ghe, anche nel 2005, individuando soggetti tenuti all'adempimento anche mediante interconnessione con altre banche dati.

Videosorveglianza

Particolare attenzione è stata data ai controlli dei trattamenti effettuati mediante sistemi di videosorveglianza soprattutto nelle aree pubbliche (porti, aeroporti, metropolitane, enti pubblici). Le ispezioni effettuate hanno evidenziato, in linea di massima, un progressivo recepimento delle indicazioni del Garante (da prima con il *Provv.* 29 novembre 2000 e, da ultimo, con il *Provv.* 29 aprile 2004).

Non sono tuttavia mancati casi di inosservanza di tali indicazioni, come quello rilevato in un'ispezione presso un ente locale nel corso della quale si è rilevata l'esistenza di un complesso sistema di videosorveglianza –non adeguatamente segnalato agli interessati– collocato presso un obitorio e dotato anche di telecamere nascoste, in grado di riprendere immagini anche all'interno delle camere mortuarie. Le modalità del trattamento dei dati raccolti mediante il sofisticato sistema, la cui istallazione era stata a suo tempo motivata dal verificarsi di alcuni episodi di vilipendio nei confronti di cadaveri, sono apparse immediatamente in contrasto con i principi previsti dall'art. 11 del Codice. Su invito dell'Autorità, l'ente interessato dall'accertamento ha provveduto a sospendere il trattamento, in attesa delle determinazioni sulla complessiva liceità dello stesso.

Sempre in materia di controlli sui trattamenti effettuati mediante sistemi di videosorveglianza, sono state contestate sanzioni amministrative per la mancanza di idonee informative da parte di un'agenzia fiscale, delle società di gestione delle metropolitane di Roma e Milano e della società di gestione dell'aeroporto della Costa Smeralda.

20.4. *Alcuni riferimenti statistici*

L'attività ispettiva effettuata nel 2004 ha avuto anche quest'anno un significativo incremento rispetto a quella svolta l'anno precedente (+45%).

In generale, il volume delle attività ispettive ha continuato a crescere ogni anno a partire dal 2001, rispondendo ad una maggiore "domanda" di controllo da parte dei cittadini come dei soggetti (pubblici e privati) chiamati a dare effettiva attuazione alla disciplina di protezione dati.

Nel 2004 le attività ispettive sono state avviate sulla base di:

- accertamenti d'ufficio (43%);
- accertamenti conseguenti a segnalazioni pervenute all'Ufficio (38%);
- autonomi accertamenti a seguito di ricorsi presentati al Garante (19%).

Come si evince dal confronto con i dati dell'anno precedente, nel 2004 è stato maggiore lo spazio degli accertamenti così detti di iniziativa, avviati cioè *motu proprio* dall'Autorità, pure in assenza di atti di impulso da parte dei cittadini, a testimonianza di un atteggiamento attivo assunto dal Garante, anche attraverso lo strumento ispettivo.

Gli accertamenti eseguiti hanno riguardato in prevalenza verifiche concernenti:

- le modalità di acquisizione del consenso, in molti casi connesse ad attività effettuate sulla rete Internet mediante l'invio di sollecitazioni commerciali non richieste via *e-mail*;
- il rispetto delle disposizioni di legge in relazione al trattamento di dati mediante sistemi di videosorveglianza;
- l'accertamento dell'origine dei dati oggetto di trattamento;
- il rispetto dell'obbligo di notificazione al Garante;
- l'adozione delle misure di sicurezza.

Le ispezioni sono state effettuate:

- in novantatre casi mediante richieste di informazioni *in loco*;
- in sette casi mediante accessi a banche dati autorizzati dal Presidente del Tribunale.

Con riferimento all'ambito territoriale la ripartizione è stata omogenea:

- Nord (trentaquattro);
- Centro (trenta);
- Sud (trentasei).

L'incidenza delle violazioni penali sui procedimenti amministrativi di controllo avviati nel 2004 è pari circa al 13%. Le violazioni segnalate riguardano ipotesi di trattamento illecito di dati personali, omessa adozione di misure di sicurezza, inosservanza dei provvedimenti del Garante e false dichiarazioni al Garante.

Valutazioni di sintesi

Confermando le indicazioni emerse l'anno precedente, le ispezioni hanno in generale consentito di rilevare che nel settore privato le aziende più grandi iniziano ad adottare la legge anche attraverso la costituzione di unità organizzative con deleghe specifiche, veri e propri "uffici *privacy*", mentre le aziende medio-piccole evidenziano a volte un livello inferiore di adeguamento alla normativa e agli indirizzi del Garante. Non sempre, però, c'è perfetta corrispondenza tra osservanza formale delle disposizioni e reale e diffusa "cultura" del trattamento di dati secondo i principi stabiliti dal Codice.

Proprio nella pubblica amministrazione, come dimostrano i casi precedentemente descritti, la cultura della protezione dei dati personali stenta ad affermarsi compiutamente. Nei processi di lavoro e nella gestione delle pratiche di ufficio prevalgono ancora approcci di tipo "burocratico" e, talvolta, ad un assetto formalmente corretto non corrisponde una piena consapevolezza dei doveri e delle responsabilità connesse al trattamento dei dati personali. Sono ancora frequenti fenomeni di noncuranza e superficialità nel trattamento dei dati, soprattutto per quanto attiene la gestione degli archivi e le connesse misure di sicurezza e l'attuazione dei principi di indispensabilità, necessità, pertinenza e non eccedenza cui si è più volte fatto cenno.

20.5. *L'attività sanzionatoria del Garante*

L'attività operativa in materia di sanzioni amministrative, alla luce delle modifiche normative delle quali si è già dato conto (v. *Relazione 2003*), ha avuto ulteriore impulso a seguito delle attività di accertamento e di controllo poste in essere dal "Nucleo speciale funzione pubblica e *privacy*" della Guardia di finanza le cui unità di vigilanza, all'esito di capillari controlli svolti presso le sedi dei titolari del trattamento, hanno provveduto in decine di casi ad effettuare direttamente l'obbligatoria contestazione al momento in cui sono state rilevate le specifiche violazioni amministrative.

La linea d'azione scelta dal Garante per gli ambiti di indagine è stata quella di individuare specifici settori verso cui indirizzare le attività sopra indicate, le quali hanno coinvolto, in qualità di titolari, soggetti pubblici e privati. A ciò va aggiunta l'attività di accertamento e controllo svolta d'ufficio ovvero a seguito di segnalazioni e reclami indirizzati al Garante per lamentare un improprio utilizzo dei dati personali, che ha portato in alcuni casi alla contestazione di violazioni amministrative.

Attraverso un'analisi dettagliata dei provvedimenti sanzionatori si possono rinvenire ed individuare le operazioni di trattamento e le modalità che sono state più volte oggetto di contestazione di infrazione. Tra queste, la più significativa ha riguardato l'obbligo di notifica dei trattamenti al Garante (art. 37 del Codice), con parti-

colare riferimento agli adempimenti in materia di notificazione da parte dei titolari di trattamenti di dati sensibili (quali aziende sanitarie pubbliche e laboratori di analisi privati) e, in un caso, del trattamento di dati biometrici da parte di un istituto di credito (rilevazione di impronte digitali).

In tema di omessa o ritardata notificazione, i soggetti pubblici e privati sottoposti agli accertamenti sopra richiamati sono risultati inadempienti e pertanto oggetto di contestazione della violazione amministrativa della omessa o incompleta notificazione (art. 163 del Codice). A seguito di tali contestazioni i titolari del trattamento, in maggioranza, si sono avvalsi della facoltà di essere sentiti dal Garante (ai sensi dell'art. 18, l. n. 689/1981), in ciò confermando la previsione in materia di obbligatoria audizione formulata nella precedente *Relazione* annuale.

Nelle audizioni tenute nel 2004, è emersa in vari casi una lettura non corretta e non conforme al dettato normativo dell'art. 37, comma 1, lett. *a*) e *b*), del Codice, che ha generato nei titolari del trattamento l'erronea convinzione di non essere tenuti all'obbligo di notificazione.

In particolare, è risultata evidente una visione non sistematica delle norme sulla protezione dei dati personali, oltre che una loro non corretta interpretazione. Eppure il Garante era intervenuto sul tema nel corso del 2004 specie in due occasioni: con *Deliberazione* n. 1 del 31 marzo 2004 e con un provvedimento indirizzato ad alcune associazioni di categoria che hanno fornito le indicazioni e la corretta interpretazione del disposto dell'articolo citato. Ed è a quanto riportato in detti provvedimenti che avrebbero potuto agevolmente attenersi le organizzazioni sopra menzionate al fine del corretto adempimento dell'obbligo di notificazione al Garante.

L'attività di monitoraggio interno, prodromica ad ogni trattamento di dati personali che voglia essere conforme alle disposizioni di legge in materia, non sempre viene svolta con l'intento di verificare in modo puntuale e compiuto la natura, le modalità e le finalità del trattamento. Al contrario, si rileva spesso una tendenza a ricercare quanto necessario a far ritenere escluso un determinato adempimento. È di tutta evidenza che un tale atteggiamento comporta, per il titolare, il rischio di effettuare un trattamento non conforme alle norme di legge vigenti e di essere pertanto oggetto di provvedimento sanzionatorio da parte del Garante.

Sempre con riferimento alle risultanze di dette attività di accertamento e controllo, verranno predisposti, ai sensi dell'art. 17 della legge n. 689/1981, i rapporti necessari all'eventuale e successiva adozione dei provvedimenti di ordinanza-ingiunzione al pagamento di somme.

L'informativa all'interessato, ad esempio nelle attività effettuate per mezzo dei nuovi strumenti multimediali di comunicazione, è stata spesso omessa o è risultata incompleta al momento del raffronto con le finalità e modalità di fatto esercitate dal titolare. Significativo, in proposito, è il caso nel quale, a seguito del ricorso di un interessato, si è accertato che i dati raccolti da un'università al momento dell'iscrizione venivano utilizzati anche per attività ulteriori rispetto a quelle per le quali era stata fornita l'informativa (nel caso di specie, comunicati a terzi che li utilizzavano per inviare comunicazioni commerciali non sollecitate).

Per quanto attiene ai trattamenti di dati personali effettuati per mezzo di strumenti di videosorveglianza, sono state nuovamente accertate e sanzionate violazioni connesse ad informative assenti o incomplete riguardo agli obbligatori riferimenti alle modalità e finalità del trattamento effettuato.

Si sono verificati infine casi di mancato riscontro alle richieste di informazioni ed esibizione di documenti rivolte dal Garante ai titolari del trattamento (art. 157 del Codice) –richieste necessarie per l'assolvimento delle funzioni di controllo rimesse all'Autorità– che hanno portato alla contestazione della relativa infrazione.

21 Relazioni istituzionali

21.1. *L'Autorità e le attività di sindacato ispettivo e di indirizzo del Parlamento*

In relazione agli aspetti di specifico interesse in materia di protezione dei dati personali, l'Autorità ha seguito con attenzione l'attività di sindacato ispettivo e di indirizzo esercitata dal Parlamento, e ha fornito al Governo, ove richiesto, i chiarimenti e le indicazioni necessarie.

Sono stati inoltrati al Governo elementi in merito ad alcuni atti, fra i quali in particolare:

a) alcune interrogazioni relative all'acquisizione da parte delle autorità doganali degli Stati Uniti dei dati dei passeggeri conservati nella banche dati dell'Alitalia, presentate dall'on. Folena (3-02017), dall'on. Delmastro Delle Vedove (4-05923) e dall'on. Pagliarulo (4-04379) (*Note* 14 aprile 2004, 28 aprile 2004 e 8 ottobre 2004). In tali occasioni l'Autorità, richiamando i pareri adottati dal Gruppo dei Garanti europei, ha ricordato che la richiesta formulata dalle autorità statunitensi di accedere ai dati registrati nel *Pnr* (*Passenger name record*) deve essere valutata alla stregua delle disposizioni comunitarie in materia e in particolare dell'art. 25 della direttiva 95/46/CE (v. più diffusamente par. 22.6);
b) un'interrogazione dell'on. Delmastro Delle Vedove (3-02307) relativa al progetto USA denominato T.I.A. (*Terrorism information awareness*) (*Nota* 28 aprile 2004);
c) due mozioni della maggioranza (1-00304 Leone ed altri) e dell'opposizione parlamentare (1-00215 Folena ed altri), di contenuto analogo ed approvate all'unanimità dal Parlamento il 14 gennaio 2004, su alcune questioni in materia di protezione dei dati personali, fra le quali, in particolare, la necessità di una più efficace tutela della riservatezza in Internet;
d) un'interrogazione dell'on. Delmastro Delle Vedove (4-04007) relativa alla mancata adozione da parte dei soggetti pubblici dei regolamenti sui dati sensibili (*Nota* 3 maggio 2004).

21.2. *L'attività consultiva del Garante sugli atti del Governo*

L'art. 154, comma 4, del Codice prevede che il Presidente del Consiglio dei ministri e ciascun ministro devono consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi che incidono sulla protezione di dati personali, al fine di prevenire delicati problemi applicativi, nell'interesse pubblico e dei cittadini, in un quadro di proficua collaborazione istituzionale che diversi ministeri hanno riconosciuto più volte.

L'Autorità ha espresso diversi pareri, fra i quali quelli riguardanti:

a) il decreto del Ministro della giustizia 14 gennaio 2005 con il quale sono inseriti nell'allegato A del Codice in materia di protezione dei dati personali, il codice di deontologia e buona condotta per i trattamenti di dati

effettuati per scopi statistici e scientifici e il codice deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo e affidabilità e puntualità nei pagamenti;

b) due schemi di convenzione fra i Ministeri della giustizia e dell'interno, da un lato, e l'Isvap, dall'altro, per la consultazione della banca dati sui sinistri per finalità di lotta alle frodi assicurative (*Pareri* 11 novembre 2004);

c) lo schema di regolamento per l'organizzazione ed il funzionamento dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (*Parere* 28 settembre 2004). Il Garante ha chiesto che il Ministero delle comunicazioni e il predetto Istituto, nell'esecuzione dei compiti loro assegnati dal Codice delle comunicazioni, rispettino i principi previsti dalla disciplina anche attuativa sulla protezione dei dati, in particolare per quanto riguarda il trattamento delle informazioni contenute negli elenchi degli abbonati ai servizi telefonici;

d) lo schema di decreto del Ministro del lavoro e delle politiche sociali di concerto con il Ministro per l'innovazione e le tecnologie in materia di *"Borsa continua nazionale del lavoro"*, adottato ai sensi del d.lg. 10 settembre 2003, n. 276 di attuazione della legge 14 febbraio 2003, n. 30 (cd. legge Biagi) (*Parere* 3 settembre 2004). Il decreto è stato recentemente pubblicato in *Gazzetta Ufficiale* (decreto 13 ottobre 2004 in *G.U.* 8 ottobre 2004, n. 262) recependo, in parte, le indicazioni fornite dal Garante (come più ampiamente riferito nel par. 11.1). Non è stata recepita, invece, la richiesta dell'Autorità di espungere dai dati identificativi del lavoratore e del datore di lavoro il codice fiscale, in applicazione del principio di pertinenza e non eccedenza dei dati trattati rispetto alle finalità della Borsa;

e) lo schema di decreto ministeriale recante regole tecnico-operative per l'uso di strumenti telematici nel processo civile (cd. Processo telematico) previsto dall'art. 3, comma 3, del d.P.R. n. 123/2001 (*Parere* 23 luglio 2004, in ordine al quale, per i profili di merito, si fa rinvio al par. 2.11).

Nei primi mesi del 2004 l'Autorità ha adottato anche altri pareri, già menzionati nella *Relazione 2003*, riguardanti:

f) lo schema di decreto concernente l'individuazione dei dati da inserire nell'anagrafe nazionale degli studenti e dei laureati (*Parere* 7 aprile 2004);

g) due schemi di regolamento in attuazione della legge n. 189 del 2002 concernenti, l'uno, il riordino del regolamento di attuazione del testo unico in materia di immigrazione e condizione dello straniero (d.P.R. n. 394/1999) e, l'altro, la razionalizzazione e l'interconnessione delle comunicazioni fra amministrazioni pubbliche in materia di immigrazione, in particolare ai fini del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (*Parere* 4 marzo 2004). Quest'ultimo è stato poi adottato con il d.P.R. 27 luglio 2004, n. 242 (in *G.U.* 18 settembre 2004, n. 220) recependo, in parte, le indicazioni fornite dal Garante;

h) lo schema di decreto interministeriale (Ministri per l'innovazione e le tecnologie e dell'interno) che disciplina il permesso di soggiorno elettronico. Dopo un primo parere del 15 ottobre 2003, a seguito di incontri tecnici fra rappresentanti dell'Autorità e del Ministero dell'interno, l'Autorità ha adottato un secondo parere il 4 marzo 2004 con il quale ha indicato, fra l'altro, gli interventi necessari per garantire gli interessati in occasione della raccolta delle impronte digitali e, in particolare, nel caso di inserimento di dati biometrici nel documento elettronico. Il decreto è stato poi

adottato il 3 agosto 2004, recependo sostanzialmente le indicazioni fornite dal Garante e pubblicato nella *Gazzetta Ufficiale* del 6 ottobre 2004, n. 235. L'Autorità ha confermato la propria disponibilità a proseguire attivamente gli incontri per approfondire i problemi e i rischi derivanti dalle differenti tecniche di identificazione e di autenticazione individuate dai Garanti europei nel parere del 1° agosto 2003 sui dati biometrici. Tali approfondimenti appaiono necessari anche allo scopo di individuare idonee cautele nella fase di attivazione del documento elettronico e di consegna dei documenti o di accesso selezionato ai dati, nonché le più elevate misure di garanzie di sicurezza disponibili. L'esito di tali approfondimenti potrebbe essere poi trasfuso nelle misure e negli accorgimenti che in materia di dati biometrici devono essere prescritti dal Garante ai sensi dell'art. 55 del Codice;

i) lo schema di decreto del Presidente della Repubblica recante il regolamento di disciplina dell'accesso al servizio di informatica giuridica del Centro elettronico di documentazione (Ced) della Corte di cassazione (*Parere* 27 febbraio 2004);

l) lo schema di regolamento (Ministri per la funzione pubblica e dell'interno) di gestione dell'Indice nazionale delle anagrafi (Ina), in attuazione dell'art. 2-*quater* del decreto-legge 27 dicembre 2000, n. 392, convertito dalla legge n. 26/2001 (*Parere* 13 febbraio 2004);

m) lo schema di decreto dirigenziale del Ministero della giustizia, di attuazione in via parziale e transitoria dell'art. 39 del d.P.R. 14 novembre 2002, n. 313 (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), concernente la consultazione del casellario giudiziale da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi (*Parere* 29 gennaio 2004). Come già riportato nella *Relazione* 2003, in occasione degli incontri di lavoro che hanno preceduto la redazione dello schema di decreto, l'Autorità aveva constatato il carattere transitorio della soluzione elaborata, in attesa di una regolamentazione definitiva della procedura di accesso diretto ai sensi dell'art. 39 del d.P.R. n. 313/2002. Nel parere del 29 gennaio 2004 è stata sottolineata la necessità che l'accesso ai dati giudiziari registrati nel casellario giudiziale, nonché il successivo utilizzo da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi, siano consentiti nel rispetto dei limiti previsti dallo stesso d.P.R. n. 313/2002 e in misura proporzionata alle finalità da perseguire.

Nel 2004 si è tuttavia registrato un incremento dei casi di mancata consultazione dell'Autorità, persino su tematiche fondamentali nel rapporto tra Stato e cittadini che implicano il trattamento di dati sensibili o comunque particolarmente delicati, come ad esempio nel caso dei decreti attuativi del sistema di monitoraggio della spesa sanitaria e di introduzione della tessera sanitaria.

Pertanto l'Autorità ha inviato al Governo un elenco dei principali regolamenti ed atti amministrativi in relazione ai quali, negli ultimi anni, non è stato richiesto il parere al Garante ai sensi dell'art. 31, comma 2, della legge n. 675/1996 e poi dell'art. 154, comma 4, del Codice, segnalando che la mancata consultazione integra una violazione di legge e del diritto comunitario, che espone peraltro i dati personali trattati in applicazione di tali atti alla conseguenza dell'inutilizzabilità (art. 11, comma 2, del Codice).

Di seguito si riportano i casi più significativi:

a) d.P.R. 6 ottobre 2004, n. 258 "Regolamento concernente le funzioni dell'Alto Commissario per la prevenzione e il contrasto della corruzione e delle altre forme di illecito nella pubblica amministrazione" (*G.U.* 22 ottobre 2004, n. 249);
b) d.P.R. 16 settembre 2004, n. 303, recante "Regolamento relativo alle procedure per il riconoscimento dello *status* di rifugiato" (*G.U.* 22 dicembre 2004, n. 299);
c) d.P.R. 23 aprile 2004, n. 108, "Regolamento recante disciplina per l'istituzione, l'organizzazione ed il funzionamento del ruolo dei dirigenti presso le amministrazioni dello Stato, anche ad ordinamento autonomo" (*G.U.* 29 aprile 2004, n. 100);
d) decreto del Ministro dell'economia e delle finanze di concerto con il Ministro della salute 30 giugno 2004, recante "Applicazione delle disposizioni di cui al comma 6 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente l'avvio del sistema di monitoraggio della spesa nel settore sanitario" (*G.U.* 2 luglio 2004, n. 153);
e) decreto del Ministro della salute 15 luglio 2004 recante "Istituzione, presso l'Agenzia italiana del farmaco, di una banca dati centrale finalizzata a monitorare le confezioni dei medicinali all'interno del sistema distributivo" (*G.U.* 4 gennaio 2005, n. 2);
f) decreto del Ministro dell'istruzione, dell'università e della ricerca 1° luglio 2004, recante "Progetto "PC alle famiglie", di cui all'art. 4, comma 10, della legge 24 dicembre 2003, n. 350" (*G.U.* 9 agosto 2004, n. 185);
g) decreto (Ministero dell'economia e delle finanze, Ministero della salute e Presidenza del Consiglio dei ministri - Ministro per l'innovazione e le tecnologie) 11 marzo 2004, recante "Applicazione delle disposizioni di cui al comma 1 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione delle caratteristiche tecniche della Tessera sanitaria (TS)" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);
h) decreto (Ministeri dell'economia e delle finanze e della salute) 18 maggio 2004, recante "Applicazione delle disposizioni di cui al comma 2 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione dei modelli di ricettari medici standardizzati e di ricetta medica a lettura ottica" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);
i) decreto (Ministero dell'economia e delle finanze) 24 giugno 2004 recante "Applicazione delle disposizioni di cui al comma 4 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione delle modalità di trasmissione telematica al Ministero dell'economia e delle finanze dei dati riguardanti l'assegnazione dei ricettari ai medici prescrittori" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);
l) decreto (Ministero dell'economia e delle finanze) 24 giugno 2004, recante "Applicazione delle disposizioni contenute nel disciplinare tecnico di cui al comma 5 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, recante disposizioni urgenti per favorire lo sviluppo per la correzione dell'andamento dei conti pubblici, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326" (*G.U.* 13 luglio 2004, n. 162, S.O. n. 123);
m) decreto (Ministero dell'economia e delle finanze) 28 giugno 2004,

recante "Applicazione delle disposizioni di cui al comma 9 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione dei dati che le regioni, nonché i Ministeri e gli enti pubblici di rilevanza nazionale che li detengono, trasmettono al Ministero dell'economia e delle finanze, con modalità telematica" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);

n) decreto del Capo del dipartimento dell'amministrazione generale, del personale e dei servizi del tesoro del Ministero dell'economia e delle finanze 12 febbraio 2004, recante "Criteri organizzativi per l'assegnazione delle domande agli organismi di accertamento sanitario di cui all'art. 9 del d.P.R. n. 461/2001, ed approvazione dei modelli di verbale utilizzati, anche per le trasmissioni in via telematica, con le specificazioni sulle tipologie di accertamenti sanitari eseguiti e sulle modalità di svolgimento dei lavori (*G.U.* 23 febbraio 2004, n. 44);

o) provvedimento dell'Agenzia delle entrate 18 febbraio 2004 recante approvazione del nuovo modello di dichiarazione per l'integrazione degli imponibili ai sensi degli articoli 8, 9, 9-*bis* e 14 della legge 27 dicembre 2002, n. 289, termini per la trasmissione e approvazione delle specifiche tecniche per la trasmissione telematica dei dati contenuti nella dichiarazione (*G.U.* 15 marzo 2004, n. 62, S.O. n. 44);

p) provvedimento dell'Agenzia delle dogane 28 febbraio 2004, recante la realizzazione di una banca dati multimediale, ai sensi dell'art. 4, commi 54 e 55, della legge 24 dicembre 2003, n. 350 (*G.U.* 10 marzo 2004, n. 58);

q) ordinanza del Ministro della salute 25 febbraio 2004 "Misure urgenti in materia di cellule staminali da cordone ombelicale" (*G.U.* 18 marzo 2004, n. 65).

21.3. *Altra collaborazione con la Presidenza del Consiglio dei ministri*

Si è già fatto cenno all'attività di monitoraggio effettuata dall'Autorità sulle leggi regionali (cfr. par. 1.4.). Sotto diverso profilo, si intende qui rendere conto dei risultati dell'attività consultiva sollecitata dalla Presidenza del Consiglio dei ministri sul contenuto di alcune leggi regionali, per gli aspetti di competenza del Garante, al fine di segnalare questioni eventualmente rilevanti in sede di conflitto di attribuzioni tra Stato e Regioni.

Se in alcune ipotesi non si sono ravvisati profili di illegittimità costituzionale, in altre si sono rilevati aspetti problematici.

È questo il caso della legge della Regione Emilia-Romagna 25 maggio 2004, n. 11, che prevede l'utilizzo integrato delle basi di dati esistenti attraverso la collaborazione con le altre pubbliche amministrazioni e la possibilità di accesso e di cessione dei dati a privati e ad enti pubblici economici.

Come già accennato, il Garante ha preliminarmente rilevato che il diritto alla protezione dei dati personali, ascrivibile tra i diritti inviolabili riconosciuti dall'art. 2 della Costituzione, è materia di competenza esclusiva dello Stato poiché concerne l'"ordinamento civile" dello Stato e la "determinazione dei livelli essenziali delle prestazioni relative ai diritti civili e sociali" (art. 117, comma 2, lett. *l*) e *m*), della Costituzione).

In relazione ai contenuti della legge regionale, l'Autorità ha poi osservato che l'interconnessione generalizzata di archivi, gli indiscriminati flussi di dati, nonché la correlata possibilità, prevista con l'approvazione di un successivo regolamento, di

rendere disponibile anche a terzi (privati ed enti pubblici economici) il patrimonio informativo, non è coerente con la normativa vigente che stabilisce la predisposizione di garanzie poste con norme di legge statale riconoscendo ai cittadini, ad esempio, il diritto di essere previamente informati sulle ulteriori finalità perseguite nell'uso dei dati a seguito delle interconnessioni che la nuova banca dati produrrebbe (*Nota* 28 giugno 2004).

Tali rilievi sono stati fatti propri dal Consiglio dei ministri nell'impugnazione della legge davanti alla Corte Costituzionale.

In sede di esame della legge istitutiva del sistema integrato di interventi e servizi sociali, approvata dalla Regione Calabria (n. 23 del 9 dicembre 2003), l'Autorità ha evidenziato che l'istituzione di tale sistema implica necessariamente un'attività di trattamento di dati personali degli assistiti –anche di natura sensibile–, che deve essere effettuata nel pieno rispetto delle disposizioni dettate dal Codice. Tra l'altro, è stato osservato che il sistema coinvolge diversi soggetti erogatori delle prestazioni sociali, rendendo quindi necessaria l'individuazione di coloro che possono qualificarsi come titolari o contitolari del trattamento. I titolari, oltre a rispettare i principi di pertinenza e non eccedenza, devono prevedere che il sistema sia configurato in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 del Codice). È stata inoltre avanzata qualche perplessità sull'istituzione di un registro degli ospiti presenti nelle strutture accreditate e di un registro degli utenti dei servizi offerti, dovendo al riguardo essere individuate con maggiore esattezza le finalità perseguite attraverso l'istituzione di detti registri e le tipologie di dati personali ivi contenute (*Nota* del 26 gennaio 2004).

In relazione alla legge della Regione Toscana 15 dicembre 2004, n. 63, recante "*Norme contro le discriminazioni determinate dall'orientamento sessuale o dall'identità di genere*" ed in particolare all'art. 7 che disciplina le modalità di prestazione del consenso informato, l'Autorità ha evidenziato che la materia è compiutamente disciplinata dal Codice, il quale, in attuazione della normativa internazionale e comunitaria, stabilisce particolari garanzie –specie ove si tratti, come nel caso in esame, di dati sensibili idonei a rivelare lo stato di salute delle persone– e disposizioni sulle modalità di acquisizione del consenso, anche nei casi di incapacità legale, naturale o temporanea (art. 20, 22, 76 e 82 ss. del Codice). Nel caso in cui la legge regionale faccia riferimento anche o solo al consenso al trattamento medico, anche se tale profilo non riguarda direttamente aspetti di competenza del Garante, sussisterebbero ugualmente profili di illegittimità costituzionale della norma, trattandosi in questo caso di diritti civili e sociali della persona. La contiguità del consenso al trattamento dei dati personali con quello relativo al trattamento sanitario è ben evidenziata, ad esempio, in un contesto normativo analogo a quello in esame, dal cd. "decreto Di Bella" che impone la contestuale acquisizione dei due consensi (art. 5-*bis*, comma 1, d.l. n. 23/1998, convertito dalla l. n. 94/1998, come modificato dall'art. 178 del Codice).

Gli stessi rilievi sono stati mossi dall'Autorità in riferimento all'articolo 8 della legge regionale, in quanto alcuni aspetti della dichiarazione di volontà che il regolamento regionale ivi previsto dovrebbe disciplinare trovano anch'essi compiuta regolamentazione nel Codice, in particolare per quanto riguarda l'individuazione di garanzie a tutela della riservatezza dei pazienti (art. 78 del Codice). La costituzione di una banca dati delle dichiarazioni di volontà viola poi il principio di proporzionalità nel trattamento dei dati personali, non apparendo giustificata la raccolta delle

informazioni in un unico archivio centrale; mancano inoltre indicazioni circa le tipologie dei dati da registrare nella banca di dati e le relative finalità della raccolta, in contrasto con i principi di necessità, indispensabilità, pertinenza e non eccedenza dei dati, in base ai quali i sistemi informativi devono essere configurati riducendo al minimo l'utilizzazione di dati personali e possono essere richiesti all'interessato i soli dati pertinenti rispetto alle finalità perseguite (artt. 3, 11 e 22 del Codice) (*Nota* 11 gennaio 2005).

L'Autorità è stata inoltre consultata dalla Regione Toscana per ciò che concerne il trattamento dei dati personali ai fini dello svolgimento delle elezioni regionali primarie del 20 febbaio 2005, inizialmente disciplinate dalla sola legge regionale 17 dicembre 2004, n. 70, recante *"Norme per la selezione dei candidati e delle candidate alle elezioni per il Consiglio regionale e alla carica di Presidente della Giunta regionale"*, che presentava profili di criticità in relazione alla protezione dei dati personali.

21.4. *Attività di cooperazione con altre istituzioni*

Anche nell'anno 2004 si è registrata un'intensa attività di cooperazione dell'Autorità con altre istituzioni su tematiche comuni.

Autorità per le garanzie nelle comunicazioni

Con l'Autorità per le garanzie nelle comunicazioni, oltre che per l'adozione del provvedimento relativo ai nuovi elenchi telefonici di cui si tratta in un apposito paragrafo, è proseguita, ai sensi dell'art. 154, comma 3, del Codice, la consueta e proficua collaborazione su vari temi come ad esempio quello relativo all'attivazione di contratti e servizi di telefonia fissa senza il preventivo consenso degli interessati.

Si è in tal modo proceduto ad esaminare in concreto il problema confrontando le segnalazioni pervenute, ciascuna per la relativa sfera di competenza. All'esito di tale scambio di informazioni il Garante ha ritenuto opportuno dar corso ad ulteriori interventi utilizzando i poteri conferiti dall'art. 157 del Codice.

Ministero delle comunicazioni

Una fattiva attività di cooperazione è stata intrapresa anche con il Ministero delle comunicazioni. In particolare, il Garante ha partecipato a numerosi incontri presso il Ministero nei quali sono stati affrontati importanti temi di interesse comune quali l'utilizzo della posta elettronica o di *Sms* telefonici per l'invio non preventivamente autorizzato di materiale pubblicitario (fenomeno comunemente noto come *spamming*) e l'illecita intestazione di utenze telefoniche mobili illecitamente operate all'insaputa degli interessati.

Per fronteggiare con uno sforzo comune il grave fenomeno della irregolare intestazione e successiva commercializzazione di carte prepagate di telefonia mobile, l'Autorità partecipa attivamente al gruppo di lavoro cui sono presenti il Ministero delle comunicazioni, l'Autorità per le garanzie nelle comunicazioni, l'Autorità garante della concorrenza e del mercato, il Ministero della giustizia e il Ministero dell'interno.

Dipartimento della protezione civile

Il Garante ha contribuito alla predisposizione di una convenzione ai sensi dell'art. 6, comma 1, della legge 24 febbraio 1992, n. 225, tra il Dipartimento della protezione civile e gli operatori di servizi di comunicazione mobile. Tale convenzione, stipulata il 28 settembre 2004, ha ad oggetto la costituzione del "Circuito nazionale dell'informazione d'emergenza" (Cnie), ossia di un sistema promosso dall'Autorità per le garanzie nelle comunicazioni, d'intesa con il Ministero delle comunicazioni e con il Dipartimento della protezione civile volto a realizzare la trasmissione di *Sms* informativi di pubblica utilità per il Dipartimento della protezione

civile, nei casi di necessità e urgenza provocati da calamità naturali e d'altra natura.

Gli operatori telefonici, in tali situazioni di emergenza, invieranno ai loro clienti messaggi *Sms* secondo le indicazioni del Dipartimento della protezione civile in relazione al contenuto del messaggio, alla tempistica, all'area geografica interessata alla diffusione. Basandosi solo su provvedimenti d'emergenza adottati ai sensi dell'art. 5, commi 1, 2 e 5, della legge n. 225/1992 (che devono indicare espressamente l'eventuale deroga a specifiche disposizioni del Codice sulla protezione dei dati personali e le relative motivazioni), l'invio può prescindere da uno specifico consenso prestato dalla clientela. Resta ferma la possibilità per gli interessati di esercitare il diritto di non ricevere messaggi.

Vi sono numerosi aspetti della convenzione che attengono, quindi, al trattamento dei dati personali. Particolare interesse riveste per l'Autorità l'individuazione dei soggetti destinatari dei messaggi *Sms*, che verrà effettuata non solo in base ai dati anagrafici degli stessi, ma anche mediante localizzazione geografica dei terminali. Il Garante, pertanto, al termine dell'attività di cooperazione svolta anche ai sensi dell'art. 154, comma 3, del Codice, ha indicato le integrazioni da inserire nella convenzione e nel relativo allegato tecnico, tenendo anche conto delle indicazioni già fornite in tema di messaggi di pubblica utilità in due diversi provvedimenti (12 marzo 2003 e 7 luglio 2004) richiamati espressamente in premessa dalla convenzione.

Nel dicembre 2004 l'Autorità è stata chiamata a prendere parte al Gruppo di lavoro interministeriale per l'istituzione del numero unico europeo per le emergenze, costituito con d.P.C.M. del 4 agosto 2003. Il Gruppo ha il compito di analizzare i problemi posti dall'attivazione sul territorio nazionale del predetto numero unico, volto a garantire agli interessati adeguata risposta alle chiamate ai servizi di emergenza. Ciò in conformità con quanto previsto in attuazione della normativa comunitaria (cfr. direttive 2002/21/CE e 2002/22/CE) e dall'art. 76 del Codice delle comunicazioni elettroniche (d.lg. n. 259/2003).

Il Garante dovrà tra l'altro valutare la conformità al Codice sulla protezione dei dati personali del sistema che consentirà di identificare la localizzazione del chiamante e di acquisirne i dati personali all'atto della ricezione della chiamata di emergenza.

21.5. *Collaborazione con la Guardia di finanza*

Nello svolgimento dell'attività ispettiva il Garante può avvalersi della collaborazione di altri organi dello Stato; 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 di tipo amministrativo proprie del Corpo.

La collaborazione nel settore delle attività ispettive è stata regolata con un protocollo d'intesa che prevede che la Guardia di finanza operi 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.

Al fine di rafforzare ulteriormente il rapporto di collaborazione, nel mese di giugno 2004 la Guardia di finanza ha costituito, come si è già detto, il "Nucleo spe-

ciale funzione pubblica e *privacy*" il cui personale, altamente specializzato, procede direttamente all'esecuzione delle attività ispettive avvalendosi, se necessario, dei reparti territoriali del Corpo.

Una delle prime attività affidate al Nucleo è stata la verifica del rispetto dell'obbligo di notificazione al Garante, in concomitanza con la scadenza del termine previsto dal Codice (30 aprile 2004), mediante accertamenti nei confronti di un primo gruppo di trenta soggetti pubblici e privati, tra cui dodici aziende sanitarie locali e dodici società di lavoro interinale, che ha portato alla contestazione di numerose sanzioni amministrative (v. specifico approfondimento in par. 20.3).

In generale il Nucleo ha svolto per l'Autorità un ruolo di valido supporto, oltre che per l'esecuzione di attività ispettive delegate, anche per la notifica di atti urgenti e per l'acquisizione di informazioni necessarie ad individuare con certezza i titolari o i responsabili del trattamento nei cui confronti dovevano essere avviati dei procedimenti.

In alcuni casi ci si è avvalsi della componente territoriale del Corpo per verificare, anche attraverso sopralluoghi, l'ottemperanza ai provvedimenti dell'Autorità adottati a seguito di ricorsi (ad esempio, riposizionamento di impianti di videosorveglianza, apposizione di informative *ex* art. 13 del Codice, avvenuta designazione di incaricati del trattamento).

La competenza acquisita dal Nucleo in virtù del rapporto di collaborazione ha fatto assumere allo stesso un ruolo di punto di riferimento cui delegare, da parte dell'autorità giudiziaria, anche attività di indagine per le violazioni al Codice costituenti reato.

Rispetto a queste attività il Garante, su esplicita richiesta dell'Autorità giudiziaria procedente, ha fornito un supporto in termini di approfondimenti sull'applicazione della legge.

22 Relazioni internazionali

22.1. *Lo stato di recepimento delle direttive comunitarie negli Stati membri dell'Unione europea*

Il 2004 è stato l'anno dell'"allargamento" dell'Unione europea con l'ingresso di dieci nuovi Stati (Cipro, Estonia, Lettonia, Lituania, Malta, Polonia, Repubblica Ceca, Slovenia, Slovacchia, Ungheria).

Nei nuovi Stati membri, le disposizioni delle direttive europee in materia di protezione dei dati (95/46/CE) e comunicazioni elettroniche e vita privata (2002/58/CE) trovano applicazione integrale a partire dalla data di adesione all'Unione europea, ossia dal 1° maggio 2004.

Guardando più in dettaglio alla situazione esistente al 31 dicembre 2004 nei venticinque Paesi dell'Ue, il quadro relativo al recepimento nella legislazione nazionale rende opportune alcune precisazioni.

Direttiva 95/46/CE

Tutti i quindici Paesi dell'Unione europea avevano recepito la direttiva prima del 1° maggio 2004 (v. *Relazione* 2003), anche se la Francia aveva notificato la legislazione adottata nel 1978, perdurando l'*iter* parlamentare (iniziato nel 2001) per l'adozione della normativa specifica. La nuova legge francese "*Informatique et libertés*", di recepimento della direttiva 95/46/CE, è stata adottata il 6 agosto 2004 ed è entrata in vigore il giorno successivo. Rispetto alla precedente legge, il nuovo testo aumenta i poteri sanzionatori dell'autorità di protezione dati (la *Commission Nationale Informatique et Libertés*, Cnil); elimina l'obbligo di notificazione alla Cnil per i titolari che designano (su base facoltativa) un "referente per la protezione dei dati" (il cosiddetto "*correspondant à la protection des données*") incaricato di vigilare sull'applicazione della normativa da parte del titolare e di monitorare la liceità e le modalità dei trattamenti di dati personali effettuati da quest'ultimo (ai sensi dell'art. 18(2) della direttiva); infine, dispone l'obbligo di sottoporre a valutazione preliminare da parte della Cnil qualsiasi trattamento che comporti il ricorso a tecniche biometriche. La legge inasprisce anche le sanzioni previste in caso di inadempimento. Il nuovo quadro normativo sarà completato attraverso l'adozione di atti di legislazione secondaria che preciseranno le procedure di valutazione preliminare ed altri aspetti concernenti, ad esempio, i requisiti da soddisfare per svolgere la funzione di "referente per la protezione dei dati".

La valutazione della qualità del recepimento per i quindici Paesi membri è in corso da parte della Commissione, secondo il programma di lavoro fissato nel Primo rapporto sull'applicazione della direttiva.

I nuovi Stati membri sono tutti provvisti di una legge nazionale in materia di protezione dei dati, che in alcuni casi è stata adottata *ex novo*, mentre in altri ha subito vari emendamenti dopo l'adozione della direttiva 95/46/CE, in particolare al fine di istituire un'autorità per la protezione dei dati incaricata di vigilare sull'applicazione delle disposizioni in materia a livello nazionale. Va sottolineato, in proposito, che dal 2001 alcuni dei nuovi Stati membri (Estonia, Lettonia, Lituania, Polonia, Repubblica Ceca, Repubblica Slovacca e Ungheria) hanno stabilito forme più strette di collaborazione e scambio di informazioni, anche attraverso un appo-

sito sito *web* (*www.ceecprivacy.org*) e l'organizzazione di due conferenze semestrali per discutere di tematiche di interesse comune.

La Commissione sta valutando l'effettiva conformità con l'*acquis* comunitario delle disposizioni nazionali.

Direttiva 2002/58/CE

La situazione relativa al recepimento della direttiva sulla vita privata e le comunicazioni elettroniche è più articolata. Nella *Relazione* 2003 si è fatto cenno alle iniziative preliminari adottate dalla Commissione europea nei confronti di alcuni Stati, per omessa comunicazione delle misure nazionali di trasposizione, ovvero per l'incompleta trasposizione della direttiva (con particolare riguardo all'art. 13, relativo alle comunicazioni indesiderate).

Dopo il parere motivato emesso il 1° aprile 2004 nei confronti di Belgio, Finlandia, Francia, Germania, Grecia, Lussemburgo e Paesi Bassi, e dopo l'adesione dei nuovi Stati membri, alla fine del mese di giugno 2004 la Commissione ha deciso di adire la Corte di giustizia nei confronti di tre Paesi (Belgio, Grecia, Lussemburgo) come previsto dal Trattato Ue per la mancata adozione della legislazione primaria di recepimento. Gli altri Paesi (Finlandia, Francia, Germania e Paesi Bassi) hanno provveduto nel frattempo a notificare le misure nazionali adottate. Tuttavia, la Commissione ha segnalato anche ad altri Paesi l'imperfetta trasposizione delle norme della direttiva 2002/58/CE. Ciò riguarda, in particolare:

- il recepimento delle disposizioni dell'art. 13, che vieta le comunicazioni indesiderate (quindi anche lo *spam*) in assenza del consenso preventivo dell'abbonato *(opt-in)*. Repubblica Ceca, Estonia, Grecia e Lussemburgo non hanno notificato le misure nazionali adottate;
- il recepimento degli articoli 5, 6 e 9 che riguardano, rispettivamente, i dati di traffico e di ubicazione e le relative modalità di trattamento e conservazione. Belgio, Repubblica Ceca, Estonia, Grecia e Lussemburgo non hanno notificato alla Commissione le misure adottate in materia.

Anche riguardo alla direttiva 2002/58/CE, la Commissione sta valutando la piena conformità della legislazione nazionale in vigore nei Paesi dell'Unione europea.

22.2. *Le iniziative a livello europeo per una migliore applicazione delle direttive comunitarie*

Recepimento della direttiva 95/46/CE

Come segnalato nella *Relazione* 2003, sia il Primo Rapporto della Commissione europea sullo stato di attuazione della direttiva 95/46/CE (pubblicato il 15 maggio 2003), sia i risultati dell'Eurobarometro pubblicati nel febbraio 2004 hanno dipinto un quadro caratterizzato da luci e alcune ombre per quanto riguarda l'effettiva trasposizione dei principi comunitari e la percezione dell'efficacia di tali principi da parte di imprese e cittadini europei.

In particolare, nel rapporto della Commissione viene delineato un programma di lavoro in dieci punti per giungere ad una migliore applicazione della direttiva tra i Paesi dell'Unione. Su molti di essi la Commissione ha previsto e richiesto iniziative comuni da parte delle autorità di protezione dei dati, le quali hanno quindi deciso di integrare le azioni richieste anche nel loro programma di lavoro a partire dal 2004.

Del resto, le stesse autorità avevano da tempo indicato fra le priorità del proprio mandato il potenziamento dell'attuazione delle norme in materia di protezione dei dati attraverso numerose strategie. Queste ultime sono state sistematizzate in un documento che il Gruppo dei Garanti europei istituito dall'art. 29 della direttiva 95/46/CE (di seguito, semplicemente, "Gruppo art. 29") ha adottato nel set-

tembre 2004 allo scopo di indicare alcune linee comuni di attività.

Per quanto concerne, in particolare, il potenziamento dell'attuazione dei principi comunitari in materia di protezione dei dati, le autorità garanti hanno messo l'accento soprattutto:

- sulle strategie per migliorare il rispetto e l'applicazione pratica delle normative nazionali in materia, attraverso l'elaborazione di approcci comuni comprendenti anche indagini ed accertamenti ispettivi "sincronizzati" in rapporto ad alcuni settori che risultano essere particolarmente problematici nella maggioranza dei venticinque Paesi Ue (si veda, in proposito, la "*Declaration on Enforcement*" approvata dal Gruppo il 25 novembre 2004);
- sulla semplificazione degli adempimenti connessi alla notificazione dei trattamenti, attraverso una *task force* incaricata di individuare gli spazi di armonizzazione (soprattutto in tema di deroghe all'obbligo di notificazione) e di elaborare un possibile modello di notificazione "unica" per i soggetti stabiliti in più Stati membri dell'Unione europea. Sulla base delle risposte pervenute ad uno specifico questionario, la *task force* ha inoltre operato una ricognizione delle disposizioni e prassi vigenti in ciascun paese riguardo all'obbligo di notificazione dei trattamenti di dati personali; ha curato altresì la predisposizione di un *vademecum* che sarà tra breve messo a disposizione di tutti i soggetti interessati (principalmente le società private che intendono operare in più di un Paese dell'Unione) mediante la pubblicazione sul sito *web* della Commissione specificamente dedicato alla protezione dei dati ed all'attività del Gruppo art. 29 (*http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm;*
- sull'armonizzazione delle previsioni in materia di informativa, in particolare attraverso l'elaborazione di un modello redatto in termini chiaramente comprensibili ed utilizzabili da tutti i titolari di trattamento, secondo un approccio "multilivello". Il Gruppo, anche sulla scorta della risoluzione adottata in materia dalla Conferenza internazionale tenutasi a Sydney nel 2003 (v. *Relazione* 2003, p. 116) e del dibattito svolto a Wroclaw, durante la Conferenza internazionale del 2004 (v. *infra*), ha elaborato un parere, pubblicato il 25 novembre 2004, che individua le caratteristiche di tale "informativa-modello".

Le decisioni assunte dal Gruppo, volte a favorire ed incrementare le forme di cooperazione al fine di pervenire a soluzioni interpretative uniformi, sono in linea di continuità rispetto a scelte compiute da diversi anni. La collaborazione internazionale fra le autorità di protezione dei dati (compreso il Garante), prevista anche dalla Convenzione n. 108 del Consiglio d'Europa, è operativa da molto tempo ed ha sistemi di scambi di informazioni sia a livello bilaterale, sia a livello multilaterale.

Oltre agli ambiti istituzionalizzati attraverso la creazione del Gruppo art. 29 ed alle Conferenze delle autorità di protezione dei dati, si segnalano brevemente alcuni significativi esempi di tale collaborazione, rimandando ai paragrafi successivi per maggiori dettagli sull'attività svolta:

- la trattazione di segnalazioni e ricorsi che hanno carattere transnazionale e lo scambio di informazioni e buone prassi sono oggetto dei seminari organizzati fin dal 2000 con cadenza semestrale nel quadro della cosiddetta "*Complaints Handling Network*", che garantisce inoltre un supporto costante alla gestione della relativa casistica;
- le questioni attinenti al settore delle telecomunicazioni sono oggetto dell'analisi condotta dall'*International Working Group on Data Protection in Telecommunications*, che si riunisce con cadenza semestrale;

- la lotta allo *spam* è oggetto della specifica cooperazione prevista dalla rete istituita fra le autorità competenti in materia di *spam* (*Contact Network of Spam Authorities*, Cnsa), che ha iniziato la sua attività alla fine del 2003.

Direttiva 2002/58/CE

Gli aspetti della direttiva che presentano maggiori difficoltà nell'armonizzazione delle modalità applicative riguardano innanzi tutto la conservazione dei dati di traffico (art. 6) ed il principio del consenso preventivo per l'invio di comunicazioni non sollecitate (art. 13).

Sul primo aspetto, come già rammentato nella *Relazione* 2003, il Gruppo art. 29 è intervenuto per ricordare agli Stati la necessità del rispetto dei tempi e dei modi previsti dalla direttiva. Nel parere 1/2003 adottato il 29 gennaio 2003, i Garanti hanno precisato che i dati memorizzati ai fini della fatturazione e dei pagamenti di interconnessione possono essere conservati soltanto per un periodo di tempo limitato e non su base routinaria per lunghi periodi, come peraltro già indicato nella Raccomandazione n. 3/99 del Gruppo.

Il Gruppo art. 29, sulla scorta dell'applicazione del principio di proporzionalità e tenendo conto che, conformemente all'art. 6, par. 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"*, ha ritenuto che i dati dovrebbero essere conservati solo 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– nei 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).

Pertanto, considerato che 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, i Garanti hanno ritenuto che tali disposizioni debbano 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, considerato inoltre che, di regola, il pagamento dei servizi resi è effettuato entro i termini di conservazione.

Il secondo importante aspetto, cui si è già accennato, concerne l'applicazione uniforme del principio dell'*opt-in* per le comunicazioni commerciali.

La direttiva 2002/58/CE sulla vita privata e le comunicazioni elettroniche ha in particolare disciplinato, armonizzandole, le condizioni alle quali le comunicazioni elettroniche (ad esempio la posta elettronica, gli *Sms*, il fax, il telefono) possono essere utilizzate a fini di commercializzazione diretta.

A partire dalle legislazioni introdotte in alcuni Stati (tra cui l'Italia) che prevedevano in materia la necessità di un consenso esplicito dell'interessato, l'art. 13 della direttiva ha introdotto un regime generale basato sul consenso preventivo ai fini dell'invio di questo tipo di comunicazioni.

La novità e la complessità del principio hanno indotto sia le istituzioni comunitarie, sia il Gruppo art. 29 ad intervenire per evitare divergenze applicative nei diversi Stati membri.

L'urgenza di un tale intervento risiede nell'enorme recente sviluppo dell'invio di comunicazioni indesiderate (cd. *spam*) e la necessità di presentarsi nella lotta a questo fenomeno, che si manifesta ormai in tutto il mondo, con un quadro giuridico realmente armonizzato a livello europeo. Da qui i richiami del Consiglio ad una puntuale applicazione della direttiva, le linee d'azione disegnate dalla Commissione