dei dati personali è divenuta una componente essenziale del nuovo concetto di cittadinanza scaturito da una realtà dominata dai rischi dell'uso massiccio delle tecnologie dell'informazione e dalla creazione di grandi banche dati. Come ha sostenuto nel suo intervento il Presidente del Garante italiano *"siamo sempre più conosciuti da soggetti pubblici e privati attraverso i nostri dati personali in forme che possono incidere sul principio di uguaglianza, sulla libertà di comunicazione, di espressione o di circolazione, sul diritto alla salute, sulla condizione di lavoratore, sull'accesso al credito e alle assicurazioni"*. I Garanti per la *privacy* europei si sono nell'occasione fermamente espressi in senso contrario circa l'introduzione generalizzata - e, quindi, senza tener conto delle garanzie e dei limiti previsti da vari strumenti internazionali e comunitari (da

ultimo, la direttiva n. 2002/58/CE pubblicata il 31 luglio 2002) - di obblighi di conservazione di dati di traffico relativi a telefonate, *e-mail*, *sms*, collegamenti *Internet*, per generiche finalità di polizia e di giustizia. Le Autorità europee considerano infatti "sproporzionata ed inaccettabile" l'ipotesi avanzata dai governi europei di registrare sistematicamente tutte le forme di telecomunicazione e comunicazione elettronica, mettendo a rischio la *privacy* dei cittadini europei. Si riporta, di seguito, il testo della Dichiarazione sulla conservazione sistematica e obbligatoria dei dati di traffico:

> *Le Autorità europee per la protezione dei dati hanno rilevato con preoccupazione che nell'ambito del Terzo Pilastro dell'UE sono all'esame alcune proposte tali da comportare la conservazione sistematica e obbligatoria dei dati di traffico relativi a tutte le forme di telecomunicazione - durata, localizzazione, numeri utilizzati per chiamate telefoniche, fax, messaggi di posta elettronica, e per altri impieghi di Internet - per un periodo di un anno o più, allo scopo di consentire l'eventuale accesso da parte delle forze dell'ordine e degli organismi preposti alla sicurezza.*
>
> *Le Autorità europee per la protezione dei dati dubitano fortemente della legittimità e liceità di misure dotate di tale ampiezza. Desiderano inoltre richiamare l'attenzione sui costi eccessivi che ciò comporterebbe per le imprese operanti nel settore telecomunicazioni ed Internet e sull'assenza di misure analoghe negli USA.*
>
> *Le Autorità europee per la protezione dei dati hanno più volte sottolineato che una conservazione siffatta costituirebbe un'indebita compressione dei diritti fondamentali garantiti ai singoli dall'articolo 8 della Convenzione europea sui diritti dell'uomo, così come ulteriormente sviluppati nella giurisprudenza della Corte europea dei diritti dell'uomo (v. Parere 4/2001 del Gruppo di lavoro ex Articolo 29, istituito dalla direttiva 95/46/CE, e la Dichiarazione di Stoccolma dell'aprile 2000).*
>
> *La tutela dei dati di traffico delle telecomunicazioni è prevista attualmente anche dalla Direttiva 2002/58/CE del Parlamento europeo e del Consiglio in materia di privacy e comunicazioni elettroniche (Gazzetta Ufficiale CE L201/37), in base alla quale il trattamento dei dati di traffico è consentito, in linea di principio, ai fini della fatturazione e dei pagamenti di interconnessione.*
>
> *All'esito di una lunga e franca discussione, la conservazione dei dati di traffico per scopi connessi all'attività delle forze dell'ordine dovrebbe essere conforme alle rigide condizioni previste dall'articolo 15(1) della Direttiva - ossia, caso per caso, solo per un periodo limitato e purché necessaria, opportuna e proporzionata all'interno di una società democratica*

Da segnalare, inoltre, la Conferenza Internazionale *"Privacy, da costo a risorsa"*. Il 5 e 6 dicembre 2002 l'Autorità ha organizzato una conferenza internazionale rivolta al mondo delle imprese, il cui sottotitolo enuncia già in qualche modo i contenuti e le finalità dell'incontro: "Garanzie per i cittadini, opportunità per le imprese; i vantaggi di un mercato *privacy-oriented*". Il convegno è stato articolato in quattro sessioni rispettivamente dedicate alla tutela dei dati personali nel mercato globale, alla privacy all'interno dell'impresa, alla tutela della riservatezza nei rapporti con utenti e consumatori e alla *privacy* come volano di sviluppo economico. Ai lavori sono intervenuti come relatori esponenti di aziende multinazionali, studiosi di fama internazionale, rappresentanti di istituzioni di paesi esteri, di associazioni di categoria, di associazioni di consumatori, di altre autorità indipendenti ed alte cariche istituzionali. Al convegno, che ha avuto una elevata partecipazione di pubblico, hanno partecipato numerosi soggetti che si occupano in modo professionale di questioni attinenti alla privacy soprattutto nel

settore privato. Il convegno è partito dall'assunto che i dati personali rappresentano una risorsa fondamentale per le aziende che operano in un sistema economico caratterizzato da un incessante flusso di informazioni. La competizione nel mercato, la conquista dei clienti e la gestione dei rapporti di lavoro interni all'azienda devono svolgersi, però, nel rispetto dei diritti dei soggetti coinvolti, e in particolare del diritto alla riservatezza. Il rispetto della *privacy*, dunque, può rappresentare un valore aggiunto per le imprese, sia come impulso a organizzare più razionalmente i flussi informativi, sia come elemento fondamentale della qualità del servizio reso. La conferenza ha voluto sottolineare, inoltre, che il diritto alla protezione dei dati personali rientra nel novero dei diritti fondamentali, e che pertanto non può essere considerato esclusivamente in un'ottica di remunerazione economica. Il diritto alla riservatezza non è assimilabile ai diritti che hanno un contenuto patrimoniale e, pertanto, non si può applicare semplicisticamente l'analisi costi-benefici, trattandosi di beni non economici. Del resto, anche l'art. 41 della Costituzione afferma che l'iniziativa economica privata non possa svolgersi in modo da recare danno alla libertà e alla dignità umana. In tal senso si è affermato che il diritto alla riservatezza costituisce una precondizione di una società democratica, il cui contenuto essenziale non può essere azzerato né per motivi di sicurezza, né per ragioni di carattere economico.

Un altro tema cruciale affrontato durante la conferenza è stato quello del confronto fra il modello americano dell'autoregolamentazione e il modello europeo incentrato sulla direttiva comunitaria 95/46. Tale contrapposizione, in realtà, risulta affievolirsi sempre più, perché in Europa aumenta la rilevanza attribuita ai codici di autoregolamentazione, mentre negli Stati Uniti vengono presentati progetti di legge organici in materia di protezione dati. Il messaggio più rilevante a questo proposito và nella direzione del superamento delle differenze formali per rivolgersi alla condivisione dei diritti fondanti, ferma restando la necessità di avere una legge di riferimento entro cui inserire l'autoregolamentazione (*regulated self-regulation*).

Dal 3 al 4 aprile 2003 si è svolta a *Siviglia* la riunione annuale dei Garanti europei. In tale occasione l'Autorità, fra i diversi temi di grande rilievo, ha sottolineato la necessità di mantenere inalterato il livello di garanzie finora assicurato ai cittadini europei in materia di tutela dei dati personali.

Intervenendo nella sessione di apertura, il presidente Rodotà ha messo in guardia da qualsiasi modifica della direttiva europea rilevando che mentre da una parte si precisa e si rafforza il sistema di protezione giuridica dei dati personali, dall'altra "crescono e si fanno sempre più insistenti le pressioni perché questo livello di protezione sia concretamente ridotto per soddisfare richieste della *business community* e per rispondere ad esigenze di sicurezza interna ed internazionale". Ma l'indubbia importanza di questi diversi interessi non consente di passare a forme di bilanciamento diverse da quelle che stanno all'origine della direttiva "madre" sulla *privacy*, la 95/46, e che finirebbero per eliminare elementi essenziali della protezione dei cittadini.

Qualsiasi intervento nella materia dei dati personali deve sempre rispettare il principio di proporzionalità, mantenere sostanzialmente inalterato l'insieme dei diritti autonomamente esercitabili dal cittadino, prevedere l'esistenza di un controllo da parte di un soggetto pubblico indipendente.

I primi risultati dello studio avviato dalla Commissione europea sull'attuazione della Direttiva "smentiscono le tesi di un suo superamento e di una sua inadeguatezza soprattutto di fronte alle innovazioni tecnologiche. Questioni come lo spamming mostrano al contrario la lungimiranza di scelte essenziali come quelle riguardanti il consenso anche nella sua versione più rigorosa di *opt-in*". Quello che serve, allora, ha concluso il Presidente del Garante, è un'azione più decisa delle autorità nazionali, fornite di mezzi più adeguati e sostenute da un consenso europeo.

Un altro tema estremamente importante, sviluppato dal vicepresidente Santaniello, è quello riguardante i codici deontologici. E' stata, infatti, posta in evidenza la loro rilevanza come modello di regolazione fondato sulla autoproduzione di regole da parte delle categorie interessate. Al riguardo l'Autorità ha dato un notevole impulso alla promozione di una numerosa serie di codici deontologici e di norme di condotta. Il primo di questi codici, quello riguardante il trattamento dei dati personali da parte dei giornalisti, ha costituito il sapiente bilanciamento tra due diritti fondamentali costituzionalmente garantiti, quale il diritto di informare e quello della riservatezza. Il codice ha incontrato largo consenso da parte degli operatori dell'informazione anche perché, "senza comprimere in alcun modo il diritto di cronaca, ha introdotto in esso un elemento qualitativo come i criteri di informazione leale, trasparente, rispettosa dei valori della dignità umana".

La terza fase di sviluppo di tale codificazione ha conferito all'Autorità il compito di promuovere e guidare la formazione di sette codici deontologici. Essi assumono particolare risalto perché incidono sul sistema comunicativo, attraverso le regole inerenti ai servizi di comunicazione e informazione per via telematica; sulla gestione dei rapporti di lavoro; sulle finalità previdenziali etc. Inoltre, dettano regole sull'innovazione tecnologica riguardo a strumenti automatizzati di rilevazione di immagini e disciplinano l'ampio settore del *direct marketing*.

Un argomento di particolare attualità ha riguardato, infine, la tutela della riservatezza nel settore delle telecomunicazioni. Quello che occorre, secondo il relatore Paissan, è una vera e propria "ecologia" delle comunicazioni: il Garante più volte è stato chiamato ad abbassare la soglia del "rumore" nelle comunicazioni e a far rispettare gli spazi individuali, a partire dal diritto di essere lasciati in pace. E' stata richiamata, inoltre, l'attenzione sulla prossima realizzazione in Italia dell'elenco telefonico generale destinato a contenere i dati degli abbonati ai servizi di telefonia fissa e mobile, evidenziando la necessità di prevedere una serie di importanti garanzie quali la possibilità di limitare i dati inseriti negli elenchi a quelli necessari alla identificazione, di chiedere gratuitamente di non essere inclusi negli elenchi, di ottenere che il proprio indirizzo sia in parte omesso e, qualora ciò sia fattibile, di non essere contraddistinto da riferimenti che rivelino il sesso.

Documentazione

Testi

Normativa

92 Legge 31 dicembre 1996, n. 675 Tutela del 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 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

(2) Comma così modificato dall'art. 2, d.lg. 28 dicembre 2001, n. 467.

(3) Per quanto concerne il presente articolo, si ricorda 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.

(5) Comma così modificato dall'art. 3, comma 2, d.lg 28 dicembre 2001, n. 467.

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;

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

(6) Lettera così modificata dall'art. 3, comma 3, d.lg. 28 dicembre 2001, n. 467. In base all'art. 24, comma 1, di tale 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.

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.

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.*

(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.
(11) Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.

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;

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

(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.

(14) Lettera così modificata dall'art. 4, d.lg. 28 dicembre 2001, n. 467. In base all'art. 24, comma 1, di tale d.lg., la disposizione in oggetto si applica a decorrere dal 1 marzo 2002.

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;

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 per-*

(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

(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 tale 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."

seguire 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)

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 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 com-

(21) Lettera inserita dall'art. 6, d.lg. 28 dicembre 2001, n. 467.
(22) Lettera inserita dall'art. 5, d.lg. 30 luglio 1999, n. 281.

portamento 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, fetmi 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;

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.*

(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.
(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.

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.

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*

(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".

(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.

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.

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 speciali-

(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.*"

(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.

stiche, 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.

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.*

(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.

(37) Articolo inserito dall'art. 9, d.lg. 28 dicembre 2001, n. 467. Ai sensi dell'art. 24, comma 2, di tale 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.

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.

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

(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.
(42) Comma così modificato dall'art. 10, comma 1, d.lg. 28 dicembre 2001, n. 467.

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 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

(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.

(47) Lettera inserita dall'art. 4, comma 3, d.lg. 30 luglio 1999, n. 281.

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 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

(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.
(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.

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 trattamento conforme alle disposizioni vigenti;

d) ricevere le segnalazioni ed i reclami degli interessati o delle associazioni che li rappresentano, relativi ad inosservanze di legge o di regolamento, e provvedere sui ricorsi presentati ai sensi dell'articolo 29;

e) adottare i provvedimenti previsti dalla legge o dai regolamenti;

f) vigilare sui casi di cessazione, per qualsiasi causa, di un trattamento;

g) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle sue funzioni;

h) promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

i) curare la conoscenza tra il pubblico delle norme che regolano la materia e delle relative finalità, nonché delle misure di sicurezza dei dati di cui all'articolo 15;

l) [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.

(52) Lettera così modificata dall'art. 11, comma 1, d.lg. 28 dicembre 2001, n. 467.

(53) Lettera così modificata dall'art. 11, comma 2, d.lg 28 dicembre 2001, n. 467.

2. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla presente legge.

3. Il registro di cui al comma 1, lettera a), del presente articolo, è tenuto nei modi di cui all'articolo 33, comma 5. Entro il termine di un anno dalla data della sua istituzione, il Garante promuove opportune intese con le province ed eventualmente con altre pubbliche amministrazioni al fine di assicurare la consultazione del registro mediante almeno un terminale dislocato su base provinciale, preferibilmente nell'ambito dell'ufficio per le relazioni con il pubblico di cui all'articolo 12 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni.

4. Contro il divieto di cui al comma 1, lettera l), del presente articolo, può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

5. Il Garante e l'Autorità per l'informatica nella pubblica amministrazione cooperano tra loro nello svolgimento dei rispettivi compiti; a tal fine, invitano il presidente o un suo delegato membro dell'altro organo a partecipare alle riunioni prendendo parte alla discussione di argomenti di comune interesse iscritti all'ordine del giorno; possono richiedere, altresì, la collaborazione di personale specializzato addetto all'altro organo.

6. Le disposizioni del comma 5 si applicano anche nei rapporti tra il Garante e le autorità di vigilanza competenti per il settore creditizio, per le attività assicurative e per la radiodiffusione e l'editoria.

Art. 32. (Accertamenti e controlli)

1. Per l'espletamento dei propri compiti il Garante può richiedere al responsabile, al titolare, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

2. Il Garante, qualora ne ricorra la necessità ai fini del controllo del rispetto delle disposizioni in materia di trattamento dei dati personali, può disporre accessi alle banche di dati o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo, avvalendosi, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 2 sono disposti previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede senza ritardo sulla richiesta del Garante, con decreto motivato; le relative modalità di svolgimento sono individuate con il regolamento di cui all'articolo 33, comma 3.

4. I soggetti interessati agli accertamenti sono tenuti a farli eseguire.

5. Resta fermo quanto previsto dall'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

6. Per i trattamenti di cui agli articoli 4 e 14, comma 1, gli accertamenti sono effettuati per il tramite di un membro designato dal Garante. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, salvo che ricorrano i motivi di cui all'articolo 10, comma 4, della legge 1° aprile 1981, n. 121, come sostituito dall'articolo 42, comma 1, della presente legge, o motivi di difesa o di sicurezza dello Stato.

7. Gli accertamenti di cui al comma 6 non sono delegabili. Qualora risulti necessario in ragione della specificità della verifica, il membro designato può farsi assistere da personale specializzato che è tenuto al segreto ai sensi dell'articolo 33, comma 6. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai membri del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti al relativo ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 33, comma 3. Per gli accertamenti relativi agli organismi e ai dati di cui all'articolo 4, comma 1, lettera b),

il membro designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

Art. 33. (Ufficio del Garante)

1. Alle dipendenze del Garante è posto un ufficio composto, *in sede di prima applicazione della presente legge,*[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 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 proce-*

(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.
(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.

dimento, 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]

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.*

(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."*

(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.

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 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.

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.

(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".*

(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.

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.*

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

(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.
(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.

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 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, pre-

(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.
(80) Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

via 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 amministrativi ed agli archivi di Stato. Restano altresì ferme le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

3. Per i trattamenti di cui all'articolo 4, comma 1, lettera e), della presente legge, resta fermo l'obbligo di conferimento di dati ed informazioni di cui all'articolo 6, primo comma, lettera a), della legge 1° aprile 1981, n. 121.

CAPO X - COPERTURA FINANZIARIA ED ENTRATA IN VIGORE

Art. 44. (Copertura finanziaria)

1. All'onere derivante dall'attuazione della presente legge, valutato in lire 8.029 milioni per il 1997 ed in lire 12.045 milioni a decorrere dal 1998, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 1997-1999, al capitolo 6856 dello stato di previsione del Ministero del tesoro per l'anno 1997, all'uopo utilizzando per il 1997, quanto a lire 4.553 milioni, l'accantonamento riguardante il Ministero degli affari esteri e, quanto a lire 3.476 milioni, l'accantonamento riguardante la Presidenza del Consiglio dei ministri e, per gli anni 1998 e 1999, quanto a lire 6.830 milioni, le proiezioni per gli stessi anni dell'accantonamento riguardante il Ministero degli affari esteri e, quanto a lire 5.215 milioni, le proiezioni per gli stessi anni dell'accantonamento riguardante la Presidenza del Consiglio dei ministri.

2. Il Ministro del tesoro è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 45. (Entrata in vigore)

1. La presente legge entra in vigore centoventi giorni dopo la sua pubblicazione nella *Gazzetta Ufficiale*. Per i trattamenti svolti senza l'ausilio di mezzi elettronici o comunque automatizzati che non riguardano taluno dei dati di cui agli articoli 22 e 24, le disposizioni della presente legge si applicano a decorrere dal 1° gennaio 1998. Fermo restando quanto previsto dall'articolo 9, comma 2, della legge 30 settembre 1993, n. 388, la presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*, limitatamente ai trattamenti di dati effettuati in esecuzione dell'accordo di cui all'articolo 4, comma 1, lettera a) e alla nomina del Garante.

(80) Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123.

93 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 al-l'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 *h)*, 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:

"*b-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 puo' 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 puo' 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, cor particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevo lezza degli utenti delle reti di telecomunicazione gestite da soggetti pubblici e privati rispetto ai tipi d dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornit in linea in modo agevole ed interattivo, per favorire una piu' ampia trasparenza e correttezza nei con fronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 9 della legge 31 dicembr 1996, n. 675, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità pre scelte e il livello di sicurezza assicurato;

b) necessari per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche spe cifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativament alla pubblicazione di annunci per finalità di occupazione e alla ricezione di *curricula* contenenti dati per sonali anche sensibili;

c) effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compiment di ricerche di mercato o di comunicazione commerciale interattiva, prevedendo anche, per i casi in cu il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e render meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni;

d) svolto a fini di informazione commerciale, prevedendo anche, in correlazione con quanto previ sto dall'articolo 10, comma 4, della legge 31 dicembre 1996, n. 675, modalità semplificate per l'infor mativa all'interessato e idonei meccanismi per favorire la qualità e l'esattezza dei dati raccolti e comuni cati;

e) effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini c concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamen da parte degli interessati, individuando anche specifiche modalità per favorire la comunicazione di da personali esatti e aggiornati nel rispetto dei diritti dell'interessato;

f) provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche indi viduando i casi in cui debba essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appro priate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla rac comandazione del Consiglio d'Europa N. R (91) 10 in relazione all'articolo 9 della legge 31 dicembr 1996, n. 675;

g) effettuato con strumenti automatizzati di rilevazione di immagini, prevedendo specifiche moda lità di trattamento e forme semplificate di informativa all'interessato per garantirne la liceità e la corre tezza 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 d trattamento dei dati.

4. I codici sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante riportati in allegato al testo unico delle disposizioni in materia previsto dall'articolo 1, comma 4, dell 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: "consenton 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 seguente:

> "1-*bis*. I fornitori di cui al comma 1 sono tenuti a documentare al Garante, entro il 30 giugn 2002, le misure predisposte. In caso di mancata documentazione si applica la sanzione ammin strativa prevista dall'articolo 39, comma 1, della legge 31 dicembre 1996, n. 675. In mancan 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 serv

zio" 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 telecomun cazioni accessibili al pubblico deve predisporre procedure adeguate e trasparenti per garantir linea per linea, l'annullamento della soppressione dell'identificazione della linea chiamante d 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 deco rere dal 1 marzo 2002.

2. I provvedimenti attuativi delle disposizioni di cui agli articoli 5, comma 2, e 9 sono adottati, i sede di prima applicazione del presente decreto, entro centoventi giorni a decorrere dal 1° ottobre 200

3. In sede di prima applicazione della disposizione di cui alla lettera *a)* del comma 4 dell'articolo 2 della legge 31 dicembre 1996, n. 675, introdotta dall'articolo 8 del presente decreto, le garanzie prev ste nella medesima lettera *a)* sono determinate dall'associazione, dall'ente o dall'organismo entro il 3 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 no mativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

94 Legge 3 febbraio 2003, n. 14 "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2002." (*)

[Estratto]

Art. 26. Modifica all'articolo 1 della legge 24 marzo 2001, n. 127.

1. All'articolo 1, comma 4, della legge 24 marzo 2001, n. 127, le parole: "Il Governo emana entro dodici mesi" sono sostituite dalle seguenti: "Il Governo, al fine di consentire il previo recepimento della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali, emana, entro diciotto mesi."

(*) Pubblicata nella G. U. 7 febbraio 2003, n. 31.

95 Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale

Provvedimento n. 13 del 31 luglio 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;

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;

Visto l'art. 31, comma 1, lettera h) della legge 31 dicembre 1996, n. 675, 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 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare il relativo art. 6, comma 1, il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi di statistica e di ricerca scientifica;

Visto l'articolo 10, comma 6, del medesimo decreto legislativo n. 281/1999, relativo ad alcuni profili che devono essere individuati dal codice per i trattamenti di dati per scopi statistici e di ricerca scientifica;

Visto altresì l'articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322, come modificato dall'articolo 12, comma 6, del decreto legislativo n. 281/1999, nel quale si prevede che la Commissione per la garanzia dell'informazione statistica debba essere sentita ai fini della sottoscrizione dei codici di deontologia e di buona condotta relativi al trattamento dei dati personali nell'ambito del Sistema statistico nazionale;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla Gazzetta Ufficiale n. 46 del 25 febbraio 2000, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi del trattamento di dati personali per scopi statistici e di ricerca scientifica ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività a darne comunicazione al Garante entro il 31 marzo 2000;

Viste le comunicazioni pervenute al Garante in risposta al provvedimento del 10 febbraio 2000 , con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare alla redazione dei codici e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro, composto, fra gli altri, da rappresentanti dei seguenti sog-

getti pubblici: Istituto nazionale di statistica - ISTAT, Istituto di studi e analisi economica - ISAE, Istituto per lo sviluppo della formazione professionale dei lavoratori - ISFOL, Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica;

Considerato che il testo del codice è stato oggetto di ampia consultazione nell'ambito dei soggetti interessati, che hanno avuto modo di far pervenire osservazioni e proposte;

Visto il decreto del Presidente del Consiglio dei ministri 9 marzo 2000, n. 152 contenente le norme per la definizione dei criteri e delle procedure per l'individuazione dei soggetti privati partecipanti al Sistema statistico nazionale (SISTAN) ai sensi dell'articolo 2, comma 1, della legge 28 aprile 1998, n. 125;

Visto il decreto del Presidente del Consiglio dei ministri 9 maggio 2001 in materia di circolazione dei dati all'interno del Sistema statistico nazionale;

Visto il decreto del Presidente del Consiglio dei Ministri 28 maggio 2002 sull'inserimento di altri uffici di statistica nell'ambito del Sistan;

Vista la nota del 2 aprile 2001 con cui il Presidente dell'ISTAT, su mandato del Comitato di indirizzo e coordinamento dell'informazione statistica, ha trasmesso il testo del Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, sottoscritto dallo stesso a nome dei soggetti interessati;

Vista la deliberazione di questa Autorità n. 23 del 4 luglio 2001 sull'esame preliminare del codice;

Ritenuto opportuno procedere all'esame definitivo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici effettuati nell'ambito del SISTAN, anche separatamente rispetto al codice che, a norma degli articoli art. 6, comma 1, e 10, comma 6 , del d.lg. n. 281/1999, deve disciplinare l'utilizzo dei dati personali a fini statistici al di fuori del SISTAN;

Sentita la Commissione per la garanzia nell'informazione statistica ai sensi dell'articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322 e sulla base degli approfondimenti curati d'intesa con l'Istat;

Rilevato che il rispetto delle disposizioni contenute nel codice costituisce condizione essenziale per la liceità del trattamento dei dati personali;

Constatata la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, ed in particolare all' art. 31, comma 1, lettera h) della legge n. 675/1996, nonché agli artt. 6 e 10, 11 e 12 del decreto legislativo n. 281/1999;

Considerato che, ai sensi dell'art. 6, comma 1, del decreto legislativo n. 281/1999 , il codice deve essere pubblicato nella Gazzetta Ufficiale della Repubblica Italiana a cura del Garante;

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 nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il prof. Gaetano Rasi;

DISPONE:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, che figura in allegato, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 31 luglio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

Preambolo

Il presente codice è volto a garantire che l'utilizzazione di dati di carattere personale per scopi di statistica, considerati dalla legge di rilevante interesse pubblico e fonte dell'informazione statistica ufficiale intesa quale patrimonio della collettività, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

Il codice è sottoscritto in attuazione degli articoli 6 e 10, comma 6, del decreto legislativo 30 luglio 1999, n. 281 e si applica ai trattamenti per scopi statistici effettuati nell'ambito del sistema statistico nazionale, per il perseguimento delle finalità di cui al decreto legislativo 6 settembre 1989, n. 322.

La sua sottoscrizione è effettuata ispirandosi alle pertinenti fonti e documenti internazionali in materia di attività statistica e, in particolare:

a) alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;

b) alla Carta dei diritti fondamentali dell'Unione Europea del 18 dicembre 2000, con specifico riferimento agli artt. 7 e 8;

c) alla Convenzione n. 108 adottata a Strasburgo il 28 gennaio 1981, ratificata in Italia con legge 21 febbraio 1989, n. 98;

d) alla direttiva n. 95/46/CE del Parlamento europeo e del Consiglio dell'Unione Europea del 24 ottobre 1995;

e) alla Raccomandazione del Consiglio d'Europa n. R(97)18, adottata il 30 settembre 1997;

f) all'articolo 10 del Regolamento (CE) n. 322/97 del Consiglio dell'Unione Europea del 17 febbraio 1997.

Gli enti, gli uffici e i soggetti che applicano il seguente codice sono chiamati ad osservare anche il principio di imparzialità e di non discriminazione nei confronti di altri utilizzatori, in particolare, nell'ambito della comunicazione per scopi statistici di dati depositati in archivi pubblici e trattati da enti pubblici o sulla base di finanziamenti pubblici.

Capo I - AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

Art. 1. Ambito di applicazione

1. Il codice si applica ai trattamenti di dati personali per scopi statistici effettuati da:

a) enti ed uffici di statistica che fanno parte o partecipano al sistema statistico nazionale, per l'attuazione del programma statistico nazionale o per la produzione di informazione statistica, in conformità ai rispettivi ambiti istituzionali;

b) strutture diverse dagli uffici di cui alla lettera a), ma appartenenti alla medesima amministrazione o ente, qualora i relativi trattamenti siano previsti dal programma statistico nazionale e gli uffici di statistica

attestino le metodologie adottate, osservando le disposizioni contenute nei decreti legislativi 6 settembre 1989, n. 322 e 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni, nonché nel presente codice.

Art. 2. Definizioni

1. Ai fini del presente codice si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675 (di seguito denominata "Legge"), nel decreto legislativo 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni. Ai fini medesimi, si intende inoltre per:

a) "trattamento per scopi statistici", qualsiasi trattamento effettuato per finalità di indagine statistica o di produzione, conservazione e diffusione di risultati statistici in attuazione del programma statistico nazionale o per effettuare informazione statistica in conformità agli ambiti istituzionali dei soggetti di cui all'articolo 1;

b) "risultato statistico", l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;

c) "variabile pubblica", il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;

d) "unità statistica", l'entità alla quale sono riferiti o riferibili i dati trattati.

Art. 3. Identificabilità dell'interessato

1. Agli effetti dell'applicazione del presente codice:

a) un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati identificativi della medesima;

b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:

- risorse economiche;
- risorse di tempo;
- archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
- archivi, anche non nominativi, che forniscano ulteriori informazioni oltre a quelle oggetto di comunicazione o diffusione;
- risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
- conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;

c) in caso di comunicazione e di diffusione, l'interessato può ritenersi non identificabile se il rischio di identificazione, in termini di probabilità di identificare l'interessato stesso tenendo conto dei dati comunicati o diffusi, è tale da far ritenere sproporzionati i mezzi eventualmente necessari per procedere all'identificazione rispetto alla lesione o al pericolo di lesione dei diritti degli interessati che può derivarne, avuto altresì riguardo al vantaggio che se ne può trarre.

Art. 4. Criteri per la valutazione del rischio di identificazione

1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto dei seguenti criteri:

a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;

b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;

c) i risultati statistici relativi a sole variabili pubbliche non sono soggetti alla regola della soglia;

d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;

e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;

f) si presume che sia adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentino la medesima modalità di una variabile.

2. Nel programma statistico nazionale sono individuate le variabili che possono essere diffuse in forma disaggregata, ove ciò risulti necessario per soddisfare particolari esigenze conoscitive anche di carattere internazionale o comunitario.

3. Nella comunicazione di collezioni campionarie di dati, il rischio di identificazione deve essere per quanto possibile contenuto. Tale limite e la metodologia per la stima del rischio di identificazione sono individuati dall'Istat che, attenendosi ai criteri di cui all'art. 3, comma 1, lett. d), definisce anche le modalità di rilascio dei dati dandone comunicazione alla Commissione per la garanzia dell'informazione statistica.

Art. 5. Trattamento di dati sensibili da parte di soggetti privati

1. I soggetti privati che partecipano al sistema statistico nazionale ai sensi della legge 28 aprile 1998, n. 125, raccolgono o trattano ulteriormente dati sensibili per scopi statistici di regola in forma anonima, fermo restando quanto previsto dall'art. 6-bis, comma 1, del decreto legislativo 6 settembre 1989, n. 322, come introdotto dal decreto legislativo 30 luglio 1999, n. 281, e successive modificazioni e integrazioni.

2. In casi particolari in cui scopi statistici, legittimi e specifici, del trattamento di dati sensibili non possono essere raggiunti senza l'identificazione anche temporanea degli interessati, per garantire la legittimità del trattamento medesimo è necessario che concorrano i seguenti presupposti:

a) l'interessato abbia espresso liberamente il proprio consenso sulla base degli elementi previsti per l'informativa;

b) il titolare adotti specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo che ciò risulti irragionevole o richieda uno sforzo manifestamente sproporzionato;

c) il trattamento risulti preventivamente autorizzato dal Garante, anche sulla base di un'autorizzazione relativa a categorie di dati o tipologie di trattamenti, o sia compreso nel programma statistico nazionale.

3. Il consenso è manifestato per iscritto. Qualora la raccolta dei dati sensibili sia effettuata con particolari modalità quali interviste telefoniche o assistite da elaboratore che rendano particolarmente gravoso per l'indagine acquisirlo per iscritto, il consenso, purché espresso, può essere documentato per iscritto. In tal caso, la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso è conservata dal titolare del trattamento per tre anni.

Capo II - INFORMATIVA, COMUNICAZIONE E DIFFUSIONE

Art. 6. Informativa

1. Oltre alle informazioni di cui all'art. 10 della Legge, all'interessato o alle persone presso le quali i dati personali dell'interessato sono raccolti per uno scopo statistico è rappresentata l'eventualità che essi possono essere trattati per altri scopi statistici, in conformità a quanto previsto dai decreti legislativi 6 settembre 1989, n. 322 e 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni.

2. Quando il trattamento riguarda dati personali non raccolti presso l'interessato e il conferimento dell'informativa a quest'ultimo richieda uno sforzo sproporzionato rispetto al diritto tutelato, in base a quanto previsto dall'art. 10, comma 4 della Legge, l'informativa stessa si considera resa se il trattamento è incluso nel programma statistico nazionale o è oggetto di pubblicità con idonee modalità da comunicare preventivamente al Garante il quale può prescrivere eventuali misure ed accorgimenti.

3. Nella raccolta di dati per uno scopo statistico, l'informativa alla persona presso la quale i dati sono raccolti può essere differita per la parte riguardante le specifiche finalità, le modalità del trattamento cui sono destinati i dati, qualora ciò risulti necessario per il raggiungimento dell'obiettivo dell'indagine -in rela-

zione all'argomento o alla natura della stessa- e purché il trattamento non riguardi dati sensibili. In tali casi, il completamento dell'informativa deve essere fornito all'interessato non appena vengano a cessare i motivi che ne avevano ritardato la comunicazione, a meno che ciò comporti un impiego di mezzi palesemente sproporzionato. Il soggetto responsabile della ricerca deve redigere un documento -successivamente conservato per almeno due anni dalla conclusione della ricerca e reso disponibile a tutti i soggetti che esercitano i diritti di cui all'art. 13 della Legge- in cui siano indicate le specifiche motivazioni per le quali si è ritenuto di differire l'informativa, la parte di informativa differita, nonché le modalità seguite per informare gli interessati quando sono venute meno le ragioni che avevano giustificato il differimento.

4. Quando le circostanze della raccolta e gli obiettivi dell'indagine sono tali da consentire ad un soggetto di rispondere in nome e per conto di un altro, in quanto familiare o convivente, l'informativa all'interessato può essere data anche per il tramite del soggetto rispondente.

Art. 7. Comunicazione a soggetti non facenti parte del sistema statistico nazionale

1. Ai soggetti che non fanno parte del sistema statistico nazionale possono essere comunicati, sotto forma di collezioni campionarie, dati individuali privi di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalità che rendano questi ultimi non identificabili.

2. La comunicazione di dati personali a ricercatori di università o ad istituti o enti di ricerca o a soci di società scientifiche a cui si applica il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati fuori dal sistema statistico nazionale, di cui all'articolo 10, comma 6, del decreto legislativo 30 luglio 1999, n. 281 e successive modificazioni e integrazioni, è consentita nell'ambito di specifici laboratori costituiti da soggetti del sistema statistico nazionale, a condizione che:

- i dati siano il risultato di trattamenti di cui i medesimi soggetti del sistema statistico nazionale siano titolari;
- i dati comunicati siano privi di dati identificativi;
- le norme in materia di segreto statistico e di protezione dei dati personali, contenute anche nel presente codice, siano rispettate dai ricercatori che accedono al laboratorio anche sulla base di una preventiva dichiarazione di impegno;
- l'accesso al laboratorio sia controllato e vigilato;
- non sia consentito l'accesso ad archivi di dati diversi da quello oggetto della comunicazione;
- siano adottate misure idonee affinché le operazioni di immissione e prelievo di dati siano inibite ai ricercatori che utilizzano il laboratorio;
- il rilascio dei risultati delle elaborazioni effettuate dai ricercatori che utilizzano il laboratorio sia autorizzato solo dopo una preventiva verifica, da parte degli addetti al laboratorio stesso, del rispetto delle norme di cui alla lettera c).

3. Nell'ambito di progetti congiunti, finalizzati anche al perseguimento di compiti istituzionali del titolare del trattamento che ha originato i dati, i soggetti del sistema statistico nazionale possono comunicare dati personali a ricercatori operanti per conto di università, altre istituzioni pubbliche e organismi aventi finalità di ricerca, purché sia garantito il rispetto delle condizioni seguenti:

a) i dati siano il risultato di trattamenti di cui i medesimi soggetti del sistema statistico nazionale sono titolari;

b) i dati comunicati siano privi di dati identificativi;

c) la comunicazione avvenga sulla base di appositi protocolli di ricerca sottoscritti da tutti i ricercatori che partecipano al progetto;

d) nei medesimi protocolli siano esplicitamente previste, come vincolanti per tutti i ricercatori che partecipano al progetto, le norme in materia di segreto statistico e di protezione dei dati personali contenute anche nel presente codice.

4. È vietato ai ricercatori ammessi alla comunicazione dei dati di effettuare trattamenti per fini diversi da quelli esplicitamente previsti dal protocollo di ricerca, di conservare i dati comunicati oltre i termini di durata del progetto, di comunicare ulteriormente i dati a terzi.

Art. 8. Comunicazione dei dati tra soggetti del sistema statistico nazionale

1. La comunicazione di dati personali, privi di dati identificativi, tra i soggetti del sistema statistico nazionale è consentita per i trattamenti statistici, strumentali al perseguimento delle finalità istituzionali del soggetto richiedente, espressamente determinati all'atto della richiesta, fermo restando il rispetto dei principi di pertinenza e di non eccedenza.

2. La comunicazione anche dei dati identificativi di unità statistiche tra i soggetti del sistema statistico nazionale è consentita, previa motivata richiesta in cui siano esplicitate le finalità perseguite ai sensi del decreto legislativo 6 settembre 1989, n. 322, ivi comprese le finalità di ricerca scientifica per gli enti di cui all'art. 2 del decreto legislativo medesimo, qualora il richiedente dichiari che non sia possibile conseguire altrimenti il medesimo risultato statistico e, comunque, nel rispetto dei principi di pertinenza e di stretta necessità.

3. I dati comunicati ai sensi dei commi 1 e 2 possono essere trattati dal soggetto richiedente, anche successivamente, per le sole finalità perseguite ai sensi del decreto legislativo 6 settembre 1989, n. 322, ivi comprese le finalità di ricerca scientifica per gli enti di cui all'art. 2 del decreto legislativo medesimo, nei limiti previsti dal decreto legislativo 30 luglio 1999, n. 281, e nel rispetto delle misure di sicurezza previste dall'art. 15 della Legge e successive modificazioni e integrazioni.

Art. 9. Autorità di controllo

1. La Commissione per la garanzia dell'informazione statistica di cui all'articolo 12 del decreto legislativo 6 settembre 1989, n. 322 contribuisce alla corretta applicazione delle disposizioni del presente codice e, in particolare, di quanto previsto al precedente art. 8, segnalando al Garante i casi di inosservanza.

Capo III - SICUREZZA E REGOLE DI CONDOTTA

Art. 10. Raccolta dei dati

1. I soggetti di cui all'art. 1 pongono specifica attenzione nella selezione del personale incaricato della raccolta dei dati e nella definizione dell'organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del presente codice e la tutela dei diritti degli interessati, procedendo altresì alla designazione degli incaricati del trattamento, secondo le modalità di legge.

2. In ogni caso, il personale incaricato della raccolta si attiene alle disposizioni contenute nel presente codice e alle istruzioni ricevute. In particolare:

a) rende nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;

b) fornisce le informazioni di cui all'art. 10 della Legge e di cui all'art. 6 del presente codice, nonché ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici o indebite pressioni;

c) non svolge contestualmente presso gli stessi interessati attività di rilevazione di dati per conto di più titolari, salvo espressa autorizzazione;

d) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;

e) assicura una particolare diligenza nella raccolta di dati personali di cui agli articoli 22, 24 e 24 bis della Legge.

Art. 11. Conservazione dei dati

1. I dati personali possono essere conservati anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, in conformità all'art. 9 della Legge e all'art. 6-bis del decreto legislativo 6 settembre 1989, n. 322 e successive modificazioni e integrazioni. In tali casi, i dati identificativi possono essere conservati fino a quando risultino necessari per:

- indagini continue e longitudinali;
- indagini di controllo, di qualità e di copertura;
- definizione di disegni campionari e selezione di unità di rilevazione;
- costituzione di archivi delle unità statistiche e di sistemi informativi;

- altri casi in cui ciò risulti essenziale e adeguatamente documentato per le finalità perseguite.

2. Nei casi di cui al comma 1, i dati identificativi sono conservati separatamente da ogni altro dato, in modo da consentirne differenti livelli di accesso, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o comporti un impiego di mezzi manifestamente sproporzionati rispetto al diritto tutelato.

Art. 12. Misure di sicurezza

1. Nell'adottare le misure di sicurezza di cui all'art. 15, comma 1, della Legge e di cui al regolamento previsto dal comma 2 del medesimo articolo, il titolare del trattamento determina anche i differenti livelli di accesso ai dati personali con riferimento alla natura dei dati stessi e alle funzioni dei soggetti coinvolti nei trattamenti.

2. I soggetti di cui all'art. 1 adottano le cautele previste dagli articoli 3 e 4 del decreto legislativo 11 maggio 1999, n. 135 in riferimento ai dati di cui agli articoli 22 e 24 della Legge.

Art. 13. Esercizio dei diritti dell'interessato

1. In caso di esercizio dei diritti di cui all'art.13 della Legge, l'interessato può accedere agli archivi statistici contenenti i dati che lo riguardano per chiederne l'aggiornamento, la rettifica o l'integrazione, sempre che tale operazione non risulti impossibile per la natura o lo stato del trattamento, o comporti un impiego di mezzi manifestamente sproporzionati.

2. In attuazione dell'art. 6-bis, comma 8, del decreto legislativo 6 settembre 1989, n. 322, il responsabile del trattamento annota in appositi spazi o registri le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio, qualora tali operazioni non producano effetti significativi sull'analisi statistica o sui risultati statistici connessi al trattamento. In particolare, non si procede alla variazione se le modifiche richieste contrastano con le classificazioni e con le metodologie statistiche adottate in conformità alle norme internazionali comunitarie e nazionali.

Art. 14. Regole di condotta

1. I responsabili e gli incaricati del trattamento che, anche per motivi di lavoro, studio e ricerca abbiano legittimo accesso ai dati personali trattati per scopi statistici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti all'atto della progettazione del trattamento;

b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute;

c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attività statistica o di attività ad essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui;

d) il lavoro svolto deve essere oggetto di adeguata documentazione;

e) le conoscenze professionali in materia di protezione dei dati personali devono essere adeguate costantemente all'evoluzione delle metodologie e delle tecniche;

f) la comunicazione e la diffusione dei risultati statistici devono essere favorite, in relazione alle esigenze conoscitive degli utenti, purché nel rispetto delle norme sulla protezione dei dati personali.

2. I responsabili e gli incaricati del trattamento di cui al comma 1 sono tenuti a conformarsi alle disposizioni del presente codice, anche quando non siano vincolati al rispetto del segreto d'ufficio o del segreto professionale. I titolari del trattamento adottano le misure opportune per garantire la conoscenza di tali disposizioni da parte dei responsabili e degli incaricati medesimi.

3. I comportamenti non conformi alle regole di condotta dettate dal presente codice devono essere immediatamente segnalati al responsabile o al titolare del trattamento.

Provvedimenti del Garante

96 Autorizzazioni generali 2002 (*)

Autorizzazione n. 1/2002 al trattamento dei dati sensibili nei rapporti di lavoro [1]

Autorizzazione n. 2/2002 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale [2]

Autorizzazione n. 3/2002 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni [3]

Autorizzazione n. 4/2002 al trattamento dei dati sensibili da parte dei liberi professionisti [4]

Autorizzazione n. 5/2002 al trattamento dei dati sensibili da parte di diverse categorie di titolari [5]

Autorizzazione n. 6/2002 al trattamento di dati sensibili da parte degli investigatori privati [6]

Autorizzazione n. 7/2002 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici [7]

(*) Pubblicate nella G.U. 9 aprile 2003 n. 83, e riportate integralmente nella Relazione 2001.
(1) v. anche *www.garanteprivacy.it*, doc. n. 47611
(2) v. anche *www.garanteprivacy.it*, doc. n. 47718
(3) v. anche *www.garanteprivacy.it*, doc. n. 47751
(4) v. anche *www.garanteprivacy.it*, doc. n. 47784
(5) v. anche *www.garanteprivacy.it*, doc. n. 47890
(6) v. anche *www.garanteprivacy.it*, doc. n. 47915
(7) v. anche *www.garanteprivacy.it*, doc. n. 47939

97 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

(*) Pubblicata nella G.U. 7 maggio 2002, n. 105

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 territorio 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

ALLEGATO

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

(*) 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.

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.

(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].

(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
(4) GU L 181 del 4.7.2001, pag.19.

(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 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 garan-

tito 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.

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.

(5) Parere n.7/2001 approvato dal Gruppo di lavoro in data 13 settembre 2001.

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, 27 dicembre 2001.

Per la Commissione
Frederik BOLKESTEIN
Membro della Commissione

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**»)

(*) Notificata con il numero C(2001)4540 - testo rilevante ai fini del SEE - 2002/16/CE.

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;

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

(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.

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 norme 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;

(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.

g) che fornirà, su richiesta, alle persone interessate dai dati, una copia delle clausole del presente allegato 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.

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 ...

(1) Il paragrafo 3 è facoltativo.

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:
.....

98 Autorizzazione al trasferimento di dati personali verso il Canada - 30 aprile 2003

Provvedimento n. 6 del 30 aprile 2003

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 pararafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 20 dicembre 2001 n. 2002/2/CE (pubblicata sulla Gazzetta Ufficiale delle Comunità europee L 2/13 del 4 gennaio 2002) con la quale si è constatato che il Canada garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea ai destinatari soggetti alla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act") del 13 aprile 2000;

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, 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 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, ovvero individuate dalla Commissione europea con le decisioni previste dagli art. 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento e del Consiglio del 24 ottobre 1995 (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, comma 4, lett. g);

Visti il considerando (5) della Decisione della Commissione sull'ambito di applicazione della legge canadese e sulle tre fasi previste per l'entrata in vigore della stessa legge, nonché i considerando (6) e (7) circa la successiva approvazione di legislazioni sulla riservatezza dei dati da parte di province canadesi;

Rilevato che la Decisione della Commissione può essere modificata in ogni momento alla luce dell'esperienza acquisita nel corso della sua applicazione o di emendamenti apportati alla legislazione canadese, compresi provvedimenti che riconoscano che una provincia canadese dispone di una legislazione sostanzialmente simile (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;

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. Stefano Rodotà;

TUTTO CIÒ PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni del settore privato, aventi sede in Canada, nei cui confronti si applica la legge canadese sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act") del 13 aprile 2000, in conformità a quanto previsto alla Decisione della Commissione europea del 20 dicembre 2001 n. 2002/2/CE;

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e all'art. 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, 30 aprile 2003

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

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 (*) (2002/2/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:

(1) 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.

(2) 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.

(3) 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].

(4) 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.

(5) La legge canadese sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act") del 13 aprile 2000 [3] si applica a organizzazioni del settore privato che rilevano, usano o comunicano informazioni personali nell'ambito di attività commerciali. Essa entra in vigore in tre fasi:

Dal 1° gennaio 2001, la legge canadese si applica alle informazioni personali, purché non a carattere sanitario, rilevate, utilizzate o comunicate da organizzazioni quali imprese, stabilimenti o aziende federali. Questi tipi di organizzazioni sono presenti nel settore del trasporto aereo, bancario, radiotelevisivo, dei trasporti interprovinciali e delle telecomunicazioni. La legge canadese si applica anche a tutte le organizzazioni che comunicano dati personali dietro compenso al di fuori della provincia o del Canada e ai dati riguardanti i dipendenti di imprese, stabilimenti o aziende federali.

(*) Notificata con il numero C(2001) 4539.

(1) GU L 281 del 23.11.1995, pag. 31.

(2) WP 12: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva comunitaria sulla tutela dei dati, documento adottato dal Gruppo di lavoro il 24 luglio 1998, disponibile al seguente indirizzo:
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wpdocs_98.htm

(3) Electronically published (paper and web) versions of the Act are available at
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html and
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-F.html. Printed versions are available at Public Works and Government Services Canada - Publishing, Ottawa, Canada K1A 0S9.

Dal 1° gennaio 2002 la legge canadese si applica anche alle informazioni riguardanti la salute personale per le organizzazioni e le attività già coperte nella prima fase.

Dal 1° gennaio 2004 la legge canadese si applica a tutte le organizzazioni, federali o non federali, che rilevano, utilizzano o comunicano dati personali nell'ambito di attività commerciali. La legge canadese non si applica a organizzazioni soggette al Federal Privacy Act o regolate dal settore pubblico a livello provinciale, alle organizzazioni caritatevoli e senza scopo di lucro a meno che non siano di natura commerciale. Analogamente, essa non copre dati sui lavoratori dipendenti usati per scopi non commerciali diversi da quelli relativi ai dipendenti del settore privato regolato a livello federale. Il "Canadian Federal Privacy Commissioner" (Autorità di vigilanza canadese sulla privacy) può fornire ulteriori informazioni in tali casi.

(6) Al fine di rispettare il diritto delle province di legiferare nei loro ambiti di competenza la legge prevede che, successivamente all'approvazione di leggi provinciali sostanzialmente simili, possa essere concessa un'esenzione alle organizzazioni o attività oggetto della legislazione provinciale sulla riservatezza dei dati. La sezione 26(2) della legge canadese sulla tutela delle informazioni personali e sui documenti elettronici autorizza il gabinetto federale (se constata che la legislazione di una provincia, sostanzialmente simile alla presente parte, si applica a un'organizzazione, a una classe di organizzazioni, a un'attività o a una classe di attività) ad esentare l'organizzazione, l'attività o la classe dall'applicazione della presente parte per quanto riguarda la rilevazione, l'utilizzo o la comunicazione di informazioni personali nell'ambito di tale provincia. Il Governor in Council (gabinetto federale canadese) autorizza le esenzioni per legislazioni sostanzialmente simili tramite un Order-in-Council.

(7) Qualora una provincia adotti una legislazione sostanzialmente simile le organizzazioni, classi di organizzazioni o attività coperte saranno esentate dall'applicazione della legge federale per le transazioni all'interno della provincia; la legge federale continuerà invece ad essere applicata a tutte le attività di rilevazione, utilizzo e comunicazione di informazioni personali fra provincie nonché in tutte le situazioni per le quali le provincie non hanno previsto, integralmente o parzialmente, una legislazione sostanzialmente simile.

(8) Il 29 giugno 1984, il Canada ha aderito formalmente agli orientamenti dell'OCSE del 1980 sulla protezione della sfera privata e i flussi transfrontalieri di dati personali. Il Canada ha altresì sostenuto gli orientamenti delle Nazioni Unite riguardanti gli archivi elettronici di dati personali, adottati dall'Assemblea generale il 14 dicembre 1990.

(9) La legge canadese comprende tutti i principi fondamentali necessari a garantire un livello adeguato di protezione alle persone fisiche, contemplando però eccezioni e limitazioni per la salvaguardia di importanti interessi pubblici e per riconoscere determinate informazioni esistenti nel settore pubblico. L'applicazione di tali norme è garantita dai ricorsi giurisdizionali nonché dal controllo indipendente esercitato da autorità quali il commissario federale per la tutela della privacy (Federal Privacy Commissioner), al quale sono conferiti poteri di investigazione e intervento. Inoltre, ai casi di trattamento illecito dei dati con conseguenze pregiudizievoli per la persona, si applicano le norme di legge canadesi riguardanti la responsabilità civile.

(10) Per garantire la trasparenza e salvaguardare la capacità delle autorità competenti degli Stati membri di tutelare i cittadini per quanto riguarda il trattamento dei loro dati personali è necessario specificare nella presente decisione le circostanze eccezionali nelle quali la sospensione di determinati flussi di dati può essere giustificata, malgrado sia stato constatato un livello di protezione adeguato.

(11) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito un parere sul livello di protezione della legge canadese di cui si è tenuto conto nella preparazione della presente decisione [4].

(12) Le misure previste dalla presente decisione sono conformi al parere del comitato di cui all'articolo 31 della direttiva 95/46/CE,

(4) Parere 2/2001 sull'adeguatezza della legge canadese sulle informazioni personali e i documenti elettronici - WP 39 del 26 gennaio 2001, disponibile al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE il Canada è ritenuto fornire un adeguato livello fornisca un livello adeguato di protezione ai dati personali trasferiti dalla Comunità a destinatari soggetti alla legge sulla tutela delle informazioni personali e sui documenti elettronici ("the Canadian Act").

Articolo 2

La presente decisione riguarda solo l'adeguatezza della protezione fornita in Canada dalla legge canadese, al fine di soddisfare i requisiti di cui all'articolo 25, paragrafo 1 della direttiva 95/46/CE e non produce alcun effetto su altre condizioni o restrizioni conseguenti all'attuazione di altre disposizioni della direttiva riguardanti il trattamento dei dati personali all'interno degli Stati membri.

Articolo 3

1. Fatti salvi i poteri di intervenire al fine di garantire il rispetto dei provvedimenti nazionali adottati in conformità delle disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri hanno la facoltà di sospendere flussi di dati verso destinatari in Canada le cui attività rientrano nel campo d'applicazione della legge canadese al fine di proteggere i cittadini nell'ambito del trattamento dei loro dati personali nei casi seguenti:

a) qualora un'autorità competente canadese abbia constatato che il destinatario non rispetta le norme applicabili relative alla protezione; oppure

b) qualora sussista una sostanziale probabilità di violazione delle norme relative alla protezione; qualora vi siano motivi ragionevoli di credere che le autorità competenti canadesi non stiano o non intendano adottare misure adeguate e tempestive per risolvere il caso in questione; se, continuando il trasferimento dei dati, si verrebbe a creare un rischio imminente di grave danneggiamento delle persone cui si riferiscono i dati e le autorità competenti degli Stati membri hanno fatto il possibile, date le circostanze, per avvertire il responsabile del trattamento in Canada, dando a quest'ultimo l'opportunità di replicare.

La sospensione cesserà non appena sarà garantito il rispetto delle norme di protezione e ne sarà stata data notifica all'autorità competente in questione nella Comunità.

2. Gli Stati membri informano la Commissione immediatamente dell'adozione di provvedimenti in base al paragrafo 1.

3. Gli Stati membri e la Commissione si informano reciprocamente anche dei casi in cui l'intervento degli organismi canadesi responsabili per il rispetto delle norme di protezione non riesce a garantire tale rispetto.

4. Se le informazioni rilevate in base ai paragrafi 1, 2 e 3 provano che gli organismi canadesi incaricati di garantire il rispetto delle norme di protezione non svolgono la loro funzione in modo efficace, la Commissione avverte le autorità canadesi competenti e, se necessario, presenta progetti di misure conformemente alla procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di abrogare o sospendere la presente decisione o limitarne il campo d'applicazione.

Articolo 4

1. La presente decisione può essere modificata in qualsiasi momento, alla luce delle esperienze relative al suo funzionamento o di modifiche della legislazione canadese, compresi provvedimenti che riconoscano che una provincia canadese dispone di una legislazione sostanzialmente simile. Tre anni dopo la notifica della presente decisione agli Stati membri la Commissione ne valuta il funzionamento in base alle informazioni disponibili; essa comunica qualsiasi elemento utile al comitato istituito dall'articolo 31 della direttiva 95/46/CE, inclusi quelli in grado di influire su quanto enunciato dall'articolo 1 della presente decisione in merito all'adeguatezza della protezione canadese ai sensi dell'articolo 25 della direttiva 95/46/CE e di provare l'esistenza di discriminazioni nell'attuazione della presente decisione.

2. Se necessario, la Commissione presenta progetti di misure conformemente alla procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE.

Articolo 5

Gli Stati membri adottano tutte le misure necessarie per uniformarsi alla presente decisione entro novanta giorni dalla data di notifica della decisione stessa.

Articolo 6

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 20 dicembre 2001.

Per la Commissione
Frederik Bolkestein
Membro della Commissione

99 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'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

(*) Pubblicato nella G.U. 8 maggio 2002, n. 106.

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

Unione europea

100 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)(*)

Preambolo

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 95,

vista la proposta della Commissione [1],

visto il parere del Comitato economico e sociale [2],

visto il parere del Comitato delle regioni,

deliberando secondo la procedura di cui all'articolo 251 del trattato [3],

considerando quanto segue:

(1) 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 [4] richiede che gli Stati membri assicurino la tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali, e particolarmente del diritto alla vita privata, al fine di garantire il libero flusso dei dati personali nella Comunità.

(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(3) La riservatezza nelle comunicazioni è garantita conformemente agli strumenti internazionali relativi ai diritti dell'uomo, in particolare alla convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali e alle costituzioni degli Stati membri.

(4) 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 [5] ha tradotto i principi enunciati dalla direttiva 95/46/CE in norme specifiche per il settore delle telecomunicazioni.

(*) Pubblicata nella G.U.C.E. L 201 del 31 luglio 2002.
(1) G.U. C 365 E del 19.12.2000, pag. 223.
(2) G.U. C 123 del 25.4.2001, pag. 53.
(3) Parere del Parlamento europeo del 13 novembre 2001, posizione comune del Consiglio del 28 gennaio 2002, decisione del Parlamento europeo del 30 maggio 2002, decisione del Consiglio del 25 giugno 2002.
(4) G.U. L 281 del 23.11.1995, pag. 31.
(5) GU L 24 del 30.1.1998, pag. 1.

La direttiva 97/66/CE deve essere adeguata agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guisa da fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate. Tale direttiva dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva.

(5) Nelle reti pubbliche di comunicazione della Comunità è in atto l'introduzione di nuove tecnologie digitali avanzate che pongono esigenze specifiche con riguardo alla tutela dei dati personali e della vita privata degli utenti. Lo sviluppo della società dell'informazione è caratterizzato dall'introduzione di nuovi servizi di comunicazione elettronica. L'accesso alle reti digitali mobili è ormai a disposizione e alla portata di un vasto pubblico. Queste reti digitali hanno grandi capacità e possibilità di trattare i dati personali. Il positivo sviluppo transfrontaliero di questi servizi dipende in parte dalla fiducia che essi riscuoteranno presso gli utenti in relazione alla loro capacità di tutelare la loro vita privata.

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(8) Occorre armonizzare le disposizioni legislative, regolamentari e tecniche adottate dagli Stati membri in materia di tutela dei dati personali, della vita privata nonché del legittimo interesse delle persone giuridiche nel settore delle comunicazioni elettroniche affinché non sorgano ostacoli nel mercato interno delle comunicazioni elettroniche, ai sensi dell'articolo 14 del trattato. L'armonizzazione dovrebbe limitarsi alle prescrizioni necessarie per garantire che non vengano ostacolate la promozione e lo sviluppo di nuovi servizi e reti di comunicazione elettronica tra Stati membri.

(9) È opportuno che gli Stati membri, i fornitori e gli utenti interessati, come pure gli organi comunitari competenti, cooperino all'introduzione e allo sviluppo delle tecnologie pertinenti laddove ciò sia necessario per realizzare le garanzie previste dalla presente direttiva, tenuto debito conto dell'obiettivo di ridurre al minimo il trattamento dei dati personali e di utilizzare dati anonimi o pseudonimi nella misura del possibile.

(10) Nel settore delle comunicazioni elettroniche trova applicazione la direttiva 95/46/CE, in particolare per quanto riguarda tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali non specificamente disciplinati dalle disposizioni della presente direttiva, compresi gli obblighi del responsabile e i diritti delle persone fisiche. La direttiva 95/46/CE si applica ai servizi di comunicazione non accessibili al pubblico.

(11) La presente direttiva, analogamente alla direttiva 95/46/CE, non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(12) Gli abbonati ad un servizio di comunicazione elettronica accessibile al pubblico possono essere persone fisiche o persone giuridiche. La presente direttiva, integrando la direttiva 95/46/CE, è volta a tutelare i diritti fondamentali delle persone fisiche e in particolare il loro diritto alla vita privata, nonché i legittimi interessi delle persone giuridiche. La presente direttiva non comporta in alcun caso per gli Stati membri l'obbligo di estendere l'applicazione della direttiva 95/46/CE alla tutela dei legittimi interessi delle persone giuridiche, tutela che è assicurata nel quadro della vigente normativa comunitaria e nazionale.

(13) Il rapporto contrattuale tra abbonato e fornitore di servizi può comportare un versamento unico o periodico per il servizio fornito o che deve essere fornito. Anche le schede prepagate sono considerate un contratto.

(14) I dati relativi all'ubicazione possono riferirsi alla latitudine, longitudine ed altitudine dell'apparecchio terminale dell'utente, alla direzione di viaggio, al livello di accuratezza dell'informazione sull'ubicazione, all'identificazione della cella di rete in cui l'apparecchio terminale è ubicato in un determinato momento, e al momento in cui l'informazione sull'ubicazione è stata registrata.

(15) Una comunicazione può comprendere qualsiasi informazione relativa al nome, al numero e all'indirizzo fornita da chi emette la comunicazione o dall'utente di un collegamento al fine di effettuare la comunicazione. I dati relativi al traffico possono comprendere qualsiasi traslazione dell'informazione da parte della rete sulla quale la comunicazione è trasmessa allo scopo di effettuare la trasmissione. I dati relativi al traffico possono tra l'altro consistere in dati che si riferiscono all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo usato, all'ubicazione dell'apparecchio terminale di chi invia o riceve, alla rete sulla quale la comunicazione si origina o termina, all'inizio, alla fine o alla durata di un collegamento. Possono anche consistere nel formato in cui la comunicazione è trasmessa dalla rete.

(16) Le informazioni trasmesse nel quadro di un servizio di radiodiffusione tramite una rete di comunicazione pubblica sono destinate a un pubblico potenzialmente illimitato e non costituiscono una comunicazione ai sensi della presente direttiva. Comunque, nei casi in cui il singolo abbonato o utente che riceve tali informazioni possa essere identificato, per esempio con servizi video on demand, le informazioni trasmesse rientrano nella nozione di comunicazione ai sensi della presente direttiva.

(17) Ai fini della presente direttiva il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata come definito ed ulteriormente determinato nella direttiva 95/46/CE. Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet.

(18) Servizi a valore aggiunto possono consistere ad esempio in consigli sui pacchetti tariffari meno costosi, orientamento stradale, informazioni sul traffico, previsioni meteorologiche, e informazioni turistiche.

(19) L'applicazione di taluni requisiti relativi alla presentazione ed alla restrizione dell'identificazione della linea chiamante e collegata e al trasferimento automatico di chiamate a linee collegate a centrali analogiche non dovrebbe essere resa obbligatoria in casi specifici in cui tale applicazione risulti essere tecnicamente impossibile o richieda uno sforzo economico sproporzionato. È importante che le parti interessati siano informate di tali casi e che gli Stati membri li notifichino alla Commissione.

(20) I fornitori di servizi dovrebbero adottare misure appropriate per salvaguardare la sicurezza dei servizi da essi offerti, se necessario congiuntamente al fornitore della rete, e dovrebbero informare gli abbonati sui particolari rischi di violazione della sicurezza della rete. Tali rischi possono presentarsi segnatamente per i servizi di comunicazione elettronica su una rete aperta come l'Internet o la telefonia mobile analogica. È di particolare importanza per gli utenti e gli abbonati di tali servizi essere pienamente informati dal loro fornitore di servizi dell'esistenza di rischi alla sicurezza al di fuori della portata dei possibili rimedi esperibili dal fornitore stesso. I fornitori di servizi che offrono servizi di comunicazione elettronica accessibili al pubblico su Internet dovrebbero informare gli utenti e gli abbonati delle misure che questi ultimi possono prendere per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di pro-

grammi o tecniche di criptaggio. L'obbligo di informare gli abbonati su particolari rischi relativi alla sicurezza non esonera il fornitore di servizi dall'obbligo di prendere, a sue proprie spese, provvedimenti adeguati ed immediati per rimediare a tutti i nuovi, imprevisti rischi relativi alla sicurezza e ristabilire il normale livello di sicurezza del servizio. La fornitura all'abbonato di informazioni sui rischi relativi alla sicurezza dovrebbe essere gratuita fatta eccezione per i costi nominali che l'abbonato può sostenere quando riceve o prende conoscenza delle informazioni, per esempio scaricando un messaggio di posta elettronica. La sicurezza viene valutata alla luce dell'articolo 17 della direttiva 95/46/CE.

(21) Occorre prendere misure per prevenire l'accesso non autorizzato alle comunicazioni al fine di tutelare la riservatezza delle comunicazioni realizzate attraverso reti pubbliche di comunicazione e servizi di comunicazione elettronica accessibili al pubblico compreso il loro contenuto e qualsiasi dato ad esse relativo. La legislazione di alcuni Stati membri vieta soltanto l'accesso intenzionale non autorizzato alle comunicazioni.

(22) Il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione. Ove ciò sia necessario per rendere più efficiente l'inoltro di tutte le informazioni accessibili al pubblico ad altri destinatari del servizio su loro richiesta, la presente direttiva non osta a che tali informazioni possano essere ulteriormente memorizzate, a condizione che esse siano in ogni caso accessibili al pubblico senza restrizioni e che tutti i dati che si riferiscono ai singoli abbonati o utenti che richiedono tali informazioni siano cancellati.

(23) La riservatezza delle comunicazioni dovrebbe essere assicurata anche nel quadro di legittime prassi commerciali. Ove necessario e legalmente autorizzato, le comunicazioni possono essere registrate allo scopo di fornire la prova di una transazione commerciale. La direttiva 95/46/CE si applica a tale trattamento. Le parti in comunicazione dovrebbero essere informate sulla registrazione, il suo scopo e la durata della sua memorizzazione preventivamente alla stessa. La comunicazione registrata dovrebbe essere cancellata non appena possibile ed in ogni caso non oltre la fine del periodo durante il quale la transazione può essere impugnata legittimamente.

(24) Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. I cosiddetti software spia, bachi invisibili ("web bugs"), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza.

(25) Tuttavia, tali dispositivi, per esempio i cosiddetti marcatori ("cookies"), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di

comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi.

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati che il fornitore dei servizi di comunicazione elettronica accessibili al pubblico volesse effettuare per la commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento. I dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione o per la fornitura di servizi a valore aggiunto dovrebbero inoltre essere cancellati o resi anonimi dopo che il servizio è stato fornito. I fornitori dei servizi dovrebbero informare sempre i loro abbonati riguardo alla natura dei dati che stanno sottoponendo a trattamento, nonché agli scopi e alla durata del trattamento stesso.

(27) Il momento esatto del completamento della trasmissione di una comunicazione, dopo il quale i dati relativi al traffico dovrebbero essere cancellati salvo ai fini di fatturazione, può dipendere dal tipo di servizio di comunicazione elettronica che è fornito. Per esempio per una chiamata di telefonia vocale la trasmissione sarà completata quando uno dei due utenti termina il collegamento. Per la posta elettronica la trasmissione è completata quando il destinatario prende conoscenza del messaggio, di solito dal server del suo fornitore di servizi.

(28) L'obbligo di cancellare o di rendere anonimi i dati relativi al traffico quando non sono più necessari ai fini della trasmissione di una comunicazione non contraddice le procedure utilizzate su Internet, come la realizzazione di copie "cache", nel sistema dei nomi di dominio, di indirizzi IP o la realizzazione di copie "cache" di un indirizzo IP legato ad un indirizzo fisico o l'uso di informazioni riguardanti l'utente per controllare il diritto d'accesso a reti o servizi.

(29) Il fornitore di servizi può trattare i dati sul traffico relativi agli abbonati ed agli utenti ove necessario in singoli casi per individuare problemi tecnici od errori materiali nella trasmissione delle comunicazioni. I dati relativi al traffico necessari ai fini della fatturazione possono anche essere sottoposti a trattamento da parte del fornitore per accertare e sospendere la frode che consiste nell'uso del servizio di comunicazione elettronica senza il corrispondente pagamento.

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari. Tutte le attività relative alla fornitura del servizio di comunicazione elettronica che va oltre la trasmissione di una comunicazione e la relativa fatturazione dovrebbero essere basate su dati relativi al traffico aggregati che non possono essere collegati agli abbonati o utenti. Tali attività, se non possono essere basate su dati aggregati, dovrebbero essere considerate come servizi a valore aggiunto per i quali è necessario il consenso dell'abbonato.

(31) Si stabilirà se il consenso necessario per il trattamento dei dati personali per fornire un particolare servizio a valore aggiunto debba essere ottenuto dall'utente o dall'abbonato in base ai dati che devono essere trattati e al tipo di servizio da fornire nonché alla possibilità tecnica, procedurale e contrattuale di distinguere l'individuo che usa un servizio di comunicazione elettronica dalla persona giuridica o fisica che si è abbonata.

(32) Se il fornitore di un servizio di comunicazione elettronica o di un servizio a valore aggiunto fa ricorso a forme di subappalto a un'altra impresa per il trattamento dei dati personali necessari per la fornitura di tali servizi, questo subappalto ed il conseguente trattamento dei dati dovrebbe essere nella piena

osservanza delle disposizioni relative ai responsabili e agli incaricati del trattamento e dei dati personali come riportato nella direttiva 95/46/CE. Se la fornitura di un servizio a valore aggiunto richiede che i dati relativi al traffico o all'ubicazione siano inviati da un fornitore di servizi di comunicazione elettronica a un fornitore di servizi a valore aggiunto, gli abbonati o utenti a cui i dati si riferiscono dovrebbero essere pienamente informati di questo invio prima di dare il loro consenso al trattamento dei dati.

(33) L'introduzione di fatture dettagliate ha aumentato le possibilità dell'abbonato di verificare l'esattezza delle somme addebitate dal fornitore del servizio ma, al tempo stesso, può mettere in pericolo la vita privata degli utenti dei servizi di comunicazione elettronica accessibili al pubblico. Pertanto, per tutelare la vita privata degli utenti, gli Stati membri dovrebbero incoraggiare lo sviluppo di opzioni per i servizi di comunicazione elettronica, quali possibilità alternative di pagamento che permettano un accesso anonimo o rigorosamente privato ai servizi di comunicazione elettronica accessibili al pubblico, per esempio carte telefoniche o possibilità di pagamento con carta di credito. Allo stesso scopo, gli Stati membri possono chiedere agli operatori di offrire ai loro abbonati un tipo diverso di fattura dettagliata, dalla quale è stato omesso un certo numero di cifre dei numeri chiamati.

(34) Con riguardo all'identificazione della linea chiamante è necessario tutelare il diritto dell'autore della chiamata di eliminare l'indicazione della linea dalla quale si effettua la chiamata, nonché il diritto del chiamato di respingere chiamate da linee non identificate. In casi specifici esistono giustificati motivi per disattivare la soppressione dell'indicazione della linea chiamante. Alcuni abbonati, in particolare le linee di assistenza e servizi analoghi, hanno interesse a garantire l'anonimato dei loro chiamanti. Con riferimento all'identificazione della linea collegata, è necessario tutelare il diritto e il legittimo interesse del chiamato a sopprimere l'indicazione della linea alla quale il chiamante è realmente collegato, in particolare in caso di chiamate trasferite. I fornitori di servizi di comunicazione elettronica accessibili al pubblico dovrebbero informare i loro abbonati dell'esistenza nella rete dell'indicazione della linea chiamante e collegata, nonché di tutti i servizi offerti in base all'identificazione della linea chiamante e collegata, come pure delle opzioni disponibili per la salvaguardia della vita privata. Ciò permetterà agli abbonati di operare una scelta consapevole in merito alle possibilità di cui desiderano avvalersi a tutela della loro vita privata. Le opzioni per la salvaguardia della vita privata offerte linea per linea non devono necessariamente essere disponibili come servizio di rete automatico, ma possono configurarsi come un servizio disponibile su richiesta rivolta al fornitore del servizio di comunicazione elettronica accessibile al pubblico.

(35) Nelle reti mobili digitali i dati relativi all'ubicazione, che consentono di determinare la posizione geografica dell'apparecchiatura terminale dell'utente mobile vengono sottoposti a trattamento in modo da consentire la trasmissione di comunicazioni. Tali dati sono quelli relativi al traffico di cui all'articolo 6 della presente direttiva. Tuttavia, in aggiunta ad essi, le reti mobili digitali possono avere la capacità di trattare dati relativi all'ubicazione che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni e che vengono utilizzati per fornire servizi a valore aggiunto, come i servizi che forniscono informazioni individuali sul traffico e radioguida. Il trattamento di dati siffatti ai fini della fornitura di servizi a valore aggiunto dovrebbe essere autorizzato soltanto previo esplicito consenso dell'abbonato. Anche in questo caso, tuttavia, gli abbonati dovrebbero disporre, gratuitamente, di un mezzo semplice per bloccare temporaneamente il trattamento dei dati relativi alla loro ubicazione.

(36) Gli Stati membri possono limitare il diritto alla vita privata degli utenti e degli abbonati riguardo all'identificazione della linea chiamante allorché ciò sia necessario per identificare le chiamate importune, e riguardo all'identificazione della linea chiamante e ai dati relativi all'ubicazione allorché ciò sia necessario per consentire ai servizi di emergenza di svolgere il loro compito nel modo più efficace possibile. A tale scopo gli Stati membri possono adottare disposizioni specifiche per autorizzare i fornitori di servizi di comunicazione elettronica a fornire l'accesso all'identificazione della linea chiamante e ai dati relativi all'ubicazione senza il previo consenso degli utenti o abbonati interessati.

(37) Occorre prevedere misure per tutelare gli abbonati dal disturbo che può essere causato dal trasferimento automatico di chiamate da parte di altri. Inoltre, in tali casi, l'abbonato deve avere la possibilità di impedire che le chiamate trasferite siano inoltrate sul suo terminale, mediante una semplice richiesta al fornitore del servizio di comunicazione elettronica accessibile al pubblico.

(38) Gli elenchi degli abbonati ai servizi di comunicazione elettronica sono pubblici ed ampiamente distribuiti. Il rispetto della vita privata delle persone fisiche e i legittimi interessi delle persone giuridiche postulano, per gli abbonati, il diritto di determinare se i loro dati personali possano essere pubblicati in un elenco e, in caso affermativo, quali. È opportuno che i fornitori di elenchi pubblici informino gli abbonati che vi figureranno degli scopi dell'elenco stesso e di ogni specifico impiego che possa essere fatto delle versioni elettroniche degli elenchi pubblici, in particolare mediante le funzioni di ricerca incorporate nel software, come ad esempio le funzioni di ricerca inversa che consentono agli utenti dell'elenco di risalire al nome e all'indirizzo dell'abbonato in base al solo numero telefonico.

(39) L'obbligo di informare gli abbonati sugli scopi di elenchi pubblici in cui i loro dati personali devono essere inclusi dovrebbe essere imposto alla parte che raccoglie i dati per tale inclusione. Se i dati possono essere trasmessi a uno o più terzi, l'abbonato dovrebbe essere informato su questa possibilità e sul ricevente o sulle categorie di possibili riceventi. Le trasmissioni dovrebbero essere soggette alla condizione che i dati non possono essere usati per scopi diversi da quelli per cui sono stati raccolti. Se la parte che raccoglie i dati dall'abbonato o i terzi a cui i dati sono stati trasmessi desiderano usarli per uno scopo ulteriore, la parte che ha raccolto i dati in origine o il terzo a cui i dati sono stati trasmessi deve ottenere nuovamente il consenso dell'abbonato.

(40) Occorre prevedere misure per tutelare gli abbonati da interferenze nella loro vita privata mediante comunicazioni indesiderate a scopo di commercializzazione diretta, in particolare mediante dispositivi automatici di chiamata, telefax o posta elettronica, compresi i messaggi SMS. Tali forme di comunicazioni commerciali indesiderate possono da un lato essere relativamente facili ed economiche da inviare e dall'altro imporre un onere e/o un costo al destinatario. Inoltre, in taluni casi il loro volume può causare difficoltà per le reti di comunicazione elettronica e le apparecchiature terminali. Per tali forme di comunicazioni indesiderate a scopo di commercializzazione diretta è giustificato prevedere che le relative chiamate possano essere inviate ai destinatari solo previo consenso esplicito di questi ultimi. Il mercato unico prevede un approccio armonizzato per garantire norme semplici a livello comunitario per le aziende e gli utenti.

(41) Nel contesto di una relazione di clientela già esistente è ragionevole consentire l'uso delle coordinate elettroniche per offrire prodotti o servizi analoghi, ma unicamente da parte della medesima società che ha ottenuto le coordinate elettroniche a norma della direttiva 95/46/CE. Allorché tali coordinate sono ottenute, il cliente dovrebbe essere informato sul loro uso successivo a scopi di commercializzazione diretta in maniera chiara e distinta, ed avere la possibilità di rifiutare tale uso. Tale opportunità dovrebbe continuare ad essere offerta gratuitamente per ogni successivo messaggio a scopi di commercializzazione diretta, ad eccezione degli eventuali costi relativi alla trasmissione del suo rifiuto.

(42) Altre forme di commercializzazione diretta che siano più onerose per il mittente e non impongano costi finanziari per gli abbonati e gli utenti, quali chiamate telefoniche vocali interpersonali, possono giustificare il mantenimento di un sistema che dà agli abbonati o agli utenti la possibilità di indicare che non desiderano ricevere siffatte chiamate. Ciò nondimeno, al fine di non ridurre i livelli di tutela della vita privata esistenti, gli Stati membri dovrebbero essere autorizzati a mantenere sistemi nazionali che autorizzano tali chiamate unicamente destinate agli abbonati e agli utenti che hanno fornito il loro consenso preliminare.

(43) Al fine di facilitare l'attuazione efficace delle norme comunitarie in materia di messaggi indesiderati a scopi di commercializzazione diretta, occorre proibire l'uso di false identità o falsi indirizzi o numeri di risposta allorché sono inviati messaggi indesiderati a scopi di commercializzazione diretta.

(44) Taluni sistemi di posta elettronica consentono agli abbonati di vedere il mittente e l'oggetto di una e-mail e, inoltre, di cancellare il messaggio senza dover scaricare il resto del contenuto dell'e-mail o degli allegati, riducendo quindi i costi che potrebbero derivare dallo scaricamento di e-mail o allegati indesiderati. Queste modalità possono continuare ad essere utili in taluni casi come strumento supplementare rispetto ai requisiti generali stabiliti dalla presente direttiva.

(45) La presente direttiva non pregiudica le misure che gli Stati membri prendono per tutelare legittimi interessi delle persone giuridiche in relazione a comunicazioni indesiderate a scopo di commercializzazione diretta. Allorquando gli Stati membri costituiscono un registro "opt-out" per siffatte chiamate a persone giu-

ridiche, principalmente imprese, sono pienamente applicabili le disposizioni dell'articolo 7 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno [6] (direttiva sul commercio elettronico).

(46) Le funzionalità necessarie per la fornitura di servizi di comunicazione elettronica possono essere incorporate nella rete o in una parte qualsiasi dell'apparecchiatura terminale dell'utente, compreso il software. La tutela dei dati personali e della vita privata dell'utente di servizi di comunicazione elettronica accessibili al pubblico dovrebbe essere indipendente dalla configurazione delle varie componenti necessarie a fornire il servizio e dalla distribuzione delle necessarie funzionalità tra queste componenti. La direttiva 95/46/CE contempla tutti i tipi di trattamento dei dati personali, indipendentemente dalla tecnologia utilizzata. L'esistenza di norme specifiche per i servizi di comunicazione elettronica, oltre che di norme generali per le altre componenti necessarie per la fornitura di tali servizi, non sempre agevola la tutela dei dati personali e della vita privata in modo tecnologicamente neutrale. Può essere pertanto necessario adottare provvedimenti che prescrivano ai fabbricanti di taluni tipi di apparecchiature impiegate per i servizi di comunicazione elettronica di costruire il loro prodotto in modo da incorporarvi dispositivi che garantiscano la tutela dei dati personali e della vita privata dell'utente e dell'abbonato. L'adozione di tali provvedimenti a norma della direttiva 1999/5/CE del Parlamento europeo e del Consiglio, del 9 marzo 1999, riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità [7], avrà l'effetto di armonizzare l'introduzione nelle apparecchiature di comunicazione elettronica di determinate caratteristiche tecniche, compresi i software, volte a tutelare i dati secondo modalità compatibili con il buon funzionamento del mercato unico.

(47) La normativa nazionale dovrebbe prevedere la possibilità di adire gli organi giurisdizionali, nei casi in cui i diritti degli utenti e degli abbonati non siano rispettati. Si dovrebbero applicare sanzioni ad ogni persona, sia essa soggetta al diritto pubblico o privato, che non ottemperi alle disposizioni nazionali adottate a norma della presente direttiva.

(48) Nel campo di applicazione della presente direttiva è opportuno ricorrere all'esperienza del "gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali", composto dai rappresentanti delle autorità nazionali di controllo degli Stati membri, istituito dall'articolo 29 della direttiva 95/46/CE.

(49) Allo scopo di agevolare l'osservanza della presente direttiva, sono necessarie alcune disposizioni specifiche per il trattamento dei dati già in corso alla data di entrata in vigore delle disposizioni nazionali emanate in attuazione alla presente direttiva,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1 - Finalità e campo d'applicazione

1. La presente direttiva armonizza le disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.

2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benes-

(6) G.U. L 178 del 17.7.2000, pag. 1.
(7) G.U. L 91 del 7.4.1999, pag. 10.

sere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale.

Articolo 2 - Definizioni

Salvo diversa disposizione, ai fini della presente direttiva si applicano le definizioni di cui alla direttiva 95/46/CE e alla direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro) [8].

Si applicano inoltre le seguenti definizioni:

a) "utente": qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

d) "comunicazione": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato;

e) "chiamata": la connessione istituita da un servizio telefonico accessibile al pubblico che consente la comunicazione bidirezionale in tempo reale;

f) "consenso" dell'utente o dell'abbonato: corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE;

g) "servizio a valore aggiunto": il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

h) "posta elettronica": messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente fino a che il ricevente non ne ha preso conoscenza.

Articolo 3 - Servizi interessati

1. La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità.

2. Gli articoli 8, 10 e 11 si applicano alle linee di abbonati collegate a centrali telefoniche digitali e, qualora sia tecnicamente possibile e non richieda un onere economico sproporzionato, alle linee di abbonati collegate a centrali telefoniche analogiche.

3. Gli Stati membri notificano alla Commissione i casi in cui l'osservanza delle prescrizioni di cui agli articoli 8, 10 e 11 risulti tecnicamente impossibile o richieda un onere economico sproporzionato.

Articolo 4 - Sicurezza

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente.

2. Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili.

(8) GU L 108 del 24.4.2002, pag. 33.

Articolo 5 - Riservatezza delle comunicazioni

1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

2. Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale.

3. Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

Articolo 6 - Dati sul traffico

1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia dato il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

4. Il fornitore dei servizi deve informare l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del trattamento ai fini enunciati al paragrafo 2 e, prima di ottenere il consenso, ai fini enunciati al paragrafo 3.

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività.

6. I paragrafi 1, 2, 3 e 5 non pregiudicano la facoltà degli organismi competenti di ottenere i dati relativi al traffico in base alla normativa applicabile al fine della risoluzione delle controversie, in particolare di quelle attinenti all'interconnessione e alla fatturazione.

Articolo 7 - Fatturazione dettagliata

1. Gli abbonati hanno diritto di ricevere fatture non dettagliate.

2. Gli Stati membri applicano norme nazionali per conciliare i diritti degli abbonati che ricevono fatture dettagliate con il diritto alla vita privata degli utenti chiamanti e degli abbonati chiamati, ad esempio garantendo che detti utenti e abbonati possano disporre, per le comunicazioni e per i pagamenti, di sufficienti modalità alternative che tutelino maggiormente la vita privata.

Articolo 8 - Presentazione e restrizione dell'identificazione della linea chiamante e collegata

1. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante, il fornitore dei servizi deve offrire all'utente chiamante la possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.

2. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuitamente, per ogni ragionevole utilizzo di tale funzione, di impedire la presentazione dell'identificazione delle chiamate entranti.

3. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avvenga prima che la comunicazione sia stabilita, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità, mediante una funzione semplice, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.

4. Qualora sia disponibile la presentazione dell'identificazione della linea collegata, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Il paragrafo 1 si applica anche alle chiamate provenienti dalla Comunità e dirette verso paesi terzi. I paragrafi 2, 3 e 4 si applicano anche alle chiamate in entrata provenienti da paesi terzi.

6. Gli Stati membri assicurano che, qualora sia disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore di servizi di comunicazione elettronica accessibili al pubblico informi quest'ultimo di tale possibilità e delle possibilità di cui ai paragrafi 1, 2, 3 e 4.

Articolo 9 - Dati relativi all'ubicazione diversi dai dati relativi al traffico

1. Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. Gli utenti e gli abbonati devono avere la possibilità di ritirare il loro consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico in qualsiasi momento.

2. Se hanno dato il consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, l'utente e l'abbonato devono continuare ad avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

3. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico ai sensi di paragrafi 1 e 2 deve essere limitato alle persone che agiscono sotto l'autorità del fornitore della rete pubblica di telecomunicazione o del servizio di comunicazione elettronica accessibile al pubblico o del terzo che fornisce il servizio a valore aggiunto, e deve essere circoscritto a quanto è strettamente necessario per la fornitura di quest'ultimo.

Articolo 10 - Deroghe

Gli Stati membri assicurano che esistano procedure trasparenti in base alle quali il fornitore di una rete

pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico:

a) possa annullare, in via temporanea, la soppressione della presentazione dell'identificazione della linea chiamante a richiesta di un abbonato che chieda la presentazione dell'identificazione di chiamate malintenzionate o importune. In tal caso, in base al diritto nazionale, i dati che identificano l'abbonato chiamante sono memorizzati e resi disponibili dal fornitore di una rete pubblica di comunicazioni e/o di un servizio di comunicazioni elettroniche accessibile al pubblico;

b) possa annullare la soppressione della presentazione dell'identificazione della linea chiamante e possa sottoporre a trattamento i dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, linea per linea, per gli organismi che trattano chiamate di emergenza, riconosciuti come tali da uno Stato membro, in particolare per le forze di polizia, i servizi di ambulanza e i vigili del fuoco, affinché questi possano reagire a tali chiamate.

Articolo 11 - Trasferimento automatico della chiamata

Gli Stati membri provvedono affinché ciascun abbonato abbia la possibilità, gratuitamente e mediante una funzione semplice, di bloccare il trasferimento automatico delle chiamate verso il proprio terminale da parte di terzi.

Articolo 12 - Elenchi di abbonati

1. Gli Stati membri assicurano che gli abbonati siano informati, gratuitamente e prima di essere inseriti nell'elenco, in merito agli scopi degli elenchi cartacei o elettronici a disposizione del pubblico o ottenibili attraverso i servizi che forniscono informazioni sugli elenchi, nei quali possono essere inclusi i loro dati personali, nonché in merito ad ogni ulteriore possibilità di utilizzo basata su funzioni di ricerca incorporate nelle versioni elettroniche degli elenchi stessi.

2. Gli Stati membri assicurano che gli abbonati abbiano la possibilità di decidere se i loro dati personali - e, nell'affermativa, quali - debbano essere riportati in un elenco pubblico, sempreché tali dati siano pertinenti per gli scopi dell'elenco dichiarati dal suo fornitore. Gli Stati membri provvedono affinché gli abbonati abbiano le possibilità di verificare, rettificare o ritirare tali dati. Il fatto che i dati non siano riportati in un elenco pubblico di abbonati la verifica, la correzione o il ritiro dei dati non devono comportare oneri.

3. Gli Stati membri possono disporre che sia chiesto il consenso ulteriore degli abbonati per tutti gli scopi di un elenco pubblico diversi dalla ricerca di dati su persone sulla base del loro nome e, ove necessario, di un numero minimo di altri elementi di identificazione.

4. I paragrafi 1 e 2 si applicano agli abbonati che siano persone fisiche. Gli Stati membri assicurano inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente all'inclusione negli elenchi pubblici.

Articolo 13 - Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso.

2. Fatto salvo il paragrafo 1, allorché una persona fisica o giuridica ottiene dai suoi clienti le coordinate elettroniche per la posta elettronica nel contesto della vendita di un prodotto o servizio ai sensi della direttiva 95/46/CE, la medesima persona fisica o giuridica può utilizzare tali coordinate elettroniche a scopi di commercializzazione diretta di propri analoghi prodotti o servizi, a condizione che ai clienti sia offerta in modo chiaro e distinto al momento della raccolta delle coordinate elettroniche e ad ogni messaggio la possibilità di opporsi, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche qualora il cliente non abbia rifiutato inizialmente tale uso.

3. Gli Stati membri adottano le misure appropriate per garantire che, gratuitamente, le comunicazioni indesiderate a scopo di commercializzazione diretta, in casi diversi da quelli di cui ai paragrafi 1 e 2, non siano permesse se manca il consenso degli abbonati interessati oppure se gli abbonati esprimono il desiderio di non ricevere questo tipo di chiamate; la scelta tra queste due possibilità è effettuata dalla normativa nazionale.

4. In ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni.

5. Le disposizioni di cui ai paragrafi 1 e 3 si applicano agli abbonati che siano persone fisiche. Gli Stati membri garantiscono inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente alle comunicazioni indesiderate.

Articolo 14 - Caratteristiche tecniche e normalizzazione

1. Salvo quanto disposto nei paragrafi 2 e 3, nell'attuare le disposizioni della presente direttiva gli Stati membri assicurano che non siano imposti, per i terminali o altre apparecchiature di comunicazione elettronica, norme inderogabili relative a caratteristiche tecniche specifiche che possano ostacolare l'immissione sul mercato e la libera circolazione di tali apparecchiature tra i vari Stati membri e al loro interno.

2. Qualora talune disposizioni della presente direttiva possano essere attuate soltanto attraverso la prescrizione di caratteristiche tecniche specifiche per le reti di comunicazione elettronica, gli Stati membri informano la Commissione secondo le procedure di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura di informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione [9].

3. All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni [10].

Articolo 15 - Applicazione di alcune disposizioni della direttiva 95/46/CE

1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.

2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.

Articolo 16 - Disposizioni transitorie

1. L'articolo 12 non si applica agli elenchi già prodotti o immessi sul mercato su supporto cartaceo o elettronico off-line prima dell'entrata in vigore delle disposizioni nazionali adottate in forza della presente direttiva.

2. Se i dati personali degli abbonati a servizi pubblici fissi o mobili di telefonia vocale sono stati inseriti

(9) G.U. L 204 del 21.7.1998, pag. 37. Direttiva modificata dalla direttiva 98/48/CE (GU L 217 del 5.8.1998, pag. 18).
(10) G.U. L 36 del 7.2.1987, pag. 31. Decisione modificata da ultimo dall'atto di adesione del 1994.

in un elenco pubblico degli abbonati in conformità con le disposizioni della direttiva 95/46/CE e dell'articolo 11 della direttiva 97/66/CE prima dell'entrata in vigore delle disposizioni nazionali adottate conformemente alla presente direttiva, i dati personali di tali abbonati possono restare inseriti in tale elenco pubblico cartaceo o elettronico, comprese le versioni con funzioni di ricerca inverse, salvo altrimenti da essi comunicato dopo essere stati pienamente informati degli scopi e delle possibilità in conformità con l'articolo 12 della presente direttiva.

Articolo 17 - Attuazione della direttiva

1. Gli Stati membri mettono in vigore le disposizioni necessarie per conformarsi alla presente direttiva entro il 31 ottobre 2003. Essi ne informano immediatamente la Commissione.

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate da un siffatto riferimento all'atto della loro pubblicazione ufficiale. Le modalità di tale riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni di diritto interno che essi adottano nel settore disciplinato dalla presente direttiva, nonché ogni loro successiva modificazione ed integrazione.

Articolo 18 - Riesame

La Commissione presenta al Parlamento europeo e al Consiglio, non oltre tre anni dalla data di cui all'articolo 17, paragrafo 1, una relazione sull'applicazione della presente direttiva e il relativo impatto sugli operatori economici e suoi consumatori, in particolare per quanto riguarda le disposizioni sulle comunicazioni indesiderate, tenendo conto dell'ambiente internazionale. A tale fine, la Commissione può chiedere agli Stati membri informazioni che saranno fornite senza ritardi ingiustificati. Ove opportuno, la Commissione presenta proposte di modifica della presente direttiva, tenendo conto dei risultati di detta relazione, di ogni modifica del settore e di ogni altra proposta che ritenga necessaria per migliorare l'efficacia della presente direttiva.

Articolo 19 - Abrogazione

La direttiva 97/66/CE è abrogata con efficacia a decorrere dalla data di applicazione di cui all'articolo 17, paragrafo 1.

I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva.

Articolo 20 - Entrata in vigore

La presente direttiva entra in vigore il giorno della pubblicazione nella Gazzetta ufficiale delle Comunità europee.

Articolo 21 - Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, addì 12 luglio 2002.

Per il Parlamento europeo
Il Presidente
P. Cox

Per il Consiglio
Il Presidente
T. Pedersen

101 Raccomandazione del Parlamento europeo al Consiglio sul futuro sviluppo di Europol e la sua integrazione a pieno titolo nel sistema istituzionale dell'Unione europea

Il Parlamento europeo,

- visto l'articolo 39, paragrafo 3 del trattato UE,
- visti gli articoli 29 e 30 del trattato UE,
- visti l'Atto del Consiglio del 26 luglio 1995, che stabilisce la convenzione basata sull'articolo K.3 del trattato sull'Unione europea che istituisce un ufficio europeo di polizia (Convenzione Europol)[1] nonché i protocolli e le sue modifiche,
- vista l'iniziativa del Regno del Belgio e del Regno di Spagna in vista dell'adozione di un atto del Consiglio che stabilisce un protocollo recante modifica della convenzione che istituisce un Ufficio europeo di polizia (convenzione Europol), del protocollo concernente l'interpretazione, in via pregiudiziale, da parte della Corte di giustizia delle Comunità europee della convenzione che istituisce un Ufficio europeo di polizia, e del protocollo relativo ai privilegi e alle immunità dell'Europol, dei membri dei suoi organi, dei suoi vicedirettori e agenti [2],
- vista la comunicazione della Commissione al Parlamento europeo e al Consiglio 'Controllo democratico dell'Europol' (COM(2002) 95),
- visto l'articolo 107 del suo regolamento,
- vista la proposta di raccomandazione della commissione per le libertà e i diritti dei cittadini, la giustizia e gli affari interni (A5-0173/2002),

A. considerando che l'Europol deve divenire uno strumento efficace nella lotta contro la criminalità organizzata nell'Unione europea, mantenendo in particolare una stretta cooperazione con Eurojust; che in un ambiente internazionale in costante cambiamento ciò richiede che l'Europol possa agire con flessibilità per apportare un contributo efficace alla lotta contro le molteplici forme di grande criminalità,

B. considerando che l'attuale procedura di modifica della convenzione, che implica la ratifica da parte di tutti gli Stati membri, in conformità delle rispettive norme costituzionali, rappresenta una procedura eccessivamente lunga e pesante e, pertanto, totalmente inadeguata,

C. considerando che per il fatto di proporre che, d'ora in poi, le modifiche alla convenzione Europol vengano adottate dal Consiglio, l'iniziativa del Regno del Belgio e del Regno di Spagna sembra effettuare un passo nella giusta direzione, ma che tuttavia essa è viziata da tre gravi carenze:

a) essa mantiene l'Europol, de jure, nel quadro della semplice cooperazione intergovernativa, contrariamente alle esplicite richieste in tal senso formulate a più riprese da questo Parlamento e in un momento in cui il Consiglio stesso attribuisce a Europol missioni sempre più numerose da svolgere per conto dell'Unione;

b) essa rischia, dopo l'ampliamento dell'Unione, di comportare un'eccessiva lentezza se non addirittura un blocco del processo decisionale, dal momento che tutte le decisioni del Consiglio relative a Europol dovranno essere prese dal Consiglio all'unanimità;

c) essa conferma il ruolo marginale di questo Parlamento per tutto ciò che riguarda Europol, privandolo al tempo stesso dei mezzi giuridici e del quadro istituzionale che potrebbero consentirgli di esercitare in futuro un reale controllo democratico,

D. considerando che esiste una strada alternativa che consente di rispondere in modo adeguato alle gravi carenze di cui sopra e che è rappresentata dall'articolo 34, paragrafo 2, lettera c) del trattato UE,

(1) GU C 316 del 27.11.1995, pag. 1.

che consentirebbe al Consiglio di sostituire la convenzione con una decisione,

E. considerando che la sostituzione della convenzione con una decisione del Consiglio basata sull'articolo 34 del trattato UE avrebbe l'effetto di integrare Europol nel terzo pilastro e quindi nel sistema del diritto comunitario, il che presenterebbe tre vantaggi non indifferenti:

a) il miglioramento delle capacità operative dell'Europol, dal momento che, in virtù dell'articolo 34 del trattato UE, tutte le misure esecutive verrebbero definite dal Consiglio a maggioranza qualificata (senza possibilità di deroghe), il che consentirebbe di reagire più rapidamente in caso di necessità;

b) il miglioramento del controllo parlamentare giacché, da un lato, il Parlamento deve essere consultato per tutte le misure di applicazione definite dal Consiglio (articolo 39 del trattato UE) e, dall'altro, esso ha la possibilità di adire la Corte di giustizia in caso di mancato rispetto dei suoi diritti;

c) l'applicazione automatica a tutte le decisioni adottate dal Consiglio sulla base dell'articolo 34 del trattato UE (e quindi anche alla convenzione stessa non appena sarà stata sostituita da una decisione del Consiglio) delle norme relative alla competenza della Corte di giustizia (articolo 35 del trattato UE),

F considerando che è inderogabile e urgente rafforzare il controllo democratico su Europol,

G. considerando che l'estensione delle competenze e delle responsabilità prevista dall'iniziativa del Regno del Belgio e del Regno di Spagna con l'introduzione di unità investigative miste inasprisce l'asimmetria che già esiste nei rapporti tra esecutivo e legislativo; che, quale organismo europeo, Europol deve essere controllato da un altro organo europeo, il Parlamento europeo, e non dai parlamenti nazionali,

H. considerando che le possibilità di controllo parlamentare offerte a questo Parlamento sarebbero notevolmente aumentate se una parte del bilancio dell'Europol fosse inserita nel bilancio della Comunità,

indirizza al Consiglio le seguenti raccomandazioni:

Raccomandazione 1: base giuridica

- chiede al Consiglio di sostituire:
- la convenzione che istituisce un Ufficio europeo di polizia (convenzione Europol),
- il protocollo riguardante l'interpretazione, a titolo pregiudiziale, da parte della Corte di giustizia delle Comunità europee, della convenzione che istituisce un Ufficio europeo di polizia,
- e il protocollo sui privilegi e le immunità di Europol, dei membri dei suoi organi, dei suoi direttori aggiunti e dei suoi agenti con una o più decisioni del Consiglio, sulla base dell'articolo 34, paragrafo 2, lettera c) del trattato sull'Unione europea; garantendo nel contempo il rispetto del sistema delle competenze proprie attribuite alle istituzioni dell'Unione, e di procedere di conseguenza, a norma degli articoli 30 e 31 del trattato sull'Unione europea, alla riformulazione delle disposizioni della convenzione Europol relative alla cooperazione di polizia e giudiziaria in materia penale, in particolare degli elementi essenziali dei reati di competenza di Europol;

Raccomandazione 2: bilancio

- chiede al Consiglio, nel quadro di tale decisione, di modificare il sistema di finanziamento dell'Europol, sostituendo una parte dei contributi degli Stati membri con un finanziamento a carico del bilancio dell'UE, rispettando le prerogative delle autorità di bilancio;

Raccomandazione 3: missioni

- chiede al Consiglio, nel quadro di tale decisione, di prevedere le disposizioni necessarie:
- per disciplinare la partecipazione dell'Europol alle unità investigative miste;
- per consentire a Europol di chiedere alle autorità competenti degli Stati membri di aprire indagini in casi specifici;
- per dotare Europol di mezzi più efficaci per lottare contro il riciclaggio di denaro e per rafforzarne la capacità di aiutare gli Stati membri in questa lotta (Atto del Consiglio del 30 novembre 2000 che stabilisce, in base all'articolo 43, paragrafo 1, della convenzione che istituisce un ufficio europeo di polizia (Convenzione Europol), un protocollo che modifica l'articolo 2 e l'allegato di detta convenzione [3]);

(3) G.U. C 358 del 13.12.2000, pag. 1.

Raccomandazione 4: controllo parlamentare

- chiede al Consiglio, nel quadro di tale decisione, di rafforzare il potere democratico di controllo del Parlamento europeo su Europol, e di prevedere a tal fine:
- una disposizione recante modifica dell'articolo 34 della convenzione Europol e che preveda che un unico rapporto di attività annuale sia trasmesso al Consiglio e al Parlamento europeo;
- una disposizione recante modifica dell'articolo 34 della convenzione Europol che conferisca al Parlamento europeo il diritto formale di avere uno scambio di opinioni con la Presidenza del Consiglio sul rapporto di attività annuale;
- una disposizione recante modifica dell'articolo 34 della convenzione Europol che conferisca al Parlamento europeo il diritto formale di invitare il direttore di Europol a presentarsi dinanzi alla commissione competente;
- una disposizione recante modifica dell'articolo 24, paragrafo 6 della convenzione Europol, che faccia obbligo all'autorità di controllo comune incaricata della protezione dei dati di elaborare un rapporto di attività annuale, di trasmetterlo al Parlamento europeo e di renderne conto alla commissione competente;
- una disposizione recante modifica dell'articolo 28 della convenzione Europol che preveda la riforma del Consiglio di Amministrazione di Europol affinché questo sia composto, oltre che da un rappresentante di ciascuno Stato membro, anche da due rappresentanti della Commissione e due del Parlamento europeo;
- una disposizione recante modifica dell'articolo 29 della convenzione Europol che preveda che il Parlamento europeo sia coinvolto nella procedura di nomina e rimozione del Direttore di Europol assieme al Consiglio;

Raccomandazione 5: tutela dei dati

- chiede al Consiglio di adottare nell'ambito della decisione che sostituisce la convenzione una decisione che garantisca un livello di protezione dei dati e di controllo del rispetto di tali norme equivalente a quello garantito nel primo pilastro (direttiva del Parlamento europeo e del Consiglio 95/46/CE(4));

Raccomandazione 6: cooperazione

- chiede al Consiglio, nel quadro di tale decisione, di prendere le misure necessarie per assicurare una stretta cooperazione tra Europol, Eurojust e OLAF, al fine di rafforzare l'efficacia operativa di questi organi nella lotta contro la criminalità organizzata e il terrorismo;

2. incarica il suo Presidente di trasmettere la presente raccomandazione al Consiglio e, per conoscenza, alla Commissione, nonché ai governi e ai parlamenti degli Stati membri.

(4) G.U. L 281 del 23.11.1995, pag. 31.

102 Risoluzione del Parlamento europeo del 13 marzo 2003 sulla trasmissione dei dati personali da parte delle compagnie aeree in occasione di voli transatlantici (*)

P5_TA-PROV(2003)0097
B5-0187/2003

Il Parlamento europeo,

- visti 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 nonchè alla libera circolazione di tali dati [1] e il regolamento del Consiglio CEE n. 2299/89 del 24 luglio 1989 su un codice di condotta per i sistemi telematici di prenotazione [2],

A. inconsapevole del fatto che dopo l'11 settembre 2001 gli Stati Uniti hanno riformato profondamente la legislazione al fine di garantire la propria sicurezza interna anche nel settore dei trasporti e che, il 19 novembre 2001, hanno adottato "l'Aviation and Transportation Security Act (ATSA)" [3], e il 5 maggio 2002 "l'Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV)" [4] nonché altre misure connesse che riguardano, per i soli voli transatlantici, circa 10/11 milioni di passeggeri l'anno,

B. considerando che inizialmente l'amministrazione degli Stati Uniti si era limitata a richiedere alle compagnie aeree la trasmissione dei dati relativi ai passeggeri e ai membri dell'equipaggio ('Passenger Manifest Information') (nota finale [5] attraverso 'l'Advance Passenger Information System (APIS)', che in seguito tuttavia ha interpretato l'accordo interinale in modo da imporre, pena gravi sanzioni, l'accesso diretto ai sistemi di prenotazione elettronica e, in particolare, al 'Passenger Name Record (PNR)' (registro dei nomi dei passeggeri) cui può essere collegata, oltre ai dati di identificazione, qualsiasi altra informazione [6], comprese informazioni delicate a norma dell'articolo 8 della direttiva 95/46/CE,

C. condividendo i dubbi e le preoccupazioni manifestate dalle autorità nazionali [7] quanto alla legittimità di una tale richiesta, anche dal punto di vista della legislazione degli Stati Uniti, e condividendo in particolare i dubbi circa la sua conformità con la normativa UE sulla protezione dei dati, visto il rischio che le basi dati dei sistemi di prenotazione possano di fatto divenire terreno di 'data mining' per l'amministrazione statunitense,

(*) (vedi anche il Parere 6/2002 adottato il 24 ottobre 2002 dal Gruppo Art. 29 Direttiva 95/46 p. 366 della *Relazione* e Joint Statement European Commission/US Customs talks on PNR Transmission) – Brussels, 17/18 February 2003 [Dichiarazione congiunta sui colloqui fra la Commissione Europea e il Servizio delle dogane USA relativi alla trasmissione del PNR]

(1) G.U. L 281 del 23.11.1995, pag. 31.

(2) G.U. L 220 del 29.7.1989, pag. 1.

(3) "Aviation and Transportation Security Act" del 19 novembre 2001 (107-71), norme provvisorie del Dipartimento del tesoro (dogane) - dati relativi a passeggeri e equipaggi richiesti per i voli passeggeri nel trasporto aereo dall'estero verso gli Stati Uniti (registro federale, 31 dicembre 2001) e trasmissione del registro dei nomi dei passeggeri richiesta per i passeggeri di voli internazionali da o verso gli Stati Uniti (registro federale, 25 giugno 2002).

(4) Che aggiorna le disposizioni pertinenti dell'"Immigration and Nationality Act".

(5)i _____

(5) TRASMISSIONE DI DATI AD ALTRE AGENZIE FEDERALI - Su richiesta, l'informazione fornita al Sottosegretario del Servizio dogane di cui in questa sottosezione, può essere condivisa con altre agenzie federali ai fini di proteggere la sicurezza nazionale.

(6) Numero PNR, data prenotazione, agenzia di viaggio, informazioni figuranti sul biglietto, dati finanziari (numero di carta di credito, data di scadenza, indirizzo della fatturazione, ecc.), itinerario, cronistoria del PNR. Quest'ultima può contenere i viaggi effettuati in passato ma anche dati di tipo religioso o etnico (scelta del pasto ...), l'affiliazione a un gruppo particolare, dati relativi alla residenza e ai mezzi per contattare un individuo (indirizzo e-mail, coordinate di un amico, luogo di lavoro ...), dati medici (assistenza medica necessaria, ossigeno, problemi di vista, udito o mobilità o qualsiasi altro problema la cui conoscenza è necessaria per il buon svolgimento del volo) nonché altri dati connessi per esempio ai programmi fedeltà.

D. esprimendo dubbi sul fatto che tali dati siano protetti (nota finalei [8]), e lo siano in modo 'adeguato', una volta trasferiti in basi di dati statunitensi; rammaricandosi che la Commissione non abbia avviato in tempo utile la procedura di valutazione della compatibilità della legislazione statunitense con il diritto comunitario [9],

E. prendendo atto che la nuova legislazione proposta dai servizi dell'immigrazione degli Stati Uniti [10] consentirebbe di sormontare le limitazioni del sistema di trasmissione attuale denominato US EDIFACT attraverso un formato più esaustivo UN EDIFACT (quest'ultimo permetterebbe l'inclusione dell'indirizzo negli Stati Uniti, il numero, la data e il luogo di rilascio del visto come richiesto dalla sezione 402 dell'EBSV) nonché di definire meglio la portata effettiva del PNR limitandola ad informazioni predeterminate,

1. deplora i ritardi in cui è incorsa la Commissione nel presentare al Parlamento europeo e al Consiglio una problematica d'attualità da oltre quindici mesi che riguarda la tutela dei dati e nel contempo ha un'enorme incidenza sulle altre politiche della comunità (trasporti, immigrazione) e dell'Unione (cooperazione di polizia e giudiziaria o lotta contro il terrorismo e la criminalità organizzata);

2. esprime disappunto per il fatto che la Commissione, in qualità di custode dei trattati e del diritto comunitario, non si sia assunta le proprie responsabilità con la dovuta solerzia, in quanto:
- non ha verificato se l'accesso ai dati dei sistemi di prenotazione abbia un fondamento reale nella legislazione degli Stati Uniti o non sia un'interpretazione estensiva da parte di questa amministrazione [11]; invita inoltre la Commissione ad approfittare delle discussioni in corso negli Stati Uniti sulla nuova legislazione sull'APIS e il PNR in modo da ottenere dalle autorità USA che questa nuova legislazione tenga conto delle esigenze di tutela dei dati che derivano dalla legislazione comunitaria;

- ha ritardato la verifica della legislazione USA prevista all'articolo 25 della direttiva 95/46/CE; un eventuale ritardo crea evidenti difficoltà alle compagnie aeree prese tra l'incudine delle sanzioni USA (se rispettano il diritto comunitario) e il martello delle autorità per la protezione dei dati (se danno seguito alle richieste delle autorità USA) e mette anche in difficoltà le autorità nazionali per la protezione dei dati che devono far rispettare le disposizioni comunitarie;

- non ha informato i cittadini che dovrebbero essere i primi a sapere qual è l'uso delle informazioni che li riguardano;

3. si rammarica della dichiarazione congiunta dei funzionari UE e USA del 19 febbraio 2003 che è priva di qualsiasi base giuridica e potrebbe venire interpretata come un invito indiretto alle autorità nazionali a non rispettare il diritto comunitario; incarica il suo Presidente di avviare la procedura prevista dall'articolo 91 del suo regolamento per verificare la possibilità di un ricorso davanti alla Corte di giustizia;

4. ritiene che, se vanno avviati negoziati, questi devono basarsi sulle competenze comunitarie in materia di trasporti aerei che, a livello di relazioni transatlantiche, riguardano 10/11 milioni di passeggeri l'anno e per i quali la Commissione si appresta a negoziare un accordo 'open skies' nonché sulle competenze in materia di politica migratoria; è altresì perplesso in quanto tali questioni non sono state affrontate a livello di accordi in materia di cooperazione giudiziaria e di polizia, ormai in una fase molto avanzata;

(8)ii nota finale 2 - (EBSV pagina 6) Sul sistema 'Chimera': ' ...Il piano previsto in questa sottosezione stabilisce le condizioni per l'uso delle informazioni di cui alla sottosezione (b) ricevute dal Dipartimento di Stato e dal Servizio d'immigrazione e naturalizzazione (A) per limitare la ridiffusione di tali informazioni; (B) per garantire che tali informazioni vengano usate esclusivamente al fine di determinare l'opportunità di rilasciare un visto ad uno straniero o di determinare l'ammissibilità o il respingimento di uno straniero da parte degli Stati Uniti, a meno che non sia previsto diversamente dalla legge federale; (C) per garantire l'accuratezza, la sicurezza e la riservatezza di tali informazioni; (D) per proteggere i diritti alla privacy degli individui soggetti a tali informazioni; (E) per fornire dati integri attraverso la tempestiva rimozione e distruzione di nomi e di informazioni obsoleti o erronei; ed (F) in un modo che protegga le fonti e i metodi usati per acquisire informazioni del tipo richiesto alla sezione 103(c)(6) del 'National Security Act' del 1947 (50 U.S.C. 403-3(c)f(6)).
(9) Secondo il concetto dell'articolo 25 della direttiva 95/46/CE.
(10) Federeal Register: gennaio 3, 2003 (Volume 68, numero 2).
(11) Per esempio la riorganizzazione dei sistemi di prenotazione isolando i dati che non sarebbero rigorosamente connessi al contratto di viaggio.

5. chiede alla Commissione di ottenere la sospensione degli effetti delle misure prese dalle autorità statunitensi finché non sarà stata adottata la decisione sulla compatibilità di tali misure con il diritto comunitario;

6. invita la Commissione ad affrontare i problemi trattati nella presente risoluzione e si riserva di esaminare il seguito dato prima del prossimo vertice UE-USA;

7. incarica il suo Presidente di trasmettere la presente risoluzione alla Commissione, al Consiglio, ai governi e ai parlamenti degli Stati membri nonché alla rappresentanza permanente degli Stati Uniti presso l'Unione europea e al Congresso degli Stati Uniti.

(F) Altre informazioni che il Sottosegretario, di concerto con il Direttore generale delle dogane, ritenga ragionevolmente necessarie per garantire la sicurezza aerea. (3) ELENCHI DEI NOMI DEI PASSEGGERI. - Il vettore mette a disposizione l'elenco dei nomi dei passeggeri al Servizio dogane competente, su richiesta. (4) TRASMISSIONE DEI DATI - A norma del paragrafo 5, i dati relativi a passeggeri e a membri dell'equipaggio richiesti per un volo di cui al paragrafo 1 devono essere trasmessi al Servizio dogane prima dell'atterraggio dell'aereo negli Stati Uniti secondo le modalità, le scadenze e la forma prevista dal Servizio dogane.

nota finale 1 - La sezione 44909 è modificata aggiungendo alla fine quanto segue: (c) VOLI NEL TRASPORTO AEREO INTERNAZIONALE VERSO GLI STATI UNITI (1) IN GENERALE. Non più di 60 giorni dopo la data di applicazione dell' 'Aviation and Transportation Security Act', ogni vettore aereo e vettore aereo straniero che opera un volo passeggeri nel trasporto internazionale verso gli Stati Uniti deve fornire al Direttore generale delle dogane mediante trasmissione elettronica i dati relativi a passeggeri e personale di bordo contenenti le informazioni specificate al paragrafo 2. I vettori possono utilizzare l' 'Advanced Passenger Information System (APIS)' di cui alla sezione 431 del 'Tariff Act' del 1930 (19 U.S.C. 1431) per fornire le informazioni richieste di cui sopra. (2) INFORMAZIONI. I dati relativi a passeggeri e equipaggio di un volo di cui al paragrafo 1 contengono le seguenti informazioni: (A) il nome completo di ciascun passeggero e membro dell'equipaggio . (B) La data di nascita e la cittadinanza di ciascun passeggero e membro dell'equipaggio. (C) Il sesso di ciascun passeggero e membro dell'equipaggio. (D) Il numero di passaporto e il paese di rilascio per ciascun passeggero e membro dell'equipaggio, qualora richiesto per il viaggio. (E) Il numero di visto degli Stati Uniti o il numero del permesso di soggiorno di ciascun passeggero e membro dell'equipaggio ove d'applicazione.

103 Decisione del Consiglio del 28 febbraio 2002 riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen (2002/192/CE) (*)



Decisione del Consiglio
del 28 febbraio 2002
riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen
(2002/192/CE)

(*) Pubblicata nella G.U.C.E. L 64/20 del 7 marzo 2002.
http://europa.eu.int/eur-lex/pri/it/oj/dat/2002/l_064/l_06420020307it00200023.pdf

104 Decisione del Consiglio del 14 ottobre 2002 relativa alla declassificazione di talune parti del manuale Sirene adottato dal comitato esecutivo istituito dalla convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 (2003/19/CE) (*)



Decisione del Consiglio
del 14 ottobre 2002
relativa alla declassificazione di talune parti del manuale Sirene adottato dal comitato esecutivo istituito dalla convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985
(2003/19/CE)

(*) Pubblicata nella G.U.C.E. L 8/34 del 14 gennaio 2003.
http://europa.eu.int/eur-lex/pri/it/oj/dat/2003/l_008/l_00820030114it00340034.pdf

105 UE Catalogo Schengen. Sistema d'Informazione Schengen, SIRENE: Raccomandazioni e migliori pratiche. Dicembre 2002 (*)

UE Catalogo Schengen. Sistema d'Informazione Schengen, SIRENE: Raccomandazioni e migliori pratiche. Dicembre 2002

(*) http://ue.eu.int/Jai/default.asp?lang=it

106 Manuale SIRENE. Informazioni supplementari richieste all'ingresso nazionale (*)

Manuale SIRENE – Informazioni supplementari richieste all'ingresso nazionale (G.U.C.E. n. 38 del 17.02.2003)

(*) Pubblicato nella G.U.C.E. L 38 del 17 febbraio 2003.
http://europa.eu.int/eur-lex/en/dat/2003/c_038/c_03820030217en00010024.pdf

Commissione europea

107 Dichiarazione del Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie in merito alla pubblicizzazione di test genetici via Internet - 24 febbraio 2003 (*)

Questa dichiarazione intende sensibilizzare la società civile ed i soggetti chiamati a ruoli decisionali rispetto ai problemi suscitati dalla pubblicizzazione di test genetici via Internet.

Si stanno moltiplicando le offerte via Internet di test genetici relativi soprattutto all'accertamento di paternità, ma anche alla predisposizione a diverse malattie (cardiache, diabete, ecc.). La pubblicità diventa sempre più aggressiva e capillare, anche in Europa: in alcuni Paesi compare, ad esempio, anche in popolari catene di negozi, nelle stazioni di servizio, negli autogrill lungo le autostrade, in televisione.

La commercializzazione di massa dei test genetici pone molti e gravi problemi etici, sociali, giuridici, sui quali il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie ritiene urgente richiamare l'attenzione. Le informazioni attualmente offerte tendono ad essere fuorvianti ed incomplete, soprattutto alla luce della bassa prevedibilità dell'insorgere di patologie sulla base dei risultati di test genetici qualora vi siano caratteri multigenici. Spesso non vi sono sufficienti garanzie che i dati genetici inviati per i test siano stati raccolti rispettando le norme sul consenso degli interessati, in particolare per i test di paternità. I test genetici possono avere conseguenze negative se non si accompagnano ad un'adeguata consulenza. L'Articolo 12 della Convenzione sui diritti dell'uomo e la biomedicina del Consiglio d'Europa condiziona la legittimità dei test genetici anche ad una "consulenza genetica appropriata". Nel Parere n. 6 sugli aspetti etici delle diagnosi prenatali (20 febbraio 1996), il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie affermava che "un'attenta consulenza genetica prima e dopo il test costituisce parte integrante del test e non dovrebbe essere disgiunta dall'attività di campionatura e dai test". Le banche dati contenenti i risultati di test genetici potrebbero essere utilizzate a fini discriminatori nei confronti di alcuni gruppi di individui.

Le conseguenze individuali e sociali dei test genetici devono essere rigorosamente valutate. Alla luce delle particolari caratteristiche dei dati genetici, è possibile che si verifichi la violazione di diritti fondamentali, in particolare l'eguaglianza. Possono essere messe a rischio sia la salute delle persone sia la riservatezza dei dati sanitari. La pubblicità dei test genetici tende a trasformarli in merce ed a produrre una domanda di test genetici che può avere effetti di disgregazione delle relazioni sociali ed interpersonali.

Il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie intende lavorare su questi temi in futuro. È in preparazione un Parere sugli aspetti etici dei test genetici sul luogo di lavoro

(*)Traduzione non ufficiale.
http://www.europa.eu.int/comm/european_group_ethics/docs/statgentest-en.pdf

Consiglio d'Europa

108 Raccomandazione R(2002)9 del Comitato dei ministri agli Stati membri sulla protezione dei dati personali raccolti e trattati per scopi assicurativi (*)

CONSIGLIO D'EUROPA
Comitato dei Ministri

Preambolo

Il Comitato dei Ministri, ai sensi dell'Articolo 15.b dello Statuto del Consiglio d'Europa,

1. considerato che scopo del Consiglio d'Europa è di raggiungere un'unione più stretta fra i suoi membri,

2. richiamandosi ai principi generali relativi alla protezione dei dati contenuti nella Convenzione per la protezione delle persone fisiche rispetto al trattamento automatizzato di dati personali (ETS n. 108), ed in particolare all'Articolo 6 della stessa, il quale afferma che i dati personali classificati come sensibili non possono essere oggetto di trattamento se il diritto interno non prevede garanzie adeguate,

3. consapevole del fatto che il trattamento automatizzato di dati personali per scopi assicurativi è sempre più diffuso, non solo per la preparazione, conclusione, attuazione e cessazione di assicurazioni, ma anche per facilitare la gestione razionale ed economica delle assicurazioni, e per la lotta contro le frodi,

4. consapevole del fatto che le assicurazioni sono fornite da diversi soggetti economici, ed in particolare da compagnie assicurative,

5. convinto dell'importanza che la qualità, l'integrità e la disponibilità dei dati personali rivestono per le persone assicurate,

6. rilevando che la quasi totalità della popolazione degli Stati membri è interessata da uno o più contratti assicurativi, e che, per tale motivo, gli operatori del settore assicurativo sono in possesso di una quantità considerevole di dati personali, alcuni dei quali sono dati sensibili,

7. convinto che sia auspicabile regolamentare la raccolta ed il trattamento di dati personali per scopi assicurativi, garantirne la riservatezza e la sicurezza, e assicurare che l'utilizzo di tali dati rispetti diritti umani e libertà fondamentali, in particolare il diritto alla vita privata,

8. alla luce del fatto che la mobilità delle persone e la globalizzazione dei mercati e delle attività commerciali rendono indispensabile lo scambio transfrontaliero di informazioni anche nel settore assicurativo, e richiedono un'equivalente protezione dei dati in tutti gli Stati membri del Consiglio d'Europa,

Raccomanda che i governi degli Stati membri

1. prendano provvedimenti in modo da garantire che i principi contenuti nell'Appendice alla presente Raccomandazione si riflettano nella legislazione e nelle prassi interne,

(*) Traduzione non ufficiale
http://cm.coe.int/stat/E/Public/2002/adopted_texts/recommendations/2002r9.htm

2. assicurino un'ampia diffusione dei principi contenuti nell'Appendice alla presente Raccomandazione fra le persone, le pubbliche autorità e gli organismi pubblici o privati che raccolgono e trattano dati personali per scopi assicurativi, nonché fra gli organismi competenti in materia di protezione dati,

3. promuovano l'accoglimento e l'attuazione dei principi contenuti nell'Appendice alla presente Raccomandazione, in particolare attraverso l'adozione di norme di legge oppure stimolando la redazione di codici deontologici.

Appendice alla Raccomandazione R(2002)9

1. Definizioni

Ai fini della presente Raccomandazione:

a. per "dato personale" si intende ogni informazione relativa ad una persona fisica identificata o identificabile ("interessato"). Una persona fisica non dovrebbe essere ritenuta "identificabile" se l'identificazione richiede tempi e attività irragionevoli.

b. per "dato sensibile" si intende un dato personale che riveli l'origine razziale, le opinioni politiche, le convinzioni religiose o di altra natura, nonché un dato personale relativo allo stato di salute e alla vita sessuale. Anche i dati relativi a procedimenti penali e condanne, ed altri dati definiti sensibili dal diritto interno, si considerano dati sensibili.

c. l'espressione "per scopi assicurativi" si riferisce ad ogni operazione che comporti la raccolta e il trattamento di dati personali con riguardo alla copertura di un rischio, in particolare sulla base di una polizza o di un contratto assicurativo.

d. per "trattamento" si intende ogni operazione o complesso di operazioni effettuate in tutto o in parte con l'ausilio di procedure automatizzate e riguardanti dati personali, come la registrazione, la conservazione o la modifica, l'estrazione, la consultazione, l'utilizzazione, la comunicazione, l'incrocio o l'interconnessione e la cancellazione o la distruzione.

e. per "comunicazione" si intende l'atto con cui dati personali sono resi accessibili a terzi, indipendentemente dallo strumento o dal supporto utilizzato.

f. per "titolare" si intende la persona fisica o giuridica, la pubblica autorità, il servizio o ogni altro organismo che, da solo o congiuntamente ad altri, definisce gli scopi e gli strumenti utilizzati nella raccolta e nel trattamento di dati personali.

g. per "responsabile" si intende la persona fisica o giuridica, la pubblica autorità, il servizio o ogni altro organismo che tratti dati personali per conto del titolare.

2. Ambito di applicazione

2.1. La presente Raccomandazione si applica ai dati personali raccolti e trattati per scopi assicurativi. Essa non si applica alla raccolta ed al trattamento di dati personali utilizzati per scopi di previdenza sociale.

2.2. Gli Stati membri sono invitati ad estendere l'applicazione della presente Raccomandazione al trattamento non automatizzato di dati personali per scopi assicurativi.

2.3. Nessun dato personale dovrebbe essere sottoposto ad un trattamento non automatizzato per evitare l'applicazione dei principi della presente Raccomandazione.

2.4. Gli Stati membri possono estendere l'applicazione dei principi fissati nella presente Raccomandazione alla raccolta ed al trattamento di dati relativi a gruppi di persone, associazioni, fondazioni, società, imprese ed ogni altro organismo costituito direttamente o indirettamente da persone fisiche, dotato o meno di personalità giuridica.

2.5. Gli Stati membri possono estendere i principi fissati nella presente Raccomandazione alla protezione di dati personali utilizzati per scopi di previdenza sociale.

3. Rispetto della vita privata

3.1. Nella raccolta e nel trattamento di dati personali per scopi assicurativi è necessario salvaguardare il rispetto di diritti e libertà fondamentali, in particolare del diritto alla vita privata.

3.2. Coloro che hanno accesso a dati personali, nel corso di un'attività assicurativa, devono essere soggetti a vincoli di riservatezza conformemente al diritto ed alle prassi interne. Inoltre, la raccolta ed il trattamento di dati sanitari devono essere effettuati esclusivamente da operatori del settore sanitario, oppure secondo vincoli di riservatezza paragonabili a quelli cui soggiacciono gli operatori del settore sanitario o nel rispetto di garanzie di pari efficacia previste dal diritto interno.

4. Raccolta e trattamento di dati personali per scopi assicurativi

Presupposti essenziali per la raccolta ed il trattamento di dati personali

4.1. La raccolta ed il trattamento (compresa la comunicazione) di dati personali dovrebbero essere effettuati in modo leale e lecito, e per scopi specifici e leciti.

I dati personali dovrebbero essere
- adeguati, pertinenti e non eccedenti in rapporto agli scopi per i quali sono raccolti o ulteriormente trattati,
- accurati e, se necessario, aggiornati.

Fonti dei dati personali

4.2. In linea di principio, i dati personali raccolti e trattati per scopi assicurativi dovrebbero essere raccolti presso l'interessato o il suo legale rappresentante.

Liceità

4.3. La raccolta ed il trattamento di dati personali per scopi assicurativi sono consentiti
a. se previsti per legge;
b. per l'esecuzione di un contratto assicurativo concluso con l'interessato, nonché per la preparazione di un contratto di questo tipo su richiesta dell'interessato;
c. se l'interessato o il suo legale rappresentante o un'autorità od ogni altra persona o soggetto previsto per legge ha dato il proprio consenso come previsto al Capo 6, oppure
d. se i dati sono necessari per il perseguimento degli interessi legittimi del titolare, purché su questi ultimi non prevalgano gli interessi della persona interessata.

Finalità

4.4. Salvo quanto previsto dai Principi 4.6, 4.7 e 4.8, 8.1 e 13.1, la raccolta ed il trattamento di dati personali sono consentiti esclusivamente per i seguenti scopi:
a. predisposizione e fornitura di assicurazioni;
b. raccolta di premi e presentazione di altre fatturazioni;
c. risoluzione di controversie in materia di indennizzo o pagamento di altri benefici;
d. riassicurazione;
e. co-assicurazione;
f. prevenzione, individuazione e/o perseguimento di frodi assicurative;
g. riconoscimento, esercizio o difesa di un diritto in sede giudiziaria;
h. adempimento di altri specifici obblighi legali o contrattuali;
i. indagini su nuovi mercati assicurativi;
j. attività gestionali interne;
k. attività attuariali.

I dati in questione non possono essere sottoposti a trattamenti ulteriori per scopi incompatibili con quelli per cui sono stati inizialmente raccolti.

Nascituri

4.5. I dati personali relativi a nascituri dovrebbero godere di una tutela paragonabile a quella riservata ai dati personali di un minore.

Salvo diversa disposizione del diritto interno, chi detiene la potestà genitoriale può agire da soggetto che ha legalmente il diritto di agire per conto del nascituro, nella misura in cui quest'ultimo sia l'interessato.

Dati sensibili

4.6. La raccolta ed il trattamento di dati sensibili dovrebbero essere proibiti salvo che, per una delle finalità di cui ai Principi 4.1, 4.8, 8.1 e 13.1,

a. l'interessato o il suo legale rappresentante o un'autorità o ogni altra persona od ente nominato per legge abbia dato il proprio consenso esplicito secondo quanto disposto al Capo 6, oppure

b. siano consentiti dalla legge e

i. salva l'esistenza di adeguate garanzie, il trattamento sia necessario per l'adempimento di altri obblighi legali o contrattuali del titolare, oppure

ii. il trattamento sia necessario per far valere, esercitare o difendere un diritto in sede giudiziaria, oppure

iii. il trattamento sia necessario per tutelare gli interessi vitali della persona interessata o di un terzo, e l'interessato non sia in grado di prestare il proprio consenso per incapacità fisica o giuridica.

c. la raccolta ed il trattamento siano consentiti, salva l'esistenza di adeguate garanzie, per motivi di interesse pubblico rilevante e sulla base di una disposizione di legge o di una decisione dell'autorità ai sensi del Principio 15.1.

Dati di natura penale

4.7. In deroga al Principio 4.6., la raccolta ed il trattamento di dati relativi a procedimenti penali e condanne possono essere effettuati per scopi assicurativi esclusivamente sulla base di adeguate e specifiche garanzie previste dal diritto interno, e purché i dati siano necessari per la lotta alle frodi assicurative, per la concessione di assicurazioni o per il pagamento di indennizzi o di altri benefici assicurativi.

Marketing diretto

4.8. Il titolare può utilizzare i dati raccolti e registrati per scopi assicurativi al fine di commercializzare e promuovere la propria offerta di servizi, purché l'interessato ne sia stato informato e non vi si sia opposto. Tuttavia, se il trattamento riguarda dati sensibili, occorre il consenso esplicito dell'interessato, salvo che ciò contrasti con il diritto interno.

L'interessato dovrebbe essere informato del fatto che la mancata prestazione del consenso o la sua opposizione rispetto all'impiego dei propri dati per scopi di marketing non influirà sulla decisione di concedergli copertura assicurativa o di consentirgli di continuare ad usufruire della copertura assicurativa già concessa.

5. Informazione della persona interessata

5.1. Gli interessati dovrebbero essere informati di quanto segue:

a. la o le finalità per cui i dati sono o saranno sottoposti a trattamento;

b. l'identità del titolare del trattamento;

c. ogni altra informazione necessaria a garantire che il trattamento sia effettuato in modo leale, come ad esempio

- le categorie di dati raccolti o dei quali si prevede la raccolta;
- le categorie di individui o organismi esterni ai quali i dati possono essere comunicati, e per quali scopi;
- l'eventuale possibilità per gli interessati di rifiutare il consenso o di ritirarlo, e le conseguenze di tale ritiro;
- le condizioni per l'esercizio dei diritti di accesso e di rettifica;
- le persone o gli organismi presso i quali i dati sono o saranno raccolti;
- la natura obbligatoria o facoltativa delle risposte alle domande che costituiscono oggetto della raccolta, e le conseguenze per la persona in caso di risposta parziale.

5.2. Qualora i dati siano raccolti presso l'interessato, il titolare dovrebbe fornire a quest'ultimo le informazioni di cui al punto 5.1. al più tardi al momento della raccolta, salvo che l'interessato sia già stato informato.

5.3. Qualora i dati personali non siano raccolti presso l'interessato, il titolare dovrebbe fornire a quest'ultimo le informazioni di cui al punto 5.1. al momento in cui i dati sono registrati, oppure, se si prevede di comunicare i dati ad un soggetto terzo, al più tardi al momento della prima comunicazione di tali dati.

L'obbligo di informare l'interessato non sussiste se
a. l'interessato ha già ricevuto le informazioni;
b. risulta impossibile fornire le informazioni, oppure se ciò comporta uno sforzo sproporzionato;
c. il trattamento o la comunicazione dei dati per scopi assicurativi sono previsti espressamente dal diritto interno.

Nei casi di cui alle lettere b. e c. devono essere previste adeguate garanzie.

5.4. Le informazioni destinate all'interessato devono essere adeguate e adatte alle singole circostanze.

5.5. Qualora l'interessato versi in stato di incapacità giuridica e non sia in grado di decidere liberamente, e il diritto interno gli vieti di agire in modo autonomo, le informazioni devono essere fornite a chi ha legalmente il diritto di agire per conto dell'interessato.

5.6. Sono ammesse limitazioni alle informazioni da fornire agli interessati purché esse siano previste per legge e siano necessarie ai fini della prevenzione, delle indagini o del perseguimento di reati penali oppure allo scopo di garantire i diritti e le libertà altrui.

6. Consenso

6.1. Qualora sia richiesto il consenso degli interessati, deve trattarsi di un consenso fornito liberamente, in modo specifico e informato. Inoltre, il consenso deve essere inequivocabile e, se riguarda dati sensibili, esplicito.

Tuttavia, possono darsi situazioni nelle quali il diritto interno non ammette il consenso come fondamento sufficiente della liceità della raccolta o del trattamento.

6.2. Qualora i dati personali riguardino persone in stato di incapacità giuridica, e il diritto interno non consenta all'interessato di agire in modo autonomo, è necessario il consenso del legale rappresentante oppure di un'autorità o di un'altra persona o un altro organismo nominato per legge.

6.3. Se, ai sensi del Principio 5.5., un interessato che sia giuridicamente incapace è stato informato dell'intenzione di raccogliere e trattare dati che lo riguardano, se ne dovrebbero tenere in considerazione i desideri [le volontà espresse] purché ciò non contrasti con il diritto interno.

7. Raccolta e trattamento da parte di responsabili

7.1. Ai sensi delle disposizioni del diritto interno, i titolari possono affidare ad altri la raccolta ed il trattamento di dati personali per uno scopo specifico, nella misura in cui essi siano autorizzati a raccogliere e trattare tali dati ed il responsabile si impegni ad agire esclusivamente sulla base delle indicazioni del titolare ed a rispettare le disposizioni di diritto interno che danno attuazione al Capo 11 dell'Appendice alla presente Raccomandazione.

7.2. I titolari dovrebbero scegliere come responsabili soggetti che offrano adeguate garanzie relativamente agli aspetti tecnici ed organizzativi del trattamento da effettuare. Devono accertarsi dell'osservanza di tali garanzie e, in particolare, della conformità del trattamento alle indicazioni da loro fornite.

7.3. La raccolta e il trattamento di dati personali da parte di responsabili dovrebbero avvenire sulla base di un contratto o di un atto legale che vincoli il responsabile al titolare e specifichi che il responsabile può agire esclusivamente secondo le indicazioni fornite dal titolare e le disposizioni del diritto interno relative agli obblighi dei responsabili.

8. Comunicazione di dati per altri scopi

8.1. I dati personali possono essere comunicati per scopi diversi da quelli indicati nel Principio 4.4. esclusivamente se

a. ciò è previsto dal diritto interno e costituisce una misura necessaria, in una società democratica, ai fini della prevenzione, delle indagini e del perseguimento di reati penali oppure per garantire un altro importante interesse pubblico, oppure

b. gli interessati o i loro legali rappresentanti o un'autorità o un'altra persona o ente nominati per legge hanno prestato il consenso secondo quanto previsto dal Capo 6, oppure

c. la comunicazione è effettuata per scopi di marketing diretto, purché l'interessato ne sia stato informato e non vi si opponga. Tuttavia, dovrebbe essere richiesto il consenso espresso dell'interessato qualora i dati oggetto di comunicazione siano di natura sensibile, secondo quanto indicato al Capo 6, oppure

d. i dati sono necessari per il perseguimento di interessi legittimi del titolare, purché non prevalgano gli interessi della persona interessata. Tuttavia, dovrebbe essere richiesto il consenso espresso dell'interessato qualora i dati oggetto di comunicazione siano di natura sensibile, secondo quanto indicato al Capo 6.

9. Decisioni individuali automatizzate

9.1. Non si dovrebbero prendere decisioni in materia assicurativa che abbiano effetti giuridici per gli interessati, o comunque effetti significativi, qualora esse si basino esclusivamente sul trattamento automatizzato di dati finalizzato a valutare determinati aspetti personali concernenti gli interessati secondo criteri predefiniti o risultati statistici.

9.2. Tuttavia, tali decisioni possono essere prese se soddisfano una richiesta formulata dagli interessati ai fini della conclusione o dell'esecuzione di un contratto assicurativo, oppure se gli interessati hanno la possibilità di far valere il proprio punto di vista al fine di garantire la tutela dei propri interessi legittimi. Tali decisioni possono essere prese anche qualora siano autorizzate da una legge che tuteli gli interessi legittimi delle persone interessate.

10. Diritti di accesso e di rettifica

10.1. Tutti gli interessati dovrebbero avere la possibilità di ottenere, su richiesta, conferma dell'esistenza o meno di trattamenti di dati personali che li riguardano, e di ottenere, in forma intelligibile, tutti i dati che li riguardano nonché di essere informati almeno rispetto agli scopi del trattamento, alle categorie di dati oggetto di trattamento, ai destinatari o alle categorie di destinatari della comunicazione dei dati, ed all'origine dei dati. Inoltre, essi dovrebbero essere informati, su richiesta, in merito alla logica posta a fondamento del trattamento automatizzato di dati che li riguardano, almeno in caso di decisioni individuali automatizzate.

10.2. Il diritto degli interessati di ottenere i dati che li riguardano non dovrebbe trovare limitazioni, salvo che ciò sia previsto per legge e risulti necessario

a. per la prevenzione, le indagini o il perseguimento di reati penali;

b. per garantire i diritti e le libertà degli interessati o di terzi.

In tal caso, il diritto di accesso può essere limitato solo fin quando sussistano le motivazioni che ne hanno imposto la limitazione.

10.3. Gli interessati dovrebbero avere il diritto di ottenere la correzione, il blocco o la cancellazione dei propri dati, a seconda dei casi, qualora tali dati siano stati raccolti o trattati in difformità dalle disposizioni del diritto interno che danno attuazione ai principi della presente Raccomandazione e, in particolare, qualora essi risultino non accurati, non pertinenti o eccedenti.

10.4. Le motivazioni della limitazione del diritto di accesso, rettifica, cancellazione e blocco dovrebbero essere specificate per iscritto. In caso di limitazione del diritto dell'interessato di ottenere l'accesso a, la rettifica, la cancellazione e il blocco dei propri dati, l'interessato dovrebbe essere informato del diritto di chiedere all'autorità competente di verificare la liceità del trattamento.

10.5. I terzi destinatari della comunicazione dei dati dovrebbero essere informati della rettifica, della cancellazione o del blocco effettuati a meno che ciò risulti manifestamente irragionevole o irrealizzabile.

10.6. I titolari dovrebbero comunicare a intervalli ragionevoli e senza ritardi eccessivi con le persone che esercitano il diritto di accesso ai dati personali che le riguardano, anche per quanto concerne le informazioni di cui al Principio 10.1 rispetto alle quali sia formulata una richiesta di accesso.

11. Sicurezza dei dati

11.1 Dovrebbero essere adottate opportune misure tecniche e organizzative per tutelare i dati personali, che devono essere trattati conformemente alle disposizioni di diritto interno adottate in attuazione dei principi della presente Raccomandazione, contro la distruzione accidentale o illecita, la perdita accidentale, l'accesso, l'alterazione o la comunicazione non autorizzati e contro ogni altra forma di illecito trattamento.

Tali misure dovrebbero assicurare un livello adeguato di sicurezza tenendo conto, da un lato, dei più recenti sviluppi tecnici e, d'altro lato, della natura sensibile dei dati raccolti e trattati per scopi assicurativi e per la valutazione di rischi potenziali. Le misure in questione dovrebbero essere oggetto di un riesame periodico.

11.2. Al fine di garantire, in particolare, la riservatezza, l'integrità e la disponibilità dei dati oggetto di trattamento, nonché la tutela degli interessati, il titolare dovrebbe adottare opportune misure

a. per impedire a soggetti non autorizzati di accedere alle installazioni utilizzate per il trattamento di dati personali (controllo all'ingresso delle installazioni);

b. per impedire la lettura, la copiatura, l'alterazione o l'asportazione di supporti informazionali da parte di soggetti non autorizzati (controllo dei supporti informazionali);

c. per impedire l'inserimento non autorizzato di dati nel sistema informatico, nonché ogni consultazione, modifica o cancellazione non autorizzata dei dati personali memorizzati (controllo di memoria);

d. per impedire che sistemi per il trattamento automatizzato di dati siano utilizzati da soggetti non autorizzati attraverso dispositivi di trasmissione dati (controllo di utilizzazione);

e. allo scopo di consentire, da un lato, l'accesso selettivo ai dati e, d'altro lato, la sicurezza dei dati personali, per fare in modo che il trattamento sia strutturato, in linea di principio, così da consentire la separazione fra

- identificatori e dati relativi all'identità delle persone,
- dati amministrativi,
- dati sensibili (controllo degli accessi);

f. per garantire la possibilità di verificare e accertare a quali persone o enti sia consentita la comunicazione di dati personali attraverso dispositivi per la trasmissione dei dati (controllo delle comunicazioni);

g. per garantire la possibilità di verificare e stabilire, a posteriori, chi abbia avuto accesso al sistema e quali dati personali siano stati inseriti nel sistema informativo, quando e da chi (controllo dell'inserimento dati);

h. per impedire la lettura, la copiatura, l'alterazione o la cancellazione non autorizzate di dati personali durante la comunicazione di tali dati ed il trasporto di supporti informazionali (controllo del trasporto);

i. per salvaguardare i dati attraverso la realizzazione di copie di sicurezza (controllo della disponibilità).

11.3. I titolari dovrebbero redigere gli opportuni regolamenti interni, ai sensi del diritto nazionale, onde rispettare i principi pertinenti di cui alla presente Raccomandazione.

11.4. Se necessario, i titolari dovrebbero nominare un soggetto indipendente quale responsabile della sicurezza dei sistemi informatici e della protezione dati, con competenze estese alla consulenza in materia.

12. Flussi transfrontalieri di dati

12.1. I principi della presente Raccomandazione si applicano al flusso transfrontaliero di dati personali raccolti e trattati per scopi assicurativi.

12.2. Il flusso transfrontaliero di dati personali verso uno Stato che ha ratificato la Convenzione per la protezione delle persone fisiche rispetto al trattamento automatizzato di dati personali (ETS N. 108), e che dispone di norme di legge tali da garantire quantomeno un'equivalente protezione dei dati, non dovrebbe essere soggetto a condizioni speciali riferite alla tutela della privacy.

12.3. Non dovrebbero essere previste limitazioni al flusso transfrontaliero di dati verso uno Stato che non ha ratificato la Convenzione ma garantisce un livello adeguato di tutela.

12.4. Salvo diversa disposizione del diritto interno, il flusso transfrontaliero di dati verso uno Stato che non garantisce un livello adeguato di tutela non dovrebbe avere luogo, a meno che

a. l'interessato vi abbia acconsentito ai sensi del Capo 6, oppure

b. siano state adottate misure, anche di natura contrattuale, necessarie a rispettare le disposizioni del diritto interno che danno attuazione ai principi della Convenzione e della presente Raccomandazione, e l'interessato abbia la possibilità di opporsi al trasferimento.

13. Conservazione dei dati

13.1. Qualora i dati personali cessino di essere necessari per la realizzazione delle finalità per cui sono stati raccolti e trattati dal titolare, dovrebbero essere cancellati. Tale principio vale anche qualora si decida di rifiutare la copertura assicurativa. Tuttavia, se i dati devono essere conservati per scopi di ricerca scientifica o di statistica, o per altri scopi previsti dalla legge, dovrebbero essere conservati in forma separata ed essere accessibili esclusivamente per tali scopi, salva l'esistenza di opportune garanzie.

13.2. Nello stabilire il periodo di conservazione dei dati, si dovrebbe tenere conto, in particolare, della necessità di conservare i dati per il periodo necessario alla difesa di un diritto in sede giudiziaria, oppure per comprovare transazioni avvenute, o per giustificare la decisione di rifiutare la copertura assicurativa.

14. Rimedi giuridici

Il diritto interno dovrebbe prevedere opportune sanzioni e rimedi giuridici in caso di violazione delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente Raccomandazione.

15. Garantire il rispetto dei principi

15.1. Gli Stati membri dovrebbero incaricare una o più autorità di garantire, in piena indipendenza, l'applicazione delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente Raccomandazione.

15.2. Le informazioni di seguito indicate dovrebbero essere pubblicizzate nei modi opportuni e rese facilmente accessibili a chiunque:

a. nominativo e indirizzo del titolare e dell'eventuale rappresentante;

b. la o le finalità del trattamento;

c. la categoria o le categorie di interessati e dei dati;

d. il destinatario o le categorie di destinatari della comunicazione dei dati;

e. i trasferimenti di dati previsti verso Paesi terzi.

109 Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance

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.

The report and guiding principles prepared by Mr Buttarelli were published on the Council of Europe's website in December 2000 for public consultation. Comments on the text were received only from the International Communications Round Table (ICRT) who considered that the principles should be restricted to video surveillance and not extend to all other sectors of surveillance. On the basis of the report and guiding principles prepared by Mr Buttarelli, the CJ-PD decided to prepare a draft containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance. Members of the CJ-PD have been asked to send final written comments on the guiding principles prepared by the Co-ordination Group of the CJ-PD (June 2002). The Co-ordination Group will submit the guiding principles to the CJ-PD at its meeting in October 2002 for examination and approval. It is also preparing the third evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector.

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.

This is confirmed by a summary overview of the development of surveillance techniques, which initially focused (especially starting from the 1970s) on the monitoring of road traffic or else on the prevention of theft and robberies in banks and shops selling luxury items.

However, the relationship between surveillance and personal rights had long been pointed out, in particular concerning labour relations - so much so that the use of audiovisual and other devices for con-

trolling employees in the workplace was prohibited or specifically regulated by various countries (see, for instance, Italy's Act no. 300/1970).

In subsequent years surveillance techniques were especially refined in respect of the workplace: indeed, it became possible to control better the security of equipment, the quality and regularity of labour performance as well as productivity. The opportunity was also created for monitoring facts and circumstances having no relevance in terms of skill assessment.

During the 1980s there was also an increased use of surveillance techniques in the transportation sector - in particular on subways and in nearby areas - as well as within certain public buildings (in order to prevent vandalism) and in recreational areas.

The growing use of surveillance techniques by an increasing number of highly patronized shops resulted in facilitating the assessment of customer habits and behaviour with regard to the arrangement of the products on sale. In this specific sector, surveillance systems (especially video surveillance systems) became a valuable tool for commercial purposes even though they had been initially (or seemingly) deployed for the prevention of theft and robberies; in turn, this made it possible to rationalize business resources both within a given shop (for example, by determining the number of tills to be opened in accordance with the time of day and the monitoring of entrances) and from a more general standpoint (for example, by devising "shopping routes" that could be found more stimulating by consumers).

Surveillance techniques have been subsequently developing uninterruptedly and have been applied to the most diverse sectors.

In the transportation sector, there has been a continued increase in the number of controlled roads - both motorways and highways - with a view to the monitoring of traffic misdemeanours (even by means of infrared devices) and, more recently, the access to town centres - both big and small.

For instance, video surveillance devices have been installed :
- in stadiums [1] and sports facilities;
- in petrol stations;
- in casinos;
- in health care centres (in particular, emergency or reanimation rooms and during surgical operations)
- in sewage and waste disposal plants.

Museums and cathedrals have been the subject of this surveillance, which has also been applied to air or satellite observation activities (in connection with regular filming, with a view to geographic research, for air traffic management and for urban planning purposes).

Similar remote control techniques based on signal transmission are being used in respect of the electronic bracelets for convicts either paroled or released on licence or under house arrest.

Additional applications are related to the following sectors:
- the fight against illegal migrants;
- security of domestic units and residential districts (in this regard, there is a significant trend towards setting up, in the industrial and commercial sectors, "fortress units" as a way of preventing thefts, burglaries and vandalism);
- taxi services (for example, in New York a few cabs have been equipped with infrared cameras filming either clients when they get on the cab or the meter as it starts operating; the relevant images are recorded on digital media and automatically erased unless either the driver or the car owner decides otherwise);
- use of web-cams or online cameras for broadcasting images in connection with tourist promotion

(1) In the Recommendation on Stewarding (99/1), adopted on 9-10 June 1999 by the Standing Committee of the European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches, attention is drawn to the surveillance of all potentially dangerous areas and the prevention of overcrowding as well as, though in general, to providing spectators with information on all the security devices deployed by organisers.

activities or else for advertising public places such as bars or night-clubs, or even for showing living conditions in prisons;

- banking institutions, where hidden devices are frequently installed allowing the taking of fingerprints and photographs so as to identify, visually and based on the relevant fingerprints, all visitors - whether they are clients or not, including possible robbers and individuals reconnoitring the place with a view to a robbery.

The voluntary use of remote control techniques for managing the so-called e-family should also be pointed out; it has even been suggested that statistical surveys could be performed on the images recorded in order to establish the behavioural patterns of members of a given community/group.

Finally, reference should be made to the economic interests related to the production of the relevant equipment and devices and to the reduction in insurance premiums granted by insurance companies if surveillance systems or sarellite anti-burglar devices are installed in a vehicle.

2) A SHORT OVERVIEW OF THE AVAILABLE TECHNIQUES

As already pointed out, the increasing pace of technological evolution makes it absolutely necessary to set the surveillance issue against the relevant background.

Based on the technical development of these systems, it has progressively become possible :

- to transmit images to a "control centre" from terminals connected either via cable, optic fibres or digital network;
- to record images that in the past were only visible via CCTV (closed circuit television);
- to obtain images with higher resolution and reproduce them in colour;
- to associate images and sound;
- to expand the visual field up to a 360° vision;
- to use fixed and/or mobile, stationary and/or rotational cameras;
- to use zooming functions and therefore, magnify - even to a considerable extent - individual areas in a photogram.

Thus, there is the actual risk that any overview in this sector will rapidly become obsolete.

On the whole, it can be argued that the most significant contribution was not made so much by the enhancement of transmitting equipment (only think of the recently developed subcutaneous transmitters that are used for the surveillance of paroled convicts) or by the possibility of recording and keeping images instead of simply watching them, but rather by the introduction of "intelligent systems" for assessment and intervention. [2]

Indeed, the latest surveillance systems do not simply include an image-freezing (and printing) function nor are they exclusively connected to a control centre whence sound or visual alarm signals can be issued or else the closing of entrances to and/or exits from places and shops can be ordered, or where the intervention of staff or even helicopters can be requested. Nowadays, surveillance systems can be equipped or associated with software for automated image retrieval. There are systems allowing the recognition of persons by means of techniques for the targeting of suspected offenders - for instance, based on automatic facial recognition techniques (facial mapping computers).

It is increasingly feasible to issue various types of alarm (including the signalling to watchmen) regarding persons suspected either on account of specific descriptions or based on behavioural patterns that are automatically classified as "abnormal" by the software (for example, in a parking place or at the entrance to a stadium).

This points to the possible identification in future of alleged misbehaviour based either on the outward appearance (physical features, clothing, skin colour) or on actions and events that are regarded as especially interesting (sudden movements, smoke, opening of doors).

(2) Only think of the DcxNet system which - allegedly - is capable of facilitating driving when coupled with radar systems by operating brakes, steering wheel, etc. or even by guiding the driver in the presence of bad weather (for example, fog). This is an example of electronic networks applied to road traffic.

Whereas in the past there was just the exchange among supermarkets of videotapes including images of consumers either "suspected" or caught in the act, the most sophisticated systems available nowadays allow identifying the voice or conversation of the persons filmed - or, at the very least, significant words spoken by such persons - and even searching for a voice or face in an indexed file. For instance, a test system implemented in 1998 allowed retrieving over 1000 images per second, in real time, in order to find a given face; the system could not be fooled by the fact that the person in question was growing a beard or moustache as camouflage.

Recent tests have also allowed tracking the route presumably followed by a person or vehicle within complex scenarios or else identifying persons who frequently or at given intervals follow a certain route.

All the above techniques can obviously be implemented not only for the prevention and control of offences, but also for different purposes - such as finding missing persons or children - and in connection with the public interest; this is why the Council of Europe recommended their utilisation in some cases. [3]

Facial recognition systems have been used even with a view to preventing false marriages and - based on consensus - in order to allow access to workplaces or buildings (for example, by providing for the automatic opening of doors and gates in respect of the members of a given family) and for purchasing air tickets and using ATMs (automated teller machines).

There are ceaseless technological innovations in this sector. [4]

3) OVERVIEW OF THE EFFECTS OF SURVEILLANCE

In evaluating the effects of surveillance it is necessary, again, to take account of the relevant background.

This type of assessment is usually carried out with delay and is committed to experts, without any information to the public as a whole. Whenever it is decided that the relevant results should be disclosed to the public, the technology is found to have developed further and new considerations and analyses are required. [5]

For instance, the use of facial recognition techniques is currently far from widespread and the considerations mentioned above have been made exclusively by enlightened scholars and journalists. Meanwhile the growing diffusion of surveillance techniques and the increased number of entities keeping recorded images would require a different, more advanced type of analysis. It is time for legal scholars not to limit themselves to stressing the dangers of surveillance, but rather pay greater attention to the issue of the real-time interconnection of images obtained via surveillance which are kept by different entities (for example, motorway management companies, banks, town councils, etc.).

Given the above premises, the issue of the effects of surveillance should not only be the province of legal scholars, as the development of control mechanisms in the public sector makes it necessary for Parliament and the relevant institutions to carry out a political analysis.

In the first place, there is the need for assessing the proportional relationship between security and privacy requirements.

Indeed, surveillance systems may have positive effects in terms of security; however, there is no uniformity in the extent to which this effect can be regarded as positive. In a few cases there has been

(3) In Recommendation No. R(96)6 of the Committee of Ministers to Member States on the Protection of the Cultural Heritage against Unlawful Acts (adopted on 19 June 1996), under item 4 (concerning "Protective strategies for preventing and responding to unlawful acts") it is said that the preventive measures applying to museums, cathedrals, etc. should also include electronic surveillance measures (detection, control centre, transmission, closed circuit TV, monitoring access, video surveillance, and so forth).

(4) See, for instance, the recently published advertisement by Visionics Corporation (http://www.visionics.com) concerning the new version of the FaceIt Sentinel/Surveillance System 2.0 produced by Visionics.

(5) Consider, for instance, that the launching of an "Echelon2" system has been already reported when, in fact, the full picture of the Echelon1 system has not been highlighted yet.

undoubtedly a decrease in the number of criminal offences in public places; in other cases this surveillance has proved ineffective or caused criminals to move to other nearby areas, or else it has simply allowed obtaining evidence against the persons filmed.

Additionally, it should be considered that facial or behavioural recognition systems may frequently result in mistakes to the detriment of "innocent bystanders" - as they are based on the reduction of a face to a few dozen building elements and on the measurement of distances between key parts.

Since surveillance systems are likely to attain wider diffusion, their beneficial effects are also likely to decrease on account of their becoming rather commonplace. Finally, there is the risk that surveillance is implemented to an excessive extent as a handy way to cope with basic flaws in organisational and/or law enforcement matters rather than in order to meet actual requirements. As an example, consider that in Italy it has been proposed by a town council that video surveillance devices be installed under the wide vaulted passages of a few downtown streets since the police patrolling those streets in a car are unable to keep such passages under visual control.

It has even been suggested that a distinction should be drawn between:
- surveillance for control purposes (i.e., aimed at allowing the taking of measures in case of misconduct), and
- surveillance for prevention purposes (i.e., aimed at establishing a relationship with citizens in order to get them to behave in accordance with a given pattern).

In other words, it is feared that modern society may inadvertently tend to replace or supplement control with the incitement to self-control and the repression of impulses.

This consideration cannot but lead to expanding the scope of the assessment concerning surveillance, instead of limiting the analysis - as is often the case - to establishing whether control mechanisms cause a disproportionate damage to individual freedom as compared with the need for preventing and controlling crime. [6]

From this standpoint there can be no doubt as to the need in future for a definitely more selective approach to the use of surveillance systems: the public as a whole should not suffer excessive limitations on account of the need to prevent the misbehaviour of a minority.

The scope of discussion should therefore be expanded by going beyond the issue of the beneficial effects on security for persons and property: it would be more appropriate to evaluate also the effects, if any, on citizens' freedom and conduct.

In other words, in addition to considering the extent to which surveillance causes a breach of privacy, one should evaluate the effects resulting from the widespread use of surveillance as regards citizens' freedom of movement and behaviour.

As to the former issue, one should actually argue whether the freedom of movement which is referred to in many constitutional charters (as well as in Article 2 of Additional Protocol no. 4 to the European Human Rights Convention) means the freedom to move not only in a physical sense, but also in a more fundamental sense - that is to say, the freedom to move without having inevitably to leave continued and/or frequent traces of one's movements for the benefit of permanent "optic informers".

As to the latter issue, it has been suggested that the fact of "being seen without seeing" may influence a person's conduct and activity. On the one hand, hidden filming and/or control devices do not promote openness for citizens; on the other hand, cameras and other devices that are known to have been installed at a given location might lead to "submissive" behaviour on the citizens' part.

It is undoubtedly true that one should expect less privacy in public places; still, the concept that no

(6) In a meeting with Italy's Minister of Justice, it was recently reported alarmingly by 220 Italian chaplains that prison inmates no longer go to confession because they are afraid that bugs may be present in the confessionals.

privacy exists in public places is to be rejected.

Indeed, reference should be made in this regard :
- to domestic laws applying to non-economic rights in connection with copyright matters, which provide for safeguards even in respect of the dissemination/broadcasting of images related to facts, events and ceremonies either of public interest or occurring in public;
- to the national measures implementing Directive 95/46/EC, under which data subjects are entitled to object, on legitimate grounds, to the processing of their personal data even though the processing is ultimately lawful.

Additionally, it should be noted that the openness requirement is sometimes complied with exclusively by providing notification of the fact that cameras or other control devices have been installed and are in operation: citizens are "compelled" to provide personal data (often consisting of images) and no information is given as to their use, even though the data or images are included in data files or used for identification purposes. Citizens may thus be turned into information "subjects", without respecting the right to information self-determination. [7]

The lack of openness deprives citizens of the right to know that certain items of evidence included in the relevant data and/or images can be used against them.

If the concern for the possible discrimination against minorities and/or the sexual orientation of persons may be regarded by some as excessive in modern democratic societies, there is the actual risk of an all-pervasive control: indeed, technology should not be an obstacle to retaining the possibility of anonymity or privacy - all the more so if images are reproduced for private purposes or else for purposes less directly related to the public interest (see the recently reported use of advertising web cams in seaside resorts, which regularly perform close-ups of persons without their being aware of it).

4) THE INSTRUMENTS ADOPTED SO FAR BY THE COUNCIL OF EUROPE

It is probably unnecessary to point out here that the principles of Convention No. 108/1981 are based on the provisions of the Human Rights Convention [8]; by the same token, there is no need to stress that the processing of any personal data relating to natural persons that have been collected in connection with surveillance activities falls - as a rule - within the scope of application of Convention No. 108.

Indeed, this type of processing is performed in part by means of automated procedures on account of the tools used (for example, video cameras, bugs, computers, microphones, satellites, GPS equipment, etc.) (see Article 2(c) of Convention No. 108).

With regard to those Parties which - as is the case with Italy - have made use of the possibility of applying the Convention to the processing of data concerning groups, associations, foundations, societies, etc. as well as to manual processing operations (see Article 3(2), litt. b) and c) of Convention No. 108), the safeguards provided in the Convention also apply to the latter sectors.

Additionally, a few Parties have also provided for the above-mentioned safeguards in respect of collection; by so doing, they have in practice applied Article 11 of the Convention in line with Directive 95/46/EC, which includes collection in the definition of processing - unlike Convention No. 108.

This entails that the processing of data for surveillance purposes falls within the scope of application of Article 5 (quality of data), 7 (security), 8 (right of access), 10 (penalties and remedies) and 12 (transborder data flows) of the Convention - without prejudice to the derogations provided by domestic law in accordance with Article 9 of the Convention.

The application of the above-mentioned provisions to surveillance raises a few issues that will be

(7) The risks related to the widespread use of video surveillance in respect of the right to information self-determination and free movement in public places are highlighted in the resolution adopted by the 59th Conference of German Data Protection Authorities of the Federation and Länder, which convened in Hannover on 14-15 March 2000 ("Risks and Limitations of Video Surveillance").
(8) Mme Marie-Odile Wiederkehr, Discours d'ouverture, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 10.

addressed subsequently in connection with possible new initiatives by the Council of Europe.

It should be pointed out, however, that the application of Article 5 to surveillance activities results in the obligation for any entity processing the data to comply with safeguards that - if domestic legislation also takes account of collection operations and the strict observance of Article 5 is ensured - markedly influence the technical mechanisms underlying data collection. Only think, for instance, of the orientation and visual field of cameras, of the sensitivity of microphones, of the choice as to recording the data or not, and so on.

As to Article 6 in the Convention, it should be noted that certain data collected for surveillance purposes fall definitely outside the scope of this article: this may be the case, for instance, of surveillance for some commercial purposes or else performed in respect of direct marketing trainees, or even for some surveillance activities carried out by private detectives in connection with civil litigations, etc. There are, however, other data categories that are undoubtedly the subject of Article 6 provisions: reference can made in this regard to the surveillance in operating or emergency rooms, or else to the targeted surveillance activities performed by the police in respect of political and/or trade-union manifestations or small areas in which racial or ethnic minority groups are resident, or else in connection with prostitution activities.

It is currently debated whether Article 6 can also apply to the data collected (in particular by law enforcement agencies) with regard to persons suspected, but not yet convicted of an offence. Based on the wording of the second sentence in Article 6, one might argue that the answer should be negative as it only refers to criminal convictions; however, it has also been pointed out that even the data related to crime should be considered sensitive data, also where there is not yet a criminal conviction, but merely suspicion. [9]

Apart from the possibility for the Parties to extend the protection by applying Article 11, this interpretation issue is quite important: with regard to the processing of sensitive data, or data equated to sensitive data pursuant to Article 6, there must be suitable safeguards as provided for by a law, specific regulations or administrative directives [10] . Conversely, pursuant to Article 9, any derogations from individual principles in the Convention should be provided for exclusively by a law which also takes account of the "necessity" principle as defined by the European Court of Human Rights. [11]

This summary overview of the Convention is based on the following preliminary considerations:

- the Parties to the Convention can exclude certain processing operations from the scope of application of the Convention, as may be the case for the processing of data in connection with State security (a declaration to this effect has been made by Ireland) or else the processing of data for personal or domestic purposes (which has been excluded by various Parties);
- the data and information collected via surveillance are subjected to the Convention insofar as they relate to an individual that is identified or identifiable by reference to other information, irrespective of whether such information concerns linguistic data, static or dynamic images or sound. In this regard, the Consultative Committee of the Convention has rejected the opinion according to which voices and images are not to be regarded as personal data if they are unaccompanied by nominal information: in fact, it is sufficient for voices and images to provide information on an individual by making him/her identifiable even though indirectly. [12]

5) CONCEPT OF SURVEILLANCE UNDER CONSIDERATION

The scope of the surveillance concept is wide-ranging by nature and goes well beyond the control via video equipment - which constitutes nevertheless a major issue at stake. It can actually include the control of phone and computerised conversations as well as of the circulation of documents. It may even apply to the distance control of specific users of a service (see, for instance, the location of mobile pho-

(9) A. Patjin, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 17.
(10) Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 46.
(11) A. Patjin, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 18.
(12) In particular, the Consultative Committee has considered the digital processing of voices and images to always represent "automatic processing", whereas the analogue processing should only be regarded as such if voices and images undergo automatic processing in order to identify data subjects or else contribute to their identification.

nes) or else of persons in connection with a judicial action (this is the case with the use of electronic bracelets).

Thus, the attempt at taking into consideration the surveillance issue as a whole either in a single Recommendation or in a single instrument laying down Guidelines is undoubtedly to be commended, but is quite ambitious and may give rise to difficulties in drafting the text and ensuring its implementation.

Reference should be made in this regard to the specific issues related to the performance of surveillance activities for the defence of a legal claim as well as to the derogations from the right of access that in such cases should be provided for on a temporary and detailed basis.

Another important issue in this sector is related to the surveillance of correspondence (whether on paper or via electronic means) with prison convicts - an issue that was the subject of a recent, non-final decision by the European Court of Human Rights (28.09.2000), in which further considerations were made with regard to the legal grounds issue (2me Section - Affaire M. c. Italie, Requete n. 25498/94).

The Council of Europe Project Group on Data Protection has been working hard and with the contribution of highly qualified experts in order to add to the array of instruments that has already been developed by the Council of Europe via the inclusion of specific suggestions also in connection with technological innovation.

On account of the importance attached to this target the utmost care will be required in order to :

- avoid overlapping, possible inconsistencies, lack of co-ordination and unwanted softening of the relevant provisions as compared with the measures laid down in the existing Council of Europe Recommendations, and
- avoid following an excessively general approach with a view to including all the existing types of surveillance in the broad sense of the word; this would entail the risk of, on the one hand, setting out measures that are applicable specifically to video surveillance but are not suitable for other sectors, and, on the other hand, failing to envisage rules or exceptions that would be actually necessary when addressing more specific issues.

The scenario resulting from the existing applicable Recommendations points to the existence of incomplete safeguards concerning surveillance; it is necessary, however, not to jeopardise these safeguards as also related to their scope of application.

A) For instance, if Recommendation No. R(87) 15 is taken into account as a term of comparison, it would be appropriate for any future initiative by the Council of Europe not to fail to consider police activities that are performed in the course of a specific investigation provided for by law, as well as activities of a state security or military intelligence agency. As to specific investigation activities, consideration might be given to the possibility of exemptions applying to investigations in connection with the committing of a criminal offence pursuant to criminal procedural laws - subject to the differences in the existing legal systems.

In the Preamble to Recommendation No. R(87)15 it is stated that member States have the possibility of extending the relevant principles to processing operations for purposes of State security; this same possibility might be provided for in any new initiative taken by the Council of Europe - subject to appropriate safeguards.

With regard to crime prevention and control and the protection of public order, an attempt should be made in order to prevent simultaneous application of both Recommendation No. R(87) 15 and a new "instrument" developed by the Council of Europe. Indeed, Recommendation No. R(87) 15 includes important provisions that should be taken duly into account in connection with future initiatives.

For instance, Recommendation No. R(87) 15

a) allows introducing new technical means for data processing only if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation (item

1.2);

b) allows the collection of personal data for police purposes insofar as this is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Exceptions to this provision can only be introduced by specific national legislation (item 2.1);

c) allows the collection of data by technical surveillance or other automated means only if this is provided for in specific provisions (item 2.3);

d) prohibits the collection of data on individuals solely on the basis of their racial origin, religious convictions, sexual behaviour or political opinions (item 2.4);

e) specifies the cases in which the data may be communicated (item 5), which makes it difficult to lay down additional measures in this regard.

Finally, attention should be paid to the provision included in Recommendation No. R(87)15 as regards the right of an individual whose personal data have been collected or stored without his knowledge to be informed if such data are not destroyed (item 2.2). This is especially important in connection with the proposals made as regards the possible limitations on the data subject's right to be informed in respect of surveillance activities if these limitations are provided for by law in order not to prejudice surveillance activities.

B) As to Recommendation No. R(89) 2 on the protection of personal data used for employment purposes, consideration might be given in particular to the provision requiring employees to be informed or consulted before introducing automated systems for data collection and utilisation (item 3.1) - in addition to the general provision on the respect for private life and human dignity of employees, with particular regard to the possibility of exercising social and individual relations in the workplace (item 2). The aforementioned provision also applies to the use of automatic telephone call logging devices in the workplace (see Recommendation No. R(95) 4, item 7.15).

Special attention should also be paid to the provisions on collection and storage of "sensitive" data concerning employees (see item 10.1 in Recommendation No. R(89)2).

C) Overlapping should be avoided in respect of Recommendation No. R(95)4, on the protection of personal data in the telecommunications sector, with particular regard to telephone services. Indeed, this Recommendation regulates also the services provided by networks allowing users to be in correspondence via images. In this regard, it is provided that anonymous systems must be made available for accessing the network; any interference with the content of communication is in principle prohibited (items 2.2, 2.3, 2.4 and 2.5). Regarding billing operations for the use of telephone services, it must be ensured that subscribers and called users are not located with precision at the time of utilisation (item 7.2.1).

D) Other Recommendations include general provisions on data processing; although these provisions are not expressly related to surveillance, they lay down safeguards and rules that are nevertheless applicable and therefore require co-ordination - especially in respect of data communication and transborder data flows.

If the Council of Europe sticks to the ambitious target of setting out standards applicable to surveillance as a whole, or else to certain types of surveillance - and in particular to video surveillance- co-ordination with a few existing Recommendations is required. There are two alternatives in this regard:

- instances of overlapping could be prevented and a statement could be made to the effect that any new initiative by the Council of Europe (for example, Guidelines on surveillance) is only meant as an addition to the previous Recommendations and applies to such matters as were not addressed by the said Recommendations, which would therefore be left unprejudiced. However, this approach might fail to be fully satisfactory as only a few Recommendations already include provisions that are applicable to this matter albeit indirectly: certain sectors might therefore be left outside the scope of the relevant provisions;
- the substance of any new initiative by the Council of Europe could be fully harmonised with that of the existing Recommendations whenever they are found to overlap, by indicating that the new instrument specifies and expands the existing requirements (for example, as regards data collection mechanisms, exercise of data subjects' rights, etc.).

Alternatively, it might be considered whether it would be appropriate to adopt a list of Guidelines, a sort of summary "decalogue" aimed more specifically at video surveillance and the provision of additional safeguards that should not overlap with those already available.

Regardless of the approach adopted, the Council of Europe might rapidly achieve a satisfactory solution by completing the analysis that has been carried out so far concerning surveillance.

To that end, I believe consideration might be given to the following initial suggestions - which should by no means be regarded as exhaustive.

6) GENERAL REMARKS

Firstly, one should be aware of the risk of drafting an instrument that is excessively broad in scope: this would make it difficult to simultaneously and reasonably take account of all the requirements and - above all - exceptions in respect of all the cases and purposes of surveillance activities without resulting in inconsistencies or reduced protection. [13]

Secondly, one should aim at preventing any new initiative by the Council of Europe in this sector from being considered - on account of its possibly broad scope of application - excessively generic and lacking in innovation as it includes no such guidelines as would be required by the specific arrangements applying to the collection and processing of data for surveillance purposes (for example, enhanced compliance with the purpose specification and proportionality principles; ad hoc mechanisms for exercising the right of access; provisions on matching and interconnection of data; more specific rules for the storage of data; ban on automatic processing operations aimed at defining personality; etc.).

7) DEFINITIONS

The surveillance concept could perhaps refer to "any activity operated by technical means, consisting in monitoring, collecting and/or recording, on a non-occasional basis, personal data concerning one or more individuals and relating to their behaviour, movements, communications and utilisation of computerised and/or electronic devices" if the Council of Europe decides to address this issue by going beyond the video surveillance concept. [14] It is actually preferable to provide for a wide-ranging definition including no excessively technical details. It would also be preferable to refer to non-occasional surveillance rather than to "systematic" operations. In addition, surveillance activities should be taken into consideration as such, irrespective of whether they may entail the possible infringement upon private life.

It may be appropriate to expressly re-affirm that personal data also include images and sound (if the relevant equipment allows identifying data subjects even indirectly) as well as traffic data or data resulting from signal transmission where such data allow locating individuals or establishing the time of and the parties to a given conversation or communication.

The definition of "processing", if provided, should clarify that reference is also made to the mere observation of behaviour without recording (unless observation is included in the definition of collection).

It should be considered whether communication is to be distinguished from dissemination.

It should be considered whether it might be appropriate to clarify that the unambiguous, conclusive conduct by the data subject can be equated to consent with regard to certain types of surveillance provided that effective, clear information is given.

(13) For instance, in setting out the lawfulness requirements applying to (video) surveillance, the safeguards provided by Recommendation No. R(87) 15 should not be reduced; the latter Recommendation actually requires data collection to be performed for the prevention of a real danger (2.1), surveillance to be provided for by specific provisions (2.3), no data to be collected concerning an individual solely on the basis of the latter's race etc. (2.4).

(14) This definition would include both the tracking of transactions on the net and satellite surveillance activities, as well as the surveillance aimed at locating a given person (for example, via the signals transmitted by mobile phones).

The exclusion of data processing operations applying to private or family life from the scope of application of any new instrument is basically acceptable, although this provision would be partly superfluous as various Parties have already excluded this sector from the scope of application of the Convention; still, it would not seem to be fully appropriate to provide for the absolute exclusion of :

- surveillance performed by law enforcement agencies in connection with specific investigations pursuant to law; indeed, it would be preferable to refer to criminal investigation activities, which in a few Parties can be performed directly by members of the judicature rather than by law enforcement agencies - in pursuance of the domestic laws regulating criminal procedure;
- surveillance performed by State security agencies; for instance, any exception concerning State security should be harmonised with the possibility granted to Parties by Recommendation No. R(87)15 of applying the latter Recommendation to these matters;
- journalistic activities: indeed, the collection of data in connection with freedom of expression activities should not provide an opportunity for boundless surveillance initiatives - partly on account of the provisions made in various European countries following Directive 95/46/EC.

8) RESPECT FOR PRIVACY

It might be appropriate to briefly refer, in any new instrument drafted by the Council of Europe, to the need for applying national provisions on video surveillance by taking account also of constitutional provisions as well as of the measures laid down in the Criminal Code concerning the protection of domicile - under which certain places such as hotel rooms, offices, public lavatories, locker-rooms, in-house phone booths are regarded as "domicile" [15] . In this regard, it should be pointed out that in a few countries items of evidence that have been collected in breach of the law are absolutely inadmissible pursuant to specific provisions of criminal procedural law [16].

It could be considered whether it might be appropriate to call upon member States, manufacturers and service and access providers as well as researchers to commit themselves to ensuring that software, technologies and technical devices are developed by paying greater attention to data subjects' fundamental rights. [17] Similar suggestions are included, for instance,

- in Recommendation No. 1/99 on invisible data processing operations on the Internet, as adopted on 23 February 1999 by the Working Party set up pursuant to Article 29 of Directive 95/46/EC, including the independent DP supervisory authorities of EU member States (this Recommendation also applies, for instance, to clickstreams);
- to a lesser extent, in Recommendation No. R(99)5 of the Council of Europe, on the protection of privacy on the Internet (see the Preamble, where the development of techniques allowing anonymity for data subjects is called upon), [18] and in Directive No. 97/66/EC, on the protection of privacy in the telecommunications sector (with regard, for instance, to new forms of anonymous or strictly private access to publicly available telecommunications services - see Recital no. 18).

Conversely, there would be no need for considering another issue which is regulated by public and civil law - namely, the cases in which the owner of a property is under the obligation to allow installation of permanent surveillance devices by a public body, a private entity or else a condominium.

9) COLLECTION AND PROCESSING OF SURVEILLANCE DATA

The principle according to which personal data should be processed lawfully, fairly and for specified, explicit, legitimate purposes could be usefully re-affirmed and highlighted.

10) LAWFULNESS REQUIREMENTS

In laying down the lawfulness requirements for surveillance or video surveillance, account will have to be taken of the safeguards that are already provided for in principle 2 of Recommendation No. R(87)15 : existence of specific legislation; prevention of a real danger.

(15) Reference should be made in this regard to two decisions by the Italian Court of Cassation: no. 7063/2000 and no. 8250/2000.

(16) This is the case, for instance, of the provision to police of images showing a pusher where such images have been filmed by chance near the restrooms of a shop by surveillance equipment installed by the owner in breach of the law.

(17) A similar indication (though aimed actually at permitting the lawful interception of communications) is included in Items II,5 and VI,15 of Recommendation No. R(95)13 concerning problems of criminal procedural law connected with information technology.

(18) See also Council of Europe Recommendation No. R(95)4 on telecommunications, where the availability of anonymous access to network and telecommunications services is also called upon (item 2.2).

On the other hand, these requirements will have to be adjusted to other cases - such as the surveillance performed by defence counsel and duly authorised private detectives for the defence of a legal claim, or else the surveillance of the behaviour and conduct of direct marketing trainees.

With regard to the level of specification of domestic legislation, consideration could be given to the decision of the European Court of Human Rights in the Rotaru v. Romania case, which was adopted on 4 May 2000, at the same time as the 5th Meeting of the CJ-PD GC of 10-12 May 2000. [19]

Adjustments will also have to be considered in respect of surveillance performed for medical purposes - i.e., in order to safeguard a data subject's life or bodily integrity or in any way protect a legitimate interest of the data subject or a third party. Special attention will have to be paid to those cases in which surveillance may be permitted by law, but neither the data subject nor the third party are in a position to give their consent. Reference is made here to cases that have occurred in Italy, concerning the continued observation of individuals either in a coma or hospitalised in an emergency room, or else individuals hospitalised and kept in isolation who were only visible at a distance to relatives and friends - in a room where other hospitalised patients could have also been visible if suitable measures had not been taken.

Finally, I would suggest that the lawfulness requirements could be supplemented by providing for the protection of data subjects against "automated individual decisions" related to their personality, professional performance, reliability, behaviour, ethnic origin and so on - as resulting in an "automatic" fashion from the processing of data that have been collected for surveillance purposes (see Article 15 of Directive 95/46/EC). Reference could be made in this regard to the issuing of alarm signals based on facial recognition techniques in connection with skin colour.

I would also like to draw the Council's attention to national laws and regulations providing for the compulsory recording of either the contents or the relevant traffic data, as the case may be, of phone calls and orders placed via computerised means in connection with brokerage activities.

11) PURPOSE

Any instrument providing manoeuvring room for the distance control of employee efficiency - which is currently prohibited in many countries - would be unacceptable. This point needs clarification by the Council of Europe: there must be an absolute ban on any system aimed at intentionally determining quality and quantity of employees' work. Based on the experience gathered by various countries, the use of systems serving different purposes should be permitted - such purposes being related to organisational and/or production requirements or else to occupational safety issues; however, given the possibility that these systems result in the distance control of employees, reference should be made to the need for respecting trade unions' rights. Indeed, in a few countries the latter category of surveillance system can only be implemented after informing and - in a few cases - reaching an agreement with the relevant trade unions.

(19) In the decision concerning the lawfulness of the processing of incorrect data by the Romanian Intelligence Service (RIS), the Court stated that:
"As regards the requirement of foreseeability, the Court noted that no provision of domestic law laid down any limits on the exercise of those powers. Thus, for instance, domestic law did not define the kind of information that could be recorded, the categories of people against whom surveillance measures such as gathering and keeping information could be taken, the circumstances in which such measures could be taken or the procedure to be followed. Similarly, the Law did not lay down limits on the age of information held or the length of time for which it could be kept.
Section 45 empowered the RIS to take over for storage and use the archives that had belonged to the former intelligence services operating on Romanian territory and allowed inspection of RIS documents with the Director's consent. The Court noted that the section contained no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that could be made of the information thus obtained.
It also noted that although section 2 of the Law empowered the relevant authorities to permit interferences necessary to prevent and counteract threats to national security, the ground allowing such interferences was not laid down with sufficient precision.
The Court also noted that the Romanian system for gathering and archiving information did not provide any safeguards, no supervision procedure being provided by Law no. 14/1992, whether while the measure ordered was in force or afterwards.
That being so, the Court considered that domestic law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. The Court concluded that the holding and use by the RIS of information on the applicant's private life had not been "in accordance with the law", a fact that sufficed to constitute a violation of Article 8. Furthermore, in the instant case that fact prevented the Court from reviewing the legitimacy of the aim pursued by the measures ordered and determining whether they had been - assuming the aim to have been legitimate - "necessary in a democratic society".

In this regard, safeguards should be set out for all data, whether sensitive or not. Nor would it be acceptable for such safeguards to apply only if the surveillance is "intended" to collect sensitive data (which would not appear to be frequently the case); this would rule out all types of safeguard for those (more frequent) cases in which the data are collected either occasionally or unintentionally or periodically by a surveillance device.

By referring (expressly or not) to Recommendation No. R(89)2 (para. 3), consideration could therefore be given to a few guidelines with a view to, at least,

- suggesting the need to abstain from the filming of places that are reserved for employees and not for work (for example, toilets, showers, locker-rooms, recreational areas);
- hearing the prior opinion of employees in connection with the installation of devices and equipment on account of organisational and/or production requirements, or else for occupational safety purposes; in the latter cases, disclosing the relevant purposes, arrangements, capabilities and utilisation as also related to time and circumstances of the recording;
- granting employees the right also to ground their counterclaims on portions of the recordings that have been taken into account, in whole or in part, in the claims raised against them.

12) BASIC PRINCIPLES TO BE INCLUDED OR SPECIFIED FURTHER

The selectivity and proportionality principles could be specified further in any new instrument that the Council of Europe might decide to develop in future concerning surveillance or video surveillance, by providing that surveillance systems should only be implemented if this is actually necessary in order to prevent or detect crime or else safeguard others' rights and the use of a less privacy-intrusive manner of collection of data proves impossible.

If compliance with the proportionality principle is not ensured, the number of public and private areas under surveillance might increase exponentially in the next few years: the final outcome would be a society placing excessive restrictions on personal freedom. As to proportionality, one should refrain from simply laying down the principle that surveillance must be related to lawful purposes as based on - often generic [20] - legislation or else with a view to preventing nondescript offences which might be construed so as to include not only breaches of criminal law, but also breaches of administrative/civil/disciplinary laws. Surveillance should not be ordered for such purposes as detecting non-compliance with the ban on smoking in public lavatories [21] or the prohibition on throwing waste and cigarette stubs on public roads. [22]

In other words, surveillance should be focused on areas that are really at risk, [23] public events that can reasonably be expected to give rise to incidents and more serious crimes.

Greater emphasis could be placed by the Council on the principle according to which data should be relevant and not excessive in relation to the purposes of their processing. In particular, with regard to video surveillance, the relevant stakeholders should be called upon to

- define precisely, in all cases, the location of cameras and the arrangements for filming (as to storage and conservation of images, visual shooting angles, possible limitations on close-ups and image scans);
- reduce the visual field in connection either with the purpose sought [24] or with the areas actually requiring surveillance, with particular regard to those cases in which cameras filming public places allow identifying sound and images from private places nearby;
- perform the filming in a way only allowing, as a rule, a panoramic view of the area under surveillance (subject to technical limitations) - without the possibility of close-ups or subsequent magnification and by avoiding the inclusion of irrelevant details or physical traits in relation to the purposes sought.

(20) A specific problem is related to local authorities planning the blanket installation of surveillance systems both in respect of crimes falling within their competence (road traffic offences; access to town centres) and as a way to facilitate crime prevention and control (even though local authorities are not always directly competent for ordre public matters).

(21) As reported in Belgium concerning a technical high school.

(22) A surveillance system was allegedly installed without informing data subjects even at a citizen advice bureau in a German town.

(23) This was the concept underlying a French circular letter of 22.10.96, in which isolated places and shops closing late at night were referred to as examples.

(24) In Italy, the Garante per la protezione dei dati personali has requested that the visual field of cameras used for detecting road traffic offences be limited to the area where number plates are usually located. This is important as regards, for instance, the driver's privacy.

13) INFORMATION FOR THE DATA SUBJECT

The information principle might actually affirm that the information provided to data subjects may fail to include the location of the surveillance devices. However,

- such devices should be precisely listed in advance by the surveillance data controller and reported in the declaration or registration document referred to above, to be deposited with a (preferably independent) public authority;
- the information should not be provided by using remote signs (for example, placed at a distance of up to 500 metres, as is already the case in a few circumstances), but rather by placing such signs at a reasonable distance;
- as to visual symbols, reference might be made very briefly to the possibility (already tested) of providing a different type of information by using the camera symbol (if images are not recorded) as opposed to another symbol if images are also recorded;
- it could be better specified that data subjects are to be informed clearly (even summarily, provided this is effective) in all cases, regardless of the use of electronic networks;
- any restrictions on the information provided to data subjects should be really in proportion to the purpose sought. It might be appropriate to specify (as is the case in a few legal systems, such as the Italian one) that the limitation resulting from the collection of data for investigational purposes or else the defense of a legal claim is a temporary measure and only applies for as long as the provision of information can be reasonably considered to jeopardise the achievement of the above purposes.

Additionally, it might be appropriate to specify with regard to consent requirements that, at least under certain circumstances, the data subject's consent may also consist in his/her conclusive conduct - provided he/she has been given clear information.

14) COMMUNICATION

It would be necessary to exclude, in principle, dissemination of images and communication to third parties who are not concerned by the surveillance activities; the cases in which this might be permitted as well as the relevant arrangements and purposes should be specified in detail.

15) INTERCONNECTION

The proportionality principle could be developed further in this regard, in order to identify those cases in which the indexing of surveillance personal data is allowed. Indexing of the data - especially on a nominal basis - should only be permitted by specific provisions pursuant to the proportionality principle.

Secondly, the proportionality principle should be better detailed so as to limit the matching of surveillance data processed by different controllers to those cases in which this is actually necessary for the purposes provided for by law - especially if the matching is aimed at tracking the "route" followed by a given individual.

16) RIGHT OF ACCESS

Data subjects' rights should be taken into account in a comprehensive fashion as is the case with Community legislation, rather than by simply referring to access and rectification rights.

Based on the considerations made, the following issues could also be addressed:

- a data subject that cannot object to the surveillance should be granted the right to object, on legitimate grounds that are found to prevail based on his/her specific circumstances, to certain types of data processing as provided for in Article 14 of Directive 95/46/EC. This should apply at least to a few of the cases in which surveillance is permitted by law even without the data subject's consent as well as whenever the data subject is informed that lawful surveillance activities are being performed and cannot in practice but give his/her consent as based on his/her conclusive conduct (for example, whenever he/she happens to be on a public road or in a bank where surveillance is signalled). Reference could be made to a case that occurred in Italy, in which an employee accepted the systematic surveillance of her activity in the workplace in order to document individual production phases (in connection with the tanning of hide), but objected to the fact that such images were broadcast for advertising purposes.

Secondly, the need to somewhat reconcile right of access and specific nature of the data undergoing processing is undoubtedly understandable, also in the light of the media used for recording. Still, it would not appear to be acceptable that this is done by ruling out the right of access if the data subject has not been identified but is identifiable.

Indeed, if limitations on the right of access are considered to be necessary, account will have to be taken of the fact that this is only permitted by Article 9(2), litt. b), of Council of Europe Convention No. 108 to a limited extent - i.e., if it is actually necessary for protecting the rights and freedoms of a third person.

For instance, it might be specified that a request for access can always be made by the data subject since it is the expression of an actual right rather than merely of a "legitimate interest"; under certain circumstances, however, the surveillance data controller can lawfully abstain from answering the request and/or processing data in order to make a data subject identifiable if this entails a manifestly disproportionate effort - without prejudice to such measures and steps as might be taken by law enforcement or judicial authorities in compliance with the law.

Furthermore, it might be considered whether it would be appropriate to provide that recovery and communication of the data be ruled out if the data are to be destroyed within a very short term (for example, 2-3 days or a week); this would be without prejudice to the possibility of accessing the data for the defence of a legal claim or else with a view to producing evidence following an order issued by law enforcement or judicial authorities.

As regards the possible exclusion of the right of access on account of the legitimate interest of a third person, this should only be permitted if the data controller is unable to take technical measures aimed at reconciling the rights of the data subject with those of the third person who is also the subject of the processing. This is the case, for instance, of the partial magnification or blurring of images in which various persons are visible. Access to the data could be permitted in any case if this is necessary for the defence of a legal claim.

Account might be taken expressly of those cases in which access may be deferred lawfully (albeit as a temporary measure) for as long as the discovery of the data by the controller would actually jeopardise the controller's right of defence of a legal claim. Reference could be made in this regard to the evidence collected in cases of conjugal or other infidelity, which defence counsel may plan to produce at trial following the investigations that a private detective has carried out in pursuance of domestic law.

Finally, reference might be made to those cases in which access can be granted by only permitting the inspection of the data as the latter cannot be recorded on any media.

17) CONSERVATION OF DATA

As regards the period of and arrangements for conservation of data, surveillance data controllers should be required to evaluate - even before deciding for how long the data are to be conserved in connection with the purposes to be accomplished - whether it is necessary to conserve the data or it is enough that these data can be visualised in the light of the purposes sought (for example, in the case of a CCTV system used for checking the opening of doors and entrances). [25]

Furthermore, the time limits established for each type of surveillance activity should be without prejudice to the possibility and/or the duty for the surveillance data controller or a third party to retain longer such data as may have been extracted with a view to establishing or defending a legal claim. It might also be suggested that surveillance data controllers should not delete or destroy the data if a request for conservation of the data is submitted either by the data subject or a third person with a view to establishing or defending legal actions.

25) For instance, regulations recently passed in Italy (no. 250/1999) provide that the systems used for surveillance of the access to town centres and pedestrianised areas only collect images in case of the commission of offences.

18) RESPECT FOR THE PRINCIPLES

It is appropriate to re-affirm the principle according to which the processing of personal data for surveillance purposes must be the subject of supervision by an independent authority - in line with item 1.1 in Recommendation No. R(87) 15.

This is especially important with regard to local authorities (municipalities, provinces, Regions): although they have in principle no direct competence on matters of public order - and might therefore be considered to fall outside the scope of application of Recommendation No. R(87) 15 - these authorities actually perform various collateral activities for surveillance purposes.

Apart from this general, solemn reference it might be considered whether to provide that surveillance systems be the subject of at least a simple declaration or registration to be made either with a law enforcement agency or an independent authority - in order to ensure transparency and promote the protection of data subjects' rights as well as control by the supervisory authority. [26] It might additionally be suggested that in respect of certain more privacy-intrusive surveillance systems the cases be specified in which either prior checking (in line with the relevant provisions included in Article 20 of Directive 95/46/EC) or the prior approval of an authority would be required.

If the surveillance activities performed by media are also taken into consideration (which would seem to be appropriate), the mechanisms envisaged for publicising the processing operations should be brought into line with Recommendation No. R(94) 13 of 22 November 1994 on measures to promote media transparency.

As a conclusion, it might be argued that the Group is faced with the alternative between a new Recommendation on surveillance and the definition of guiding principles to be included in a different type of instrument.

Both solutions are of interest. Twenty years after the adoption of Council of Europe Convention No. 108 what really matters is for the Council of Europe to let its authoritative voice be heard once again.

(26) The Parties might use, for instance, a portion of the notification form that is commonly available for the notification of a wide range of processing operations.

110 Guiding principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance

FOREWORD

Many public and private entities have been increasingly using surveillance systems for various purposes and in different sectors, by controlling, in particular, movement of persons and goods, access to property as well as events, situations and conversations - whether by telephone, electronic networks or at a physical location.

Surveillance systems often result into the collection of personal data even though their collection and/or storage is sometimes not aimed at by the surveillance data controller.

A considerable portion of these activities are performed by means of video surveillance devices, which raises specific issues as regards data protection.

Indeed, the data collected during video surveillance activities consist mainly in images and sound which either identify or allow identifying data subjects, whether directly or not, in addition to monitoring their conduct.

Video surveillance activities entailing the processing of personal data fall within the scope of application of Council of Europe Convention No. 108 - whose principles are based on the provisions included in the Convention on the Protection of Human Rights and Fundamental Freedoms.

Additional rights and safeguards are laid down in various Council of Europe Recommendations, in particular:

a) Recommendation No. R(87) 15 on the use of personal data in the police sector;

b) Recommendation No. R(89) 2 on the protection of personal data used for employment purposes;

c) Recommendation No. R(95) 4 on the protection of personal data in the telecommunications sector;

d) various other Recommendations which - though not expressly referring to video surveillance - include safeguards and rules that are relevant in terms of personal data protection as also related to data communication and transborder data flows.

Video surveillance raises specific data protection issues which are not addressed in detail in the instruments that have been referred to, partly on account of the mechanisms of data collection and storage as well as in the light of technological development.

It is therefore necessary to lay down additional guiding principles in order to expand and specify further the safeguards applying to data subjects - without prejudice to the protection already provided by the above instruments in various sectors - as regards any type of video surveillance activity allowing, by means of technical equipment, non-occasional observation, collection and/or storage of personal data relating to one or more individuals in respect of their conduct, movement, communications and use of computers and electronic networks.

These guiding principles are intended for the widest possible dissemination among all public and private users of video surveillance systems, devices and techniques; additionally, they are addressed to

Member States, manufacturers, dealers, service and access providers and researchers with a view to developing software and technologies that can pay greater attention to data subjects' fundamental rights in respect of video surveillance.

These guiding principles should also be implemented with regard to other surveillance activities that are not based on the use of video surveillance devices, subject to appropriate adjustments.

GUIDING PRINCIPLES FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE COLLECTION AND PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE

Any video surveillance activity should be undertaken :

1) by checking if and to what an extent it is permitted on suitable grounds of law for lawful, specific, explicit, legitimate purposes and be carried out in a fair manner. Video surveillance activities for police purposes should only be undertaken for the prevention of a real danger or the suppression of a specific criminal offence;

2) by taking such measures as are necessary in order to ensure that this activity complies with personal data protection principles;

3) by only using video surveillance devices if less privacy-intrusive systems cannot be implemented;

4) by complying with the selectivity and proportionality principles as regards the purposes sought in the individual cases, in order to prevent data subjects' freedoms and conduct (where appropriate, these freedoms may include the data subjects consent, which might be expressed, at least, in conclusive manner) from being unreasonably impinged upon, with particular regard to freedom of movement and right to informational self-determination, and by ensuring a reasonable privacy expectation even in public places;

5) by complying with the principle according to which data must be relevant and not excessive in relation to the image, sound and biometric data collected, by taking especially into account the mechanisms of data collection (e.g. as regards the use of fixed or mobile cameras; extent of visual field; possibility of magnifying images, and so on) and preventing the collected information from being stored, indexed or kept for a long time if this is not necessary for the specific purpose(s);

6) by refraining from video surveillance activities if they are likely to result in discrimination or have been ordered with regard to certain data subjects exclusively on account of their opinions, beliefs or sex life;

7) by complying with the transparency principle, i.e., by publicising the specific video surveillance activity (by submitting a publicly accessible notification to a preferably independent public authority) and informing the data subjects (by providing clear-cut, even summary, information with easily visible signs pointing to the location of filming devices). Restrictions on openness and information requirements should only be permitted to a reasonable, proportionate extent and where they are necessary for protecting the rights, freedoms and purposes which are referred to in Article 9 of Convention No. 108;

8) by ensuring enhanced protection in the presence of specific dangers for data subjects and/or more pervasive controls, e.g. as regards:
- association of images and biometric data;
- use of intelligent analysis and intervention systems;
- software for automatic image retrieval or facial recognition;
- indexing of collected data;
- profiling of data subjects;
- possibility of taking automated decisions in connection with professional skills, performance, reliability, ethnic origin;

- video surveillance aimed at getting citizens to behave in accordance with a given pattern.

9) communication of personal data to third parties who are not concerned by the surveillance activity should be prohibited in principle, subject to specification of the cases in which this can be permitted including the relevant arrangements and purposes;

10) by laying down ad hoc arrangements for the exercise of right of access and other rights by data subjects and only providing for restrictions on these rights to a reasonable, proportionate extent where this is necessary for protecting the rights, freedoms and purposes which are referred to in Article 9 of Convention No. 108. In particular, the exercise of the right of access should also be permitted (even by means of the visual inspection of images) if the data subject can be identified. The surveillance data controllers should be entitled to refuse access if this entails a clearly disproportionate effort or the data are to be destroyed within a very short time - subject to judicial and legal defense requirements, e.g. as regards postponement of access for defense purposes;

11) by refraining from the use of systems aimed at the intentional surveillance of quality and quantity of performance in the workplace and by ensuring that employees are suitably informed - if necessary by seeking the agreement of the relevant trade unions if such systems are to be implemented on account of organizational and/or production requirements or else for occupational safety purposes entailing distance control; employees' human dignity should be respected in all cases, including the possibility of establishing social and personal relationships in the workplace. In this context, employees should be able to ground their counterclaims on the recordings made.

Autorità di controllo comune Schengen

111 Implementation of Schengen in the UK

JOINT SUPERVISORY AUTHORITY

Brussels, 11 March 2002
(OR. EN)
SCHAC 2502/2/02
REV 2

NOTE
from : The Chairman of the JSA
to : The Chairman of the Article 36 Committee (EU/Iceland and Norway Mixed Committee)
Subject : Implementation of Schengen in the UK

I. Introduction

By Council Decision of 29 May 2000 the Council decided that the United Kingdom and Northern Ireland shall participate in the provisions of the Schengen Acquis. This participation includes the provisions concerning the Schengen information system to the extent that they do not relate to Article 96.

In its opinion (SCHAC 2520/01) of 23 October 2001 the JSA Schengen informed you that the UK solution as described in document 8913/01 COMIX 374, leads to processing Article 96 data by the UK in breach of Article 94 of the Schengen Agreement.

In reaction to your request for an opinion regarding new solutions of the UK and Dutch delegations (doc.nr. 6340/02 SIS 12 COMIX 115), the JSA Schengen has reviewed this matter at its meeting of 8 March 2002.

This opinion is closely related to the opinion of the JSA Schengen of 23 October 2001.

II. Grounds for the JSA Opinion

The Schengen Convention that was signed on 19 June 1990, regulates in Title IV a co-operation between the Contracting Parties with the Schengen Information System (SIS) as an instrument to support that co-operation. Leading principle is the full participation of all Contracting Parties in the provisions of Title IV.

The first three chapters of Title IV contain specific rules for the setting up of the SIS, the operation, utilization and the data protection rules. These rules are tailored for a SIS that is composed of identical national sections (N.SIS) and a technical support function (C.SIS).

Since the Council Decision of 29 May 2000 concerning the participation of the United Kingdom and Northern Ireland in some provisions of the Schengen acquis, the questions arises if the provisions in Title IV can be applied in situations where the basis principle of full co-operation is set aside.

From a data protection point of view this means that the proposals which are subject of this opinion must be assessed on the basis of the meaning of the data protection provisions in Title IV. These provisions that are also integrated in the rules regarding the operation and utilization of the SIS are not imposed to the Contracting Parties with the sole purpose of protection the rights of an individual. These pro-

visions also focus on aspects of decent processing of data, confidentiality, reliability and more in general a professional organisation.

The SIS is composed of the N.SIS of the Contracting Parties and the C.SIS that is established to keep the N.SIS identical. Since the questions concerning the participation of the United Kingdom and Northern Ireland focus on the data that will be processed in the N.SIS, the opinion of the JSA will in principal be limited to the N.SIS.

Data in the N.SIS

According to Article 92(2) the data files of the N.SIS of all Contracting Parties must be materially identical. Article 94(1) explicitly limits the processing of data in the N.SIS to those data that are required for the purposes laid down in the Articles 95-100.

This principle of Article 94(1) originates from the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 1981 (Convention 108) and the Recommendation nr. (87) 15 adopted by the Committee of Ministers of the Council of Europe on 17 September 1987 regulating the use of personal data in the police sector, and is also incorporated in the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

A decision to keep all the N.SIS 100% identical with all categories of data, even if some Contracting Parties do not participate fully with Article 95-100, will be in breach of Article 94(1) and lead to an infringement with the rights of an individual that cannot be justified by mere motives of economic and operational aspects.

A decision to allow a co-operation with only certain aspects of Title IV may cause an operational problem with the C.SIS and the N.SIS, but the non-compliance with Article 92(2) does, from a data protection point of view, not cause an infringement on the rights of an individual. If a procedure is set in place that upholds the principle that an individual can still exercise his rights in every Contracting Party, the mere fact that not every Contracting Party has all the SIS information will cause no infringement on his rights.

This means that applying the Articles 92 and 94 in view of the partial participation by the United Kingdom and Northern Ireland, the principle of Article 94(1) that limits the processing of data in the SIS to the purpose for which the data were entered in the SIS, prevails the principle of Article 92(2).

The effect of the Council Decision regarding the participation of the United Kingdom and Northern Ireland leads - from a data protection point of view- to an interpretation of Article 92(2) that allows the national sections of the SIS not to be materially identical.

The question if Article 92(2) allows the existence of N.SIS-files that are not materially identical with other N.SIS files can also be answered from an operational point of view. The wordings "data-files" in Article 92(2) may correspond to all the data regarding an individual that must be identical in all the N.SIS, as well as to data regarding all the individuals whose data are processed in the N.SIS.

The first interpretation makes participation with some provisions of the Schengen acquis in compliance with Article 92(2) as long as the data regarding an individual, processed in view of one of the purposes mentioned in Article 95-100, will be processed identical in all the N.SIS.

Access to- and use of the SIS data.

Article 92 (1) describes the different sections of the SIS and restricts the access to the alerts for purposes of border checks and controls and other police and customs checks.

Article 101 (1) specifies the categories of authorities that shall have the right of access. The main principle in this article is that only those authorities that are responsible for the checks and controls as mentioned in Article 92 (1) may be granted the right to have access to the data in the N.SIS.

Article 102(1) limits the use of data provided for in the Articles 95-100 to the purposes laid down

for each type of alert referred to in those articles.

Access and use are thus restricted to the purposes for each type of alert as referred to in the Articles 95-100. Since the United Kingdom and Northern Ireland do not participate with the provisions of Article 96, access and use of these data cannot be related to the purpose of Article 96. This also applies to the special provisions that allows the use of these data for examining visa applications and residence permits (Article 101(2)).

The right of access for an individual

The JSA has in its first opinion already described this item in detail and refers to its opinion of 23 October 2001 (SCHAC 2520/01)

The problem with the double alerts

The access to- and use of the N.SIS data is primarily regulated through the Articles 94, 101 and 102. In order to prevent the existence of conflicting alerts in the N.SIS, Article 107 contains a special procedure.

To comply with Article 107, a Contracting Party must check if an alert that it intends to process in the SIS conflicts with an existing alert on the same person.

This obligation to check can be regarded as a special rule for access to - and use of to data for the sole purpose of complying with Article 107. The way this access and use is granted and exercised must be limited to such as is necessary for the prevention of conflicting double alerts.

Since the present Contracting Parties already processed the data that must be checked to comply with Article 107, and provided that this check is exercised in a way limited to such as is necessary for the prevention of conflicting alerts, no problem exists.

In the situation of the participation of the United Kingdom and Northern Ireland the requirement to prevent conflicting alerts needs a different solution compared with those Contracting Parties that have access to all the categories of data.

The requirement to comply with Article 107, does, in the situation where the processing including the use and access to some of some of categories of data is not permitted by the Articles 94(1), 101(1) and 102(1), not provide a legal ground for processing these categories of data. The obligation to limit the access to data for the sole purpose of complying with Article 107 forces to look for a solution that minimise the infringement of the rights of the individual. In practice this solution is generally found in technical- and organisational solutions.

Since the United Kingdom and Northern Ireland are not allowed to process data on reports for purposes, to which they do not participate, a technical- and organisational solution must be established to comply with Article 107.

III. The UK and Dutch solutions

The JSA has assessed these solutions on the basis of the legal grounds as described in Paragraph II.

The proposals of the UK and Dutch delegations give various alternatives for enabling the UK to fulfil all the obligations of participating in the provisions of the Schengen acquis.

The proposed UK solutions start from the idea that all SIS-data are transmitted to and processed by the UK. The access to the Article 96 data is subsequently restricted to a limited number of people with a strictly regulated access.

Since these proposals upholds the principle of transmitting data regarding Article 96 to the UK, these proposals will be in breach of Article 94 of the Schengen Agreement.

The proposed Dutch solutions both starts from the idea that the Article 96 data are not transmitted to the UK but vary in the way this is worked out.

The first Dutch option places a filter at the technical support function (C.SIS) that prevents transmitting Article 96 data to the UK and at the same time provides for a special data base for the purpose of checking for double alerts.

If this check in the special data base is limited to such as is necessary for the prevention of conflicting double alerts, this technical- and organisational solution is in line with the opinion of the JSA as described in Paragraph II.

The second Dutch option places the unfiltered UK data base within the C.SIS. Since this proposal is closely related to the discarded option in annex 1 of doc.nr 6340/02, the JSA shall not comment on that option.

IV Proposal for amending the Schengen Acquis

In the request for a further opinion a request was included to indicate what rules of the Schengen acquis might have to be adapted in respect of each of the available options.

In view of the limited time for the JSA to prepare and adopt this opinion, this request can not be met. However, changing the Schengen acquis in a sense that all the Article 95-100 data shall be distributed to all the N.SIS, even in the case that one or more Contacting Parties do not participate with all the provisions of Title IV, shall not be possible. A change like that shall always be in breach with the basic legal principle underlying Article 94.

V. Opinion

The choice for one of the options in doc.nr. 6340/02 SIS 12 COMIX 15 must be in compliance with the basic data protection principle as laid down in Article 94(1) of the Schengen Convention. The NSIS of the United Kingdom and Northern Ireland may only process data that are required for the purpose laid down in the Articles 95-100 of the Schengen Convention.

The only solution that is in compliance with this basic principle is the Dutch solution, option 1.

Mr. Giovanni Buttarelli , Chairman

112 SIS II developments

EUROPEAN UNION
JOINT SUPERVISORY AUTHORITY
SCHENGEN

Brussels, 3 December 2002
(OR. en)
SCHAC 02

OPINION
Subject: SIS II developments

I.Introduction.

The need to develop a new, second generation Schengen Information System (SIS), as well as the wish to introduce new functions for the SIS have been subject of discussion in the past years.

On the initiative of the Kingdom of Spain, a Council Regulation (OJ C160, 4.7.2002, p.5) and a Council Decision (OJ C, 4.7.2002, p.7) has been drafted concerning the introduction of some new functions for the SIS, in particular in the fight against terrorism.

The Chairman of the SIS Working Group has requested the JSA on 28 June 2002 to give its opinion on these initiatives. During the preparatory activities concerning the development of the SIS II, the Schengen Joint Supervisory Authority (JSA) has on 13 June 2002, already presented an opinion on this subject to the SIS Working Group.

The JSA considers it at its task to give an opinion on the draft Council Decision and the draft Council Regulation.

The JSA is aware of the fact that further discussions in the Schengen Acquis Working Group may lead to amendments of the proposed Council Regulation and Council Decision. Since the present opinion of the JSB only relates to the initiatives of the Kingdom of Spain as published in the Official Journal on 4 July 2002, the JSB stresses the need to be informed on any amendments of these initiatives and given the opportunity to state its opinion.

II. General remarks.

One of the implications of the signing on 19 June 1990 of the Convention implementing the Schengen Agreement of 14 June 1985 was the establishment of a SIS.

In view of the purpose of this Schengen Convention, the SIS was developed to enable the authorities designated by the Member States to have access by an automated search procedure, to alerts on persons and property for the purpose of border checks and other police and customs checks. In case of the alerts referred to in Article 96 - aliens for the purpose of refusing entry - the data may be also be used for the purposes of issuing visas, residence permits and for the administration of legislation on aliens in the context of the application of the provisions relating to the movement of persons. The need to have data available within a very short period of time, lead to the development of a system that may be characterised as a hit-no-hit system. The SIS processes only those data that are necessary for the purposes for which it was created. If a person is subject of a control and a search procedure is started in the SIS, this system only reveals if there is an alert and if so what immediate action should be taken. Any other information needed for a further action is not processed in the SIS but made available for the authorities via the SIRENE bureau's.

The responsibility for the data processing in the SIS and the necessary provisions to safeguard the right of the individual are clearly defined in the Schengen Convention. These provisions are "tailor made" for the categories of data that are processed, for the technical aspects of the SIS and for the use of these data.

The draft Council Decision and the Council Regulation contain changes of the Schengen Convention of a different nature. Some of the proposals contribute to the further elaboration of legal structure of the SIS and the way the rights of the individual are safeguarded. Other proposals fill in a need that exists in practice to have more information on identity documents or other objects.

The draft Council Decision and the Council Regulation also contain specific proposals that are apparently inspired by a more general wish to connect different data files in order to improve the police- and judicial co-operation between the Member States. The experience with the SIS, the work of Europol and the establishment of Eurojust apparently lead to the present proposals concerning the connecting of their data files.
The JSA acknowledges the need to improve co-operation in the field of justice- and home affairs.

The JSA stresses that the Schengen Convention and the SIS are created to support the Member States on certain area's of public order and security, were a resemblance seems to be present with the tasks of Europol and Eurojust. However, this resemblance does not necessarily qualify the SIS as an instrument that may be used to enable Europol and Eurojust to fulfil their tasks. If it is considered that the SIS must be regarded as an important component for this co-operation, a fundamental discussion on the position of the SIS should take place and a clear view on the future of the SIS including the necessary safeguards for the rights of the individual developed.
The JSA offers to participate in that discussion.

The present proposals to develop the SIS II including its new functions shall be assessed on their compliance with the present provisions of the Schengen Convention.

In view of the close relation between the proposals in the draft Council Regulation and the draft Council Decision, the JSA shall in this opinion assess these proposals to change the provisions of the 1990 Schengen Convention as one. The JSA took note of the explanatory memorandum relating to these initiatives.

III. Specific remarks.
(i) Article 94(3) of the Schengen Convention.

Article 1(1) of the draft Council Decision proposes to add two extra categories of data to the list of data that may be processed on persons for whom an alert has been issued. These new categories of data concern the type of offence in cases of alerts under Article 95 and information concerning the absconding from a place of detention in cases of alerts under Article 95 and
Article 99.

According to the explanatory memorandum, these new categories provide for a possibility to add certain information concerning people notably to enhance the security of officers checking the person. The JSA acknowledges the need to provide a certain security level for those authorities who are executing the SIS alerts. For this reason Article 94(3) already foresees the possibility of adding a warning that a person is armed or may be violent. While executing an Article 95 or Article 99 alert, an executing officer shall always act with his professional and appropriate prudence. The fact that a person is reported for an arrest for extradition, a specific check or discreet surveillance, gives every reason to be cautious. The mere mention of the type of offence or the fact that someone has absconded from a place of detention shall not enhance the security of the officer checking the person.

Since no other argument is presented to motivate the necessity of the adding of these two new categories of data, this proposal should not be adopted. *The JSA suggests that for those alerts where the absconding form a place of detention leads to expectation that the person involved is expected to try to escape any arrest, an extra category should be added to Article 94(3) stating that there is a risk of escape.*

(following paragraph deleted)

(ii) Article 99(1 and 3) of the Schengen Convention.

Article 1(2)(3) of the draft Council Decision proposes to change Article 99 concerning its content and the procedure when alerts are made at the request of the authorities responsible for national security. The JSA has no comments on the adding of categories of data concerning ships, aircraft and containers to the categories as mentioned in Article 99(1).

The procedure as described in Article 99(3) was dictated by motives of safeguarding the accuracy and liability of data as well by motives of an operational point of view. It prevented that actions may be requested that could harm ongoing investigations from another Member State.

The proposed change of this prior consultation into a system of "keeping each other informed" is motivated in the explanatory memorandum as simplifying the procedure. In its opinion of 13 June 2002, the JSA has already stated that the promotion of a better use of these alerts is in itself no reason to overlook the safeguards for accuracy and liability of the data.

Since no other arguments *are presented* that motivate the amendment of Article 99(3), the JSA underlines the need to hold on to the procedure as described in Article 99(3).

(iii) Article 100(3) of the Schengen Convention.

The JSA has no comments to this proposal.

(iv) Article 101(1)(b) of the Schengen Convention.

Both the draft Council Decision (Article 1(5)) as the draft Council Regulation (Article 1(1)), propose to amend this Article. The amendment opens the possibility to grant access to the SIS-data to authorities that have a judicial supervision on police- and customs checks as well as the judicial supervision on the co-ordination of such checks. The proposed definition seems to allow access for a court of law as well as access for authorities that have a legal responsibility to assess the actions performed by their subordinates. Since the proposed judicial supervision also covers the supervision on the co-ordination of the checks, *and shall be difficult* to implement in those Member States where the co-ordination of the checks in some Member States is done by public prosecutors, this *wide definition need to be clarified further.*

Last paragraph is deleted

(v) Article 101(2) of the Schengen Convention.

The draft Council Regulation proposes in Article 1(2)(3), to add in Article 101(2) the access to data entered under Article 100(3)(d) and (e). The JSA has no principle objections against the proposal to create access to these documents.

The JSA underlines the importance of safeguarding that the use of these data shall not limit the rights of citizens whose identity documents were stolen. *The JSA refers further to its opinion of 13 June 2002 and to its opinion of 15 February 200 on SIS alerts on persons whose identity has been usurped.*

(vi) New Article 101A of the Schengen Convention.

Article 1(6) of the draft Council Decision proposes a new Article 101A that regulates the access to certain SIS alerts for Europol. The explanatory memorandum does not explain the motives to allow Europol access to these data, which makes it difficult to assess this proposal. Since this proposal comprises a fundamental deviation from the basic principles of Article 102 of the Schengen Convention concerning the use of SIS-data, an explanation on the motivation of this deviation should be presented.

As already explained in III (i), the character of the SIS can be described as a hit-no-hit system. Europol shall -if the proposal will be adopted- only be able to see if an alert is issued against a certain individual. The SIS does not contain any data concerning the details of the case leading to the alert. Therefor, the need for Europol to have this information in order to perform its task is not clear. Except for the information as mentioned in Article 100, the data in Article 95 and 99 of the Schengen Convention do not have sufficient comprehensive substance that allows an organisation as Europol to further process these data.

It is a basic data protection principle that the processing of data, including the access and further use, must be lawfully and for a legitimate purpose. *Since no sufficient grounds are presented, the JSA is not able to assess if the proposal is in compliance with that principle.*

Last paragraph is deleted

(vii) New Article 101B of the Schengen Convention.

Article 1(6) of the draft Council Decision proposes a new Article 101B that regulates the access to certain SIS alerts for Eurojust. The explanatory memorandum does not explain the motives to allow Eurojust access to the SIS data, which makes it difficult to assess this proposal. Since this proposal comprises a fundamental deviation from the basic principles of Article 102 of the Schengen Convention concerning the use of SIS-data, an explanation on the motivation of this deviation should be presented. The same remarks as made under point vi of this opinion concerning the content of the SIS apply for Eurojust.

The access to SIS data is exclusively dealt with in the Schengen Convention. According to 101(1) of this Convention, the access to the SIS data is restricted to those persons who are responsible for the co-ordination of the checks as mentioned in that article. If Article 1(5) of the draft Council Decision and Article 1(1) of the draft Council Regulation are adopted, Article 101(1) also regulates the access of the authorities that have the judicial supervision on the checks as mentioned in that article. The national law of the Member States applies and determines which authorities have that specific task.

It is also noticed that Article 9 (4) of the Eurojust Council Decision connects the access to national data files to the applicable national law.

Since the Schengen Convention and the Eurojust Council Decision both connect the access to national files to the national law, it is the Member State that has to determine in what way it shall implement the proposal of the draft Council Decision and -Regulation.

The task of the national members in Eurojust as described in Article 6 of the Eurojust Council Decision is different from the task of national magistrates. When access is created to SIS data, the task for which that access will be granted must be in compliance with those articles of the Schengen Convention that deal with access and use of the SIS data.

Although the Eurojust Council Decision and the Schengen Convention both use the words "co-ordination" as an element of the task, the subject of co-ordination seems to be different. A further explanation is needed to delimit the access and use of SIS-data and show a similarity in the co-ordination for SIS checks and the co-ordination task in Article 6 of the Eurojust Council Decision.

If access is granted it should be clarified what is meant by this access. Does it mean that a check can be made on the existence of an alert on a specific person, or is it also meant as a possibility to process these data according to Article 14 and 15 of the Eurojust Council Decision.

In that case Article 102(2) forbids the duplication or copying of reports in national data files applies. Although Eurojust is not a national data-file, the purpose of Article 102(2) is clear on this point.

Access and further processing of SIS-data by Eurojust shall also cause a problem concerning the data integrity. When a SIS alert is executed and the data is deleted, who will inform Eurojust on the deletion and in what way?

In order to prevent these integrity problems, the JSA holds the opinion that, if the proposal shall be adopted, only a view-access should be allowed if and when all other conditions that are mentioned in this opinion have been fulfilled.

A last question relates to the access to categories of data as mentioned in Article 95 and 98 data. In view of the task of Eurojust, and more specifically the co-ordination task, it should be clarified which specific role Eurojust needs to fulfil that makes it necessary to have access to all the data mentioned in those articles. This is particular the case when it concerns data on convicted persons and witnesses.

In comparison with the proposed new Article 101A, the present proposal for a new Article 101B. contains less limitations for Eurojust then imposed on Europol. Since there is no reason for not having the same limitations and obligations, the JSA proposes -in case a new Article 101B shall be adopted- to have similar limitations and obligations for Europol and Eurojust.

(viii) Article 102(4) of the Schengen Convention.

The JSA has no comments to this proposal.

(ix) Article 103 of the Schengen Convention.

Both the draft Council Decision (Article 1(7)) as the draft Council Regulation (Article 1(4)), propose to amend this article.

The JSA welcomes every contribution to the control and monitoring of the use of the system. The JSA refers to its opinion (SCHAC 97(70))[1] in which the JSA has determined what data should be recorded. The most important elements for appropriate logging include:

a. biographical data transmitted concerning the person on whom the search is run;

b. identification of the terminal or the authority which carried out the search, ensuring that all the necessary measures are taken to enable the user to be identified;

c. place, date and time of search;

d. grounds for consultation, such as the legal basis for an alert.

The JSA has no objections to extend the storage period of these records to one year, but stresses the need to amend Article 103 in order to establish a clear and specific regulation of the recording of searches and where all the elements of the recording are specified.

(x) Article 108 of the Schengen Convention.

Both the draft Council Decision (Article 1(8)) as the draft Council Regulation (Article 1(5)), propose to amend this article. *According to the explanatory memorandum, a new paragraph is proposed to create a common legal basis for the existence and functioning of the SIRENE bureaux.*

The creation of this legal basis in the Convention by introducing a new paragraph added to Article 108 completes the legal structure for the Schengen information circuit, starting at the issuing of alerts and finishing with the concluding of the actions to be taken in connecting with an alert. Since the SIRENE bureaux are designated to exchange information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in relation with an alert, the new paragraph 5 should also contain rules concerning the use of the SIRENE data, similar to the rules concerning the SIS-data. This use should be limited to the purposes for which the data are processed by the SIRENE bureaux as mentioned in the proposed new paragraph added to Article 108.

(xi) Article 113 of the Schengen Convention.

Both the draft Council Decision (Article 1(9)) as the draft Council Regulation (Article 1(6)), propose to amend this article. A new paragraph is proposed that sets up rules for the archiving of SIRENE files. The JSA welcomes the view that the Convention specifically relates the deletion of SIRENE-data to the deletion of SIS-data. This proposal completes the provisions relating to the existence and work of the SIRENE bureaux.

The provisions in the Schengen Convention concerning the reviewing and deletion of data are divided in two articles. Article 112 contains specific rules concerning the reviewing and deletion of personal data. Article 113 contains specific rules concerning the reviewing and deletion of other non-personal data.

In view of this, the proposed amendment should follow the same distinction as between these articles. In order to prevent any misunderstandings, the deletion of personal data processed by the SIRENE bureaux should be subject of a new paragraph added to Article 112 and not of Article 113.

IV General conclusions

On the various proposals to change the Schengen Convention, the JSA has made its observations and specific remarks . The JSA urges to reconsider the draft Council Decision and Council Regulation in the light of the considerations made in this opinion.

The JSA also envisaged a change in the role and character of the SIS in the future. The JSA stresses the need to have a fundamental discussion on this point and offers to participate in that discussion.

(1) Published in the Second annual report of the JSA

113 Opinion concerning the relation between Article 112 and 113 of the Schengen Convention

JOINT SUPERVISORY AUTHORITY

Brussels, 7 October 2002
(OR. EN)
SCHAC 2510/1/02
REV 1

OPINION

Subject: Opinion concerning the relation between Article 112 and 113 of the Schengen Convention

Opinion nr.SCHAC 2510 r1
concerning the relation between Article 112 and 113 of the Schengen Convention

1. Introduction

The Greek Personal Data Protection Authority has requested the Joint Supervisory Authority of Schengen (JSA) for an opinion concerning the relation between Article 96 and the Articles112 and 113 of the Schengen Convention. The reason for this request was a question of the Aliens Directorate of the Greek Police to the Greek Personal Data Protection Authority concerning the retaining period for alerts based on Article 96 of the Schengen Convention.

The Greek Personal Data Protection Authority decided to ask the opinion of the JSA on this subject in view of its task according to Article 115(3) of the Schengen Convention.

The JSA defines the question as: does Article 112 of the Schengen Convention, that provides for a retaining period period of three years or Article 113 that provides for a retaining period of ten years, apply in relation to the alerts as described in Article 96 of the Schengen Convention.

2 Relevant Law.

Article 92 of the Schengen Convention

1. ...The Schengen Information system shall enable the authorities designated by the Contracting Parties, by means of automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks carried out within the country in accordance with national law and, in the case of the specific category of alerts referred to in Article 96, for the purposes of issuing visa, residence permits and the administration of legislation on aliens in the context of the application of the provisions in this Convention relating to the movement of persons.
2. ...
3. ...

Article 93 of the Schengen Convention

The Purpose of the Schengen Information System shall be in accordance with this Convention to

maintain public policy and public security, including national security, in the territories of the Contracting Parties and to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system.

Article 96 of the Schengen Convention.

1. Data on aliens for whom a alert has been issued for the purposes of refusing entry shall be entered on the basis of a national alert resulting from the decisions taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law.

Article 112 of the Schengen Convention.

1. Personal data entered into the Schengen Information System for the purposes of tracing persons shall be kept only for the time required to meet the purposes for which they were supplied. The Contracting Party which issued the alert must review the need for continued storage of such data not later than three years after they were entered. The period shall be one year in the case of the alerts referred to in Article 99.

2. ...

3. ...

4. The Contracting Party issuing the alert may, within the review period, decide to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the technical support function. The provisions of paragraph 1 shall apply to the extended alert.

Article 113 of the Schengen Convention.

1. Data other than that referred to in Article 112 shall be kept for a maximum of 10 years, data on issued identity papers and suspect banknotes for a maximum of five years and data on motor vehicles, trailers and caravans for a maximum of three years.

2. ...

3. The request.

In its Decision No. 54/2002, the Greek Personal Data Protection Authority has decided to submit the question concerning the retaining period of personal data processed according to Article 96 of the Schengen Convention to the JSA. The JSA is asked for its interpretation of the applicability of Article 112 or of Article 113 of the Schengen Convention in relation with the personal data as mentioned in Article 96.

In that decision the Greek Personal Data Protection Authority also concluded the following:

Article 112 of the Schengen Convention, which provides that the need to retain entries should be reviewed every three years, refers to data entered for the purpose of tracing persons.

These are mainly persons wanted for arrest under a warrant or other document having the same force or pursuant to a judgement for the purpose of their extradition, i.e. the persons referred to in Article 95 of the Schengen Convention.

Conversely, the data referred to in Article 96 of the Schengen Convention are not entered for the purpose of tracing persons but with the aim of preventing entry into the Schengen area of aliens believed to represent a danger to public order and security or against whom removal measures have been applied. Accordingly, the length of time such data may be retained should be governed by Article 113 of the Schengen Convention, which provides that such data may be retained for a maximum of ten years, and not Article 112.

4. Findings

The Decision No. 54/2002 of the Greek Personal Data Protection Authority links categories of alerts to different provisions for the reviewing and deletion of data. The requested kind of action to be taken

in connection with an alert determines if Article 112 or Article 113 of the Schengen Convention is applicable.

According to Article 92 and 93, the SIS contains data on persons that enables the authorities on the occasion of a check on a person (normal border - or police control), to see if there is an alert concerning that person and subsequently inform the controlling authority what specific action (according to Article 95-99 of the Schengen Convention) must be taken. Although the purposes of the alerts may be different, the function of the SIS is for all those alerts the same: alerting the authorities that a certain action is required. No data are processed in the SIS that could be used for other police investigations then a simple checking if an alert exists.

The Schengen Convention and the SIS do not make a distinction between different kind of police actions.

Article 112 of the Schengen Convention contains provisions for the reviewing and the deletion of personal data entered into the SIS for the purposes of tracing persons.

Article 113 of the Schengen Convention contains similar provisions concerning other data than that referred to in Article 112. Since a clear distinction is made between personal data in Article 112 and other data in Article 113, it can be concluded that Article 112 of the Schengen Convention exclusively covers the reviewing and deletion of personal data.

According to Article 112(4), personal data may only be processed in the SIS after the reviewing period when this is proved to be necessary for the purposes for which the alert was issued. This paragraph creates the possibility to retain data in the SIS if an assessment of the facts justifies this explicitly.

Since the Schengen Convention does not distinguishes different kind of police actions in relation with the SIS, no argument can be found that links Article 112 to those personal data that are used for tracing people and that personal data that are not used for tracing people will fall within the scope of Article 113.

The meaning of the word" tracing" in Article 112 (1) of the Schengen Convention has in itself and in relation with Article 92 and 93 of the Schengen Convention no sufficient comprehensive substance that justifies a conclusion that Article 113 is applicable on personal data that is not used for tracing but for other forms of police action.

The JSA has found no other argument in the Schengen Convention that would direct to another interpretation of the Schengen Convention. It should further be noted that the SIS information functionality as mentioned in Article 112(3) covers all the personal data processed according to the Articles 95-99

5. Opinion

Based on the text of the Schengen Convention, its objective, the implementation of the SIS and its technical structure, the JSA comes to the opinion that the reviewing and the deletion period of personal data in the SIS, is exclusively dealt with in Article 112 of the Schengen Convention.

Done at Brussels , 7 October 2002

Mr. Giovanni Buttarelli , Chairman

114 SIS II developments

EUROPEAN UNION
JOINT SUPERVISORY AUTHORITY SCHENGEN

Brussels, 3 December 2002
(OR. en)
SCHAC 2513/02

OPINION

Subject: SIS II developments

I. Introduction.

The Chairman of the SIS Working Group requested the JSA on 26 November 2002 to give its opinion on the initiatives of the Kingdom of Spain for a Council Regulation and a Council Decision concerning the introduction of some new functions for the SIS, in particular in the fight against terrorism.

During the preparatory activities concerning the development of the SIS II, the Schengen Joint Supervisory Authority (JSA) has on 13 June 2002, and on 1 October 2002 (SCHAC 2509/2/02 Rev2) already presented an opinion on this subject to the SIS Working Group.

The JSA brings to mind the guidelines for the cooperation with the JSA concerning the requirements for SIS II. These guidelines that were adopted by both the JSA as the Article 36 Committee provide for a reasonable period (i.e. one to two months) for the JSA to state its opinions.

The time made available for the JSA to study the new draft and to adopt an opinion - no more then three working days - only allows the JSA to present a preliminary opinion on the draft Council Decision and Council Regulation.

In view of the close relation between the proposals in the draft Council Regulation and the draft Council Decision, the JSA shall in this preliminary opinion assess these proposals to change the provisions of the 1990 Schengen Convention as one. The JSA took note of the documents 5970/02 SIS 8, Europol l9,Comix 80 and 9323/02 SIS 35, Europol 42, Comix 363.concerning the access to SIS for Europol, and the documents 11653/02, SIS 58, Schengen 7, Comix 492 and 13389/02 SIS 76, Schengen 15, Comix 594 concerning the access to SIS for Eurojust.

II. Specific remarks.

(i) Article 92(4).of the Schengen Convention

The JSA supports the creation of a legal basis in the Convention for the existence and functioning of the SIRENE bureaux. The JSA repeats its comments in its opinion of 1 October that since the SIRENE bureaux are designated to exchange information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in relation with an alert, the new paragraph 4 should also contain rules concerning the use of the SIRENE data, similar to the rules concerning the SIS-data. This use should be limited to the purposes for which the data are processed by the SIRENE bureaux as mentioned in the proposed new paragraph added to Article 92.

(ii) Article 94(2)(b) of the Schengen Convention
The JSA has no comments.

(iii) Article 94(3) of the Schengen Convention.
In its opinion of 1 October the JSA stated that the introduction of the fact that someone has absconded from a place of detention might be considered if better proof could be provided that this would enhance the security of the officer checking the person. The JSA suggested to consider alternative approaches. It could for instance be evaluated whether for those alerts where absconding from a place of detention means that the person absconding can be expected to try to escape arrest, an extra category should be added to Article 94(3) stating that there is a risk of escape.

The draft Council Decision that was published (OJ C 160,4.7.2002, p.7) and that was subject of the opinion of 1 October, linked this extra category of data to cases of alerts under Article 95 and 99. In view of the special character of these alerts, it seemed logical to attach any specific warning regarding the behaviour of the persons involved to these alerts. The present draft makes it possible to add these data to every alert. The JSA would like to see an explanation why these data have added value in case of alerts under Article 97 and 98. Since this extra category of data does not provide for a legal ground to arrest the person involved, the combination of the warning with Article 97 and 98 seems to be useless.

The JSA suggests considering the alternative approach as mentioned above.

(iv) Article 99(1) of the Schengen Convention.
The JSA has no comments.

(v) Article 99(3) of the Schengen Convention.
The JSA refers to its comments made in its opinion of 1 October.

(vi) Article 99(5) of the Schengen Convention.
The JSA has no comments.

(vii) Article 100(3) of the Schengen Convention
The JSA has no comments.

(viii) Article 101(1) of the Schengen Convention
The draft opens the possibility for access to SIS data and the right to search by national judicial authorities in the performance of their tasks as set out in national legislation.

The purpose of the SIS and the use of the SIS data are regulated in Article 92(1) and 102(1). Basic principle is that these data may only be used for the purposes provided for in the Articles 95 to 100. The tasks of judicial authorities for which they should be granted access must thus be limited to the purposes of the alerts in the SIS and not be extended to (any) task as set out in national legislation. In order to avoid any misunderstanding, the JSA suggests to amend the proposal in the following way:" ...may also be exercised by national judicial authorities in the performance of their tasks related to the SIS alerts as set out in national legislation."

(ix) Article 101(2) of the Schengen Convention
The JSA repeats the importance of safeguarding that the use of these data shall not limit the rights of citizens whose identity documents were stolen. The JSA refers further to its opinion of 13 June 2002 and to its opinion of 15 February 2000 on SIS alerts on persons whose identity has been usurped.

(x) Article 101A of the Schengen Convention
In its opinion of 1 October the JSA stated that the JSA was not able to assess the reasons and the legal basis for access and use of SIS data by Europol. No information on that subject was made available.

The JSA took good notice of the arguments to justify access to the SIS by Europol presented in the document 9323/02 of 28 May 2002.

The JSA acknowledges that the access and use as described in that document may have an added value for maintaining public security in the Schengen area as well as a contribution to the objective of Europol.

The new Article 101A appears to be a good elaboration of the access and use of SIS data for Europol. However, the JSA stresses that this proposal involves a fundamental departure from the basic principles of Article 102 of the Schengen Convention concerning the use of SIS data.

The introduction of the new Article 101A should lead to the amendment of Article 102 of the Schengen Convention. This amendment should be similar as Article 102(4), that provides for a derogation from the basic principle in view of issuing visas and residence permits.

The JSA underlines that a same situation shall be present with the proposal to grant access for Eurojust (see xi).

(xi) Article 101B of the Schengen Convention

In its opinion of 1 October the JSA stated that the JSA was not able to assess the reasons and the legal basis for access and use of SIS data by Eurojust. No information on that subject was made available. The JSA took good notice of the arguments to justify access to the SIS by Eurojust presented in the document 13389/02 of 22 October 2002.

The JSA acknowledges that the access and use as described in that document may have an added value for the work of Eurojust. However, the JSA stresses that this proposal involves a fundamental departure from the basis principles of Article 102 of the Schengen Convention concerning the use of SIS data. The introduction of the new Article 101A should lead to the amendment of Article 102 of the Schengen Convention.

In the light of the consequences of the proposals to grant access to Europol and Eurojust, the JSA stresses the need to maintain a careful balance between the need for those institutions to have that access and the data protection consequences of these proposals.

(xii) Article 102(4) of the Schengen Convention

The JSA has no comments.

(xiii) Article 103 of the Schengen Convention

The JSA repeats its comments made in the opinion of 1 October. The JSA could agree with extending the retention period from six months to one year. It appears now that in the new proposal the one year deadline is a minimum period for retention. Data should be deleted after one year but not later ten three years. In view of the purpose of processing these data, to check whether the search was admissible or not, the proposed period is not proportional for the purpose for which data are processed.

(xiv) Article 112A of the Schengen Convention

The JSA has no comments.

(xv) Article 113(1) of the Schengen Convention

The JSA has no comments.

(xvi) Article 113A of the Schengen Convention

The JSA has no comments.

III General conclusions

On the various proposals to change the Schengen Convention, the JSA has made its observations and specific remarks . The JSA underlines the advisability to reconsider the draft Council Decision and Council Regulation in the light of the considerations made in this opinion.

The JSA reaffirms that it is ready to contribute to the relevant discussion in a constructive manner.

Mr. Giovanni Buttarelli , Chairman

115 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

(*) Pubblicata integralmente nella Relazione 2001, p. 286

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

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

116 Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro (*)

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



5401/01/IT/def.
WP 55

Documento di lavoro riguardante
la vigilanza sulle comunicazioni elettroniche sul posto di lavoro

Adottato il 29 maggio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_it.pdf

117 Documento di lavoro sulla determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento dei dati personali su Internet da parte di siti web non stabiliti nell'UE (*)

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

5035/01/IT/def.
WP 56

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

costituito in virtù della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 [1],

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, di tale direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente documento di lavoro:

1. Introduzione

Il presente documento si propone di analizzare la questione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento, in particolare alla rilevazione, dei dati personali da parte dei siti Web stabiliti al di fuori dell'Unione europea [2]. Il presente documento di lavoro è inteso a costituire un utile strumento e un punto di riferimento per i responsabili del trattamento e per quanti forniscono loro consulenza in sede di valutazione di casi di trattamento di dati personali su Internet da parte di siti Web non stabiliti nell'UE. In considerazione della complessità dell'argomento e dell'estrema dinamicità che caratterizza Internet, il presente documento non fornirà soluzioni definitive riguardo a tutti i possibili aspetti di tale problematica.

Nel suo documento di lavoro "Tutela della vita privata su Internet" [3], il gruppo per la tutela dei dati personali ("articolo 29") ha individuato una chiara necessità di precisare l'applicazione concreta della norma concernente il diritto applicabile, contenuta nella direttiva relativa alla tutela dei dati (articolo 4,

(*) Gruppo di lavoro sulla protezione dei dati - Articolo 29
Il Gruppo, istituito in virtù dell'articolo 29 della direttiva 95/46/CE, è l'organo consultivo indipendente dell'UE per la tutela dei dati personali e del diritto alla riservatezza. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE.
Segretariato: Commissione europea, DG Mercato interno, Funzionamento ed impatto del mercato interno - Coordinamento - Protezione dei dati
B-1049 Bruxelles - Belgio - Ufficio: C100-6/136
Indirizzo Internet: http://europa.eu.int/comm/privacy

(1) GU L 281 del 23/11/1995, pag. 31, disponibile al sito:
http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

(2) La direttiva 95/46/CE relativa alla tutela dei dati è stata applicata anche all'interno dello Spazio economico europeo (SEE). Il riferimento all'Unione europea nel presente documento va inteso come riferimento al SEE.

(3) "Tutela della vita privata su Internet - Un approccio integrato dell'UE alla protezione dei dati on-line", WP 37, 21 novembre 2000.

paragrafo 1, lettera c)[4]), in particolare al trattamento on-line dei dati personali da parte di un responsabile non stabilito nel territorio della Comunità. Le autorità nazionali preposte al controllo in materia di tutela dei dati sono continuamente sollecitate a fornire consulenza alle imprese e ai privati a questo riguardo.

La necessità di determinare l'applicabilità o meno del diritto nazionale in situazioni interessanti più paesi non è circoscritta alla tutela dei dati, a Internet o all'Unione europea: si tratta di una questione generale di diritto internazionale che si pone nelle situazioni on-line e off-line laddove sono presenti uno o più elementi che riguardano più di un paese. Prima che possa essere sviluppata una soluzione nella sostanza è necessario decidere quale diritto nazionale sia applicabile.

Tali decisioni implicano la considerazione di numerosi fattori. Innanzitutto, ogni paese si preoccupa di tutelare i diritti e gli interessi dei propri cittadini, dei residenti, dell'industria e delle altre istanze riconosciute dall'ordinamento nazionale. In molti paesi il diritto penale (che costituisce l'altra faccia delle leggi che riconoscono diritti e libertà) sollecita l'applicazione più ampia con effetti internazionali. Casi eclatanti quali Yahoo![5] o CompuServe [6] illustrano come i tribunali applichino il diritto penale nazionale per proibire l'accesso a contenuti pornografici o razzisti su server di Internet stranieri. Recentemente la suprema corte tedesca in materia penale ha condannato un editore della "Auschwitz Lüge" (negazione dell'esistenza di Auschwitz) in un sito Web australiano anche in mancanza della prova di un effettivo accesso a tale sito dalla Germania [7]. Secondo la corte, nel contesto di questo particolare reato, è sufficiente che il contenuto di Internet "sia suscettibile" di influenzare negativamente l'ordine pubblico in Germania, senza che sia necessario che ciò sia accaduto effettivamente.

Tali effetti internazionali di norme protettive riflettono generalmente la preoccupazione del legislatore o del magistrato di tutelare i cittadini, se necessario, nonostante le difficoltà intrinseche di attuazione connesse alla situazione di internazionalità e di applicarle nella pratica onde garantire che l'intento perseguito sia raggiunto.

A livello del diritto comunitario, numerosi esempi illustrano tale ricerca di coerenza.

Nel campo della concorrenza la Commissione europea può prendere decisioni riguardanti società stabilite al di fuori dell'UE allorché operano all'interno dell'UE. Un buon esempio è costituito dalla recente decisione della Commissione [8] di bloccare il progetto di fusione [9] tra General Electric e Honeywell, due società statunitensi. Tale decisione, presa nel luglio 2001, dichiarava all'articolo 1 che una fusione tra le due società avrebbe creato una "concentrazione incompatibile con il mercato comune". La Commissione ha stabilito che il fatturato totale a livello comunitario delle due società ammontava a più di 250 milioni di euro e ha pertanto concluso che l'operazione notificata presentava una "dimensione comunitaria".

La dimensione extraterritoriale del diritto comunitario è osservabile anche con riguardo alla protezione dei consumatori. L'articolo 12 della direttiva [10] riguardante le vendite a distanza stabilisce che un consumatore non è privato della tutela assicurata dalla direttiva a motivo della scelta della clausola giuridica in un contratto, se il diritto del paese non membro prescelto fornisce una tutela inferiore di quella del diritto comunitario. Ciò avviene allorché il contratto presenti un "legame stretto" con il territorio di uno o più Stati membri [11]. L'espressione "legame stretto" è tratta dall'articolo 7 della convenzione di Roma del 1980. Tale articolo stabilisce che le "norme imperative" di un paese debbano essere applicate a situazioni disciplinate dal diritto di un altro Stato laddove tale situazione presenti uno "stretto legame" con il paese.

(4) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31), disponibile al sito: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

(5) TGI di Parigi, ordonnance du référé del 20 novembre 2000 http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_o.htm

(6) AG di Monaco, sentenza del 28.5.1998 – 8340 Ds 465 Js 173158/95.

(7) BGH, sentenza del 12.12.2000, Az: 1 StR 184/00.

(8) Decisione del 3.7.2001 (COMP/M.2220) in virtù dell'articolo 8, paragrafo 3, del regolamento (CEE) n. 4064/89 del Consiglio relativo al controllo delle operazioni di concentrazione tra imprese.

(9) In base all'accordo notificato Honeywell era destinata a diventare una controllata al cento per cento della General Electric.

(10) Direttiva 97/7/CE..4

(11) L'articolo 6, paragrafo 2, della direttiva 93/13/CEE concernente le clausole abusive nei contratti stipulati con i consumatori e l'articolo 7, paragrafo 2, della direttiva 1999/44/CE su taluni aspetti della vendita e delle garanzie dei beni di consumo sono molto simili all'articolo 12, paragrafo 2. Entrambi insistono sull'applicazione del diritto comunitario e utilizzano espressioni analoghe a "legame stretto".

Esiste inoltre una giurisprudenza che sviluppa le stesse argomentazioni con riguardo alla direttiva concernente gli agenti commerciali [12]. La Corte di giustizia europea ha stabilito [13] che allorché un agente commerciale che esercita la propria attività nella Comunità dipende da un mandante stabilito in un paese extracomunitario, quest'ultimo non può eludere le disposizioni della direttiva con l'espediente di una clausola contrattuale che afferma che alla relazione si applica il diritto di un paese terzo. La Corte ha stabilito che il diritto comunitario deve trovare applicazione "allorquando il fatto presenti un legame stretto con la Comunità".

Un ulteriore esempio pratico può essere citato con riguardo all'industria aeronautica. Il Consiglio ha approvato un regolamento relativo a un codice di comportamento in materia di sistemi telematici di prenotazione (CRS)[14]. Tale regolamento (che disciplina le modalità di utilizzo dei sistemi CRS) si applica "a tutti i sistemi telematici di prenotazione (...) qualora siano offerti per l'uso e/o utilizzati nel territorio della Comunità indipendentemente dallo status o dalla nazionalità del venditore del sistema (...) o dall'ubicazione della relativa unità centrale di elaborazione dati". Pertanto se a un sistema si può accedere dall'UE, anche nel caso in cui l'unità centrale del sistema non sia ubicata nell'UE (e i dati siano inseriti nel sistema attraverso terminali nell'UE o diversamente), il diritto comunitario si applica automaticamente.

Pertanto dall'esame dell'applicabilità del diritto comunitario a tali casi con una dimensione extraterritoriale si può concludere che sono generalmente applicati criteri simili. Pur essendo prescritto che la relazione abbia una "dimensione comunitaria" o un "legame stretto" con la Comunità, in talune situazioni la Corte di giustizia europea, il Parlamento europeo e il Consiglio nonché la Commissione europea ritengono opportuno imporre norme comunitarie a organismi stabiliti al di fuori dell'UE.

In altri paesi, ad esempio negli Stati Uniti d'America, la magistratura e i legislatori partono da premesse simili per assoggettare i siti Web stranieri alle norme locali. La legge statunitense sulla tutela della privacy dei bambini on-line del 1998 (Children's Online Privacy Protection Act - COPPA) si applica anche ai siti Web stranieri che raccolgono informazioni personali dai bambini sul territorio statunitense [15]. In virtù di tale legge federale, il gestore di un sito Web diretto verso bambini di meno di 13 anni (o di un sito con un pubblico più ampio, ma il cui gestore è effettivamente a conoscenza del fatto che il sito raccoglie informazioni da bambini) è obbligato a ottemperare alle disposizioni della COPPA. Tale legge stabilisce quali informazioni un gestore deve fornire nella sua privacy policy, quando e con quali modalità un gestore è obbligato a ottenere il consenso verificabile di un genitore e quali sono le responsabilità di un gestore ai fini della tutela della privacy dei bambini e della sicurezza in linea. Quel che è interessante ai fini della presente trattazione è che tale legge non si applica specificamente alle imprese statunitensi, bensì alle imprese "situate su Internet" e pertanto, in termini della sua giurisdizione, l'ubicazione fisica del sito Web non ha importanza nel caso in cui esso operi negli Stati Uniti. Se così avviene, il sito è assoggettato alla legge statunitense in materia.

Da un'indagine sul diritto internazionale emerge che gli Stati hanno la tendenza a utilizzare molteplici criteri alternativi per determinare estensivamente il campo d'applicazione del diritto nazionale al fine di coprire il maggior numero di casi possibile a beneficio della più ampia tutela dei consumatori e delle imprese nazionali. Inevitabilmente tale tendenza determina l'applicazione di molteplici diritti nazionali a una situazione che comporta un elemento di transnazionalità. Gli strumenti giuridici internazionali tentano pertanto di determinare i pertinenti criteri in modo neutro e non discriminatorio. Tuttavia il più recente tentativo di far avanzare il progetto di convenzione sul diritto applicabile ai contratti sotto gli auspici della "Conferenza dell'Aia" è fallito perché i paesi non hanno potuto accordarsi sul criterio decisivo. Questo evidenzia il nocciolo del problema in sede di discussione sul diritto applicabile: occorre trovare un giusto equilibrio tra i diversi interessi dei paesi implicati.

A questo riguardo va osservato che la direttiva comunitaria in materia di tutela dei dati contiene una disposizione esplicita riguardo al diritto applicabile che suggerisce un criterio. A prescindere che tale disposizione sia o no di facile comprensione o utilizzo, il fatto che la direttiva affronti questa questione fondamentale costituisce tuttavia un vantaggio per i privati e le imprese.

(12) Direttiva 86/653/CEE.

(13) Causa C-381/98, Ingmar GB Ltd contro Eaton Leonard Technologies Inc.

(14) Codice di comportamento in materia di sistemi telematici di prenotazione (versione combinata dei regolamenti (CEE) n. 2299/89 del Consiglio, come modificato dal regolamento (CEE) n. 3089/93 e dal regolamento (CE) n. 323/1999).

(15) 15 U.S.C., § 6502 (1)(A)(I), riferito da Joel R. Reidenberg, cfr. nota 5.

2. Articolo 4 della direttiva 95/46/CE in merito al diritto applicabile

L'articolo 4 della direttiva recita:
"Diritto nazionale applicabile

1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:

a)effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;

b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;

c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.

2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento."

Tale articolo analizza i casi che fanno insorgere il problema del diritto applicabile alle operazioni di trattamento dei dati personali: si tratta di casi in cui almeno un aspetto del trattamento di dati personali oltrepassa le frontiere di uno Stato membro. Ad esempio, un'impresa di marketing diretto elabora mailing list di consumatori in più Stati membri e li utilizza in uno Stato membro per consentire l'invio di pubblicità a tali consumatori, oppure un sito Web statunitense inserisce un cookie sul personal computer di privati nell'UE al fine di rendere identificabile il PC al sito, in vista del collegamento di tale informazione con altre.

La direttiva distingue in termini generali tra le situazioni in cui gli elementi transnazionali sono limitati agli Stati membri dell'UE oppure a territori al di fuori delle frontiere geografiche dell'Unione europea in cui si applica tuttavia la legislazione di uno Stato membro a norma del diritto internazionale pubblico ("caso diplomatico")[16], da una parte, e le situazioni in cui il trattamento comprende elementi che travalicano le frontiere dell'Unione europea [17], dall'altra.

In merito alle situazioni all'interno della Comunità, l'obiettivo della direttiva è duplice: evitare vuoti legislativi (non applicazione di una normativa in materia di tutela dei dati) e evitare una duplice o molteplice applicazione delle normative nazionali. Poiché la direttiva affronta la questione del diritto applicabile e stabilisce un criterio ai fini della determinazione della legge idonea a fornire la soluzione al caso, la direttiva stessa assolve il compito di una cosiddetta "norma di conflitto" rendendo inutile ogni ricorso ad altri criteri esistenti di diritto internazionale privato.

Per fornire una risposta la direttiva utilizza il criterio o il "fattore di connessione" del "luogo di stabilimento del responsabile del trattamento" o, in altre parole, il principio del paese di origine usualmente applicato nel mercato interno. In concreto ciò significa quanto segue.

Allorché il trattamento è effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio di uno Stato membro, si applica al trattamento la normativa in materia di protezione dei dati di tale Stato membro.

Qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, ciascuno degli stabilimenti deve ottemperare agli obblighi fissati dalle rispettive normative di ciascuno degli Stati membri per il trattamento da essi effettuato nel corso delle proprie attività. Ciò non rappresenta un'ecce-

(16) Questo caso non viene analizzato nel presente documento. Va altresì rilevato come la direttiva e pertanto anche l'articolo 4 si applichino tanto al settore pubblico quanto al settore privato che trattano i dati personali assoggettati al diritto comunitario. Il presente documento di lavoro non tratta tuttavia dell'applicazione dell'articolo 4 ai casi del settore pubblico.

(17) Tale distinzione si applica principalmente al responsabile del trattamento. È opportuno tuttavia chiarire che l'applicabilità della direttiva non è influenzata dal fatto che per conto del responsabile del trattamento nell'UE agisca un incaricato operante al di fuori dell'UE. Anche in tale caso la direttiva si applica all'insieme delle operazioni di trattamento.

zione al principio del paese di origine, bensì rappresenta semplicemente una sua rigorosa applicazione: qualora il responsabile scelga di disporre non di un solo stabilimento bensì di molti stabilimenti non beneficia del vantaggio che l'osservanza di una normativa è sufficiente per le sue attività in tutto il mercato interno. Tale responsabile si trova a far fronte all'applicazione parallela delle pertinenti normative nazionali ai vari stabilimenti. Il gruppo potrebbe trattare tale questione in futuro.

L'applicazione del principio del paese d'origine è giustificata in un mercato interno in cui le normative nazionali in materia di tutela dei dati garantiscono una protezione equivalente in virtù dell'armonizzazione dei diritti alla tutela dei dati delle persone e degli obblighi delle imprese e degli altri responsabili del trattamento di dati personali. In tal modo il principio del paese d'origine, che rappresenta in qualche modo una restrizione del campo d'applicazione delle normative degli Stati membri in materia di tutela dei dati, non incide negativamente sui diritti e sugli interessi dei suoi residenti o delle imprese. Infatti anche se le legislazioni degli Stati membri non sono applicabili a tutti gli aspetti del trattamento concernente una persona interessata del paese o effettuato sul territorio nazionale, il fatto che sia applicabile solo la legislazione di un altro Stato membro presenta un impatto molto limitato, considerato che entrambe le normative sono armonizzate dalla direttiva e pertanto sono equivalenti. Inoltre la cooperazione tra le autorità nazionali preposte alla tutela dei dati dà fiducia e garantisce una reale esecuzione a prescindere dal diritto applicabile [18].

La situazione si presenta diversa per le operazioni di trattamento in cui interviene un responsabile di un paese terzo. Le leggi nazionali di questi paesi terzi non sono armonizzate, la direttiva non è applicabile in tali paesi e la tutela delle persone per quanto concerne il trattamento dei loro dati personali può pertanto risultare lacunosa o mancare del tutto. Il principio del paese d'origine, connesso allo stabilimento del responsabile del trattamento, non può essere più utilizzato ai fini della determinazione del diritto applicabile. È necessario scegliere un altro fattore di connessione. Il Parlamento europeo e il Consiglio hanno deciso di ritornare a uno dei fattori di connessione classici nel diritto internazionale, ossia al legame fisico tra l'azione e un sistema giuridico. Il legislatore comunitario ha scelto il paese dell'ubicazione territoriale degli strumenti utilizzati [19]. La direttiva si applica pertanto allorché il responsabile non stabilito nel territorio della Comunità decide di trattare dati personali a fini specifici e ricorre a strumenti, automatizzati o non automatizzati, situati nel territorio di uno Stato membro.

L'obiettivo di tale disposizione contenuta nell'articolo 4, paragrafo 1, lettera c), della direttiva 95/46/CE è quello di garantire che una persona non sia priva di tutela per quanto riguarda il trattamento effettuato nel suo paese per il solo fatto che il responsabile non è stabilito sul territorio comunitario. Il motivo potrebbe essere semplicemente che il responsabile non ha, in linea di principio, nulla a che vedere con la Comunità, ma è immaginabile anche che i responsabili trasferiscano il loro stabilimento al di fuori dell'UE al fine di eludere l'applicazione della normativa comunitaria.

È opportuno notare come non sia necessario che la persona sia un cittadino comunitario o sia fisicamente presente o residente nell'UE. La direttiva non opera alcuna distinzione sulla base della nazionalità o della residenza in quanto armonizza le normative degli Stati membri in materia di diritti fondamentali riconosciuti a tutti gli esseri umani, indipendentemente dalla loro nazionalità. Pertanto nei casi che verranno discussi in appresso la persona in questione potrebbe essere un cittadino tanto statunitense quanto cinese. In termini di applicazione della normativa comunitaria in materia di tutela dei dati, tale persona è protetta allo stesso modo di qualsiasi cittadino comunitario. Ciò che conta è l'ubicazione degli strumenti del trattamento.

La decisione del legislatore comunitario di assoggettare il trattamento tramite strumenti ubicati nell'UE alla sua normativa in materia di tutela dei dati riflette pertanto una reale preoccupazione di proteggere le persone sul proprio territorio. A livello internazionale è riconosciuto che gli Stati possono fornire tale protezione. L'articolo XIV del GATS consente di stabilire eccezioni alle norme in materia di libera circolazione al fine di tutelare le persone con riguardo al loro diritto alla tutela della privacy e dei dati personali e di applicare tali normative.

Qui di seguito vengono spiegati i termini pertinenti ai fini della determinazione del diritto applicabile.

(18) Si veda l'articolo 28, paragrafo 6, primo comma, della direttiva 95/46/CE: "Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3" e l'ultimo comma dello stesso paragrafo in merito al loro obbligo di cooperazione.

(19) Ciò non vale nel caso in cui gli strumenti siano utilizzati ai soli fini di transito nel territorio della Comunità europea.

2.1 Stabilimento

La nozione di stabilimento è contenuta nell'articolo 4, paragrafo 1, lettera c), della direttiva nel senso che il responsabile non è stabilito nel territorio della Comunità. Il luogo in cui è stabilito il responsabile implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile e deve essere determinato in conformità con la giurisprudenza della Corte di giustizia delle Comunità europee. Secondo la Corte la nozione di stabilimento implica l'esercizio effettivo di un'attività economica per una durata di tempo indeterminata mediante l'insediamento in pianta stabile [20]. Tale condizione è soddisfatta anche nel caso in cui una società sia costituita a tempo determinato.

Il luogo di stabilimento, per le società che forniscono servizi tramite siti Internet, non è là dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività [21]. Si consideri il caso di una società di marketing diretto registrata a Londra che sviluppa da lì le sue campagne a livello europeo: anche se utilizza server a Berlino e a Parigi resta sempre stabilita a Londra.

2.2. Il responsabile del trattamento

Il responsabile del trattamento è secondo la nozione generale contenuta nella direttiva la persona fisica o giuridica che, da sola o insieme ad altre, determina le finalità e gli strumenti del trattamento di dati personali (articolo 2, lettera d), della direttiva 95/46/CE). La definizione è neutra per quanto riguarda il luogo di stabilimento del responsabile. È generale perché tutto il trattamento deve essere attribuibile ad uno o più responsabili. Nel contesto dell'articolo 4, paragrafo 1, lettera c), della direttiva, ciò significa che è imprescindibile l'esistenza di un responsabile nel senso della direttiva. Sembra inoltre necessario che il trattamento sia effettuato nel corso di un'attività che rientri nell'ambito del diritto comunitario e a cui si applichi quindi la direttiva. Il trattamento da parte di una persona fisica nel corso di un'attività puramente personale o familiare non rientra nell'ambito della direttiva.

Ai fini dell'applicazione dell'articolo 4, paragrafo 1, lettera c), della direttiva, il responsabile deve far ricorso, ai fini del trattamento di dati personali (e non ai soli fini di transito) a strumenti situati nel territorio di uno Stato membro [22]. Ciò sembra suggerire che il responsabile deve essere attivo e perseguire uno scopo particolare. La sua decisione in merito alle finalità e agli strumenti di trattamento comprende pertanto tale aspetto.

2.3. Strumenti

La direttiva non contiene una definizione di tale termine. Il dizionario inglese Collins definisce il termine "equipment" come un complesso di strumenti o dispositivi riuniti per un fine specifico.

Ne sono un esempio i personal computer, i terminali e i server, che possono essere utilizzati per quasi ogni tipo di operazione di elaborazione.

La direttiva chiarisce che gli strumenti in quanto tali possono essere automatizzati o non automatizzati, purché non siano utilizzati ai soli fini di transito delle informazioni sul territorio della Comunità europea.

Un tipico esempio in cui gli strumenti in questione sono utilizzati ai soli fini di transito è costituito dalle reti di telecomunicazioni (reti dorsali, cavi, ecc.), che formano parte di Internet e attraverso le quali le comunicazioni viaggiano dal punto di spedizione al punto di destinazione.

2.4. Ricorso agli strumenti

La determinazione del momento in cui il responsabile ricorre a strumenti ai fini del trattamento di dati personali di cui all'articolo 4, paragrafo 1, lettera c), della direttiva costituisce un elemento decisivo per quanto riguarda l'applicazione della normativa in materia di tutela dei dati nell'UE.

(20) Causa C-221/89 Factortame [1991] Raccolta della giurisprudenza I-3905, paragrafo 20.

(21) Direttiva 2000/31/CE, diciannovesimo considerando.

(22) Va osservato che esiste una differenza tra il termine "equipment" utilizzato nella versione inglese dell'articolo 4, paragrafo 1, lettera c), e i termini, più vicini al vocabolo inglese "means" (strumenti), utilizzati in altre versioni dell'articolo 4, paragrafo 1, lettera c). La terminologia utilizzata in altre versioni dell'articolo 4, paragrafo 1, lettera c), è coerente con la formulazione dell'articolo 2, lettera d), per definire il responsabile del trattamento: la persona che determina le finalità e gli strumenti ("means") del trattamento di dati personali. Va tuttavia riconosciuto che il testo inglese della direttiva nelle versioni precedenti (ad esempio, nella proposta emendata del 1992) utilizzava anch'esso il termine "means", modificato successivamente nel corso dei negoziati, a uno stadio assai avanzato, nel termine "equipment" come emerge dal testo della posizione comune del marzo 1995.

Il gruppo raccomanda cautela in sede di applicazione ai casi concreti di tale norma della direttiva sulla tutela dei dati. Il suo obiettivo è quello di garantire che i privati beneficino della tutela delle normative nazionali in materia e della supervisione del trattamento dei dati da parte delle competenti autorità nazionali in quei casi in cui è necessario, è giustificato ed esiste un grado ragionevole di attuabilità tenuto conto del connesso elemento di transnazionalità.

Premesso questo, il gruppo è del parere che non tutte le interazioni tra un utente di Internet nell'UE e un sito Web stabilito al di fuori dell'UE portino necessariamente all'applicazione della normativa comunitaria in materia di tutela dei dati. Il gruppo ritiene che gli strumenti debbano essere a disposizione del responsabile per il trattamento dei dati personali.

Nel contempo non è necessario che il responsabile eserciti un pieno controllo sugli strumenti. La misura in cui essi sono a sua disposizione può variare. Il necessario grado di disposizione è raggiunto se il responsabile, determinando le modalità di funzionamento degli strumenti, prende le pertinenti decisioni in merito alla sostanza dei dati e alla procedura della loro elaborazione: in altre parole, se il responsabile determina quali dati sono rilevati, archiviati, trasferiti, modificati, ecc., con quali modalità e con quali finalità.

Il gruppo ritiene che il concetto di "ricorrere" presuppone due elementi: una qualche forma di attività esercitata dal responsabile e l'intenzione dello stesso di trattare dati personali. Ciò significa che la direttiva non si applica a qualsiasi "ricorso" a "strumenti" nell'Unione europea.

Il potere di disposizione del responsabile non va tuttavia confuso con la proprietà degli strumenti da parte del responsabile o della persona. In effetti la direttiva non attribuisce alcuna rilevanza alla proprietà di uno strumento.

L'interpretazione avanzata dal gruppo è perfettamente conforme alla motivazione della disposizione contenuta nell'articolo 4, paragrafo 1, lettera c), della direttiva fornita dal legislatore comunitario. Il ventesimo considerando spiega che *"la tutela delle persone prevista dalla presente direttiva non deve essere impedita dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; che, in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva"*. Si tratta del corollario necessario per conseguire l'obiettivo più ampio della direttiva, consistente nell'evitare *"che una persona venga privata della tutela cui ha diritto in forza della presente direttiva"*.

3. Esempi pratici

Il presente capitolo è inteso a tradurre in soluzioni concrete gli orientamenti contenuti nell'articolo 4. Un elemento comune ai casi esaminati qui di seguito è che l'utente di Internet non è sempre necessariamente a conoscenza del fatto se il sito Web da lui visitato o a cui fornisce dati (coscientemente o meno) sia situato nell'UE o no. La determinazione dell'ubicazione fisica per i domini privi di suffissi geografici non è possibile in mancanza di informazioni aggiuntive e persino per quelli per cui esistono elementi geografici non esiste alcuna garanzia che il sito Web sia effettivamente ospitato su un server nel paese indicato.

Caso A: cookie

Il responsabile decide di rilevare dati personali con l'ausilio di un file di testo (cookie) posto sul disco rigido del personal computer di un utente, mentre una copia può essere tenuta dal sito Web o da un terzo [23]. In caso di ulteriori comunicazioni, il sito Web accede alle informazioni memorizzate nel cookie (e pertanto nel PC dell'utente) al fine di rendere identificabile tale PC al responsabile del trattamento. Quest'ultimo è quindi in grado di collegare tutte le informazioni raccolte nel corso delle precedenti sessioni con le informazioni rilevate durante le sessioni successive. In tal modo è possibile creare profili assai dettagliati degli utenti.

I cookie rappresentano una componente standard del traffico HTTP e, in quanto tali, possono essere trasportati senza ostacoli con il traffico IP. Contengono informazioni sull'individuo che possono essere rilette dal sito Internet che li ha creati. Un cookie può contenere tutte le informazioni che il sito desidera includervi: pagine visualizzate, annunci pubblicitari selezionati, numero di identificazione dell'utente, ecc.[24].

Il SET-COOKIE si trova nell'intestazione di risposta HTTP [25], segnatamente nei collegamenti ipertestuali invisibili. Se viene stabilita una scadenza [26], il cookie verrà memorizzato sul disco rigido dell'utente e ritrasmesso al sito Web che lo ha originato (o ad altri siti Web dello stesso sottodominio) per la durata prefissata. Questa ritrasmissione assumerà la forma di un campo COOKIE, che farà parte del browser chattering descritto in precedenza e avverrà senza alcun intervento dell'utente.

Come precisato in precedenza il PC dell'utente può essere considerato uno strumento ai sensi dell'articolo 4, paragrafo 1, lettera c), della direttiva 95/46/CE. È situato sul territorio di uno Stato membro. Il responsabile del trattamento ha deciso di utilizzare tale strumento ai fini del trattamento di dati personali e, come spiegato nei precedenti paragrafi, numerose operazioni tecniche si svolgono senza il controllo della persona interessata. Il responsabile dispone dello strumento dell'utente e tale strumento non è utilizzato ai soli fini di transito nel territorio della Comunità europea.

Il gruppo è pertanto del parere che il diritto nazionale dello Stato membro in cui è ubicato il personal computer dell'utente sia applicabile con riguardo alla domanda in quali condizioni i suoi dati personali possono essere rilevati collocando cookie sul suo disco rigido.

Come indicato in una precedente raccomandazione del gruppo [27], l'utente dovrebbe essere informato quando un cookie viene ricevuto, memorizzato o spedito dal software Internet. Il messaggio fornito all'utente dovrebbe specificare, in termini chiari, quali informazioni si intendono memorizzare nel cookie e a quale fine, nonché il periodo di validità del cookie stesso. L'utente dovrebbe quindi poter scegliere se accettare o respingere la trasmissione o la memorizzazione di un cookie nel suo insieme e dovrebbe anche potere scegliere di decidere quali informazioni dovrebbero essere conservate o eliminate da un cookie, in funzione ad esempio del periodo di validità dello stesso o dei siti Web che lo spediscono e lo ricevono [28].

Caso B: JavaScript, banner e altre applicazioni simili

I JavaScripts sono applicazioni software inviate da un sito Web al computer di un utente e consentono ai server remoti di far girare applicazioni sul PC dell'utente. In funzione del contenuto del software, i JavaScripts possono essere utilizzati per visualizzare informazioni su una pagina Web, ma anche per introdurre virus nei computer (i cosiddetti Java maligni) e/o per raccogliere e trattare dati personali memorizzati nel computer. Se decide di utilizzare tali strumenti ai fini della raccolta e del trattamento dei dati personali, il responsabile ricorre a strumenti nel senso della direttiva e dovrà ottemperare alle disposizioni della normativa comunitaria.

Una società di pubblicità, in virtù di un accordo con i proprietari di siti (ad esempio, i siti di motori di ricerca) ordina al browser (più in generale al computer) della persona interessata di collegarsi non soltanto con il motore di ricerca che intende visitare, ma anche con il server della società di pubblicità. In tal modo a tale società viene consentito non soltanto di inviare banner [29] sullo schermo della persona interessata, ma anche, utilizzando il browser dell'utente, di rilevare l'indirizzo e le informazioni che la persona invia al motore di ricerca. I banner vengono inseriti nel sito Web richiesto mediante un collegamento ipertestuale invisibile con la società di pubblicità [30]. Il responsabile del trattamento controlla pertanto, dal luogo in cui

(23) I cookie sono dati creati da un server che possono essere memorizzati in file di testo sul disco rigido di un utente di Internet, mentre una copia può essere conservata dal sito Web. Costituiscono una componente standard del traffico HTTP e, in quanto tali, possono essere trasportati senza ostacoli con il traffico IP. Un cookie può contenere un numero esclusivo (GUI, Global Unique Identifier) che consente una migliore personalizzazione rispetto agli indirizzi IP dinamici. I cookie permettono al sito Web di essere al corrente dei comportamenti e delle preferenze dell'utente. I cookie contengono una serie di URL (indirizzi) per i quali sono validi. Allorché il browser incontra nuovamente tali URL, spedisce gli specifici cookie al server. I cookie possono avere natura diversa: possono essere permanenti, ma possono anche avere una durata limitata (session cookies).

(24) Cfr. HAGEL III, J. e SINGER, M., Net Worth: the emerging role of the informediary in the race for customer information, Harvard Business School Press, 1999, pag. 275.

(25) In termini tecnici è possibile anche implementare cookie in JavaScript o nei campi <META-http EQUIV> presenti nel codice HTML.

(26) I cookie privi di scadenza fissa sono denominati "session cookies" e scompaiono quando il browser viene scaricato o al termine della sessione.

(27) Raccomandazione 1/99 (WP 17) "Trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware".

(28) Per ulteriori informazioni sulla natura dei cookie e sulle migliori modalità del loro trattamento si rinvia al documento di lavoro WP 37 (doc. 5063/00) "Tutela della vita privata su Internet - Un approccio integrato dell'UE alla protezione dei dati on-line". Alla pagina 16 è fornita una descrizione generale: "i cookie sono dati che possono essere memorizzati in file di testo sul disco fisso dell'utente Internet e conservati in copia dal sito Web". Alla pagina 79 sono fornite informazioni sui "cookie killer" analizzando sia la risposta dell'industria ai problemi di tutela della privacy comportati dai cookie (il meccanismo di opposizione ai cookie) sia la risposta dei vari attivisti in materia di tutela della vita privata (programmi indipendenti, quali cookie washer, cookie cutter e cookie master).

(29) I banner sono piccole caselle grafiche che appaiono in testa alle pagine Web oppure sono integrate nel loro contenuto.

(30) Per maggiori informazioni si rinvia al capitolo 8 "Cybermarketing" del documento WP 37 "Tutela della vita privata su Internet".

si trova, il funzionamento del browser in modo da metterlo in connessione con terzi e di trasmettere a questi informazioni.

Inoltre, al fine di fornire al cliente il banner più "adeguato", i pubblicitari in rete creano profili utilizzando cookie posti attraverso collegamenti ipertestuali invisibili. In funzione della configurazione del browser, l'utente può essere a conoscenza del fatto che viene copiato un cookie e può fornire o meno il suo consenso. Il profilo del cliente è collegato al numero identificativo del cookie della società di pubblicità in modo tale che può essere arricchito ogni volta che il cliente visita un sito Web legato contrattualmente con il pubblicitario. In tal modo si verifica una rilevazione aggiuntiva di dati personali dell'utente, attraverso il suo computer e senza il suo intervento, ogni volta che egli visita il sito Web contenente il banner.

La direttiva si applicherebbe anche alle informazioni rilevate attraverso spyware, ossia software segretamente installati in un computer ad esempio in occasione del downloading di un software più vasto (come un software per ascoltare musica) al fine di inviare informazioni personali riguardo alla persona interessata (ad esempio, i titoli delle canzoni che la persona preferisce ascoltare). I programmi software di questo tipo sono comunemente conosciuti come applicazioni E.T. *"perché dopo aver alloggiato nel computer dell'utente e aver appreso quel che gli interessa sapere, fanno ciò che faceva l'extraterrestre di Steven Spielberg: chiamano casa"*[31].

Queste nuove applicazioni software di monitoraggio utilizzano spesso JavaScript e altre tecniche simili e fanno chiaramente ricorso agli strumenti della persona interessata (computer, browser, disco rigido, ecc.) per rilevare dati e inviarli ad un altro sito. Poiché sono per definizione utilizzate senza informare l'utente (il nome spyware non lascia dubbi in proposito), tali tecnologie rappresentano una forma di trattamento invisibile e illegittimo.

***

Il gruppo "articolo 29" è consapevole del fatto che, in aggiunta ai due esempi citati in precedenza, esistono altri casi pratici connessi a Internet che potrebbero sollevare difficoltà di interpretazione, in parte a causa della complessità tecnica di alcuni dei sistemi utilizzati.

Il gruppo continuerà la sua riflessione sulla materia e potrebbe prendere in considerazione altri casi pratici alla luce dell'esperienza nazionale e degli sviluppi tecnici che potrebbero assumere rilievo in futuro.

Il gruppo desidera sottolineare che anche nei casi in cui l'applicazione della direttiva non è perfettamente chiara esso è impegnato a continuare il dialogo con le imprese e le organizzazioni dei paesi terzi che raccolgono dati personali nell'Unione europea al fine di promuovere adeguati standard di tutela dei dati per le persone interessate.

4. Cosa significa questo nella pratica?

a) Applicazione dei principi disciplinanti la rilevazione di dati personali

In tutti questi casi l'applicazione della normativa comunitaria in materia di tutela dei dati significa tra l'altro quanto segue:

- al fine di rendere la rilevazione dei dati personali corretta e lecita, il responsabile del trattamento deve definire chiaramente le finalità di tale trattamento;
- il responsabile deve anche garantire che i dati sono adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati;
- la rilevazione deve essere fondata su motivi legittimi (consenso inequivocabile, esecuzione di un contratto, adempimento di un obbligo legale, perseguimento di interessi legittimi del responsabile, ecc.) e all'interessato è riconosciuto il diritto di accesso, rettifica o cancellazione dei propri dati personali;
- l'interessato deve essere come minimo informato in merito all'identità del responsabile del trattamento e del suo eventuale rappresentante, alle finalità della rilevazione, ai destinatari e ai propri diritti [32];

(31) Si veda la storia di copertina della rivista Time di Adam COHEN del 31 luglio 2000: How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them.

(32) L'articolo 10 della direttiva stabilisce che vengano fornite informazioni aggiuntive qualora necessario per garantire un trattamento leale nei confronti della persona interessata. Nel caso dei cookie, alla persona deve essere offerta la possibilità di accettare o rifiutare il cookie e inoltre di determinare quali dati desidera siano trattati dal cookie e quali no.

- un altro importante aspetto è costituito dalla sicurezza del trattamento dei dati che può richiedere al responsabile, fin dalla rilevazione, di adottare specifiche misure tecniche ed organizzative al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete; tali misure devono garantire un livello di sicurezza appropriato rispetto ai possibili rischi e alla natura dei dati da proteggere;
- per quanto concerne i dati sensibili, la loro rilevazione è disciplinata da disposizioni specifiche riguardanti in particolare i requisiti di sicurezza [33].

Maggiori informazioni circa il modo in cui le direttive in materia di tutela dei dati si applicano al trattamento dei dati da parte dei siti Web sono fornite nella raccomandazione 2/2001 del gruppo relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione europea [34].

b) Aspetti procedurali

Ai sensi dell'articolo 4, paragrafo 2, della direttiva 95/46/CE, il responsabile del trattamento deve designare un rappresentante stabilito nel territorio dello Stato membro in cui sono situati gli strumenti utilizzati.

Le informazioni in merito all'identità del responsabile del trattamento e all'identità del suo rappresentante potrebbe essere facilmente incluse nella privacy policy del sito Web o nelle informazioni generali che permettono l'identificazione del responsabile del sito in modo che il responsabile per il trattamento responsabile anche per il sito Web possa essere facilmente individuato e contattato.

Si potrebbe raccomandare di fare ampiamente ricorso alla possibilità che un solo rappresentante agisca per conto di numerosi responsabili del trattamento o di cercare altre soluzioni pragmatiche.

Per quanto riguarda la notificazione della prevista operazione di trattamento (segnatamente la raccolta) alle autorità nazionali di tutela dei dati, la direttiva prevede alcune scelte. L'articolo 18, paragrafo 1, primo comma, contempla a carico del responsabile del trattamento o del suo rappresentante un obbligo di notificazione presso l'autorità di controllo prima di procedere alla realizzazione di un trattamento o di un insieme di trattamenti. L'articolo 19, paragrafo 1, lettera a), stabilisce che la notificazione deve includere tra gli altri elementi il nome e l'indirizzo del responsabile del trattamento e del suo rappresentante.

Conformemente all'articolo 18, paragrafo 2, secondo trattino, gli Stati membri possono prevedere una semplificazione o l'esonero dall'obbligo di notificazione in due casi: qualora si tratti di categorie di trattamento che non siano tali da recare pregiudizio ai diritti e alle libertà della persona interessata o qualora il responsabile del trattamento designi un incaricato della protezione dei dati a cui è demandato di assicurare in maniera indipendente l'applicazione interna della legislazione in materia di tutela dei dati [35].

Il gruppo è consapevole del fatto che l'applicazione di tali disposizioni può sollevare problemi pratici e potrebbe approfondire ulteriormente tali temi in futuro.

c) Applicazione

È evidente che l'applicazione di norme in un contesto internazionale non è altrettanto semplice della loro esecuzione in un solo paese. Il cittadino deve essere (reso) consapevole di questo. Esistono tuttavia diverse possibilità che possono essere sviluppate nell'intento di ottenere un ragionevole grado di applicazione.

Un buon livello di ottemperanza richiede in primo luogo una sensibilizzazione delle organizzazioni sia

(33) Alcuni Stati membri richiedono un controllo preventivo prima che possa essere avviato il trattamento di dati sensibili.
(34) Si veda il documento WP 43 "Raccomandazione 2/2001 relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione europea". Resta da verificare se tutti gli elementi citati in tale documento si applichino anche alla raccolta di dati on-line nell'UE da parte di responsabili non stabiliti nell'UE.
(35) Per le specifiche misure nazionali di esecuzione di tale articolo della direttiva si veda il sito:
http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm.

europee sia internazionali circa le prescrizioni della direttiva per quanto riguarda la raccolta di dati nell'Unione europea. La più ampia diffusione di tale raccomandazione può rappresentare soltanto il primo passo: sarebbero necessarie anche soluzioni tecnologiche che forniscano una struttura prestabilita per la raccolta di dati personali, incorporante negli strumenti di software utilizzati per tale raccolta le prescrizioni descritte. Il gruppo ha già fatto riferimento alla possibilità di concepire procedure di autorizzazione di prodotti implicanti un controllo del rispetto delle prescrizioni giuridiche per la tutela dei dati personali. Un sistema europeo di etichette/marchi Web aperto anche a siti Web extracomunitari, potrebbe rappresentare la base di tale azione.

Inoltre, nella pratica, un cittadino dell'Unione europea che abbia problemi con un sito Web non comunitario può segnalare il suo caso alla competente autorità nazionale di controllo in materia di tutela dei dati. Tale autorità determina se è applicabile la direttiva, oppure la normativa nazionale in materia di tutela dei dati. In caso affermativo, l'autorità potrebbe contattare il sito Web straniero al fine di risolvere il problema. Nel caso in cui sia adita l'autorità giudiziaria nello Stato membro in cui l'interessato è residente, questa decide se sia competente in materia (ciò che è possibile in conformità al diritto di procedura internazionale in quanto la parte più interessata è la persona che vive nello stesso territorio su cui ha la giurisdizione l'autorità giudiziaria). Una volta verificata tale competenza, l'autorità giudiziaria applica l'articolo 4 della direttiva 95/46/CE o la pertinente normativa nazionale di attuazione e può constatare che il sito Web straniero tratta in maniera illecita e non corretta i dati personali dell'interessato. Molti paesi terzi già prevedono il riconoscimento e l'attuazione della sentenza, ma anche in caso contrario esistono esempi che lasciano intendere che il sito Web straniero si adeguerà comunque alla sentenza e apporterà modifiche al proprio trattamento dei dati al fine di sviluppare buone prassi commerciali e di salvaguardare una buona immagine commerciale.

Nei paesi terzi in cui sono previste autorità e norme in materia di tutela dei dati l'applicazione è ovviamente meno problematica.

5. Conclusioni

• Il gruppo per la tutela dei dati personali ("articolo 29") è del parere che un'interpretazione delle leggi nazionali, così come indicato nel presente documento di lavoro, sarebbe di grande beneficio in vista del conseguimento della certezza del diritto per i siti Web stabiliti al di fuori dell'Unione europea. Il gruppo è convinto che un elevato livello di protezione delle persone può essere assicurato soltanto se i siti Web non stabiliti nell'Unione europea che utilizzano strumenti nell'UE come spiegato nel presente documento di lavoro rispettano le garanzie in merito al trattamento dei dati personali, segnatamente la raccolta, e i diritti delle persone riconosciuti a livello europeo e applicabili comunque a tutti i siti Web stabiliti nell'Unione europea.

• Il gruppo per la tutela dei dati personali ("articolo 29") ritiene che lo sviluppo di un programma per la promozione in modo pragmatico di norme europee in materia di tutela dei dati contribuirebbe a permettere ai responsabili del trattamento in paesi terzi di essere maggiormente sensibilizzati, nonché di rispettare e dimostrare attenzione per la privacy. Un sistema europeo di etichette/marchi Web, aperto anche a siti extracomunitari, potrebbe costituire la base di una siffatta azione.

• Il gruppo per la tutela dei dati personali ("articolo 29") invita la Commissione a tener conto del presente documento di lavoro nell'adozione di future iniziative.

Fatto a Bruxelles, il 30 maggio 2002

Per il gruppo
Il presidente
Stefano RODOTÀ

118 Parere 1/2002 riguardo alla relazione CEN/ISSS sulla standardizzazione delle modalità di tutela della vita privata in Europa (*)

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



10761/02/IT/def.
WP 57

Parere 1/2002 riguardo alla relazione CEN/ISSS sulla standardizzazione delle modalità di tutela della vita privata in Europa

Adottato il 30 maggio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp57_it.pdf

119 Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6 (*)

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



10750/02/IT/def.
WP 58

Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6.

Adottato il 30 maggio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp58_it.pdf

120 Parere 3/2002 sulle prescrizioni in merito alla tutela dei dati contenute nella proposta della Commissione di una direttiva relativa all'armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di credito al consumo (*)

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



11190/02/IT/def.
WP 61

Parere 3/2002 sulle prescrizioni in merito alla tutela dei dati contenute nella proposta della Commissione di una direttiva relativa all'armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di credito al consumo.

Adottato il 2 luglio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp61_it.pdf

121 Documento di lavoro sul funzionamento dell'Accordo di approdo sicuro (*)

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

11194/02/IT
WP 62

IL GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE PER QUANTO RIGUARDA IL TRATTAMENTO DEI DATI PERSONALI

costituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [1],
considerando gli articoli 29 e 30, paragrafi 1, lettera (a) e 3 di tale direttiva,
considerando le sue norme procedurali ed in particolare gli articoli 12 e 14,
ha approvato il presente documento di lavoro:

Data la prossima conclusione del primo periodo d'attuazione della decisione della Commissione del 26 luglio 2000 riguardante l'accordo d'Approdo sicuro, il gruppo di lavoro ha ritenuto necessario iniziare a considerare lo stato di attuazione di detto accordo [2].

Il gruppo di lavoro ha preso nota, innanzitutto, del documento di lavoro della Commissione recentemente pubblicato [3], nel quale si forniscono ragguagli circa la presenza di tutti gli elementi dell'Approdo sicuro, così come le prime esperienze note sulle disposizioni riguardanti la trasparenza, il funzionamento dei meccanismi di risoluzione delle controversie e la protezione dei diritti.

Successivamente il gruppo di lavoro ha fatto una visita a Washington, il 13 e 14 marzo 2002, dove una delegazione ha effettuato un'approfondita analisi in collaborazione con svariate autorità competenti, organizzazioni non governative e organi di risoluzione delle controversie.

Le informazioni raccolte attraverso questo primo insieme di iniziative è alquanto utile ad evidenziare la necessità di collaborazione di tutte le autorità competenti a dare piena esecuzione all'accordo.

Il gruppo di lavoro contribuirà brevemente all'analisi della questione assolvendo i propri compiti di controllo sull'applicazione delle leggi nazionali riguardanti flussi di dati transfrontalieri ed il livello di tutela in paesi terzi, nonché di consigliere per quanto attiene ai provvedimenti da adottare per la tutela dei diritti e delle libertà delle persone fisiche [4], oltre alle linee guida fornite nei sei pareri emessi prima dell'adozione della decisione da parte della Commissione il 26 luglio 2000 [5].

(*) *Gruppo per la tutela dei dati personali - Articolo 29*
Il Gruppo di lavoro è stato costituito ex articolo 29 della direttiva 95/46/EC. È un organo europeo consultivo indipendente per la tutela dei dati e la privacy. Le sue funzioni sono descritte nell'articolo 30 della direttiva 95/46/CE e nell'articolo 14 della direttiva 97/66/CE.
La segreteria è fornita dalla direzione A (Funzionamento ed impatto del mercato unico - Coordinamento - Protezione dei dati) della Direzione generale della Commissione europea, DG Mercato interno, B-1049 Bruxelles, Belgio, ufficio C100-6/136.
Sito Web: www.europa.eu.int/comm/privacy

(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) Decisione della Commissione 520/2000/CE del 26 luglio 2000 in applicazione 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 in GU 215 del 28 agosto 2000, pagina 7.
(3) Documento di lavoro SEC(2002)196 del 13.02.2002.
(4) Articolo 30, paragrafo 1, direttiva 95/46/CE.
(5) Parere 4/2000, parere 3/2000, parere 7/1999, parere 4/1999, parere 2/1999, parere 1/1999.

In particolare, il gruppo di lavoro desidera studiare in maniera costruttiva se si possano superare eventuali divergenze nei pareri riguardanti l'attuazione di determinati provvedimenti dell'Approdo sicuro, ed in che modo colmare possibili divari tra i principi stabiliti nell'Accordo e la prassi esecutiva. Si prenderanno in seria considerazione anche i requisiti di trasparenza cui le organizzazioni devono adempiere, sia per quanto riguarda la loro autocertificazione di conformità all'Approdo sicuro, sia per quanto attiene alle loro politiche sulla privacy.

Il gruppo di lavoro è di conseguenza dell'opinione che è opportuno gli vengano fornite informazioni aggiornate con particolare attenzione alle poche questioni collegate all'attuazione dell'accordo. Il gruppo di lavoro si riserva, in base a tali informazioni, di richiamare tutti gli enti, organizzazioni ed imprese coinvolti affinché compiano rinnovati sforzi per adempiere ai principi e ai prerequisiti di un accordo prossimo alla scadenza del proprio periodo di avvio – iniziato l'1 novembre 2000, al momento dell'entrata in vigore dell'Approdo sicuro. Ciò è altresì opportuno alla luce della possibile applicazione di tale accordo, strettamente legato alla peculiare esperienza statunitense, ad altre operazioni di trattamento di dati personali negli Stati Uniti.

Stanti le summenzionate premesse, il gruppo di lavoro ritiene necessaria una rapida analisi dei passi da effettuare al fine di aumentare la consapevolezza in Europa sulle possibili violazioni dei principi salienti.

Inoltre il gruppo di lavoro ritiene opportuno valutare la consapevolezza dei soggetti di dati, dell'uso dei propri dati personali per ulteriori scopi.

Conformemente alla richiesta fatta dal Parlamento europeo nella sua risoluzione del 5 luglio [6], il gruppo di lavoro richiama le autorità, organizzazioni ed associazioni coinvolte a collaborare per raccogliere - in particolare attraverso le autorità nazionali per la protezione dei dati e la Commissione europea - informazioni aggiornate, con particolare attenzione

- ad accordi per l'aumento della trasparenza nei confronti delle organizzazioni firmatarie, in particolare se una dichiarazione di adesione ad AS non è accompagnata da adeguate politiche per la privacy,
- alla possibilità di fornire meccanismi di controllo addizionali nei confronti della procedura d'adesione all'accordo, la conformità di condotta degli aderenti allo stesso con le proprie politiche di privacy e l'eventuale perdita dei benefici dell'Approdo sicuro,
- alle iniziative da adottare al fine di aumentare la conoscenza dei prerequisiti per l'adesione all'Approdo sicuro, anche attraverso documenti brevi, facilmente comprensibili e l'eventuale integrazione nel Safe Harbor Workbook,
- ai provvedimenti da adottare per mettere a punto meccanismi di risoluzione delle controversie, aumentare l'uniformità e la conoscenza dei criteri salienti, aumentare la trasparenza circa l'esito delle controversie e semplificarne i meccanismi di pubblicazione,
- alle eventuali difficoltà derivanti dall'esistenza di molteplici politiche di privacy dichiarate dal medesimo operatore,
- ai criteri di priorità ed alle possibili ulteriori iniziative intraprese dalle competenti autorità statunitensi ed agli accordi per una rinnovata cooperazione tra il comitato europeo per la protezione dei dati, gli organi di risoluzione delle controversie e la Federal Trade Commission.

Il gruppo di lavoro ritiene che sarebbe auspicabile raccogliere le summenzionate informazioni entro il prossimo 31 ottobre e si riserva il diritto di esprimere un parere su tale questione non appena entri in possesso di dati aggiornati.

Fatto a Bruxelles, 2 luglio 2002

Per il gruppo di lavoro
Il Presidente
Stefano RODOTÀ

(6) Risoluzione del Parlamento europeo su progetto di decisione della Commissione sull'adeguatezza della protezione ..., pubblicata nella GU C121 del 24.04.2001, pagina 152.

122 Parere 4/2002 sul livello di tutela dei dati personali in Argentina (*)

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



11081/02/IT/def.
WP 63

Parere 4/2002 sul livello di tutela dei dati personali in Argentina

Adottato il 3 ottobre 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp63_it.pdf

123 Parere 5/2002 sulla dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni (*)

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

11818/02/IT/def.
WP 64

IL GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI

istituito in virtù della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 1 ,
visti gli articoli 29 e 30, paragrafi 1 (a) e 3 della direttiva,
visto il regolamento di procedura del comitato , e in particolare gli articoli 12 e 14,
considerando la dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni
approva incondizionatamente tale dichiarazione.

Fatto a Bruxelles, 11 ottobre 2002

Per il gruppo di lavoro
Il Presidente
Stefano RODOTÀ

Dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni

I Commissari europei per la protezione dei dati rilevano con preoccupazione che, nell'ambito del cosiddetto "terzo pilastro" dell'UE, sono state avanzate proposte che comporterebbero l'obbligo sistematico di mantenimento dei dati di traffico concernenti tutti i tipi di telecomunicazioni (ossia luogo, data, e numeri utilizzati per comunicazioni telefoniche, fax, posta elettronica, e altri usi di Internet) per un periodo di un anno o anche oltre, allo scopo di consentire la possibilità di accesso a tali dati da parte delle autorità di polizia e di sicurezza.

(*) Gruppo per la tutela dei dati personali - Articolo 29
Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. Esso costituisce l'organismo consultivo indipendente dell'UE in materia di riservatezza e protezione dei dati. Le funzioni del gruppo sono stabilite dall'articolo 30 della diretttiva 95/46/CE e dell'articolo 14 della direttiva 97/66/CE. La segreteria è assicurata dalla Direzione A (Funzionamento e impatto del mercato unico - Coordinamento - Protezione dei dati) della Commissione europea, Direzione generale del Mercato interno,, B-1049 Bruxelles, Belgio, Ufficio C100-6/136.
Indirizzo Internet: www.europa.eu.int/comm/privacy

I Commissari europei per la protezione dei dati nutrono gravi dubbi sulla legalità e legittimità di misure di così vasta portata. Inoltre, essi desiderano richiamare l'attenzione sull'eccessivo livello dei costi di tali provvedimenti per l'industria di Internet e delle telecomunicazioni, e sull'assenza di provvedimenti siffatti negli Stati Uniti.

I Commissari europei per la protezione dei dati hanno ripetutamente sottolineato che simili provvedimenti costituirebbero un'impropria lesione dei diritti fondamentali garantiti ai cittadini dall'articolo 8 della Convenzione europea sui diritti dell'uomo, come ulteriormente specificato dalla giurisprudenza della Corte europea dei diritti dell'uomo (vedi parere 4/2001 del gruppo di lavoro di cui all'articolo 29 istituito in virtù della direttiva 95/46/CE e Dichiarazione di Stoccolma dell'aprile 2000).

La protezione dei dati di traffico delle telecomunicazioni è adesso prevista anche dalla direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche (Gazzetta ufficiale L 201/37), in base alla quale, in linea di principio, il trattamento dei dati di traffico è consentito a fini di contabilità e di riscossione dei canoni di collegamento. Dopo lungo e approfondito dibattito, è stato deciso che il mantenimento dei dati di traffico a fini di pubblica sicurezza debba essere strettamente subordinato alle condizioni di cui all'articolo 15 della direttiva, ossia, sempre e comunque, soltanto per un periodo limitato e qualora strettamente necessario, opportuno e proporzionato nell'ambito di una società democratica.

Perché i dati di traffico possano essere mantenuti in casi specifici, è quindi necessario che sussista una necessità dimostrabile in tal senso, che il periodo in cui vengono mantenuti sia più breve possibile e che tale attività venga esplicitamente regolata dalla legge, in maniera da garantire un'adeguata salvaguardia in caso di illecito accesso e qualsiasi altro abuso. L'archiviazione sistematica di tutti i tipi di dati di traffico per un periodo di un anno o più sarebbe chiaramente sproporzionata e quindi inaccettabile comunque.

I Commissari europei per la protezione dei dati si aspettano che il Gruppo di lavoro di cui all'articolo 29 venga consultato sui provvedimenti che potrebbero emergere dalle discussioni sul "terzo pilastro" prima della loro adozione.

(2) GU L 281 del 23/11/1995, pag. 31, disponibile presso: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

124 Documento di lavoro sulle "liste nere" (*)

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



11118/02/IT/def.
WP 65

Documento di lavoro sulle liste nere

Adottato il 3 ottobre 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp65_it.pdf

125 Parere 6/2002 relativo alla trasmissione da parte delle compagnie aeree d'informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti (*)

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

11647/02/IT/def.
WP 66

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

costituito in base alla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [1],

visto l'articolo 29 e l'articolo 30, paragrafo 1, lettera a) e paragrafo 3 di tale direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il seguente parere:

1. OGGETTO DI DISCUSSIONE

1.1 Contesto e finalità

In seguito agli avvenimenti dell'11 settembre 2001 [2] gli Stati Uniti hanno adottato il 19 novembre 2001 la legge sulla sicurezza del trasporto aereo (Aviation and Transportation Security Act) [3] la quale prescrive che le compagnie aeree che si trovano a volare in territorio statunitense debbano comunicare alle autorità competenti dati personali relativi ai passeggeri ed ai membri dell'equipaggio (Informazioni sugli elenchi dei passeggeri) [4]. Tale comunicazione deve avvenire per via elettronica ed essere completata prima del decollo dell'aereo, al più tardi 15 minuti dopo la partenza per quanto riguarda i dati personali dei passeggeri. Quantunque il "Commissario alle dogane" sia il destinatario dei dati inoltrati agli Stati Uniti, siffatti dati sono successivamente messi a disposizione di tutte le autorità federali statunitensi. La trasmissione dei dati personali non riguarda unicamente la sicurezza aerea ma negli Stati Uniti rappresenta altresì una questione d'ordine pubblico.

Il 14 maggio 2002 gli Stati Uniti hanno adottato un'altra legge per aumentare la sicurezza delle fron-

(*) Gruppo di lavoro sulla protezione dei dati - Articolo 29
Il Gruppo di lavoro è stato istituito a norma dell'articolo 29 della direttiva 95/46/CE. È un organismo consultivo europeo indipendente per la protezione dei dati personali e della vita privata. Le finalità dell'organismo sono stabilite all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. La segreteria ha la propria sede presso: Commissione europea, DG Mercato interno, "Funzionamento ed impatto del mercato interno; coordinamento; protezione dei dati". B-1049 Bruxelles - Belgio - Ufficio: C100-6/136
Telefono : linea diretta (+32 2) 299.27.19, centralino 299.11.11. Fax : 296.80.10
Indirizzo Internet: http://europa.eu.int/comm/privacy

(1) La Gazzetta Ufficiale n. L 281 del 23.11.1995, pag. 31 è consultabile al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

(2) Prima dell'11 settembre 2001 le compagnie aeree trasmettevano già su base volontaria alcune informazioni agli Stati Uniti.

(3) Legge sulla sicurezza del trasporto aereo (Aviation and Transportation Security Act) del 19 novembre 2001 (107-71), Norme transitorie ("Interim Rules") del Dipartimento del Tesoro (Dogana) statunitense – Informazioni sugli elenchi dei passeggeri e dell'equipaggio richieste nell'ambito dei voli con passeggeri nel trasporto aereo internazionale verso gli Stati Uniti (Registro federale, 31 dicembre 2001) e Informazioni sui dati relativi ai nomi dei passeggeri richiesti nell'ambito dei voli passeggeri nel trasporto aereo internazionale da e verso gli Stati Uniti (Registro federale, 25 giugno 2002).

(4) I medesimi obblighi sono stati introdotti per il trasporto marittimo.

tiere, la quale dispone che le compagnie aeree trasmettano all'ufficio americano per l'immigrazione e la naturalizzazione le informazioni relative ai passeggeri e all'equipaggio dei loro voli in arrivo e in partenza dagli Stati Uniti [5]. Per i passeggeri e gli equipaggi che arrivano negli Stati Uniti, gli obblighi di comunicazione dei dati sono identici a quelli stabiliti dalle autorità doganali statunitensi. Per i passeggeri e gli equipaggi che partono dagli Stati Uniti tale comunicazione deve invece avvenire per via elettronica ed essere completata al più tardi 15 minuti dopo il decollo, con la possibilità di correggere ed aggiornare la lista dei passeggeri non oltre i 15 minuti successivi alla partenza. All'occorrenza l'ufficio per l'immigrazione e la naturalizzazione americano si riserva il diritto di richiamare a terra l'aereo entro un'ora dalla partenza.

Tutti i dati vanno trasmessi ad una banca di dati centralizzata [6] gestita congiuntamente dalle autorità doganali e dall'ufficio per l'immigrazione e la naturalizzazione. In un secondo momento essi sono messi a disposizione di altre agenzie federali e non sono più oggetto di una tutela specifica.[7]

1.2 Categorie di dati trasmessi

L'APIS (un acronimo di "Advanced Passenger Information System" - sistema avanzato d'informazione sui passeggeri) è stato oggetto di una serie di cambiamenti di rilievo che riguardano in particolare l'ampliamento della lista di dati. Inizialmente le informazioni richieste erano specificamente correlate al tipo di volo in oggetto, al visto o al permesso di soggiorno valido per gli Stati Uniti, nonché a dati a carattere identificativo contenuti, ad esempio, nei passaporti.

In particolare le più recenti disposizioni statunitensi in merito alla sicurezza delle frontiere prescrivono che per i voli in partenza ed in arrivo dagli Stati Uniti, vengano comunicati i seguenti dati all'ufficio per l'immigrazione americano: nome, data di nascita, nazionalità, sesso, numero di passaporto e luogo di rilascio, stato di residenza, numero del visto americano, data e luogo di rilascio (all'occorrenza), numero di registrazione estero (all'occorrenza), indirizzo durante la permanenza negli Stati Uniti ed ogni altro dato ritenuto significativo per l'identificazione dei viaggiatori e per l'applicazione delle disposizioni in tema d'immigrazione e protezione della sicurezza nazionale e dell'incolumità personale [8].

È altresì prescritto che vengano a richiesta comunicati anche i dati trattati nei sistemi di prenotazione e controllo delle partenze (Departure control systems - DCS), in particolare quelli contenuti nei registri dei nomi dei passeggeri (Passenger Name Records - PNR) [9]. Tali dati non si limitano ai soli passeggeri in arrivo nel territorio statunitense e possono variare notevolmente da compagnia a compagnia. Essi riguardano: dati d'identificazione [10] (cognome, nome, data di nascita, numero di telefono); numero di prenotazione PNR, giorno della prenotazione, al caso l'agenzia di viaggio, informazioni presenti sul biglietto; informazioni di natura finanziaria (numero della carta di credito, data di scadenza, indirizzo di fatturazione ecc.); itinerario, informazioni sul volo fornite dal vettore (numero del volo ecc.), numero del posto assegnato nonché precedenti dati del sistema PNR. Tra questi ultimi possono rientrare non solo viaggi precedentemente effettuati ma anche informazioni a carattere religioso ed etnico (scelta del pasto ecc.), affiliazione ad un particolare gruppo, informazioni concernenti il luogo di residenza o contatti personali (indirizzo di posta elettronica, dettagli su un amico, luogo di lavoro ecc.), informazioni mediche (qualsiasi richiesta di assistenza sanitaria, ossigeno, problemi di vista, udito, mobilità o di ogni altra sorta la cui comunicazione è necessaria per garantire un volo soddisfacente) ed altri tipi di dati connessi, ad esempio, a programmi per clienti abituali (numero d'identificazione corrispondente) [11].

(5) Legge per aumentare la sicurezza delle frontiere (Enhanced Border Security) e legge sulla riforma dei visti d'ingresso (Visa Entry Reform Act) del 2002; si veda anche la legge sull'immigrazione e le nazionalità (Immigration and Nationality Act).

(6) Il sistema interagenzie di ispezione delle frontiere (IBIS - Interagency Border Inspection System).

(7) Alcune di queste informazioni possono all'occorrenza essere rese pubbliche conformemente alla legge in tema di accesso all'informazione in possesso del settore pubblico.

(8) Decisione del procuratore generale di concerto con il segretario di stato ed il segretario del tesoro.

(9) Norma transitoria (Registro federale, 25 giugno 2002), Registro dei nomi dei passeggeri richiesto nell'ambito dei voli con passeggeri nel trasporto aereo internazionale da e verso gli Stati Uniti.

(10) E' espressamente indicato che tale lista "intende illustrare unicamente i dati cui le autorità doganali possono richiedere di avere accesso".

(11) Questi dati, contenuti nelle norme transitorie ("interim rules") e pubblicati dal Dipartimento delle dogane (Department of Customs), non sono pero' presenti in quanto tali nella legge 107-71.

Per tutti i paesi che aderiscono al programma per l'esenzione dall'obbligo del visto (Visa Waiver Program) diverrà inoltre obbligatorio a partire da ottobre 2004 la trasmissione dei dati biometrici [12].

1.3 Sanzioni

La mancata trasmissione delle informazioni richieste o una loro trasmissione non corretta o incompleta è punibile con severe sanzioni, quali la perdita dei diritti di atterraggio ed il pagamento di pesanti ammende [13].

A questo riguardo il gruppo di lavoro s'interroga sulla compatibilità di tali provvedimenti unilaterali con gli accordi e le convenzioni internazionali in merito al trasporto e al traffico aereo nonché con le disposizioni applicabili a livello nazionale nel rispetto per quanto riguarda i paesi in cui le compagnie aeree operano in modo permanente.

1.4 Estensione ad altri paesi

Altri paesi quali Canada, Messico [14], Australia, Nuova Zelanda, Sudafrica e Regno Unito hanno già applicato o prevedono di porre in essere provvedimenti simili atti a soddisfare le proprie esigenze.

2. COMPATIBILITÀ' CON LA DIRETTIVA 95/46/CE

2.1 Attuazione della direttiva

I dati trasmessi dalle compagnie aeree si riferiscono a persone fisiche identificate ed in seno all'Unione europea il loro trattamento, è affidato in alle varie compagnie aeree (raccolta, registrazione, modificazione, archiviazione, rettificazione, estrazione, utilizzo, comunicazione ecc.). In quanto tali, siffatti dati sono soggetti alle disposizioni contenute nella direttiva 95/46/CE.

Lo sviluppo del sistema APIS solleva inoltre questioni specifiche, presentate nel seguito di cui molte trascendono la sfera di competenza delle singole compagnie aeree. Queste ultime si trovano spesso dinanzi ad un dilemma poiché, se da un canto sono tenute ad osservare le misure nazionali di esecuzione della direttiva 95/46/CE in tema di protezione dei dati personali, dall'altro la legislazione statunitense le obbliga alla comunicazione di questi stessi dati per mezzo di sanzioni severe.

2.2 Informazione degli interessati

Le persone interessate dal trasferimento dei propri dati personali devono esserne necessarie a garantirne un trattamento adeguato. Nel novero di tali informazioni dovrebbero rientrare le finalità specifiche del trattamento nonché i destinatari di tali dati.

Non è giustificabile un ricorso all'articolo 13 della direttiva 95/46/CE al fine di limitare quest'obbligo quando la comunicazione avviene in modo sistematico e le categorie di dati richieste sono state già parzialmente rese note al pubblico degli Stati Uniti mediante la pubblicazione della normativa. Più specificamente, tali informazioni dovrebbero essere fornite agli interessati nel momento stesso in cui i dati vengono rilevati e concernere tra l'altro le finalità ultime di trattamento negli Stati Uniti e i destinatari di siffatti dati [15].

2.3 Misure di sicurezza

A norma della direttiva 95/46/CE le compagnie aeree sono tenute ad applicare misure di sicurezza idonee per la protezione dei dati personali. Tale obbligo non contempla eccezioni. Si ritiene che le misure di natura tecnica imposte alle compagnie aeree dagli Stati Uniti consentano l'accesso ai dati da parte di terzi non autorizzati.

2.4 Osservanza del principio di finalità

Dati gli sviluppi recenti del sistema, la comunicazione dei dati personali descritta al precedente para-

(12) Sezione 203 della legge per aumentare la sicurezza delle frontiere (Enhanced Border Security), e della legge sulla riforma dei visti d'ingresso (Visa Entry Reform Act) del 2002.

(13) Circa 5000 dollari per errore da corrispondere alle autorità doganali statunitensi (in casi, ad esempio, di errore riguardante il nome del passeggero o altre categorie di dati al di sotto della media settimanale accettata) e di circa 1000 per comunicazione erronea del nome all'ufficio per l'immigrazione e la naturalizzazione.

(14) Anche il Messico trasmetterà tutti i dati in suo possesso sui voli in arrivo dagli Stati Uniti verso il proprio territorio.

(15) Tale disposizione non si applica se gli interessati sono sospetti sotto inchiesta.

grafo 1.2 (che va oltre la tipologia limitata di dati forniti normalmente dai passeggeri in occasione dell'organizzazione di un viaggio) non può considerarsi compatibile con le finalità originarie di raccolta dei dati personali da parte di compagnie aeree ed agenzie di viaggi, in particolare nell'ambito del rispetto degli obblighi contrattuali nei confronti dei passeggeri. L'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE vieta che vengano successivamente trattati dati raccolti per finalità determinate, esplicite e legittime, in modo incompatibile con tali finalità.

Tenuto conto della grande e multiforme quantità di dati in gioco, è impossibile ritenerli adeguati, pertinenti e non eccedenti rispetto alle finalità per cui vengono rilevati e/o successivamente trattati a norma dell'articolo 6, paragrafo 1, lettera c) della direttiva 95/46/CE.

Rimane tuttavia la possibilità di ricorrere all'articolo 13 della direttiva 95/46/CE, il quale autorizza gli Stati membri ad adottare provvedimenti legislativi miranti a circoscrivere la portata di questi due obblighi nella misura in cui tale restrizione si renda necessaria per la salvaguardia degli interessi elencati nella stessa direttiva (prevenzione e inchieste penali, sicurezza pubblica, ecc.). È ovviamente auspicabile che gli Stati membri seguano un'impostazione comune in materia.

2.5 Flussi transfrontalieri di dati

La direttiva 95/46/CE dispone che il trasferimento di dati personali in un paese terzo sia consentito solo se ed in quanto il paese in questione è in grado di assicurare un adeguato livello di protezione. Lo sviluppo del sistema APIS solleva a questo proposito, alcune perplessità. Il trattamento di dati trasmessi dalle compagnie aeree da parte delle autorità federali statunitensi non ottempera pienamente a tale condizione [16]. L'ambito ristretto di applicazione dell' "approdo sicuro" (Safe Harbor) non consente una sua applicazione a salvaguardia della protezione del trasferimento dei dati in favore delle autorità governative.

Le deroghe contemplate all'articolo 26 della direttiva 95/46/CE non sembrano altresì applicabili.

– Attualmente, il requisito del consenso inequivocabile non costituisce una soluzione adeguata perché giacché per molti versi continuano a sussistere forti perplessità. Non sembra infatti che il consenso del passeggero venga richiesto in ogni caso a differenza di quanto previsto dalla normativa in vigore. La direttiva 95/46/CE definisce il consenso come qualsiasi manifestazione di volontà libera, specifica ed informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento. Tale consenso può' risultare difficile da ottenere non da ultimo a causa delle difficoltà pratiche da affrontare quando si vogliano comunicare chiaramente tutte le informazioni necessarie ai passeggeri che acquistano un biglietto aereo nell'ambito di sistemi globali i quali consentono di prenotare un volo dall'Unione europea verso gli Stati Uniti a partire da quasi tutti i paesi del mondo, attraverso molteplici canali (diverse compagnie aeree, agenzie di viaggio, ecc.). Le informazioni fornite agli interessati devono includere le indicazioni stabilite agli articoli 10 e 11 della direttiva in oggetto, compresa, all'occorrenza, l'inadeguatezza della tutela nei paesi terzi.

– È difficile invocare la necessità del trasferimento ai fini dell'esecuzione di un contratto tra gli interessati e il responsabile del trattamento dei dati vista la portata dei dati trasmessi. La comunicazione di grandi quantità di dati non può infatti essere considerata "necessaria" ai fini dell'esecuzione di un contratto. L'impossibilità fisica per le compagnie aeree di adempiere ai propri obblighi contrattuali in seguito alla perdita ei diritti non rappresenta in questo caso una condizione sufficiente. È inoltre impossibile applicare siffatta eccezione a tutela della comunicazione di dati attinenti a persone non dirette verso gli Stati Uniti.

– Risulta parimenti impossibile la comunicazione di dati invocata in nome della salvaguardia d'importanti interessi pubblici. In primo luogo non è dimostrata la necessità di tale comunicazione; secondariamente, non è accettabile che una decisione unilaterale adottata da un paese terzo nel proprio interesse pubblico debba portare al trasferimento in massa d'informazioni tutelate a norma della presente direttiva.

(16) La normativa sulla vita privata, applicabile alle autorità federali statunitensi, tutela solo i dati relativi ai cittadini americani.

– E' infine difficile legittimare la liceità della comunicazione di siffatti dati per finalità connesse alla tutela degli interessi vitali delle persone coinvolte.

La direttiva 95/46/CE autorizza nondimeno il trasferimento dei dati personali in presenza di un adeguato livello di protezione all'interno del paese terzo quando il responsabile del trattamento (destinatario) è in grado di fornire garanzie sufficienti per la tutela dei dati personali.

Sarebbe pertanto auspicabile un negoziato tra Stati membri dell'Unione ed autorità statunitensi per trovare una soluzione atta ad assicurare livelli adeguati di protezione per i dati trasmessi.

2.6 Problemi specifici attinenti alla comunicazione ed all'accesso ai dati PNR trattati nell'ambito di sistemi telematici di prenotazione e di controllo delle partenze

Le osservazioni fatte a questo riguardo integrano quelle già presentate.

2.6.1 Collegamenti elettronici diretti tra il servizio doganale statunitense e i sistemi di prenotazione e controllo delle partenze

Nei casi in cui sia preferibile che il servizio doganale americano possa accedere direttamente ai sistemi informativi ubicati sul territorio europeo, per selezionare e raccogliere i dati, invece di essere il destinatario convenzionale di flussi transfrontalieri d'informazione, tutte le disposizioni contenute nella direttiva possono essere direttamente e pienamente applicate. L'articolo 4, paragrafo 1, lettera c) dispone le modalità d'applicazione della direttiva nei casi in cui il responsabile del trattamento non sia stabilito nel territorio della comunità e ricorra, ai fini del trattamento di dati personali, a strumenti, automatizzati o no situati sul territorio di uno Stato membro [17]. La piena applicazione di questa direttiva presenta ancora molti aspetti controversi.

2.6.2 Informazioni riguardanti viaggiatori non diretti negli Stati Uniti

Le informazioni riguardanti viaggiatori non diretti negli Stati Uniti non sono rilevanti e possono quindi non essere trasmesse, fatto salvo un eventuale impiego nell'ambito di specifici accordi in tema di giustizia e affari interni (assistenza reciproca).

2.6.3 Dati sensibili

Il registro PNR può contenere dei dati in grado di rivelare l'origine etnica o razziale, il credo religioso, o altri dati sensibili a termini dell'articolo 8 della direttiva 95/46/CE. Tale direttiva vieta in linea di massima qualsiasi tipo di trattamento dei dati sensibili fatto salvo il caso di autorizzazioni specifiche (consenso esplicito al trattamento per un determinato fine, informazioni di ovvia natura pubblica, ecc.) Come già visto, il ricorso al consenso crea molti problemi che dovrebbero essere tenuti in maggior considerazione data la natura estremamente delicata di siffatte informazioni [18].

L'articolo 8, paragrafo 4 della direttiva autorizza gli Stati membri o le autorità di controllo a stabilire ulteriori deroghe per seri motivi di interesse pubblico purché siano previste le opportune garanzie. In tali condizioni gli Stati membri potrebbero conseguentemente autorizzare il trasferimento di dati sensibili contenuti nel registro PNR [19].

2.6.4 Trattamento dei dati in sistemi di prenotazione e controllo delle partenze (DCS)

Il problema dell'accesso al registro PNR su richiesta delle autorità statunitensi solleva immediatamente la questione della legittimità del trattamento dei dati all'interno dei sistemi di prenotazione e con-

(17) Il ventesimo considerando della direttiva 95/46/CE rileva che la tutela delle persone disposta dalla presente direttiva non è ostacolata dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva. In un parere recentemente espresso in merito all'interpretazione del campo di applicazione dell'articolo 4, paragrafo 1, lettera c) della direttiva (Documento di lavoro sulla determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento dei dati personali su Internet da parte di siti Web non stabiliti nell'UE - 30 maggio 2002), il gruppo di lavoro (ex articolo 29) ha fatto notare come non occorra che il responsabile del trattamento eserciti un pieno controllo sugli strumenti ma sia importante che egli determini quali dati sono rilevati, archiviati, trasferiti, modificati, ecc., e con quali finalità.

(18) Conformemente all'articolo 8, paragrafo 2, lettera a) della direttiva, le normative degli Stati membri possono disporre che il divieto di trattamento dei dati personali di cui all'articolo 8, paragrafo 1 della direttiva in questione non debba applicarsi nel caso in cui l'interessato abbia dato il proprio consenso esplicito.

(19) Continua ad applicarsi l'articolo 13 della direttiva.

trollo delle partenze [20]. Tali dati possono essere utilizzati se ritenuti adeguati, rilevanti e non eccessivi rispetto alle finalità in base alle quali vengono trattati. I dati personali non dovrebbero più essere inseriti nei sistemi di prenotazione poiché il loro impiego non è più finalizzato al viaggio in occasione del quale vengono registrati.

2.7 Comunicazione di dati biometrici

La comunicazione di dati biometrici è disciplinata dalla direttiva 95/46/CE. Occorre notare che tale direttiva obbliga gli Stati membri a determinare a quali condizioni un mezzo identificativo di portata generale può essere oggetto di trattamento. Gli identificatori biometrici consentono unicamente l'identificazione d'individui e potrebbero pertanto formare l'oggetto di questa stessa norma [21].

Conclusioni

1. Il gruppo di lavoro riconosce che Stati sovrani possono decidere circa le categorie di dati da richiedere a chi intende accedere al loro territorio. Le proposte attuali attinenti al sistema APIS, benché legittimate da un contesto storico di nefandezze terroristiche, comporterebbero tuttavia una diffusione sproporzionata e sistematica di dati da parte delle compagnie aeree la cui attività è soggetta alle disposizioni della direttiva 95/46/CE. Tali dati potrebbero essere usati quotidianamente per fini doganali e legati all'immigrazione e, più in generale, per motivi di sicurezza nazionale americana e potrebbero così essere diffusi quanto meno tra tutte le agenzie federali.

2. Alla luce della recente evoluzione del sistema APIS il gruppo di lavoro ritiene che il rispetto delle prerogative statunitensi crei difficoltà nell'applicazione della direttiva 95/46/CE. Molti dei problemi in questione trascendono la sfera delle singole compagnie aeree e ricadono nella sfera di competenza degli Stati membri e, conseguentemente, della Commissione.

3. In definitiva, stando al parere del gruppo di lavoro la comunicazione di dati relativi a viaggiatori non diretti verso gli Stati Uniti non dovrebbe essere autorizzata fatto salvo il loro impiego nell'ambito di specifici accordi di cooperazione in tema di giustizia ed affari interni.

4. Qualsiasi altro tipo di trasferimento di dati effettuato a partire da sistemi di prenotazione e di controllo delle partenze relativi ai passeggeri ed ai membri dell'equipaggio è possibile solo nel rispetto delle normative in vigore negli Stati membri.

Tali normative devono disporre che le necessarie restrizioni su diritti ed obblighi soggetti alla direttiva 95/46/CE siano conformi all'articolo 13 di tale direttiva, e che siano poste in essere le garanzie a tutela delle persone interessate.

È auspicabile che si persegua un approccio comune a livello comunitario.

5. Occorre ponderare attentamente la comunicazione di dati che possono essere considerati alla stregua di dati sensibili. Tali comunicazioni necessitano infatti all'occorrenza di prove atte a dimostrare l'esistenza di 1) motivi di interesse pubblico rivelante per gli Stati membri, 2) garanzie appropriate e 3) talvolta di una legislazione nazionale in materia o di una decisione dell'autorità di controllo.

6. Qualora si ritenga inoltre necessario l'accesso diretto da parte del servizio doganale o del servizio per l'immigrazione e la naturalizzazione statunitense ai dati contenuti nei sistemi di prenotazione e controllo delle partenze, tali autorità sono tenute a garantire il pieno rispetto della direttiva.

7. Il sistema dovrebbe essere concordato con le autorità statunitensi. Il negoziato dovrebbe vertere specificamente sul chiarimento e la definizione di obiettivi, finalità e destinatari dei dati nonché sulle categorie di dati che possono essere trasferiti, tenuto conto delle presenti osservazioni nonché dell'in-

(20) Si veda la raccomandazione 1/98 in materia di sistemi telematici di prenotazione nel trasporto aereo che dispone, per regolare le controversie e trattare i dati relativi ai clienti abituali, una loro archiviazione limitata ad un determinato arco temporale, previo ottenimento del consenso delle persone interessate. Il gruppo di lavoro ex articolo 29 ritiene che l'archiviazione dei dati reperiti on-line debba essere limitata a sole 72 ore e che la loro distruzione avvenga ai più tardi entro i tre anni successivi (con un accesso ristretto per richieste di indagini) o in tempi ancor più lunghi (solo ai fini dell'adempimento di un obbligo legale).

(21) Il dibattito sui dati biometrici è attualmente in corso presso il gruppo di lavoro.

sieme delle condizioni e garanzie che caratterizzano il processo di trattamento dei dati personali, con particolare riguardo ad una loro diffusione presso le autorità federali statunitensi (ed in tal caso una comunicazione limitata alle sole autorità incaricate dell'applicazione della legge).

8. Nei casi di comunicazione di dati personali da parte delle compagnie aeree agli Stati Uniti è preferibile un'impostazione di tipo globale. Occorrerebbe in primo luogo tenere conto di altre comunicazioni programmate o in corso verso gli Stati Uniti. A tal proposito di particolare interesse potrebbe risultare l'introduzione del concetto del terzo pilastro. Ciò significa che i trasferimenti alle autorità pubbliche di paesi terzi di dati richiesti per motivi d'ordine pubblico all'interno di questi stessi paesi andrebbero analizzati nel più ampio contesto dei meccanismi di cooperazione fissati nell'ambito del terzo pilastro (cooperazione giudiziaria e di polizia). Questi ultimi dovrebbero inoltre andare di pari passo con le garanzie a tutela delle informazioni comunicate.[22] Tali meccanismi di cooperazione concordati nell'ambito del terzo pilastro non devono essere elusi ricorrendo al primo pilastro. La soluzione elaborata per comunicare i dati verso gli Stati Uniti potrebbe infine rivelarsi utile anche per i trasferimenti APIS verso altri paesi terzi.

Fatto a Bruxelles, 24 ottobre 2002

Per il gruppo di lavoro
Il presidente
Stefano RODOTA

(22) I dati personali sono esportati dagli Stati membri ai fini della cooperazione giudiziaria e di polizia. Tali dati sono stati trasferiti da Europol per analizzare gli avvenimenti dell'11 settembre 2001 come parte di una procedura eccezionale. E' attualmente in corso un dibattito per creare una cooperazione stabile conformemente alle disposizioni della convenzione Europol (articolo 18). Si veda altresì la decisione Eurojust (articolo 27) ed i negoziati in corso sull'articolo 38 del trattato.

126 Documento di lavoro sul trattamento di dati personali tramite videosorveglianza (*)

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

11750/02/IT
WP 67

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE RIGUARDO AL TRATTAMENTO DI DATI PERSONALI

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 IL PRESENTE DOCUMENTO DI LAVORO:

1. INTRODUZIONE

Negli ultimi anni, gli organismi pubblici e privati in Europa hanno fatto sempre maggior ricorso ai sistemi di acquisizione di immagini. Tale circostanza ha suscitato un acceso dibattito tanto a livello comunitario quanto a quello dei singoli Stati membri al fine di identificare presupposti e restrizioni applicabili all'installazione di attrezzature di videosorveglianza, nonché le necessarie garanzie per le persone interessate.

Dall'esperienza acquisita negli ultimi anni, anche a seguito del recepimento, a livello nazionale, della direttiva 95/46/CE, si constata un'enorme proliferazione di sistemi a circuito chiuso, videocamere e altri strumenti più sofisticati utilizzati nei settori più diversi.

Inoltre, lo sviluppo delle tecnologie disponibili, digitalizzazione e miniaturizzazione, aumentano notevolmente le possibilità offerte dai dispositivi di registrazione di immagini e suoni, anche in relazione con la loro utilizzazione in intranet e Internet.

Oltre alle operazioni di trattamento nel contesto dell'occupazione, trattate dal gruppo di lavoro in un documento particolare (parere 8/2001 sul trattamento di dati personali nell'ambito dell'occupazione [2]), la crescente proliferazione delle tecniche di videosorveglianza può essere facilmente rilevata da tutti i cittadini.

Un'analisi non esaustiva delle principali applicazioni dimostra che la videosorveglianza può servire a

(*) Gruppo di lavoro per la tutela dei dati personali - Articolo 29
Il gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, Proprietà intellettuale e industriale, Media e Protezione dei dati) della Commissione europea, Direzione generale mercato interno, B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136.
Website: www.europa.eu.int/comm/privacy
(1) Gazzetta ufficiale n. L 281 del 23/11/1995, pag. 31, disponibile su: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm
(2) WP 48, adottato il 13 settembre 2001, disponibile su: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

fini molteplici [3], che possono essere raggruppati peraltro in alcuni settori principali:

1) protezione degli individui,
2) protezione della proprietà,
3) interesse pubblico,
4) scoperta, prevenzione e controllo delle infrazioni,
5) presentazione di prove,
6) altri interessi legittimi.

Requisiti di vario genere si applicano inoltre agli impianti di videocamere e dispositivi simili.

In alcuni casi, l'utilizzazione di un sistema di videoregistrazione può essere effettivamente obbligatoria, sulla base di disposizioni specifiche degli Stati membri – ciò è stato il caso, ad esempio, in alcuni casinò - oppure per fini ai quali i familiari delle persone in causa attribuiscono speciale importanza – ad esempio ricerca di bimbi e adulti dispersi. D'altro canto, si possono menzionare casi di utilizzo stravagante – principalmente in paesi terzi – nei quali sono stati usati sistemi di riconoscimento facciale per evitare la bigamia oppure quando un'autorità di polizia ha deciso di divulgare immagini della vita difficile condotta nelle prigioni, senza il consenso dei detenuti.

Di conseguenza, se da un lato la videosorveglianza può apparire in certo qual modo giustificata in particolare circostanze, esistono però casi in cui impulsivamente si ricerca la protezione per mezzo di videocamere senza considerare adeguatamente le condizioni e le disposizioni applicabili. Talvolta questo è dovuto tanto ai benefici economici concessi su larga scala dagli organismi pubblici quanto all'offerta di condizioni assicurative migliori in relazione all'utilizzo di attrezzature di videosorveglianza.

Si tratta quindi di un settore diversificato, in continua evoluzione, nel quale molte tecniche sono già disponibili.

Obiettivo del presente documento di lavoro è quello di fornire un'analisi iniziale, partendo dall'esistenza di regolamenti parzialmente diversi nonché dall'esistenza di disposizioni esageratamente particolareggiate nelle varie legislazioni nazionali, per cui è necessario un approccio più sistematico ed armonizzato.

Il presente documento di lavoro riguarda la sorveglianza mirante al controllo a distanza di eventi, situazioni e avvenimenti, mentre non considera direttamente altri casi in cui certi avvenimenti vengono pubblicizzati su base occasionale e/o abituale, ad esempio in relazione con la trasparenza delle attività di enti locali e/o organismi parlamentari.

Ogni operatore sarà quindi in grado di specificare ulteriormente le indicazioni qui fornite, sia nel rispettivo settore sia per quanto riguarda i futuri sviluppi tecnologici che il gruppo di lavoro intende analizzare.

Inoltre, i principi di cui si tiene conto in questa sede si applicano all'acquisizione di immagini, even-

(3) Sistemi di videosorveglianza di vario genere sono installati:
a) all'interno e in prossimità di edifici di accesso pubblico e/o privato, ad esempio musei, luoghi di culto o monumenti, al fine di evitare infrazioni e/o atti minori di vandalismo,
b) presso stadi e impianti sportivi, specialmente in relazione con determinate manifestazioni,
c) nel settore dei trasporti e in relazione con il traffico stradale, al fine di sorvegliare il traffico delle autostrade, oppure per rilevare infrazioni per eccesso di velocità e/o infrazioni del regolamento del traffico in zone urbane, oppure ancora per controllare locali sotterranei che danno accesso alle linee della metropolitana, controllare stazioni di rifornimento e l'interno dei taxi,
d) per evitare e/o rilevare comportamenti illegali in prossimità delle scuole, anche in relazione con l'adescamento dei minori,
e) presso installazioni mediche durante operazioni chirurgiche e/o, ad esempio, per prestare cure a distanza o controllare pazienti nelle unità di rianimazione e/o in zone in cui sono ricoverati pazienti gravemente malati e/o in quarantena,
f) negli aeroporti, a bordo di imbarcazioni e in prossimità delle zone di frontiera, al fine di controllare le entrate clandestine di stranieri, come pure per facilitare la ricerca di minori e di altre persone disperse,
g) dagli investigatori privati,
h) all'interno e in prossimità di supermercati e di negozi, specialmente di articoli di lusso, al fine di presentare prove in caso di infrazioni, come pure per promuovere prodotti e/o elaborare un profilo dei clienti,
i) presso condomini privati e zone adiacenti, sia per ragioni di sicurezza sia per presentare prove in caso di infrazione,
j) a fini giornalistici e pubblicitari, mediante webcam o videocamere on-line utilizzate per la promozione turistica e pubblicitaria, anche relativamente a stazioni balneari e locali da ballo, filmando su base regolare clienti e visitatori senza alcun preavviso.

tualmente in associazione con dati sonori e/o biometrici, ad esempio le impronte digitali [4].

I principi sopra menzionati possono essere altresì presi in considerazione, ove concretamente applicabili, in relazione al trattamento di dati personali non effettuato da attrezzature video ma tramite altri tipi di sorveglianza, ad esempio controllo a distanza, com'è il caso, ad esempio, con i sistemi GPS via satellite.

Il presente documento di lavoro mira anzitutto ad attirare l'attenzione sulla vasta gamma di criteri di valutazione della legittimità e dell'adeguatezza in materia di installazione di vari sistemi di videosorveglianza.

Si è peraltro tenuto conto degli aspetti seguenti:

a) occorre che le istituzioni competenti degli Stati membri valutino la videosorveglianza da un punto di vista generale, anche al fine di promuovere un approccio globalmente selettivo e sistematico della questione. L'eccessiva proliferazione di sistemi di acquisizione di immagini in zone pubbliche e private non dovrà tradursi nell'applicazione di ingiustificate restrizioni dei diritti e delle libertà fondamentali dei cittadini; in caso contrario, i cittadini sarebbero effettivamente obbligati a sottoporsi a procedure sproporzionate di raccolta di dati, il che li renderebbe identificabili in massa in numerosi posti pubblici e privati.

b) Le tendenze che riguardano l'evoluzione delle tecniche di videosorveglianza potrebbero essere valutate utilmente per evitare che lo sviluppo di applicazioni di software basate sia sul riconoscimento facciale sia sullo studio e sulla previsione del comportamento umano si traducano avventatamente in una sorveglianza dinamico-preventiva, al contrario della sorveglianza statica convenzionale, che si prefigge principalmente di documentare avvenimenti specifici e i loro autori. Questa nuova forma di sorveglianza si basa sull'acquisizione automatica dei lineamenti degli individui, come pure sulla loro condotta "anormale" in associazione con la disponibilità di allarmi e avvisi automatizzati, che potrebbero implicare pericoli di discriminazione.

2. STRUMENTI GIURIDICI INTERNAZIONALI.

a) Convenzione per i diritti umani e le libertà fondamentali

La protezione della vita privata è garantita dall'articolo 8 della Convenzione sui diritti umani.

b) Convenzione n. 108/1981 del Consiglio d'Europa per la protezione delle persone relativamente al trattamento automatizzato di dati a carattere personale.

L'ambito di questa Convenzione non è limitato, come la direttiva 95/46/CE, alle attività di primo pilastro (vedi sotto). Le attività di videosorveglianza che comportano il trattamento di dati personali rientrano nel campo d'applicazione di tale Convenzione. Il comitato consultivo istituito da tale convenzione ha affermato che voci e immagini sono considerate dati personali, ove esse forniscano informazioni su un individuo rendendolo, anche se indirettamente, identificabile.

Il Consiglio d'Europa sta attualmente elaborando una serie di principi di orientamento per la protezione degli individui rispetto alla raccolta e al trattamento di dati tramite videosorveglianza. Tali principi dovrebbero specificare ulteriormente le garanzie applicabili alle persone interessate, contemplate nelle disposizioni degli strumenti del Consiglio d'Europa.

c) Carta dei diritti fondamentali dell'Unione europea

La Carta dei diritti fondamentali dell'Unione europea dispone, all'articolo 7, la protezione della vita privata e familiare, del domicilio e delle comunicazioni, mentre l'articolo 8 riguarda la protezione di dati di carattere personale.

3. SORVEGLIANZA AI SENSI DELLA DIRETTIVA 95/46/CE.

Le caratteristiche specifiche del trattamento delle informazioni personali incluse in dati sonori e visivi sono state espressamente sottolineate dalla direttiva 95/46/CE (di seguito denominata "la direttiva") che le menziona espressamente in vari punti.

(4) L'aspetto più generale dell'applicazione della direttiva 95/46/CE alla biometria sarà trattato dal gruppo di lavoro in un documento a parte.

La direttiva garantisce la protezione della vita privata nonché la protezione più ampia di dati personali relativamente alla tutela dei diritti e delle libertà fondamentali delle persone fisiche (articolo 1, paragrafo 1).

Una parte notevole delle informazioni raccolte per mezzo della videosorveglianza riguarda persone identificate e/o identificabili filmate quando frequentavano locali pubblici e/o di accesso pubblico. Persone del genere, in transito, potrebbero sì prevedere un minore livello di riserbo, ma non di essere private totalmente dei propri diritti e libertà anche riguardo alla propria sfera ed immagine privata.

In questo contesto occorre anche considerare il diritto alla libera circolazione delle persone che si trovano legalmente nel territorio di uno Stato, diritto tutelato dall'articolo 2 del protocollo n. 4 addizionale della Convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali.

Tale libertà di circolazione può essere oggetto di restrizioni necessarie in una società democratica, e proporzionate al raggiungimento di fini specifici. Le persone interessate hanno il diritto di esercitare la propria libertà di circolazione senza dover essere soggette ad eccessivi condizionamenti psicologici quanto ai loro movimenti e comportamento e senza dover essere sottoposte ad un controllo particolareggiato, come quello del loro comportamento a seguito dell'applicazione sproporzionata della videosorveglianza in vari locali pubblici e/o di accesso pubblico.

Nelle parti iniziali della direttiva vengono sottolineate la specificità e la sensibilità del trattamento di dati in forma di suoni e immagini relative alle persone fisiche. Oltre alle considerazioni che verranno formulate di seguito quanto al campo d'applicazione, tali assunti ed i rispettivi articoli della direttiva chiariscono che:

a) la direttiva si applica, in linea di massima, a questo caso tenendo conto altresì dell'importanza degli sviluppi delle tecniche utilizzate per captare, manipolare o altrimenti utilizzare la categoria specifica di dati personali raccolti in questo modo (cfr. considerando n. 14),

b) i principi di protezione della direttiva si applicano a qualsiasi informazione – incluse quelle sotto forma di suoni e immagini – concernenti una persona identificata o identificabile, prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona (cfr. articolo 2, lettera a), e considerando n. 26).

Oltre ai riferimenti specifici sopra menzionati, la direttiva ovviamente produce tutti i suoi effetti nel quadro delle sue disposizioni individuali riguardanti, in particolare:

1) Qualità dei dati. Le immagini devono essere trattate lealmente e lecitamente per finalità determinate, esplicite e legittime. Le immagini debbono essere utilizzate conformemente al principio che i dati debbono essere adeguati, pertinenti e non eccedenti e non trattati successivamente in modo incompatibile con tali finalità; essi vanno conservati per un periodo limitato, ecc. (cfr. articolo 6),

2) Principi relativi alla legittimazione del trattamento dei dati. In base a tali principi, il trattamento di dati personali tramite videosorveglianza va fondato almeno su uno dei requisiti preliminari di cui all'articolo 7 – consenso inequivocabile, necessità per obblighi contrattuali, per osservanza ad un obbligo legale, per la protezione degli interessi vitali della persona interessata, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, equilibrio degli interessi,

3) Trattamento di categorie particolari di dati, soggetto alle garanzie applicabili all'utilizzazione di dati sensibili o di dati concernenti infrazioni nell'ambito della videosorveglianza (conformemente all'articolo 8),

4) Informazioni da fornire alla persona interessata (cfr. articoli 10 e 11),

5) Diritti delle persone interessate, in particolare diritto di accesso e diritto di opposizione per motivi preminenti e legittimi (cfr. articoli 12 e 14, lettera a),

6) Garanzie applicabili in relazione alle decisioni individuali automatizzate (conformemente all'articolo 15),

7) Sicurezza dei trattamenti (articolo 17),

8) Notificazione delle operazioni di trattamento (conformemente agli articoli 18 e 19),

9) Controllo preliminare delle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone (ai sensi dell'articolo 20), e

10) Trasferimenti di dati verso paesi terzi (conformemente agli articoli 25 e seguenti.).

La specificità e la sensibilità del trattamento di dati sotto forma di suoni e immagini sono infine riconosciuti nel penultimo articolo della direttiva, in cui la Commissione si impegna ad esaminare, in particolare, l'applicazione della direttiva in questione e di presentare opportune proposte di modifica, tenuto conto dell'evoluzione della tecnologia dell'informazione e alla luce dei progressi della società dell'informazione (cfr. articolo 33).

4. DISPOSIZIONI NAZIONALI APPLICABILI ALLA VIDEOSORVEGLIANZA

In vari Stati membri sono già stati svolti studi analitici riguardo alla videosorveglianza, in base a disposizioni costituzionali [5] o legislazioni specifiche, ordinanze o altre decisione promulgate dalle competenti autorità nazionali [6] [7].

In alcuni paesi esistono anche disposizioni specifiche applicabili indipendentemente dal fatto che la videosorveglianza possa comportare il trattamento di dati personali. Ai sensi di tali regolamentazioni, l'installazione e l'uso di televisioni a circuito chiuso e attrezzature simili di sorveglianza debbono essere autorizzati preventivamente da un ente amministrativo, che può essere rappresentato, in tutto o in parte, dall'autorità nazionale per la protezione dei dati. Tali regolamentazione possono differire a seconda della natura pubblica o privata dell'ente responsabile del funzionamento delle attrezzature in questione.

In altri paesi, la videosorveglianza non forma attualmente oggetto di legislazioni specifiche; peraltro, le autorità per la protezione dei dati hanno svolto lavori per garantire la corretta applicazione delle disposizioni generali in materia di protezione dei dati, tra l'altro elaborando pareri, orientamenti o codici di comportamento, che sono già state adottati nel Regno Unito e che sono ad esempio in corso di elaborazione in Italia.

Belgio - Pareri dell'autorità per la protezione dei dati, in particolare parere 34/99 del 13 dicembre 1999, relativo al trattamento di immagini, in particolare attraverso l'utilizzazione di sistemi di videosorveglianza; parere 3/2000 del 10 gennaio 2000 relativo all'utilizzazione di sistemi di videosorveglianza nei vestiboli dei condomini.

Danimarca - Testo unico n. 76 del 1° febbraio 2000 relativo al divieto della videosorveglianza.

La decisione dell'autorità per la protezione dei dati, del 3 giugno 2002, relativa alla videosorveglianza da parte di un grande gruppo di supermercati e la trasmissione in diretta su Internet da un pub.

Francia - Legge n.78-17, del 6 gennaio 1978 relativa al trattamento dei dati, agli archivi e alle libertà (CNIL)

Raccomandazione n. 94-056 dell' autorità per la protezione dei dati, del 21 giugno 1994

Orientamento dell'autorità per la protezione dei dati relativo alla videosorveglianza sul posto di lavoro: http://www.cnil.fr/thematic/index.htm; su altri aspetti (ad esempio. webcam)

Legge specifica riguardante la videosorveglianza per la sicurezza pubblica in luoghi pubblici: legge n. 95-73, del 21 gennaio 1995, sulla sicurezza (modificata dall'ordinanza 2000-916 del 19 settembre 2000)

Decreto n. 96-926, del 17 ottobre 1996, e circolare del 22 ottobre 1996 sull'attuazione della legge n. 95-73

Grecia - Decisione dell'autorità per la protezione dei dati del 28 gennaio 2000 (metropolitana di Atene)

(5) Cfr. decisione 255/2002 del tribunale costituzionale portoghese. Il tribunale ha concluso che "l'utilizzazione di attrezzature elettroniche di sorveglianza e il controllo dei cittadini da parte di enti di sicurezza privati costituiscono una limitazione o una restrizione al diritto di tutelare la vita privata, contemplato nell'articolo 26 della Costituzione".

(6) Quanto meno in un paese (Belgio – causa Gaia), la non osservanza della legislazione in materia di protezione dei dati nel quadro della raccolta di immagini ha comportato un rifiuto di prove ammissibili in tribunale.

(7) Cfr. le relazioni annuali della "Commission Nationale de l'Informatique et des Libertés" francese.

Germania - Sezione 6, b della legge federale del 2001.

Irlanda - Studio analitico n. 14/1996 (utilizzazione di televisioni a circuito a chiuso)

Italia. Sezione 20 del decreto legge n. 467 del 28.12.2001 (che prevede l'adozione di codici di comportamento)
Decisione del garante n. 2, del 10 aprile 2002 (che promuove l'adozione di codici di comportamento), 28 settembre 2001 (biometria e tecniche di riconoscimento facciale applicate dalle banche) e 29 novembre 2000 (denominata "decalogo della videosorveglianza")
Decreto presidenziale n. 250, del 22.06.1999 (che regola l'accesso di veicoli al centro città e alle zone ad accesso limitato)
Decreto n. 433 del 14.11.1992 e legge n. 4/1993 (applicabile a musei, biblioteche e archivi di stato)
Decreto legislativo n. 45 del 04.02.2000 (navi passeggeri su rotte nazionali)
Sezione 4 della legge n. 300 del 20.05.1970 (denominata "statuto dei lavoratori")

Lussemburgo - Articoli 10 e 11 della legge del 02.08.2002 sulla protezione delle persone riguardo al trattamento dei dati personali

Paesi Bassi - Relazione dell'autorità per la protezione dei dati pubblicata nel 1997, che contiene orientamenti in merito alla videosorveglianza specialmente per la protezione delle persone e delle proprietà in luoghi pubblici.
La Camera bassa ha recentemente approvato un progetto di legge che estenderà l'ambito di atto criminale alla ripresa di fotografie di luoghi accessibili al pubblico senza informare le persone interessate.
Tra breve sarà presentato al Parlamento un progetto di legge che attribuirà esplicitamente alle giunte comunali la competenza di utilizzare sistemi di videosorveglianza a certe condizioni.

Portogallo - Decreto legge 231/98, del 22 luglio 98 (attività di sicurezza private e sistemi di autoprotezione)
Legge 38/98 del 4 agosto 98 (misure da adottare in caso di violenza connessa con manifestazioni sportive)
Decreto legge 263/01, del 28 settembre 2001 (luoghi destinati alle danze)
Decreto legge 94/2002, del 12 aprile 2002 (manifestazioni sportive)

Spagna - Legge organica n. 4/1997 (videosorveglianza da parte di agenzie di sicurezza in luoghi pubblici)
Real decreto n. 596/1999 in applicazione della legge n. 4/1997

Svezia - La videosorveglianza è specificatamente regolamentata nella legge (1998:150) sulla videosorveglianza generale e dalla legge (1995:1506) sulla videosorveglianza segreta (nelle indagini criminali)[8].

(8) In Svezia la videosorveglianza richiede in generale l'autorizzazione degli organi di amministrazione locale quantunque vi siano varie esenzioni, ad esempio per quanto riguarda la sorveglianza di uffici postali, filiali bancarie e negozi. La videosorveglianza segreta deve essere autorizzata da un tribunale. Una decisione degli organi di amministrazione locali secondo la legge sulla videosorveglianza generale può essere oggetto di ricorso da parte del Cancelliere di giustizia, al fine di tutelare gli interessi pubblici. La registrazione video con l'utilizzo di camere digitali è stata ritenuta come trattamento di dati personali ai sensi della legge sui dati personali svedese ed ha quindi successivamente formato oggetto della supervisione dell'autorità per la protezione dei dati. Una commissione inquirente sta attualmente analizzando l'utilizzazione della videosorveglianza da una prospettiva di prevenzione della criminalità. Tra l'altro, la commissione valuterà la legge sulla videosorveglianza generale e appurerà se sono necessarie modifiche. La commissione inquirente esaminerà altresì il campo di applicazione della legge svedese sui dati personali rispetto alla videosorveglianza e alla eventuale necessità di una legislazione specifica in materia di trattamento di dati personali in relazione alla videosorveglianza.

Regno Unito - Codice di comportamento 2000 per televisioni a circuito chiuso (Commissario per l'informazione)

Altri importanti strumenti normativi sono stati anche adottati in Islanda (sezione 4, legge n. 77/2000), Norvegia (titolo VII della legge n. 31, del 14.04.2000), Svizzera (raccomandazione del Commissario federale) e Ungheria (raccomandazione dell'autorità per la protezione dei dati, del 20.12.2000).

5. SETTORI IN CUI LA DIRETTIVA 95/46/CE È INAPPLICABILE, IN TUTTO O IN PARTE

La direttiva non si applica al trattamento di dati sotto forma di suoni e immagini per fini connessi con la sicurezza pubblica, la difesa, la sicurezza dello Stato e le attività dello Stato relative al diritto penale e/o nell'esercizio di altre attività che rientrano nel campo di applicazione della legislazione comunitaria [9]. Nonostante ciò, molti Stati membri, nel recepire la direttiva 95/46/CE, hanno contemplato tali aspetti in modo generale, disponendo peraltro esenzioni specifiche.

A) In alcuni paesi, le operazioni di trattamento effettuate per i fini sopra menzionati sono altresì soggette, in ogni caso, alle garanzie in conformità della convenzione n. 108/1981 e alle relative raccomandazioni del Consiglio d'Europa come pure a certe disposizioni nazionali (cfr. articolo 3, paragrafo 2, e il considerando n. 16 della direttiva 95/46/CE). Tenendo conto della sua peculiare natura e dell'esistenza di disposizioni specifiche connesse con attività di indagine di polizia e delle autorità giudiziarie, anche per fini di sicurezza dello Stato [10]- che possono includere la videosorveglianza "occulta", ossia effettuata senza fornire informazioni nei luoghi interessati - tale categoria di operazioni di trattamento non verrà trattata in dettaglio nel presente documento.

Il gruppo di lavoro vorrebbe far rilevare comunque che, al pari di altre simili operazioni di trattamento di dati personali anch'esse non rientranti nel campo d'applicazione della direttiva, la videosorveglianza effettuata per motivi di reale necessità di sicurezza pubblica o per la ricerca, prevenzione e controllo di atti criminali deve rispettare i requisiti fissati dall'articolo 8 della convezione dei diritti umani e delle libertà fondamentali e, nel contempo, essere disciplinata da disposizioni specifiche rese note al pubblico e connesse e proporzionate alla prevenzione di rischi concreti e reati specifici – ad esempio, in luoghi esposti a tali rischi o in relazione a manifestazioni pubbliche con probabilità ragionevole di tradursi in tali reati [11]. Vanno considerati gli effetti prodotti dai sistemi di videosorveglianza, ad esempio il fatto che attività illecite potrebbero spostarsi in altre aree o settori, mentre il responsabile del trattamento dei dati va sempre chiaramente specificato, affinché le persone interessate possano esercitare i loro diritti.

Quest'ultimo requisito è altresì connesso con il fatto che la videosorveglianza è sempre più utilizzata dalla polizia e da altre autorità pubbliche (ad esempio, gli enti locali) e/o da enti privati (banche, associazioni sportive, imprese di trasporti), con il rischio di rendere indistinti i ruoli e le responsabilità individuali per quanto riguarda i compiti da eseguire [12].

B) In secondo luogo, la direttiva non si applica alle operazioni di trattamento effettuate da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico (cfr. articolo 3, paragrafo 2, e considerando n. 12).

Mentre le circostanze sopra menzionate possono applicarsi, ad esempio, alla videovigilanza effettuata per il controllo a distanza oppure per vedere cosa succede in casa propria – ad esempio, per prevenire furti, oppure in relazione con la gestione della cosiddetta "famiglia elettronica" - ciò non è il caso qualora l'impianto di videosorveglianza sia installato all'esterno o in prossimità di luoghi privati, al fine di proteggere la proprietà e/o di garantire la sicurezza.

(9) Cfr. considerando 16.

(10) A questo proposito si potrebbe fare riferimento ai princípi fissati dal tribunale europeo dei diritti dell'uomo nella causa Rotaru /. Romania, esaminato il 4 maggio 2000. Vedi sopra.

(11) Ad esempio, una circolare pubblicata in Francia il 22.10.1996 faceva riferimento a luoghi isolati e a negozi aperti fino a tardi.

(12) Un esempio significativo di questo rischio è rappresentato dalle attività svolte da un certo numero di comuni in Italia al fine di controllare, mediante videosorveglianza, aree pubbliche frequentate di notte da prostitute. Un certo numero di comuni avevano argomentato, in passato, di essere – discutibilmente – competenti per la prevenzione di questo fenomeno, mentre altri comuni avevano emesso ordinanze che proibivano unicamente ai clienti delle prostitute di parcheggiare e/o di guidare in tali aree e avevano minacciato di inviare un fotografo al loro domicilio in caso di non osservanza dell'ordine. L'autorità italiana ha pubblicato una decisione al fine di chiarire le adeguate disposizioni per punire la violazione delle disposizioni pertinenti.

In questi casi, potrebbe trattarsi, anzitutto, di un sistema non utilizzato da singoli proprietari per controllare le porte che danno accesso alla loro residenza, ma piuttosto da vari proprietari in base ad un accordo oppure da un consorzio o da un condominio al fine di controllare varie entrate e zone del caseggiato – il che rende la direttiva applicabile a dette attività.

Laddove il sistema è gestito a beneficio di una famiglia e per controllare una sola porta, pianerottolo, parcheggio, ecc., il fatto che la direttiva non sia applicabile a motivo dell'utilizzazione esclusivamente personale nonché della non disponibilità dei dati per terzi non esenta il responsabile del trattamento dal rispetto dei diritti e interessi legittimi dei suoi vicini e di altre persone di passaggio. Negli Stati membri dell'UE, tali diritti e interessi sono effettivamente protetti indipendentemente dai principi della protezione dei dati da disposizioni generali (diritto civile) che tutelano i diritti personali, l'immagine, la vita familiare e la sfera privata – basta pensare, ad esempio, all'angolo visuale di una videocamera installata fuori dalla porta di un appartamento, che potrebbe permettere sistematicamente la registrazione dei pazienti di una clinica medica e/o i clienti di uno studio legale che si trova sullo stesso piano e causare quindi un'indebita interferenza con il segreto professionale.

Sarà necessario prestare particolare attenzione all'orientamento dell'attrezzatura video, alla necessità di affiggere avvisi ed informazioni e alla tempestiva eliminazione delle immagini, da effettuare entro poche ore – nel caso non si siano verificati effrazioni o reati.

C) Infine, l'articolo 9 della direttiva prevede che gli Stati membri debbono fissare esenzioni e deroghe da alcune delle disposizioni qualora il trattamento fosse effettuato unicamente a fini giornalistici o di espressione artistica o letteraria, in particolare nel campo audiovisivo (cfr. considerando n. 17). Vanno fissate unicamente le eccezioni necessarie per conciliare il diritto alla vita privata con le norme sulla libertà di espressione [13]. A tal riguardo, sarà necessaria una speciale attenzione in particolare nell'installazione di webcam e/o di videocamere on-line, al fine di evitare vizi e lacune nella protezione delle persone oggetto di videosorveglianza con fini che possono essere di pubblicità e/o di attività di promozione turistica [14].

6. VIDEOSORVEGLIANZA E TRATTAMENTO DI DATI PERSONALI

Alla luce delle varie situazioni sopra menzionate, il gruppo di lavoro è del parere che occorra attirare l'attenzione sul fatto che la direttiva 95/46/CE si applica al trattamento di dati personali, inclusi i dati sotto forma di immagini e suoni tramite circuiti chiusi di televisione o altri sistemi di videosorveglianza, in totalità o in parte tramite mezzi automatici, e al trattamento diverso da quello automatico di dati personali che formano parte di un sistema di archivio o che sono destinati a formar parte di un sistema di archivio.

I dati in forma di immagini e suoni relativi a persone fisiche identificate o identificabili rappresentano dati personali:

a) anche se le immagini sono utilizzate nel quadro di un sistema di circuito chiuso e non sono connesse con caratteristiche specifiche di una persona,

b) anche se non riguardano individui i cui volti sono stati filmati, anche se contengono altre informazioni, ad esempio numeri di targa di automobili o numeri di codice PIN acquisiti nel contesto della sorveglianza di sportelli automatici,

c) indipendentemente dal supporto utilizzato per il trattamento, ad esempio, sistemi fissi e/o mobili quali ricevitori videoportatili, immagini a colori e/o in bianco e nero, dalle tecniche utilizzate, ad esempio apparecchi con cavi o fibre ottiche, dal tipo di attrezzatura, ad esempio fissa, rotativa, mobile, dalle caratteristiche applicabili all'acquisizione di immagini, ad esempio continua (all'opposto di discontinua), il che potrebbe essere il caso se l'acquisizione di immagini occorre unicamente in caso del superamento del limite di velocità e non ha alcuna relazione con immagini video captate in forma interamente casuale e frammentaria e dagli strumenti di comunicazione utilizzati, ad esempio collegamento con un "centro" e/o trasmissione di immagini a terminal remoti, ecc. .

(13) Cfr. raccomandazione 1/97 del gruppo di lavoro sulla legislazione in materia di protezione di dati e media.

(14) Una webcam installata di nascosto presso le scale di una stazione di metropolitana a Milano mostrava direttamente nel Net immagini delle parti intime delle donne di passaggio, per fini solo apparentemente connessi ad attività giornalistiche. Il fatto che le persone coinvolte non potevano essere identificate non ha consentito all'autorità nazionale per la protezione dei dati di intraprendere iniziative in merito.

L'identificabilità, nel senso della direttiva, potrebbe essere anche determinata dalla combinazione di dati con informazioni detenute da terzi oppure dall'applicazione, in casi individuali, di tecniche e/o dispositivi specifici.

Di conseguenza, una delle prime precauzione che il responsabile del trattamento deve prendere è quella di controllare se la videosorveglianza implica il trattamento di dati personali nella misura in cui si riferisca a persone identificabili. In questo caso, la direttiva è applicabile indipendentemente dalle disposizioni nazionali che richiedono, inoltre, autorizzazione a fini di sicurezza pubblica.

Ciò può essere il caso, ad esempio, di attrezzature situate all'entrata oppure all'interno di una banca per consentire l'identificazione dei clienti; al contrario, in talune circostanze l'applicabilità della direttiva può essere esclusa per immagini di rilevamento aereo che non possono essere ingrandite o non includono informazioni connesse con persone fisiche – immagini raccolte, ad esempio, per rilevare fonti idriche o aree di eliminazione dei residui – come pure per attrezzature che forniscono immagini generiche del traffico in autostrada.

7. OBBLIGHI E PRECAUZIONI ADEGUATE APPLICABILI AL RESPONSABILE DEL TRATTAMENTO DEI DATI

A) Legittimità del trattamento

Anche tenendo conto che il trattamento deve essere lecito (conformemente all'articolo 6, lettera a), della direttiva), il responsabile del trattamento deve verificare in anticipo se la sorveglianza è conforme alle disposizioni generali e specifiche applicabili al settore, ad esempio leggi, regolamenti, codici di comportamento con significato giuridico. Tali disposizioni possono altresì essere fissate in relazione a fini di sicurezza pubblica nonché a fini diversi da quelli connessi con la protezione dei dati personali – ad esempio, la necessità di ottenere autorizzazioni ad hoc da organi amministrativi specifici e di attenersi alle loro istruzioni.

Occorre adottare tutte le misure necessarie per garantire che la videosorveglianza sia conforme ai principi di protezione dei dati, e devono essere evitati riferimenti inappropriati alla vita privata [15].

In proposito, occorre tener conto delle migliori prassi che potrebbero essere stabilite in raccomandazioni pubblicate da autorità di supervisione e in altri strumenti di autoregolamentazione.

È necessario altresì verificare le restanti disposizioni di diritto nazionale – inclusi i principi costituzionali, disposizioni di diritto civile e di diritto penale – per quanto riguarda, in particolare, quelle applicabili al "droit à l'image"[16] o alla protezione del domicilio di una persona; va tenuto conto della giurisprudenza in materia che potrebbe aver deciso che luoghi diversi da quelli connessi con il domicilio di una persona – ad esempio stanze d'albergo, uffici, bagni pubblici, vestiari, cabine telefoniche interne, ecc. – debbono considerarsi come luoghi privati.

Se l'attrezzatura è stata installata da enti privati o pubblici, in special modo enti locali, presumibilmente per fini di sicurezza o per la ricerca, la prevenzione e il controllo di reati, occorrerà prestare speciale attenzione, nella determinazione e informazione di tali fini, ai compiti che potrebbero essere lecitamente eseguiti dal responsabile del trattamento – dato che talune funzioni pubbliche possono essere esercitate legalmente da organismi specifici non amministrativi, come ad esempio, in particolare, organi di polizia.

Tale questione è stata sollevata in special modo a proposito di alcune autorità locali che non hanno alcuna diretta competenza in questioni di ordine pubblico e di sicurezza pubblica ma che svolgono comunque attività ausiliarie a fini di sorveglianza. Allo stesso modo, la sorveglianza spesso giustificata per motivi di controllo della criminalità è destinata invece, ad ottenere prove in caso di perpetrazione di atti criminali.

(15) Di recente, una banca e una locale stazione di polizia non hanno soddisfatto la richiesta di un cliente di estrarre, dalle immagini registrate da una videocamera che filmava anche uno sportello automatico, le immagini di un ladro che, dopo aver rubato la carta bancaria del cliente, l'aveva utilizzata illegalmente per ritirare denaro da uno sportello automatico – allegando motivi di "vita privata".

(16) In Francia e in Belgio questo diritto richiede un "consenso preliminare".

B) Specificità, specificazione e legittimità delle finalità

Il responsabile del trattamento dei dati deve garantire che le finalità non siano poco chiare né ambigue, anche per poter disporre di un criterio preciso al momento di valutare la compatibilità delle finalità del trattamento (cfr. articolo 6, lettera b), della direttiva).

Tale chiarimento è altresì necessario per illustrare le finalità tanto nelle informazioni da fornire alle persone interessate, tanto nella rispettiva notifica, quanto in relazione all' eventuale controllo preliminare da effettuare eventualmente conformemente all'articolo 20 della direttiva.

Deve essere chiaramente specificato che le immagini raccolte non possono essere utilizzate per altre finalità, in particolare per quanto riguardo le possibilità di riproduzione tecnica – ad esempio vietandone espressamente la copia.

Le finalità specificate debbono essere menzionate in un documento in cui dovrebbero essere anche ricapitolate altre caratteristiche importanti della politica della "vita privata" – fondamentali quali la documentazione del momento di cancellazione delle immagini, eventuali richieste di accesso da parte delle persone interessate e/o consultazione legittima dei dati.

C) Criteri per rendere il trattamento legittimo

Il responsabile del trattamento dei dati deve verificare che la videosorveglianza soddisfi le disposizioni specifiche di cui al punto A), ed almeno uno dei criteri che rendono il trattamento legittimo ai sensi dell'articolo 7 della direttiva – per quanto riguarda in modo particolare la protezione di dati personali.

Oltre ai casi meno frequenti in cui un obbligo giuridico va rispettato – si è fatto riferimento alle attività in un casinò, dove il trattamento è necessario per proteggere interessi vitali – ad esempio per il controllo a distanza di pazienti in unità di rianimazione – accade spesse volte che un responsabile del trattamento dei dati debba svolgere una missione di interesse pubblico o nell'esercizio di autorità pubblica di cui è investito, possibilmente in conformità di regolamentazioni specifiche – ad esempio, per individuare violazioni del codice stradale o un comportamento violento su mezzi di trasporto pubblici in zone di alta criminalità – conformemente all'articolo 7, lettera e), della direttiva; alternativamente, il responsabile del trattamento dei dati può perseguire interessi legittimi, in cui non prevalgono l'interesse o i diritti e le libertà fondamentali della persona interessata (cfr. articolo 7, lettera f)).

In entrambi i casi, specialmente nell'ultimo caso, la natura sensibile dell'operazione di trattamento richiede un'attenta considerazione della portata dei compiti, dei poteri e degli interessi legittimi del responsabile del trattamento. In tale analisi devono essere eliminate in assoluto superficialità e ampliamento senza fondamenti della portata di tali compiti e poteri.

Per quanto riguarda, in particolare, l'equilibrio dei vari interessi, si dovrà prestare un'attenzione particolare anche ascoltando in via preliminare le parti interessate, sulla possibilità che un interesse da proteggere può essere in conflitto con l'installazione del sistema oppure con taluni accordi di conservazione dei dati o con altre operazioni di trattamento [17].

Infine, per quanto riguarda l'ottenimento del consenso della persona interessata, quest'ultimo dovrà essere inequivocabile e basato su informazioni ben definite. Il consenso dovrà essere concesso separatamente e specificamente per attività di sorveglianza riguardanti luoghi in cui la persona passa la sua vita privata [18].

La legittimità del trattamento va anche valutata tenendo conto delle disposizioni della direttiva che fissano garanzie specifiche per i dati relativi alle infrazioni (cfr. articolo 8, paragrafo 5) della direttiva) [19]

(17) Ai sensi della sezione 6b della nuova legge federale tedesca sulla protezione dei dati, che è entrata in vigore il 23 maggio 2001, l'osservazione di aree di accesso pubblico per mezzo di dispositivi ottici ed elettronici è permessa se, tra l'altro, non sussistono motivi di credere che prevalgano gli interessi delle persone in causa, da proteggere.

(18) Occorre prestare un'attenzione specifica alla reale possibilità di esprimere un consenso valido nel senso dell'articolo 2, lettera h) della direttiva 95/46/CE ("qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento") in caso di installazione di sistemi di videosorveglianza in coproprietà (condomini, etc.).

(19) In proposito si può fare riferimento alla sezione 8 della legge portoghese relativa ai dati riguardanti persone sospette di attività illecite e/o criminali.

Le operazioni di trattamento per mezzo della videosorveglianza devono basarsi sempre su disposizioni giuridiche espresse, ove vengano eseguite da organismi pubblici.

D) Proporzionalità del ricorso alla videosorveglianza

Il principio in base al quale i dati debbono essere adeguati e proporzionati alle finalità da raggiungere significa, in primo luogo che la televisione a circuito chiuso e altre attrezzature simili di videosorveglianza possono essere utilizzate unicamente in via sussidiaria, cioè: per fini che giustifichino effettivamente il ricorso a tali sistemi.

Occorre evitare, ad esempio, che un organo amministrativo installi un'attrezzatura di videosorveglianza in relazione a infrazioni minori – ad esempio, per rafforzare il divieto di fumare nelle scuole ed in altri luoghi pubblici oppure il divieto di lasciare mozziconi di sigarette e rifiuti in luoghi pubblici.

In altre parole, è necessario applicare, caso per caso, il principio di adeguatezza alle finalità perseguite, il che implica un specie di dovere di minimizzazione dei dati da parte del responsabile del trattamento.

Mentre un sistema proporzionato di videosorveglianza e di allarme può essere ritenuto legittimo in caso di attacchi ripetuti a bordo di autobus in zone periferiche o in prossimità delle fermate di autobus, ciò non è il caso con un sistema destinato a impedire insulti ai conducenti di autobus e l'imbrattamento di veicoli – conformemente ad una descrizione fornita ad un'autorità per la protezione dei dati – oppure a identificare cittadini responsabili di infrazioni amministrative minori, quali l'abbandono di sacchetti di rifiuti fuori dai rispettivi contenitori e/o in zone in cui non si debbono lasciare rifiuti.

La proporzionalità deve essere valutata sulla base di criteri ancora più rigorosi per quanto riguarda luoghi non accessibili al pubblico.

In questo contesto potrebbe rivelarsi utile lo scambio di informazioni e di esperienza tra le competenti autorità dei vari Stati membri [20]; inoltre, tali sistemi possono essere applicati qualora altre misure di protezione di sicurezza che non comporta l'acquisizione di immagini – ad esempio l'utilizzazione di porte blindate contro il vandalismo, l'installazione di cancelli automatici e dispositivi per l'autorizzazione a passare, sistemi congiunti di allarmi, migliore e più forte illuminazione delle strade di notte, etc. – si rivelino chiaramente insufficienti e/o inapplicabili nell'ottica delle finalità legittime sopra menzionate.

Tali considerazioni si applicano, in particolare, all'utilizzazione sempre più frequente della videosorveglianza a fini di autodifesa e di protezione della proprietà – soprattutto in prossimità di edifici pubblici e uffici, incluse le aree circostanti. Questo tipo di applicazione richiede una valutazione, da un punto di vista più generale, degli effetti indiretti prodotti dal ricorso massiccio alla videosorveglianza – ad esempio, se un'installazione di vari dispositivi sia un elemento effettivamente dissuasivo, oppure se i trasgressori e/o vandali passano semplicemente in altre aree ed attività.

E) Proporzionalità delle attività di videosorveglianza

Il principio secondo il quale i dati debbono essere adeguati, pertinenti e non eccessivi implica un'attenta valutazione della proporzionalità delle disposizioni applicabili al trattamento dei dati, una volta accertata la legittimità di tale trattamento.

Le modalità relative alla ripresa di immagini dovranno essere considerate in particolare riguardo ai seguenti aspetti:

a) l'angolo visuale in relazione alla finalità prevista [21]– ad esempio se la sorveglianza è effettuata in un

(20) Ciò consentirebbe altresì una migliore armonizzazione degli approcci regolamentari e delle decisioni amministrative, talvolta divergenti – come è stato il caso, ad esempio, per le sale di Bingo.

(21) In due disposizioni formulate dall'autorità italiana per la protezione dei dati si possono trovare esempi di precauzioni specifiche da prendere riguardo all'angolo visuale. Un ente sanitario, che intendeva introdurre un servizio che consentisse ai familiari di osservare continuamente, a distanza, pazienti in coma, quarantena e/o gravemente malati in una unità di pronto soccorso è stato informato della necessità di adottare adeguate misure per impedire la visualizzazione simultanea di altri pazienti. In un altro caso, l'autorità ha fatto presente alle autorità amministrative di polizia che, per un sistema di rilevamento del superamento dei limiti di velocità era necessario unicamente filmare le targhe piuttosto che l'interno dei veicoli.

luogo pubblico, l'angolo non dovrà consentire la visualizzazione di dettagli e/o di tratti somatici irrilevanti ai fini prefissi, oppure aree all'interno di luoghi privati situati nelle vicinanze, soprattutto se vengono utilizzate funzioni di "zoom",

b) il tipo di attrezzatura utilizzato per filmare, ad esempio fisso o mobile,

c) le disposizioni effettive di installazione, ad esempio la localizzazione delle videocamere, l'utilizzazione di videocamere ad immagine fissa e/o mobile, etc.,

d) la possibilità di ingrandire e/o ravvicinare (funzioni di zoom) immagini nel momento in cui esse sono filmate o successivamente, ad esempio riguardo ad immagini memorizzate,

e) funzioni di blocco di immagini,

f) collegamento con un "centro" per inviare allarmi sonori e/o visivi,

g) misure adottate a seguito della videosorveglianza, a esempio chiusura delle vie d'accesso, intervento del personale di sorveglianza, etc. .

In secondo luogo, è necessario considerare la decisione da prendere per quanto riguarda la conservazione delle immagini e il periodo di conservazione – quest'ultimo deve essere di breve durata e conforme alle caratteristiche specifiche del caso in questione.

Mentre in alcuni casi potrebbe essere sufficiente un sistema che consente unicamente la visualizzazione di immagini a circuito chiuso, senza registrazione – ad esempio nel caso della casse di un supermercato –, in altri casi – ad esempio per proteggere luoghi privati – potrebbe essere giustificato registrare le immagini durante un certo numero di ore ed eliminarle automaticamente, entro la fine della giornata e quanto meno alla fine della settimana. Una eccezione a questa regola sarà ovviamente il caso in cui sia stato lanciato un allarme o inoltrata una richiesta meritevole di attenzione particolare; in tali casi sussistono motivi ragionevoli per aspettare, per un breve periodo di tempo, la decisione eventualmente adottata dalla polizia oppure dalle autorità giudiziarie.

Per citare un altro esempio, un sistema destinato a rilevare accessi non autorizzati a veicoli nei centri città e in zone di traffico limitato dovrebbe registrare immagini unicamente ove fossero commesse infrazioni.

La questione della proporzionalità dovrebbe essere altresì tenuta in considerazione ove siano ritenuti necessari periodi di conservazione meno lunghi che non devono comunque superare una settimana [22] – ad esempio per quanto riguarda immagini ottenute tramite videosorveglianza che potrebbero essere utilizzate per identificare le persone presenti in una banca prima di una rapina.

In terzo luogo occorrerà fare attenzione ai casi in cui l'identificazione di una persona è facilitata dall'associazione di immagini del viso della persona con altre informazioni relative al comportamento e/o alle attività osservate – ad esempio, nel caso di associazione tra immagini e attività di clienti in una banca in un momento facilmente identificabile.

In questo contesto, si dovrà tener conto della chiara differenza tra la conservazione temporanea delle immagini di videosorveglianza ottenute per mezzo di attrezzature situate all'entrata di una banca e l'elaborazione decisamente più invadente di banche dati che includono fotografie e impronte digitali fornite dai clienti della banca con il loro consenso.

Infine, occorrerà tener conto delle decisioni da adottare riguardo all'eventuale comunicazione dei dati a terzi – che, di massima, non devono coinvolgere organismi senza relazioni con le attività di videosorveglianza – e la loro divulgazione, totale o parziale, addirittura all'estero o on-line – anche alla luce delle disposizioni relative ad un'adeguata protezione, cfr. articolo 25 e seguenti della direttiva.

Ovviamente, la necessità che le immagini siano pertinenti e non eccessive si applica altresì alla combinazione di informazioni detenute da vari responsabili dei sistemi di videosorveglianza.

Le garanzie sopra citate sono destinate ad applicare, anche a livello operativo, il principio menzio-

(22) Le autorità per la protezione di dati danesi e svedesi hanno espresso il parere che la videoregistrazione può essere conservata unicamente per un breve periodo e che tale periodo non deve essere superiore a 30 giorni.

nato nelle legislazioni nazionali di alcuni paesi come il principio di moderazione nell'utilizzazione di dati personali – che mira ad evitare o a ridurre, nei limiti del possibile, il trattamento di dati personali.

Questo principio deve essere applicato in tutti i settori tenendo inoltre conto del fatto che molte finalità possono essere effettivamente raggiunte senza dover ricorrere a dati personali, oppure utilizzando dati realmente anonimi, anche se inizialmente sembrino richiedere l'utilizzazione di informazioni personali.

Le considerazioni di cui sopra si applicano inoltre in presenza di un'esigenza motivata di razionalizzare le risorse commerciali [23] oppure di migliorare i servizi offerti agli utenti [24].

F) Informazione delle persone interessate

L'apertura e l'adeguatezza dell'utilizzazione di attrezzature di videosorveglianza comporta la trasmissione di informazioni adeguate alle persone interessate, conformemente agli articoli 10 e 11 della direttiva.

Le persone interessate debbono essere informate, conformemente agli articoli 10 e 11 della direttiva. Le persone debbono essere consapevoli del fatto che viene effettuata una videosorveglianza, anche se quest'ultima si riferisce a manifestazioni e spettacoli pubblici oppure ad attività pubblicitarie (web cam); esse devono essere informate in dettaglio circa i luoghi sotto vigilanza.

Non è necessario specificare la localizzazione esatta dell'attrezzatura di sorveglianza, peraltro il contesto della sorveglianza va chiarificato inequivocabilmente.

Le informazioni dovrebbero essere affisse ad una ragionevole distanza dai luoghi sotto vigilanza – al contrario di quanto si è fatto in alcuni casi, in cui si era ritenuta accettabile la collocazione a 500 metri dalle zone sotto sorveglianza dei cartelli informativi – anche a seconda del tipo di ripresa di immagini.

Le informazioni debbono essere visibili e possono essere fornite in forma sommaria, a condizione che sia efficace; tali informazioni possono includere simboli che si sono già dimostrati utili in relazione con la videosorveglianza e informazioni circa il divieto di fumare – che possono differire a seconda che le immagini siano registrate o meno. Le finalità della videosorveglianza e il responsabile del trattamento devono essere specificati in tutti i casi. Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni.

Potranno essere permesse limitazioni specifiche e ben motivate ai requisiti di informazione unicamente nei casi di cui agli articoli 10, 11 e 13 della direttiva – ad esempio, può essere applicata una limitazione temporanea a dati raccolti nel corso di indagini effettuate legalmente da un avvocato della difesa, oppure al fine di esercitare il diritto di difesa durante il periodo in cui ciò potrebbe mettere a rischio le finalità specifiche perseguite.

Infine particolare attenzione deve essere rivolta al modo appropriato di fornire informazioni alle persone non vedenti.

G) Requisiti supplementari

Per quanto riguarda i requisiti, le precauzione e le garanzie supplementari menzionate nella legislazione relativa alla protezione dei dati e ricapitolate al punto 3) precedente – anche rispetto l'esigenza di notificare il trattamento di dati personali e di sottoporlo alla supervisione di un'autorità indipendente, conformemente agli articoli 18, 19 e 28 della direttiva – , il gruppo di lavoro gradirebbe attirare l'attenzione, in particolare, sugli aspetti seguenti:

a) Un numero limitato di persone fisiche, da specificare, deve poter visualizzare o accedere all' eventuali immagini registrate esclusivamente per le finalità prefisse tramite videosorveglianza o al fine di pro-

(23) Ciò può essere il caso, ad esempio, della necessità di calcolare il numero di casse che devono restare aperte simultaneamente in un supermercato a seconda dell'affluenza dei clienti, nonché della creazione di un "percorso d'acquisti" ottimale per i consumatori in un supermercato.

(24) Per facilitare l'accesso in un luogo di lavoro e/o a bordo di un mezzo di trasporto specifico che richieda controlli di identità, è sufficiente utilizzare carte di identità con foto della persona interessata, eventualmente su supporto informatico, evitando l'installazione di un sistema di riconoscimento facciale.

cedere alla manutenzione delle attrezzature in questione per verificarne il corretto funzionamento; in alternativa, il caso può scaturire della richiesta di una persona interessata ed avere accesso ai dati o da un ordine legale emesso da una autorità di polizia o giudiziaria per la scoperta di atti criminali.

Ove la videosorveglianza sia destinata unicamente ad evitare, scoprire e controllare infrazioni, la soluzione dell' utilizzazione di due chiavi di accesso – una detenuta dal responsabile del trattamento e l'altra dalla polizia – potrebbe essere utile per garantire che le immagini siano viste soltanto dal personale di polizia e da nessun altro personale non autorizzato – fatto salvo l'esercizio legittimo della persona interessata dei suoi diritti di accesso, tramite richiesta espressa durante il breve periodo di conservazione delle immagini.

b) Devono essere applicate adeguate misure di sicurezza al fine di prevenire il verificarsi di eventi di cui all'articolo 17 della direttiva, inclusa la diffusione dell'informazione che potrebbe essere utile a proteggere un diritto della persona interessata, di un terzo o dello stesso responsabile del trattamento – anche per evitare la manipolazione, l'alterazione o la distruzione di prove.

c) È anche fondamentale la qualità delle eventuali immagini registrate – in particolare se lo stesso supporto di registrazione viene utilizzato ripetutamente; incorre il rischio di non poter cancellare interamente le immagini registrate in precedenza.

d) Infine, è indispensabile che gli operatori concretamente coinvolti nelle attività di videosorveglianza siano adeguatamente formati e resi consapevoli delle iniziative da adottare per soddisfare interamente i requisiti.

H) Diritti della persona interessata

Le caratteristiche peculiari dei dati personali raccolti non escludono l'esercizio, da parte della persona interessata, dei diritti di cui agli articoli 13 e 14 della direttiva, in particolare riguardo al diritto di opporsi al trattamento. La direttiva 95/46 permette effettivamente che la persona interessata si opponga, in qualsiasi momento, al trattamento di dati a lei relativi [25] per motivi preponderanti e legittimi relativi alla sua situazione particolare.

Il diritto della persona interessa all'oblio e il periodo di conservazione relativamente breve delle immagini riduce effettivamente il campo di applicazione del diritto della persona interessata all'accesso di dati personali che la rendono identificabile; tuttavia, tale diritto va garantito specialmente in caso di richiesta particolareggiata che consenta di ritrovare le immagini facilmente, tenuto conto altresì della necessità di salvaguardare l'interesse di terzi in modo temporaneo.

Qualsiasi limitazione fondata sugli sforzi per recuperare le immagini, e nel caso in cui tali sforzi siano chiaramente sproporzionati, tenuto conto del breve periodo di conservazione delle immagini, deve essere fissata esclusivamente tramite diritto secondario (cfr. articolo 13, paragrafo 1, della direttiva) con il debito rispetto del diritto della persona interessata alla difesa nel contesto di eventi specifici che possono essere occorsi nel periodo considerato.

I) Garanzie supplementari relative ad operazioni specifiche di trattamento

Deve essere proibita la videosorveglianza esclusivamente basata sull'origine etnica delle persone osservate, il loro credo religioso o opinioni politiche, la loro appartenenza a sindacati o alle loro abitudini sessuali (articolo 8 della direttiva).

Senza pretendere di elaborare un elenco esaustivo delle varie applicazione della videosorveglianza, il gruppo di lavoro gradirebbe rilevare la necessità di prestare maggiore attenzione – di massima, se del caso, nel contesto del controllo preliminare delle operazioni di trattamento di cui all'articolo 20 della direttiva – e specifici contesti in cui sono raccolte immagini relative a persone identificate o identificabili, dato che tali contesti dovrebbero essere valutati caso per caso.

Si fa riferimento, in particolare, ai casi seguenti, risultanti da esperienze e/o prove in corso:

a) interconnessione permanente di sistemi di videosorveglianza gestiti da più responsabili del trattamento,

b) possibile associazione di immagini e di dati biometrici, quali impronte digitali (ad esempio, all'en-

(25) Tranne quando disposto altrimenti dalla legislazione nazionale.

trata delle banche),

c) utilizzazione di sistemi di identificazione vocale,

d) applicazione, conformemente ai principi di proporzionalità e basata su disposizioni specifiche, di sistemi di indicizzazione applicabili ad immagini registrate e/o sistemi per il loro recupero simultaneo automatico, specialmente attraverso dati di identificazione,

e) utilizzazione di sistemi di riconoscimento facciale che non si limitano all'identificazione del camuffamento di persone in transito, (ad esempio barbe o parrucche false) ma che si basano su tecniche che consentono di segnalare le persone sospette – cioè la capacità del sistema di identificare automaticamente certi individui, in base a modelli e/o identikit standard risultanti da talune caratteristiche esterne (ad esempio colore della pelle di una persona, occhi, zigomi sporgenti, etc.), oppure sulla base di un comportamento anomalo predefinito (movimenti bruschi, passaggi successivi ad intervalli determinati, modo di parcheggiare l'autovettura, etc.). A questo riguardo, l'intervento umano è adeguato anche alla luce di errori che possono succedere in tali casi, come anche menzionato al punto f) seguente,

f) possibilità di seguire automaticamente percorsi e tragitti e/o ricostruire o prevedere il comportamento di una persona,

g) adozione di decisioni automatizzate basate sul profilo di una persona o su sistemi intelligenti d'analisi e d'intervento non connessi con allarmi standard – ad esempio, accesso senza identificazione o allarme d'incendio.

8. VIDEOSORVEGLIANZA NEL CONTESTO DELL'OCCUPAZIONE

Nel suo parere n. 8/2001 sul trattamento di dati personali nel contesto dell'occupazione, adottato il 13 settembre 2001 e nel suo documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sul posto di lavoro, adottato il 29 maggio 2002 [26], il gruppo di lavoro ha già richiamato l'attenzione, in termini più generali, su alcuni principi destinati a salvaguardare i diritti, le libertà e la dignità delle persone interessate, nell'ambito dell'occupazione.

Oltre alle considerazioni formulate nei documenti sopra menzionati, nella misura in cui essi sono effettivamente applicabili alla videosorveglianza, è opportuno rilevare che i sistemi di videosorveglianza miranti direttamente a controllare da un luogo remoto la qualità e la quantità delle attività lavorative, implicando di conseguenza il trattamento di dati personali in questo contesto, non dovrebbero essere di regola permesse.

La situazione è diversa per quanto riguarda i sistemi di videosorveglianza utilizzati con le debite garanzie, per soddisfare requisiti di sicurezza della produzione e/o dell'occupazione e che, sebbene indirettamente [27], comportano il controllo a distanza.

L'esperienza di applicazione ha dimostrato inoltre che la sorveglianza non deve includere locali riservati all'uso privato dei dipendenti o non destinati allo svolgimento dei compiti connessi con l'occupazione – ad esempio bagni, docce, armadietti e zone di ricreazione; che le immagini raccolte esclusivamente per tutelare la proprietà e/o per scoprire, prevenire e controllare infrazioni gravi non devono essere utilizzate per incolpare un dipendente di infrazioni disciplinari minori, che i lavoratori dipendenti debbano poter sempre presentare una domanda riconvenzionale utilizzando il contenuto delle immagini raccolte.

Le informazioni vanno fornite ai dipendenti e ad ogni persona che lavori nei luoghi in questione. Le informazioni dovrebbero includere l'identità del responsabile del trattamento e la finalità della sorveglianza, nonché altre informazioni necessarie per garantire un trattamento reale nei confronti della persona interessata, ad esempio in quali casi le registrazioni vengono esaminate dall'amministrazione delle imprese, il periodo di registrazione e quando la registrazione è trasmessa alle autorità giudiziarie. La fornitura di informazioni, ad esempio attraverso un simbolo, non può essere ritenuta sufficiente nel contesto dell'occupazione.

(26) Entrambi i documenti sono disponibili al seguente indirizzo: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.

(27) In questi casi, oltre alle considerazioni espresse nel presente documento, occorre anche tener conto in modo speciale dell'esigenza di rispettare i diritti menzionati negli accordi collettivi, che talvolta si basano su informazioni collettive dei dipendenti e/o dei loro sindacati – ossia, oltre alle informazioni da fornire individualmente in osservanza delle legislazioni sulla protezione dei dati; in altri casi, va ricercato un accordo preliminare con i rappresentanti dei dipendenti o con le organizzazioni sindacali riguardo disposizioni in merito all'installazione, anche per quanto concerne la durata della sorveglianza ed altre disposizioni di ripresa di immagini. In alcuni paesi, può essere necessario l'intervento dello Stato qualora non si raggiungano accordi tra le parti interessate.

9. CONCLUSIONE

Il gruppo di lavoro ha elaborato il presente documento per contribuire all'applicazione uniforme delle misure nazionali adottate ai sensi della direttiva 95/46/CE nel campo della videosorveglianza.

In questo contesto, è anche indispensabile che gli Stati membri forniscano orientamenti quanto all'attività dei produttori, prestatori di servizi e distributori, nonché ricercatori in vista dello sviluppo delle tecnologie, dei software e dei dispositivi tecnici conformi ai principi illustrati nel presente documento.

Fatto a Bruxelles, il 25 novembre 2002

Per il gruppo di lavoro
Il Presidente
Stefano RODOTÀ

127 Documento di lavoro relativo ai servizi di autenticazione *on-line* (*)

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



10054/03/IT
WP 68

Documento di lavoro relativo ai servizi di autenticazione on-line

Adottato il 29 gennaio 2003

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_it.pdf

128 Parere 1/2003 sulla memorizzazione dei dati relativi al traffico a fini di fatturazione

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

12054/02/IT
WP 69

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

costituito in virtù della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 [1],

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, di tale direttiva e l'articolo 14, paragrafo 3, della direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL PRESENTE PARERE:

1. Introduzione

1.1 Il presente parere verte sul periodo di tempo durante il quale i dati relativi al traffico, originati dall'effettuazione delle comunicazioni elettroniche, possono essere sottoposti a trattamento ai fini della fatturazione.

Nel suo parere 7/2000 sulla proposta della Commissione che ha portato all'adozione della direttiva 2002/58/CE [2], il gruppo osservava che il progetto di direttiva non prevedeva alcuna armonizzazione del periodo durante il quale può essere legalmente contestata la fattura. Il presente parere intende ritornare sulla raccomandazione 3/99 [3] che ha già fornito alcuni orientamenti in materia, in particolare nei casi in cui le bollette sono state pagate e non sono contestate, al fine di contri-

(1) G.U L 281 del 23.11.1995, pag. 31, disponibile al sito: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
(2) Proposta della Commissione europea di una 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.
(3) Raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_99.htm

buire all'uniforme applicazione delle direttive comunitarie in materia di tutela dei dati, nell'intento di essere di ausilio alle società di telecomunicazioni, alle autorità nazionali [4] e agli interessati.

1.2 In seno all'Unione europea la direttiva 95/46/CE armonizza le disposizioni che disciplinano la tutela delle persone fisiche con riguardo al trattamento dei dati personali.

L'articolo 6 di tale direttiva stipula che:

> *« 1. Gli Stati membri dispongono che i dati personali devono essere:*
> *(a) trattati lealmente e lecitamente;*
> *(...)*
> *(e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.»*

2. Applicazione delle direttive comunitarie in tema di telecomunicazioni e di tutela dei dati

2.1 La direttiva 97/66/CE è finalizzata all'armonizzazione delle normative nazionali degli Stati membri atte a garantire un livello equivalente di tutela dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni, nonché a garantire la libera circolazione di tali dati e delle apparecchiature e dei servizi di telecomunicazione all'interno della Comunità. L'articolo 6 di tale direttiva stabilisce che:

«1. I dati sul traffico relativi agli abbonati e agli utenti, trattati per inoltrare chiamate e memorizzati dal fornitore di una rete pubblica e/o di un servizio di telecomunicazione offerto al pubblico, devono essere cancellati o resi anonimi al termine della chiamata, fatte salve le disposizioni dei paragrafi 2, 3 e 4.

2. Ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento i dati indicati nell'allegato. Il trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. »

2.2 Tale direttiva sarà sostituita nel novembre 2003 dalla direttiva 2002/58/CE, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [5].

L'articolo 6 della direttiva 2002/58/CE conferma la scelta fatta nella direttiva 97/66/CE e ne estende l'ambito al contesto più generale delle comunicazioni elettroniche. Esso stabilisce che:

(4) Il presente parere dovrebbe essere di ausilio alle autorità competenti in materia di tutela dei dati allorché verificano l'applicazione delle disposizioni adottate dagli Stati membri in virtù delle direttive sulla tutela dei dati o allorché sono consultate in sede di redazione da parte degli Stati membri di misure o disposizioni amministrative in tema di trattamento dei dati sul traffico. Dovrebbe anche essere di ausilio agli Stati membri in sede di elaborazione delle disposizioni nazionali di attuazione della direttiva 2002/58/CE.
(5) Pubblicato nella G.U.C.E. L 201 del 31 luglio 2002

« 1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. »

2.3 Nella sua raccomandazione 3/99, il gruppo "articolo 29" ha ricordato l'obbligo previsto all'articolo 6 della direttiva 97/66/CE di cancellare i dati relativi al traffico o di renderli anonimi al termine della comunicazione (articolo 6, paragrafo 1). Il gruppo spiegava che "ciò si deve alla delicatezza di tali dati, che possono consentire l'elaborazione di profili individuali di comunicazione, ivi comprese le fonti delle informazioni e la località geografica dell'utente di telefoni fissi o mobili, e ai pericoli per la riservatezza che derivano dalla raccolta, trasmissione o ulteriore utilizzazione di tali dati". Infine il gruppo ricordava che l'articolo 6, paragrafo 2, stabiliva un'eccezione in merito al trattamento dei dati relativi al traffico ai fini delle attività di fatturazione agli abbonati e della riscossione dei canoni di interconnessione "ma *solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento*".

2.4 L'articolo 6, paragrafo 2, della direttiva 97/66/CE (così come l'articolo 6, paragrafo 2, della direttiva 2002/58/CE) deve essere interpretato in conformità agli obiettivi delle direttive generali e specifiche. A questo proposito il decimo considerando della direttiva 95/46/CE ricorda che:

«(10) considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario; che pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità; »

2.5 L'articolo 6, paragrafo 5, della direttiva 2002/58/CE (articolo 6, paragrafo 4, della direttiva 97/66/CE) stabilisce che "il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 (...) deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività". Il diciassettesimo considerando della direttiva 97/66/CE fornisce un ausilio interpretativo rispetto all'articolo 6, paragrafo 2 *(si veda anche il ventiseiesimo considerando della direttiva 2002/58/CE)*:

«(17) considerando che i dati relativi agli abbonati, trattati per stabilire le chiamate, contengono informazioni sulla vita privata delle persone fisiche e riguardano il loro diritto al rispetto della propria corrispondenza o i legittimi interessi delle persone giuridiche; che ***tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini di fatturazione e di pagamenti di interconnessione, nonché per un periodo di tempo limitato****; che un ulteriore trattamento che il fornitore di un servizio di telecomunicazione offerto al pubblico volesse effettuare per*

la commercializzazione dei suoi servizi di telecomunicazione può essere permesso unicamente se l'abbonato ha dato il proprio consenso sulla base di informazioni esaurienti ed accurate date dal fornitore del servizio di telecomunicazione offerto al pubblico riguardo al genere dei successivi trattamenti che egli intende effettuare; »

2.6 Risulta evidente da tali considerando che i dati memorizzati ai fini della fatturazione e dei pagamenti di interconnessione possono esserlo soltanto per un periodo di tempo limitato e non devono essere conservati su base routinaria per lunghi periodi come indicato anche nella raccomandazione 3/99 del Gruppo.

Data questa situazione si pone la domanda per quanto tempo i dati personali relativi al traffico possano essere memorizzati "ai fini della fatturazione e dei pagamenti di interconnessione" **in particolare in quei casi in cui la fattura è stata pagata e non è oggetto di contestazioni.**

2.7 I diversi sistemi giuridici degli Stati membri contemplano varie disposizioni in merito all'estensione del periodo durante il quale possono essere avviate iniziative nell'ambito del diritto contrattuale. Tali periodi sono talvolta utilizzati per stabilire il termine massimo di memorizzazione in caso di contestazione di una fattura o di richiesta di pagamento. Tali disposizioni devono tuttavia essere applicate in conformità al principio per cui il trattamento dei dati personali deve essere limitato a quanto è strettamente necessario per conseguire i fini per i quali i dati sono stati rilevati e successivamente trattati. Nella grande maggioranza dei casi una fattura è pagata entro i termini prescritti.

A parere del gruppo, l'applicazione del principio di proporzionalità e il fatto che, conformemente all'articolo 6, paragrafo 2, della direttiva 97/66/CE (e dell'articolo 6, paragrafo 2, della direttiva 2002/58/CE), i dati relativi al traffico possono essere sottoposti a trattamento "sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento" dovrebbero normalmente essere intesi come segue:

I dati relativi al traffico dovrebbero essere conservati per il periodo necessario a consentire il pagamento delle fatture e la composizione delle controversie. Normalmente ciò implica un periodo di memorizzazione massimo di 3-6 mesi e non più lungo in quei casi in cui le fatture sono state pagate e non sembrano essere state oggetto di contestazione o di richieste di delucidazioni (tenuto conto del diritto alla tutela della vita privata dei singoli abbonati) [6].

In casi particolari di contestazioni o di richiesta di delucidazioni, i dati possono essere memorizzati per un periodo più lungo al fine di facilitare il pagamento della fattura. Anche dopo il pagamento di una fattura un periodo di memorizzazione più lungo potrebbe eventualmente essere giustificato in particolari casi eccezionali allorché esistano indicazioni concrete di una possibile contestazione o richiesta di delucidazioni. In ognuna di tali situazioni i periodi di memorizzazione dei dati devono essere valutati tenendo conto delle particolari circostanze di ogni singolo caso onde permettere la composizione delle controversie in corso. Il limite massimo di questi periodi più lunghi coincide con il termine di prescrizione stabilito nel diritto nazionale [7].

Il periodo di riferimento dovrebbe decorrere dal momento in cui i dati relativi al traffico non sono più necessari ai fini della trasmissione di una comunicazione, conformemente all'articolo 6 della diret-

(6) Si veda al riguardo in particolare la situazione in Grecia. In forza di una decisione del comitato nazionale greco per le poste e le telecomunicazioni (EETT) (cui ha fatto seguito una decisione positiva del garante della tutela dei dati greco), gli abbonati possono avvalersi della possibilità di chiedere al fornitore la cancellazione dei dati sul traffico che li riguardano a condizione di escludere ogni successiva contestazione del pagamento. In tal caso il fornitore è obbligato a cancellare i dati sul traffico indipendentemente dal periodo di tempo stabilito dalla legge.(7) In paesi quali l'Irlanda e il Regno Unito tale periodo è di sei anni.

tiva 97/66/CE (o della direttiva 2002/58/CE) [8]*. Il momento esatto del completamento della trasmissione di una comunicazione può dipendere dal tipo di servizio di comunicazione elettronica prestato* [9].

2.8. Il gruppo desidera mettere in evidenza che, come già affermato, conformemente all'articolo 6 della direttiva 95/46/CE e all'articolo 6, paragrafo 4, della direttiva 97/66/CE (e all'articolo 6, paragrafo 5, della direttiva 2002/58/CE), i dati relativi al traffico memorizzati devono limitarsi ai dati « necessari ». Possono essere sottoposti a trattamento soltanto i dati che sono adeguati, pertinenti e non eccedenti in relazione alle finalità di fatturazione e dei pagamenti di interconnessione (principio di proporzionalità dei dati sottoposti a trattamento). Ciò implica, tra l'altro, che se non si procede a fatturazione per taluni tipi di comunicazioni, i dati relativi al traffico non possono essere sottoposti a trattamento per le suddette finalità.

Il gruppo richiama l'attenzione sul fatto che la direttiva 2002/58/CE ha previsto un regime unificato per tutti i dati che rientrano nella definizione di "dati relativi al traffico" (cfr. articolo 2, lettera b), della direttiva). Conformemente al principio di proporzionalità dei dati sottoposti a trattamento di cui al precedente paragrafo, è responsabilità degli Stati membri e, a seconda delle circostanze, delle autorità nazionali di controllo nell'ambito delle proprie competenze, in sede di applicazione della direttiva 2002/58/CE, adottare le misure necessarie con riguardo alle diverse categorie di dati relativi al traffico. A questo proposito è opportuno prestare particolare attenzione per impedire la memorizzazione prolungata dei dati relativi al traffico non necessari ai fini della fatturazione o dei pagamenti di interconnessione. Specifica attenzione dovrebbe essere inoltre rivolta alle implicazioni dei sistemi di comunicazione interamente basati su tariffe forfettarie.

3. Trattamento dei dati personali a fini fiscali

Il gruppo è a conoscenza del fatto che, per giustificare periodi lunghi di memorizzazione dei dati, i responsabili del trattamento si appellano talvolta alle finalità di natura fiscale. Le finalità di natura fiscale sono effettivamente connesse alle finalità di fatturazione. Tuttavia, sebbene possa essere necessario per i responsabili del trattamento serbare per diversi anni a fini fiscali la prova dei pagamenti, compresi gli importi aggregati delle fatture, tale obbligo non dovrebbe essere esteso ai corrispondenti dati sul traffico su cui si basano le bollette telefoniche. Conformemente all'articolo 6 della direttiva 97/66/CE (e all'articolo 6 della direttiva 2002/58/CE), tale obbligo può giustificare soltanto il trattamento di importi aggregati di fatturazione, ma non il trattamento di dati relativi al traffico su cui sono basate le fatture relative alle comunicazioni.

4. Raccomandazione

4.1 Sono emerse indicazioni dell'esistenza di divergenze nella prassi seguita dalle società di comunicazioni elettroniche negli Stati membri riguardo ai periodi di memorizzazione dei dati relativi al traffico. Il Gruppo è del parere che qualsiasi prassi non conforme ai principi stabiliti ai paragrafi 2.7 e 2.8 di cui sopra e non chiaramente autorizzata da disposizioni legislative ai sensi dell'articolo 14 della direttiva 97/66/CE (e dell'articolo 15 della direttiva 2002/58/CE)[10] sia, prima facie, incompatibile con le disposizioni della normativa comunitaria in materia di tutela dei dati.

4.2 È quindi importante adottare misure per interpretare in maniera armonizzata il **periodo limitato** durante il quale i fornitori di servizi di telecomunicazioni sono autorizzati a trattare i dati

(8) La formulazione utilizzata nella direttiva 97/66/CE è stata modificata nella direttiva 2002/58/CE al fine di tener conto dei diversi tipi di servizi di comunicazione elettronica.

(9) Cfr. ventisettesimo considerando della direttiva 2002/58/CE.

(10) L'articolo 14 della direttiva 97/66/CE autorizza gli Stati membri ad adottare disposizioni legislative volte a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni della direttiva, incluso l'articolo 6 relativo ai dati sul traffico. Tuttavia tali restrizioni devono essere « necessarie » alla salvaguardia di uno degli interessi elencati (sicurezza dello Stato, difesa, pubblica sicurezza, prevenzione, ricerca, accertamento e perseguimento di reati, ovvero uso non autorizzato del sistema di telecomunicazione). [segue]

relativi al traffico a fini di fatturazione e di pagamenti di interconnessione. Conformemente al principio di cui al paragrafo 2.7, il gruppo ritiene che un'interpretazione ragionevole delle direttive in tema di tutela dei dati è quella secondo la quale un periodo di memorizzazione normale ai fini della fatturazione dura un massimo di 3-6 mesi, **fatta eccezione** per casi particolari di controversie in cui i dati possono essere sottoposti a trattamento per un periodo più lungo. Inoltre possono essere sottoposti a trattamento soltanto i dati relativi traffico che sono adeguati, pertinenti e non eccedenti ai fini della fatturazione e dei pagamenti di interconnessione. Gli altri dati relativi al traffico devono essere cancellati.

Fatto a Bruxelles, lì 29 gennaio 2003

Per il gruppo
Il Presidente
Stefano RODOTÀ

[segue] L'articolo 15 della direttiva 2002/58/CE non modifica tali disposizioni in maniera sostanziale. Esso precisa che le restrizioni devono essere « necessarie, opportune e proporzionate » « all'interno di una società democratica » e aggiunge anche che gli Stati membri possono, tra l'altro, adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati all'articolo 15, paragrafo1, e che le misure di cui a tale paragrafo devono essere conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.
Si veda al riguardo il parere 5/2002 del gruppo sulla dichiarazione dei Commissari europei per la protezione dei dati alla Conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni, in particolare laddove si afferma che la conservazione sistematica di tutti i tipi di dati di traffico per un periodo di un anno o più sarebbe chiaramente sproporzionata e quindi inaccettabile in una società democratica.

OCSE

129 Raccomandazione del Consiglio Ocse relativa alle linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza

(adottata dal Consiglio nel corso della sua 1037ma riunione, il 25 luglio 2002)

OCSE
Organizzazione per la cooperazione e lo sviluppo economico

C(2002)131/FINAL

RACCOMANDAZIONE DEL CONSIGLIO OCSE RELATIVA ALLE LINEE-GUIDA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DELLE RETI: VERSO UNA CULTURA DELLA SICUREZZA

IL CONSIGLIO

Vista la Convenzione sull'Organizzazione per la cooperazione e lo sviluppo economici del 14 dicembre 1960, ed in particolare gli articoli 1 b), 1 c), 3 a) e 5 b) della stessa,

Vista la Raccomandazione del Consiglio relativa alle Linee-guida sulla protezione della vita privata e sui flussi transfrontalieri di dati personali, del 23 settembre 1980 [C(80)58(Final)],

Vista la Dichiarazione sui flussi transfrontalieri di dati personali, adottata dai governi dei Paesi membri dell'OCSE l'11 aprile 1985 [Allegata a C(85)139],

Vista la Raccomandazione del Consiglio relativa alle Linee-guida per le politiche crittografiche, del 27 marzo 1997 [C(97)62/FINAL],

Vista la Dichiarazione ministeriale relativa alla tutela della privacy sulle reti globali, del 7-9 dicembre 1998 [Allegata a C(98)177/FINAL],

Vista la Dichiarazione ministeriale relativa all'autenticazione per il commercio elettronico, del 7-9 dicembre 1998 [Allegata a C(98)177/FINAL],

Riconoscendo che le reti ed i sistemi di informazione trovano impiego crescente, e rivestono sempre maggiore importanza, per quanto concerne governi, imprese, altri enti e singoli utenti,

Riconoscendo che il ruolo sempre più significativo dei sistemi informativi e delle reti e la loro crescente rilevanza ai fini della stabilità e dell'efficienza delle economie nazionali e del commercio internazionale nonché nella vita sociale, culturale e politica richiedono un impegno particolare al fine di tutelare e promuovere la fiducia nei loro confronti,

Riconoscendo che i sistemi informativi e le reti e la loro proliferazione a livello mondiale sono stati accompagnati da nuovi e crescenti rischi,

Riconoscendo che i dati e le informazioni conservati e trasmessi attraverso i sistemi informativi e le reti sono esposti a rischi legati a varie modalità di accesso e utilizzazione indebiti, alla loro sottrazione o

alterazione, alla trasmissione impropria di codici, ad attacchi tipo DoS [Denial of Service] o alla loro distruzione, e necessitano di opportune garanzie,

Riconoscendo la necessità di sensibilizzare rispetto ai rischi per i sistemi informativi e le reti ed alle politiche, prassi, misure e procedure disponibili per fare fronte a tali rischi, e di promuovere un comportamento corretto quale presupposto essenziale ai fini dello sviluppo di una cultura della sicurezza,

Riconoscendo l'esigenza di rivedere le politiche, prassi, misure e procedure correnti in modo da contribuire ad assicurarne l'adeguatezza rispetto alle sfide in continua evoluzione derivanti dalle minacce ai sistemi informativi ed alle reti,

Riconoscendo l'esistenza di un interesse comune a promuovere la sicurezza dei sistemi informativi e delle reti attraverso una cultura della sicurezza che favorisca il coordinamento e la cooperazione internazionali per fare fronte alle sfide derivanti dai danni che deficit di sicurezza possono causare alle economie nazionali, al commercio internazionale ed alla partecipazione alla vita sociale, culturale e politica,

Riconoscendo, inoltre, che le Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza definite nell'Allegato alla presente Raccomandazione hanno natura volontaria e non incidono sui diritti sovrani delle nazioni,

Riconoscendo che le presenti Linee-guida non intendono indicare l'esistenza di una soluzione univoca per garantire la sicurezza, né quali politiche, prassi, misure e procedure siano adeguate in rapporto a specifiche situazioni, bensì intendono fornire un quadro di principi finalizzati a promuovere una migliore comprensione del modo in cui le parti in causa possono trarre vantaggio dallo sviluppo di una cultura della sicurezza e, al contempo, contribuire a tale sviluppo,

RACCOMANDA le presenti Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza a governi, imprese, altri enti e singoli utenti che sviluppino, possiedano, forniscano, gestiscano, mantengano e utilizzino reti e sistemi di informazione,

RACCOMANDA agli Stati membri:

di definire nuove politiche, prassi, misure e procedure, ovvero di modificare quelle esistenti, in modo da riflettere e tenere conto delle Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza adottando e promuovendo una cultura della sicurezza secondo le indicazioni fornite nella Linee-guida,

di consultarsi, coordinarsi e collaborare a livello nazionale e internazionale al fine di dare attuazione alle Linee-guida,

di diffondere la conoscenza delle Linee-guida nei settori pubblico e privato, compresi governi, imprese, altri enti e singoli utenti, in modo da promuovere una cultura della sicurezza, e

di invitare tutte le parti interessate ad un comportamento responsabile e all'adozione delle misure necessarie per dare attuazione alle Linee-guida secondo modalità consone ai rispettivi ruoli,

di mettere le Linee-guida a disposizione degli Stati che non sono membri OCSE, tempestivamente e nei modi opportuni,

di rivedere le Linee-guida ad intervalli quinquennali al fine di promuovere la cooperazione internazionale su temi attinenti alla sicurezza dei sistemi informativi e delle reti,

DA' MANDATO al Comitato OCSE per le politiche dell'informazione, dell'informatica e della comunicazione di promuovere l'attuazione delle Linee-guida.

La presente Raccomandazione sostituisce la Raccomandazione del Consiglio relativa alle Lineegui da per la sicurezza dei sistemi informativi del 26 novembre 1992 [C(92)188/FINAL].

ALLEGATO

LINEE-GUIDA PER LA SICUREZZA DEI SISTEMI INFORMATIVI E DELLE RETI VERSO UNA CULTURA DELLA SICUREZZA PREFAZIONE

1. L'impiego di sistemi informativi e di reti e l'intero settore delle tecnologie dell'informazione sono considerevolmente diversi rispetto al 1992, quando l'OCSE pubblicò le Linee-guida per la sicurezza dei sistemi informativi. Questa continua evoluzione comporta significativi benefici, ma richiede anche un'attenzione alla sicurezza molto più consistente da parte di governi, imprese, altri enti e singoli utenti che sviluppino, possiedano, forniscano, gestiscano, mantengano e utilizzino sistemi informativi e reti ("parti in causa").

2. Personal computer sempre più potenti, la convergenza di tecnologie diverse e l'impiego diffuso di Internet hanno fatto scomparire i sistemi isolati e più modesti, situati all'interno di reti prevalentemente chiuse. Oggi l'interconnessione di tutte le parti in causa è sempre più accentuata, e le connessioni travalicano i confini nazionali. Inoltre, Internet supporta infrastrutture critiche come energia, trasporti e finanze e svolge un ruolo essenziale nell'attività delle imprese, nella fornitura di servizi a cittadini e imprese da parte dei governi, e nelle comunicazioni e nello scambio di informazioni fra i singoli cittadini. Anche la natura e la tipologia delle tecnologie che formano l'infrastruttura comunicativa e informativa si sono modificate significativamente. Numero e natura dei dispositivi per l'accesso a tale infrastruttura si sono moltiplicati fino a comprendere dispositivi fissi, wireless e mobili, e l'accesso avviene in misura crescente attraverso connessioni "sempre attive". Pertanto, sono aumentati in misura sostanziale la natura, il volume e la delicatezza delle informazioni trasmesse.

3. A seguito della crescente interconnettività, i sistemi informativi e le reti sono esposti attualmente a minacce e rischi sempre più numerosi e di più varia tipologia. Tutto ciò solleva nuove problematiche di sicurezza. Per tali motivi, le presenti Linee-guida sono rivolte a tutte le parti in causa nella nuova società dell'informazione, e indicano l'esigenza di una maggiore consapevolezza e comprensione delle problematiche attinenti la sicurezza oltre che la necessità di sviluppare una "cultura della sicurezza".

I. VERSO UNA CULTURA DELLA SICUREZZA

4. Le presenti Linee-guida intendono fornire una risposta alla continua evoluzione del settore della sicurezza promuovendo lo sviluppo di una cultura della sicurezza – ossia, un'attenzione particolare alla sicurezza nello sviluppo di sistemi informativi e reti e l'adozione di nuovi approcci mentali e comportamentali nell'utilizzazione di sistemi informativi e reti e nelle interazioni che avvengono al loro interno. Le Linee-guida segnano una netta soluzione di continuità con l'epoca in cui la progettazione e l'utilizzazione di reti e sistemi secondo criteri di sicurezza rappresentavano troppo di frequente una valutazione a posteriori. Cresce di continuo la dipendenza delle parti in causa da sistemi informativi e reti e dai relativi servizi, che devono essere affidabili e sicuri. Solo un approccio che tenga nel debito conto gli interessi di tutte le parti in causa e la natura dei sistemi, delle reti e dei relativi servizi, può garantire un'efficace sicurezza.

5. Ciascuna parte in causa rappresenta un soggetto importante ai fini della sicurezza. Le parti in causa, ciascuna secondo il rispettivo ruolo, dovrebbero essere consapevoli dei rischi per la sicurezza che le riguardano e delle corrispondenti misure preventive, assumersi proprie responsabilità ed agire al fine di potenziare la sicurezza di sistemi informativi e reti.

6. Per promuovere una cultura della sicurezza saranno necessarie una visione ispiratrice e un'ampia partecipazione, con l'obiettivo di conferire maggiore priorità alla pianificazione e gestione della sicurezza, nonché la comprensione diffusa fra tutte le parti in causa della necessità di garantire la sicurezza. Le questioni attinenti la sicurezza dovrebbero essere oggetto di attenzione responsabile a tutti i livelli governativi e imprenditoriali ad opera di tutte le parti in causa. Le presenti Linee-guida costituiscono le fondamenta di un'attività mirante a diffondere una cultura della sicurezza in tutti settori sociali. In tal modo le parti in causa potranno inserire la sicurezza come parte integrante della progettazione e utiliz-

zazione di tutti i sistemi informativi e tutte le reti. Con le presenti Linee-guida si propone a tutte le parti in causa di adottare e promuovere una cultura della sicurezza nel considerare, valutare e intervenire sul funzionamento di sistemi informativi e reti.

II. OBIETTIVI

7. Le presenti Linee-guida intendono

- promuovere una cultura della sicurezza fra tutte le parti in causa come strumento per tutelare i sistemi informativi e le reti,
- sensibilizzare rispetto ai rischi per i sistemi informativi e le reti, alle politiche, prassi, misure e procedure disponibili per affrontare tali rischi, e all'esigenza che esse siano adottate e messe in pratica,
- stimolare la fiducia fra tutte le parti in causa rispetto ai sistemi informativi ed alle reti ed alle modalità della loro fornitura e utilizzazione,
- creare un quadro generale di riferimento che aiuti le parti in causa a comprendere le tematiche della sicurezza ed a rispettare valori etici nello sviluppo e nell'applicazione di politiche, prassi, misure e procedure coerenti per la sicurezza di sistemi informativi e reti,
- promuovere fra tutte le parti in causa la cooperazione e lo scambio di informazioni, nei modi opportuni, rispetto allo sviluppo e all'attuazione di politiche, prassi, misure e procedure di sicurezza,
- promuovere l'inserimento delle tematiche di sicurezza fra gli obiettivi importanti per tutte le parti in causa che siano impegnate nella definizione o nell'attuazione di standard.

III. PRINCIPI

8. I nove principi indicati di seguito sono complementari e dovrebbero essere letti come un insieme unitario. Essi riguardano le parti in causa a tutti i livelli, fra cui il livello politico e quello operativo. Secondo le presenti Linee-guida, la responsabilità delle parti in causa varia in rapporto al ruolo rispettivamente svolto. Per tutte le parti in causa saranno utili la conoscenza, l'educazione, lo scambio di informazioni e la formazione in quanto seguite dall'adozione di migliori prassi e da una migliore comprensione delle tematiche di sicurezza. L'impegno mirante a potenziare la sicurezza di sistemi informativi e reti dovrebbe essere coerente con i valori di una società democratica, in particolare con l'esigenza della libera circolazione delle informazioni, e con l'attenzione fondamentale alla privacy dell'individuo.

1) Sensibilizzazione

Le parti in causa dovrebbero essere consapevoli dell'esigenza di garantire la sicurezza di sistemi informativi e reti e delle misure alle quali ricorrere per potenziare la sicurezza. La sensibilizzazione rispetto ai rischi ed alle tutele disponibili costituisce la prima linea di difesa per la sicurezza di sistemi informativi e reti. I sistemi informativi e le reti possono essere soggetti a rischi sia esterni sia interni. Le parti in causa dovrebbero comprendere che deficit di sicurezza possono danneggiare in misura significativa reti e sistemi soggetti al loro controllo. Dovrebbero inoltre essere consapevoli dei pregiudizi potenzialmente arrecabili a terzi per effetto dell'interconnettività e dell'interdipendenza. Le parti in causa dovrebbero essere a conoscenza della configurazione e degli aggiornamenti disponibili in rapporto al proprio sistema, della collocazione di quest'ultimo nelle reti, delle buone prassi da esse applicabili per potenziare la sicurezza, e delle esigenze di altre parti in causa.

2) Responsabilità

Tutte le parti in causa sono responsabili della sicurezza di sistemi informativi e reti Tutte le parti in causa fanno riferimento a sistemi informativi e reti interconnessi a livello locale e globale, e dovrebbero essere consapevoli delle rispettive responsabilità per quanto concerne la sicurezza di tali reti e sistemi. Dovrebbero risponderne ciascuna nei modi opportuni in rapporto alla funzione rispettivamente svolta. Le parti in causa dovrebbero riesaminare periodicamente le proprie politiche, prassi, misure e procedure valutando se siano adeguate al rispettivo contesto. I soggetti responsabili dello sviluppo, della progettazione e della fornitura di prodotti e servizi dovrebbero prendere in considerazione le tematiche della sicurezza di reti e sistemi e diffondere tempestivamente le informazioni opportune – ivi compresi eventuali aggiornamenti – in modo che gli utenti possano più facilmente comprendere le funzioni di sicu-

rezza dei prodotti e servizi in questione e le rispettive responsabilità in termini di sicurezza.

3) Reazione

Le parti in causa dovrebbero agire tempestivamente ed in modo cooperativo per prevenire, individuare e rispondere a problemi di sicurezza In ragione dell'interconnettività dei sistemi informativi e delle reti e dei rischi potenziali di danni rapidi e diffusi, le parti in causa dovrebbero agire tempestivamente ed in modo cooperativo per affrontare problemi di sicurezza. Dovrebbero scambiarsi informazioni su rischi e vulnerabilità, nei modi opportuni, e mettere in atto procedure finalizzate ad una rapida ed efficace collaborazione in modo da prevenire, individuare e rispondere a problemi di sicurezza. Quando ammissibile, ciò può comportare uno scambio di informazioni e attività di cooperazione transfrontalieri.

4) Etica

Le parti in causa dovrebbero rispettare i legittimi interessi di terzi. In considerazione della pervasività dei sistemi informativi e delle reti nelle nostre società, le parti in causa devono comprendere che le loro azioni o omissioni possono danneggiare soggetti terzi. Pertanto, è fondamentale adottare comportamenti eticamente corretti, e le parti in causa dovrebbero mirare alla definizione e all'adozione di prassi esemplari e promuovere comportamenti che tengano conto delle esigenze di sicurezza e rispettino i legittimi interessi di terzi.

5) Democrazia

La sicurezza dei sistemi informativi e delle reti dovrebbe essere compatibile con valori fondamentali di una società democratica La sicurezza dovrebbe essere garantita in modi compatibili con i valori riconosciuti dalle società democratiche e, in particolare, con la libertà di manifestazione del pensiero, la libera circolazione delle informazioni, la riservatezza delle informazioni e delle comunicazioni, la protezione adeguata dei dati personali, l'apertura e la trasparenza.

6) Analisi dei rischi

Le parti in causa dovrebbero effettuare un'analisi dei rischi L'analisi dei rischi permette di evidenziare rischi e vulnerabilità e dovrebbe essere sufficientemente ampia da tenere conto di fattori fondamentali sia interni sia esterni, come le componenti tecnologiche, i fattori fisici e umani, le politiche ed i servizi gestiti da terzi che abbiano implicazioni in termini di sicurezza. L'analisi dei rischi permetterà di definire la soglia accettabile di rischio e faciliterà l'individuazione di controlli adeguati per gestire il rischio di danni potenziali ai sistemi informativi ed alle reti, tenendo conto della natura e dell'importanza delle informazioni da tutelare. A causa della crescente interconnettività dei sistemi informativi, l'analisi dei rischi dovrebbe prendere in considerazione i pregiudizi potenzialmente derivanti da terzi o arrecabili a terzi.

7) Progettare e realizzare in un'ottica di sicurezza

Le parti in causa dovrebbero fare della sicurezza una componente fondamentale di sistemi informativi e reti. E' necessario progettare, realizzare e coordinare in modo corretto sistemi, reti e politiche al fine di ottimizzare la sicurezza. Un fattore importante, ma non esclusivo, in tale contesto è rappresentato dalla progettazione e dall'adozione di garanzie e soluzioni adeguate in modo da evitare o limitare il pregiudizio potenzialmente derivante dai rischi e dalle vulnerabilità già individuate. Occorrono garanzie e soluzioni di natura tecnica e non tecnica, che devono essere proporzionate al valore delle informazioni presenti sui sistemi e sulle reti del singolo organismo. La sicurezza dovrebbe rappresentare una componente fondamentale di tutti i prodotti, i sistemi, i servizi e le reti, nonché costituire parte integrante della progettazione e dell'architettura di sistema. Per quanto riguarda gli utenti finali, progettare e realizzare in un'ottica di sicurezza significa soprattutto individuare e configurare prodotti e servizi per i rispettivi sistemi.

8) Gestione della sicurezza

Le parti in causa dovrebbero adottare un approccio globale alla gestione della sicurezza La gestione della sicurezza dovrebbe basarsi sulla valutazione dei rischi ed essere di tipo dinamico, abbracciando le attività delle parti in causa a tutti i livelli e tutti gli aspetti delle rispettive operazioni. Dovrebbe prevedere una risposta lungimirante rispetto ai rischi emergenti e comprendere la prevenzione, l'individuazione e la reazione a possibili incidenti, il ripristino dei sistemi, la manutenzione permanente, attività di

verifica e di controllo indipendente. Le politiche di sicurezza relative a sistemi informativi e reti, nonché le prassi, misure e procedure connesse, dovrebbero essere coordinate e integrate in modo da creare un sistema di sicurezza coerente. Le esigenze gestionali dipendono dal livello di partecipazione, dal ruolo del singolo soggetto parte in causa, dai rischi associati e dai requisiti di sistema.

9) Riesame

Le parti in causa dovrebbero sottoporre a riesame e ad una nuova valutazione la sicurezza di sistemi informativi e reti, e modificare nei modi opportuni politiche, prassi, misure e procedure di sicurezza Rischi e vulnerabilità sempre nuovi e mutevoli vengono incessantemente alla luce. Le parti in causa dovrebbero costantemente riesaminare, rivedere e modificare tutti gli aspetti di sicurezza per fare fronte all'evolversi delle situazioni di rischio.

Consiglio dell'Unione europea

130 Risoluzione del Consiglio dell'Unione europea del 18 febbraio 2003 su un approccio europeo per una cultura della sicurezza delle reti e dell'informazione (2003/C 48/01)(*)

IL CONSIGLIO DELL'UNIONE EUROPEA,

RICORDANDO

1. la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni, sulla sicurezza delle reti e sicurezza dell'informazione: Proposta di un approccio strategico europeo;

2. la risoluzione del Consiglio del 30 maggio 2001 concernente un "Piano d'azione eEurope: sicurezza dell'informazione e delle reti";

3. la risoluzione del Consiglio del 28 gennaio 2002 relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione (1);

4. il Piano d'azione eEurope 2005 confermato dal Consiglio europeo di Siviglia del giugno 2002;

5. il parere del Parlamento europeo circa la comunicazione della Commissione europea sulla sicurezza dell'informazione e delle reti: proposta di un approccio strategico europeo;

SOTTOLINEA PERTANTO CHE:

1. con lo sviluppo dei servizi della società dell'informazione, la sicurezza delle reti e delle informazioni assume sempre maggiore importanza per la vita quotidiana dei cittadini, così come per gli operatori economici e le amministrazioni pubbliche, contribuendo al corretto funzionamento del mercato interno;
2. gli Stati membri e le Istituzioni europee devono sviluppare ulteriormente una strategia europea globale per la sicurezza delle reti e delle informazioni e adoperarsi per conseguire una "cultura della sicurezza" tenendo conto dell'importanza della cooperazione internazionale;
3. gli orientamenti dell'OCSE per la sicurezza dei sistemi e delle reti di informazione sono considerati un modello valido per lo sviluppo delle politiche che perseguono una cultura della sicurezza, nel rispetto dei valori democratici e dell'importanza della protezione dei dati personali;
4. occorre rispettare il diritto alla vita privata. I cittadini e le imprese devono poter confidare che l'informazione è trattata con accuratezza, riservatezza e affidabilità;
5. nello sviluppare una cultura della sicurezza, uno dei compiti fondamentali sarà la precisazione della responsabilità della sicurezza delle reti e dei sistemi di informazione per tutti gli interessati;
6. all'Europa occorre garantire l'elaborazione e lo sviluppo dell'appropriata qualificazione nel settore della sicurezza delle reti e delle informazioni;
7. occorrono maggiori trasparenza, scambio di informazioni e cooperazione tra gli Stati membri, le Istituzioni europee e il settore privato;
8. l'elaborazione di una politica coerente in materia di sicurezza a livello europeo richiede trasparenza e cooperazione interpilastri;
9. devono essere proseguiti i lavori in corso per adempiere l'impegno preso nella risoluzione del

(*) G.U.C.E. n. C 48/2, del 28.2.2003
(1) GU C 43 del 16.2.2002, pag. 2.

Consiglio del 28 gennaio 2002 sull'approccio comune e le azioni specifiche nel settore delle reti e della sicurezza dell'informazione.

INVITA PERTANTO GLI STATI MEMBRI A:

1. promuovere la sicurezza quale componente essenziale del governo pubblico e privato, in particolare incoraggiando l'assegnazione delle responsabilità;
2. prevedere un'appropriata istruzione e formazione professionale, nonché l'aumento della consapevolezza, in particolare tra i giovani, nei confronti dei problemi della sicurezza;
3. adottare provvedimenti adeguati per impedire e reagire agli incidenti in materia di sicurezza, soprattutto tramite:

a) il costante miglioramento del processo di identificazione e di valutazione dei problemi di sicurezza e l'applicazione di controlli adeguati;

b) la creazione di mezzi efficaci per comunicare la necessità di agire a tutti gli interessati mediante il rafforzamento del dialogo a livelli sia europeo che nazionale e, ove opportuno, internazionale in particolare con i fornitori di tecnologia e servizi della società dell'informazione;

c) la presa in considerazione di un adeguato scambio di informazioni rispondente all'esigenza della società di essere tenuta al corrente delle buone prassi connesse alla sicurezza.

4. incoraggiare la cooperazione e il partenariato tra le università e le imprese in modo da fornire servizi e tecnologie sicure e favorire lo sviluppo di norme riconosciute.

ACCOGLIE CON FAVORE L'INTENZIONE DELLA COMMISSIONE DI:

1. applicare il metodo aperto di coordinamento per quanto riguarda le attuali azioni degli Stati membri e valutare il relativo impatto sulla sicurezza;

2. istituire un gruppo interdisciplinare provvisorio in stretta collaborazione con gli Stati membri e composto di loro rappresentanti, incaricato dei lavori preparatori in vista della creazione di una "Cyber-Security Task Force", come previsto dalla risoluzione del Consiglio del 28 gennaio 2002;

3. avviare uno studio come base della prevista relazione sulle applicazioni dei sistemi di autenticazione biometrica;

4. sviluppare ulteriormente, in collaborazione con gli Stati membri, un dialogo con l'industria del settore per migliorare la sicurezza nell'elaborazione dei prodotti hardware e software e garantire la disponibilità dei servizi e dei dati;

5. istituire la "Cyber-Security Task Force" di cui sopra.

INVITA:

1. l'industria del settore a far sì che la gestione dei rischi in materia di sicurezza sia integrata nel pensiero manageriale e nell'ingegneria economica;

2. tutti gli utenti ad avere una visione olistica dei rischi associati ai sistemi di informazione e valutare le minacce conseguenti ad eventi materiali, carenze umane, nonché a vulnerabilità tecnologiche e ad aggressioni deliberate.

3. l'industria e tutti gli utenti a dialogare coi governi per sviluppare una cultura della sicurezza.