Relazione 2004

L'attuazione del Codice nel quadro della Costituzione per l'Europa

www.garanteprivacy.it

Indice

I. STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Il quadro normativo

II. L'ATTIVITÀ SVOLTA DAL GARANTE

2. Trattamenti effettuati in ambito pubblico

3. Sanità

4. Dati genetici

5. Ricerca statistica e scientifica

Indice

Indice

Indice

III. L'UFFICIO DEL GARANTE

24. La gestione amministrativa dell'Ufficio

25. Dati statistici

DOCUMENTAZIONE

Provvedimenti normativi

Indice

Provvedimenti del Garante

Unione europea

Autorità di controllo comune dell'Europol

Autorità di controllo comune Schengen

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

Indice

Consiglio d'Europa

26ª Conferenza internazionale sulla protezione dei dati Wroclaw (Polonia) 13-16 settembre 2004

Elenco delle abbreviazioni

La presente Relazione è riferita al 2004 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 25 gennaio 2005, relative a sviluppi 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
par.	paragrafo
Provv.	provvedimento
Relazione	Relazione del Garante per la protezione dei dati personali
r.d.	regio decreto
reg.	regolamento
S.p.A.	società per azioni
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

Stato di attuazione del Codice in materia di protezione dei dati personali

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Il quadro normativo

1.1. *L'entrata in vigore del Codice*

L'entrata in vigore del "Codice in materia di protezione dei dati personali" (decreto legislativo 30 giugno 2003, n. 196, di seguito, semplicemente, "Codice"), avvenuta il 1° gennaio 2004, ha rappresentato una tappa fondamentale per la tutela dei diritti della persona e ha concluso il processo di recepimento delle direttive europee in materia (95/46/CE e 2002/58/CE). È stato così completato il complesso percorso di razionalizzazione della disciplina inizialmente introdotta con la legge 31 dicembre 1996, n. 675, riunendo in un unico testo una regolamentazione che si era, nel tempo, stratificata a seguito di numerosi interventi modificativi e integrativi.

In un quadro complessivo di rafforzate garanzie –con il riconoscimento del diritto alla protezione dei dati personali (art. 1 del Codice), in armonia con quanto ora previsto nel Trattato che ha adottato la Costituzione europea– la nuova disciplina ha provveduto a semplificare alcuni adempimenti e ad attribuire un ruolo significativo, anche in una prospettiva di deflazione legislativa, ai codici di deontologia e di buona condotta, soggetti alla preventiva verifica da parte del Garante.

1.2. *Le modifiche (già) apportate*

Devono comunque rilevarsi alcuni segnali che sembrano muoversi in controtendenza rispetto al progetto di "stabilizzare" le regole di protezione dei dati personali.

Già nel primo anno di vigenza del Codice, infatti, sono stati introdotti alcuni, seppur circoscritti, interventi modificativi in settori di rilievo, e segnatamente in relazione al regime dei dati relativi al traffico telefonico, nel contesto sanitario e con riferimento alle ripetute proroghe dei termini per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili da parte dei soggetti pubblici.

La conservazione dei dati di traffico

Importanza particolare assumono le modifiche legislative apportate all'art. 132 del Codice (prima della sua entrata in vigore) con riguardo alla materia, di rilevanza costituzionale, della conservazione dei dati relativi al traffico telefonico per finalità di accertamento e di repressione dei reati (decreto-legge 24 dicembre 2003, n. 354, come modificato dalla legge di conversione 26 febbraio 2004, n. 45). Questa tema-

tica si è riproposta anche nel contesto delle misure adottate per contrastare la diffusione telematica abusiva di materiale audiovisivo, nell'ambito del dibattito parlamentare relativo alla materia regolata nel decreto-legge 22 marzo 2004, n. 72 (convertito con legge 21 maggio 2004, n. 128).

Il profilo della conservazione dei dati di traffico telefonico e telematico è nuovamente riemerso, con tutte le criticità che lo caratterizzano, nel corso delle audizioni effettuate in sede d'esame del disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (AC 4599) (in merito si rinvia al par. 15.2).

Il trattamento di dati idonei a rivelare lo stato di salute in ambito sanitario

Alcune modifiche al Codice –a brevissima distanza di tempo dalla sua entrata in vigore– hanno riguardato altresì i trattamenti di dati personali effettuati in ambito sanitario. In merito a tali interventi il Garante aveva peraltro manifestato i propri dubbi al Senato, trattandosi di modifiche in alcuni casi non necessarie (ad esempio, in quanto volte ad esonerare i medici di base dall'adozione di misure alle quali essi non erano comunque tenuti) e in altri non opportune (in quanto suscettibili di incrinare gravemente l'armonia del quadro normativo).

Con tali innovazioni è stata esclusa l'applicabilità ai medici di base dell'obbligo di notificare al Garante alcuni trattamenti effettuati a fini sanitari (art. 37, comma 1-*bis*, del Codice) e di alcune disposizioni del Codice (v. ora l'art. 83, comma 2-*bis*) a garanzia dell'"anonimato" del paziente in sala d'attesa (già, peraltro, limitato sin dall'origine alle sole "strutture" sanitarie). Inoltre, si è subordinata l'omissione delle generalità del paziente in alcune ricette mediche ad un'esplicita richiesta dell'interessato (art. 89, comma 2-*bis*).

È stato poi soppresso l'art. 181, comma 1, lett. *e*), del Codice, che prevedeva il termine del 30 settembre 2004 per adottare modalità semplificate per l'acquisizione del consenso e il rilascio dell'informativa previste dall'art. 76, comma 2; con il risultato, quindi, di cancellare inopportunamente il termine transitorio che era stato previsto a favore dei soggetti contemplati nella disposizione (decreto-legge 29 marzo 2004, n. 81, convertito con modificazioni con legge 26 maggio 2004, n. 138; pochi mesi prima, un analogo provvedimento d'urgenza non era stato approvato alla Camera: decreto-legge 21 gennaio 2004, n. 10).

Nel corso dei lavori di conversione del decreto-legge è stato anche presentato, e poi ritirato, un emendamento parlamentare che prevedeva una sorta di "consenso presunto" del paziente al trattamento dei propri dati personali. L'Autorità ha evidenziato al Governo e al Parlamento il contrasto di tale disposizione con i principi normativi, anche comunitari, in materia di consenso –che deve essere comunque "esplicito", oltre che inequivoco–, soprattutto in relazione ai dati sensibili. Tuttavia, a conclusione dei lavori, il Governo ha accettato come raccomandazione una proposta di ordine del giorno in base alla quale dovrebbero essere adottate, in via transitoria, misure che consentano ai pazienti già in carico ai medici di base di esprimere il consenso mediante una procedura di silenzio-assenso.

Proroga dei termini

Nel pur breve lasso di tempo dall'entrata in vigore del Codice, ricorrendo alla decretazione d'urgenza, si sono differiti i termini per l'adempimento di taluni obblighi posti a garanzia dell'interessato, relativamente all'applicazione delle "nuove" misure minime di sicurezza (per l'introduzione delle quali il Codice aveva fissato il termine del 30 giugno 2004 all'art. 180, comma 1) e all'adozione dei regolamenti in materia di dati sensibili da parte dei soggetti pubblici (su entrambi gli argomenti si vedano pure, rispettivamente, i par. 16.1 e 2.2).

Con specifico riguardo alle misure minime di sicurezza, malgrado la scadenza originariamente fissata potesse ritenersi congrua rispetto alle esigenze prospettate (tanto più che era previsto il più ampio termine del 1° gennaio 2005 per i soggetti che alla data di entrata in vigore del Codice non disponessero di strumenti elettronici tali da consentire l'immediata applicazione delle misure di sicurezza), essa ha subito, in appena un anno, un duplice rinvio: inizialmente al 31 dicembre 2004 e, quindi, al 30 giugno 2005. Analogamente, è stato prorogato anche il termine per l'adozione delle misure di sicurezza da parte dei soggetti che alla data di entrata in vigore del Codice disponevano di strumenti elettronici "obsoleti": prima al 31 marzo 2005 e, da ultimo, al 30 settembre 2005 (art. 3, decreto-legge 24 giugno 2004, n. 158, convertito, con modificazioni, con legge 27 luglio 2004, n. 188; decreto-legge 9 novembre 2004, n. 266, convertito, con modificazioni, con legge 27 dicembre 2004 n. 306).

Adozione delle misure minime di sicurezza

Il citato decreto-legge n. 158/2004 ha prorogato anche il termine previsto dal Codice per approvare i regolamenti delle pubbliche amministrazioni in materia di dati sensibili e giudiziari, originariamente fissato al 30 settembre 2004 (art. 181, comma 1, lett. *a*). Si tratta dell'ennesimo rinvio dell'attuazione di una disciplina (che riguarda un settore assai delicato), prevista ora dagli artt. 20 e 21 del Codice, ma introdotta già con il d.lg. n. 135/1999 e rimasta largamente inattuata, come più volte rilevato dal Garante che ha peraltro richiamato sul punto l'attenzione del Governo (v., fra l'altro, *Provv*. 17 gennaio 2002).

Adozione dei regolamenti sul trattamento dei dati sensibili e giudiziari

1.3. *Legge finanziaria 2005 e altre novità normative con riflessi in materia di protezione dei dati personali*

Nel corso dell'anno sono stati approvati altri provvedimenti normativi che riguardano la materia del trattamento dei dati personali e l'attività del Garante.

Si fa riferimento, in particolare, alla legge finanziaria per il 2005 (legge 30 dicembre 2004, n. 312, alla *G.U.* 31 dicembre 2004, n. 306, S.O. n. 193), che prevede la trasmissione per via telematica del certificato di diagnosi sull'inizio e sulla durata presunta della malattia da parte del medico curante all'Inps (art. 1, comma 149) ovvero dei cedolini per il pagamento delle competenze stipendiali del personale della pubblica amministrazione (art. 1, comma 197); presenta poi profili di sovrapposizione con alcune norme del Codice la disciplina, dettata a fini di contrasto di fenomeni di elusione fiscale, che mira a circoscrivere la riutilizzazione commerciale dei documenti e dei dati acquisiti dagli archivi catastali o da pubblici registri immobiliari (art. 1, commi 367-373). La predetta legge, infine, modificando l'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito dalla legge 24 novembre 2003, n. 326, prevede che la tessera sanitaria sia consegnata a tutti gli assistiti entro il 31 dicembre 2005.

La medesima legge finanziaria ha poi ridotto considerevolmente le risorse finanziarie a disposizione del Garante, comportando gravi difficoltà per il funzionamento dell'Ufficio, come ampiamente segnalato dal Garante al Governo e al Parlamento durante i lavori di approvazione del disegno di legge.

Di particolare interesse, inoltre, è una recente ordinanza del Presidente del Consiglio dei ministri, approvata previo parere del Garante, finalizzata alla localizzazione dei cittadini italiani presenti nelle aree colpite dai recenti eventi calamitosi che hanno investito il sud-est asiatico (ordinanza n. 3390 del 29 dicembre 2004, in *G.U.* 4 gennaio 2005, n. 2). Con tale provvedimento, i gestori di sistemi di telefonia sono stati autorizzati a fornire al Ministero degli affari esteri dati e informazioni utili per

rintracciare i titolari di utenze di telefonia mobile presenti nei luoghi del disastro.

In materia di Carta nazionale dei servizi si registra, infine, l'adozione del d.m. 6 dicembre 2004 (adottato dal Ministro dell'interno, di concerto con i Ministri dell'innovazione e le tecnologie, nonché dell'economia e delle finanze), recante regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della "Carta" medesima. Il decreto individua altresì i dati personali registrati nella memoria riscrivibile del microcircuito, le misure di sicurezza, i servizi e le infrastrutture delle pubbliche amministrazioni coinvolte nel circuito di emissione.

1.4. *Il monitoraggio delle leggi regionali*

Nel corso dell'anno si è proceduto, con riferimento alle disposizioni più rilevanti in materia di protezione dei dati personali, a monitorare le leggi regionali pubblicate sulla Gazzetta Ufficiale.

I testi sui quali è stata effettuata un'analisi più approfondita riguardano disposizioni relative ai settori più vari, in ragione del carattere ampio e trasversale della disciplina di protezione dei dati personali.

Tra le questioni più rilevanti esaminate vi è quella dei limiti della potestà legislativa nelle materie riservate alle regioni rispetto a quella esclusiva dello Stato in tema di protezione dei dati personali alla luce dell'art. 117 Cost. (così come novellato dalla legge costituzionale 18 ottobre 2001, n. 3). Trattasi, com'è noto, di un tema al centro del vivace dibattito al quale l'Autorità è stata chiamata a prendere parte in passato (per i profili di propria competenza), anche con l'audizione del Presidente del Garante alla Commissione affari costituzionali della Camera dei deputati, avvenuta il 30 ottobre 2001 (*Indagine conoscitiva sugli effetti nell'ordinamento delle revisioni del titolo V della parte II della Costituzione*).

Sotto tale profilo è stata in particolare registrata la crescente adozione di provvedimenti legislativi che, pur attenendo direttamente a materie di competenza regionale, contengono disposizioni anche in materia di protezione dei dati personali; si tratta, tuttavia, di discipline a volte ripetitive rispetto alla legislazione nazionale e quindi inidonee ad incidere sul livello di protezione dei diritti della persona garantito dalla legislazione comunitaria e da quella statale (salvo riproporne caratteri e problematiche).

A titolo esemplificativo, si menziona la normativa in materia di prestazioni sociali agevolate che, com'è noto, prevede il ricorso all'indicatore della situazione economica equivalente ai fini della redazione della graduatoria dei beneficiari (cfr. d.lg. 31 marzo 1998, n. 109 successivamente integrato dal d.lg. 3 maggio 2000, n. 130 e dai regolamenti applicativi). A questo proposito, è stato rilevato che la genericità e la frammentarietà della legislazione nazionale in materia di prestazioni sociali agevolate, a suo tempo evidenziate dall'Autorità (cfr. *Pareri* 27 marzo 1998, 26 maggio 1999 e 5 aprile 2000), si riflettono sulle legislazioni regionali in merito all'esatta individuazione delle medesime, degli enti erogatori e dei soggetti, anche privati, legittimati al trattamento dei dati, delle condizioni e dei limiti delle interconnessioni con gli archivi pubblici e privati.

Nell'evidenziare la sostanziale conformità a volte anche letterale tra le disposizioni regionali e quelle statali, è emersa anche, con riferimento alla normativa sugli enti locali –che riconosce ai consiglieri comunali e provinciali il diritto di ottenere dalle amministrazioni di appartenenza notizie ed informazioni connesse all'espletamento del proprio mandato (art. 43, comma 2, d.lg. 18 agosto 2000, n. 267)– la dibattuta questione dei limiti del predetto diritto di accesso; mentre alcune pronunce giuri-

sprudenziali (per esempio Cons. Stato, 4 maggio 2004, n. 2716) lo configurano in modo piuttosto ampio (ritenendo ad esempio che la motivazione relativa alla richiesta di accesso avanzata "per l'espletamento del mandato" basti a giustificarla, senza che occorra alcuna ulteriore precisazione circa le specifiche ragioni della richiesta), altre significative prese di posizione evidenziano, al contrario, una delimitazione dell'accesso ai soli dati personali comunque pertinenti e non eccedenti rispetto alle finalità perseguite nel caso specifico dal richiedente.

Anche con riferimento alla legislazione regionale, in più casi è emersa la mancata, o inadeguata specificazione dei dati sensibili oggetto di trattamento, che necessitano pertanto di un'ulteriore individuazione con atto regolamentare ai sensi dell'art. 20, comma 2, del Codice, nei pur più ampi termini temporali accordati dal menzionato decreto-legge n. 158/2004.

È allo studio dell'Autorità la questione se ipotesi di accordi tra Stato e regioni nonché, più specificamente, forme di intesa su materie che presentino riflessi rilevanti sulla riservatezza delle persone siano soggette al preventivo parere del Garante (cfr. art. 154, comma 4, del Codice).

1.5. *Lavori parlamentari*

Oltre ai provvedimenti normativi approvati, menzionati nel paragrafo precedente, vanno segnalati alcuni lavori parlamentari in corso, anch'essi di interesse per la materia della protezione dei dati personali. In proposito vanno ricordati, in particolare:

Costituzione

a) il disegno di legge costituzionale di modifica della Parte II della Costituzione (AC 4862), nell'ambito del quale la Camera, il 30 settembre 2004, ha approvato un emendamento che "inserisce" le autorità indipendenti nella Carta costituzionale. L'emendamento, presentato da esponenti della maggioranza e modificato da subemendamenti presentati da parlamentari dell'opposizione, è stato approvato quasi all'unanimità (352 sì e 10 no). Esso ha inserito nella Costituzione l'art. 98-*bis* ai sensi del quale, per lo svolgimento di attività di garanzia o di vigilanza in materia di diritti di libertà riconosciuti dalla Costituzione e su materie di competenza dello Stato, si possono istituire con legge apposite autorità indipendenti, stabilendo i requisiti di eleggibilità e le condizioni di indipendenza dei componenti e la durata del relativo mandato. Tali autorità riferiscono alle Camere sui risultati delle attività svolte;

Sfruttamento sessuale dei bambini e pedopornografia in Internet

b) il disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (AC 4599), che mira ad istituire, presso il Dipartimento della pubblica sicurezza, un ufficio centrale per il contrasto della pedopornografia sulla rete Internet. A tale unità organizzativa (Centro nazionale) verrebbe attribuita una pluralità di compiti: raccogliere dalle forze di polizia segnalazioni di siti che diffondono materiale pedopornografico; tenere un registro dei medesimi, dei loro gestori, dei soggetti beneficiari dei pagamenti connessi al commercio di materiale pedopornografico; raccogliere, inoltre, le segnalazioni dei fornitori di servizi di comunicazione elettronica relative a contratti con imprese o soggetti che diffondono o commerciano il predetto materiale. Il disegno di legge pone, poi, a carico dei fornitori di connettività ad Internet obblighi finalizzati ad impedire o a filtrare l'accesso ai siti segnalati e prevede scambi informativi fra il menzionato Centro nazionale, l'Ufficio italiano cambi e il sistema bancario e finanzia-

rio per l'individuazione delle persone che beneficiano dei pagamenti sopra menzionati. Per l'individuazione delle modalità di trasmissione in via telematica di tali informazioni riservate è prevista l'adozione di un regolamento, previo parere del Garante. Nell'ambito dei lavori in Commissione giustizia della Camera si sono tenute una serie di audizioni informali, che hanno interessato anche l'Autorità, nell'ambito delle quali è stato sollevato il problema della conservazione dei dati di traffico in Internet (sul quale si rinvia al par. 15.2), ritenuta utile dalle forze di polizia per finalità d'indagine e repressione dei reati commessi in via telematica;

Siti aventi natura editoriale e testate editoriali

c) il disegno di legge del Governo in materia di editoria e di diffusione della stampa (AC 4163), in discussione presso la Commissione cultura della Camera, che all'art. 1 reca disposizioni in materia di siti aventi natura editoriale e testate editoriali. In un'audizione informale tenuta il 4 novembre u.s., il Presidente del Garante ha richiamato l'attenzione della Commissione sulla necessità di coordinare le emanande disposizioni con le norme del Codice che disciplinano le responsabilità e i compiti del titolare e del responsabile del trattamento, in particolare quando i dati sono trattati mediante un sito Internet. Il Garante ha ritenuto inoltre opportuno un migliore coordinamento tra alcune disposizioni del disegno di legge, la normativa vigente in materia di registrazione delle testate giornalistiche e il progetto di legge recentemente approvato dalla Camera in materia di diffamazione a mezzo stampa, che ha esteso ai siti aventi natura editoriale l'intera disciplina della legge sulla stampa (AS 3176);

Dna dell'imputato o dell'indagato

d) due proposte di legge in materia di analisi del Dna dell'imputato o dell'indagato in ambito processuale, che prevedono un'integrazione del codice di procedura penale e, a certe condizioni, l'obbligo per tali soggetti di sottoporsi al prelievo di materiale biologico a fini di confronto con quello presente su materiale probatorio rinvenuto nel corso delle indagini (AC 4682 e AC 4161). Nelle ultime sedute è stato sollevato dal Presidente della Commissione giustizia della Camera e dal relatore il problema dell'eventuale istituzione di una banca dati in cui conservare i campioni di materiale genetico e i dati personali dei soggetti interessati. Ogni approfondimento al riguardo richiederà un'attenta valutazione delle implicazioni di rilievo costituzionale che ne deriverebbero per i diritti fondamentali della persona e, in particolare, per la riservatezza e la dignità degli interessati;

Accesso ai dati sanitari da parte dell'interessato

e) alcuni disegni di legge recanti disposizioni in materia di consenso informato e di dichiarazioni di volontà anticipate nei trattamenti sanitari (AASS 1437, 2279 e 2943) sono all'esame congiunto della Commissione sanità del Senato. Fra gli aspetti d'interesse in materia di protezione dei dati personali, i disegni di legge prevedono il diritto del paziente di "conoscere i dati sanitari" che lo riguardano, diritto che però dovrebbe essere opportunamente coordinato con il diritto di accesso ai dati personali già previsto dall'art. 7 del Codice (oltre che con la disposizione contenuta nell'art. 84 del Codice relativa alle modalità di comunicazione all'interessato dei dati idonei a rivelare lo stato di salute). Le proposte di legge introducono, poi, il "testamento di vita" e il "mandato in previsione dell'incapacità", definiti, rispettivamente, come l'atto scritto con cui si dispone in merito ai trattamenti sanitari, nonché in ordine all'uso del proprio corpo, e come il contratto con cui si attribuisce al mandatario il potere di compiere atti giuridici in nome e nell'interesse del rappresentato in caso di incapacità sopravvenuta. Sia il "testamento di vita", sia il "mandato in pre-

visione dell'incapacità" sarebbero conservati in un registro informatico istituito nell'ambito di un archivio unico nazionale presso il Consiglio nazionale del notariato, consultabili, in via telematica, da notai, autorità giudiziaria, dirigenti sanitari e medici responsabili del trattamento di soggetti ove ricorrano le condizioni di incapacità previste dal disegno di legge. Il contenuto del testamento di vita e le convenzioni oggetto del mandato non verrebbero considerati, ai fini dell'applicazione della norma, dati sensibili. Anche per questi aspetti, le disposizioni richiedono un diverso e adeguato coordinamento con la normativa in materia di protezione dei dati personali;

Cd. "abusi di mercato"

f) il disegno di legge comunitaria 2004 (AS 2742-B), il cui art. 8 conferisce delega al Governo per il recepimento della direttiva 2003/6/CE del Parlamento europeo e del Consiglio del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (cd. abusi di mercato). La disposizione, originariamente all'esame delle Commissioni VI e X della Camera nell'ambito del testo di riforma della normativa in materia di tutela del risparmio, attribuisce alla Consob poteri di informazione e di indagine in relazione ai quali l'Autorità ha suggerito alla Commissione per le politiche dell'Unione europea della Camera alcune proposte emendative volte ad armonizzarne il testo con le disposizioni del Codice, in particolare per quanto riguarda l'applicazione delle garanzie in materia di comunicazione o diffusione dei dati e di acquisizione di dati di traffico;

Disciplina dell'accesso ai documenti amministrativi

g) il disegno di legge di riforma della legge 7 agosto 1990, n. 241 (AS 1281-B) in relazione al quale l'Autorità ha segnalato alla Commissione affari costituzionali del Senato la necessità di alcune modifiche in vista di un opportuno coordinamento con le norme del Codice che disciplinano l'accesso ai dati personali, anche per quanto riguarda la prevista "collaborazione" fra il Garante e la Commissione per l'accesso ai documenti amministrativi, istituita presso la Presidenza del Consiglio, in procedimenti nei quali rilevino allo stesso tempo questioni concernenti l'accesso ai documenti e a dati personali. Solo due delle proposte suggerite dall'Autorità sono state, poi, approvate dal Senato;

Fallimento

h) il progetto di riforma della normativa in materia di fallimento (r.d. 16 marzo 1942, n. 267), predisposto da un comitato ristretto istituito nell'ambito della Commissione giustizia del Senato, che presenta alcuni aspetti di interesse in materia di protezione dei dati personali, sui quali la predetta Commissione ha richiesto, informalmente, un contributo all'Autorità per un più ampio approfondimento della materia;

Modifiche al codice di procedura civile

i) nell'ambito dei lavori in Commissione giustizia del Senato per la modifica del codice di procedura civile (AS 2430, approvato dalla Camera), cui si è già fatto cenno nella *Relazione 2003*, l'Autorità ha segnalato l'opportunità di armonizzare alcune disposizioni del testo con le modifiche apportate dal Codice in materia di notifica di atti giudiziari e di pubblicazione degli avvisi di esecuzione immobiliare (art. 490 c.p.c., modificato dall'art. 174, comma 9, del Codice);

Anagrafi tributarie nell'Ue

l) sono stati seguiti i lavori relativi ad alcune indagini conoscitive riguardanti tematiche d'interesse, fra le quali, in particolare, l'indagine sull'armonizzazione dei sistemi di gestione dell'anagrafe tributaria, presso la competente Commissione parlamentare di vigilanza. In tale ambito, il 21 gennaio 2004 si è tenuta un'audizione del Presidente del Garante,

79

nella quale si sono auspicate modalità armonizzate nella circolazione delle informazioni personali conservate nelle anagrafi tributarie dei vari Paesi europei, rispettose dei principi di protezione dei dati. Il documento conclusivo dell'indagine approvato il 6 aprile 2004, nel riportare le indicazioni del Garante, dà risalto al sistema delle garanzie e di tutela degli interessati, mettendo in luce l'importanza del rispetto delle disposizioni del Codice per assicurare un equilibrio fra le esigenze di riservatezza e quelle di conoscenza dei dati di tipo fiscale ed economico, anche in ambito europeo.

L'attività svolta dal Garante

II - L'attività svolta dal Garante

Prologo

I compiti del Garante, in buona parte descritti all'art. 154 del Codice (ma non esauribili in questa disposizione) sono molteplici ed implicano attività dal contenuto composito.

Per renderne conto compiutamente, questa sezione della *Relazione* è idealmente strutturata in due corpi: il primo (compreso tra i paragrafi 2 e 16), è orientato sui macro-settori nei quali le norme contenute nel Codice incidono (semplificando: trattamenti in ambito pubblico, attività economiche e libertà fondamentali e tecnologie dell'informazione); il secondo (compreso tra i paragrafi 17 e 23), tralasciando il criterio della materia, mette in luce la multiforme tipologia di attività posta in essere dal Garante e dall'Ufficio, a livello nazionale e sovranazionale, finalizzata all'attuazione della disciplina di protezione dei dati.

2 Trattamenti effettuati in ambito pubblico

2.1. *Notazioni introduttive*

A otto anni dall'introduzione nel nostro ordinamento della disciplina di protezione dei dati personali, il settore pubblico manifesta (anche alla luce dei quesiti pervenuti al Garante nel 2004) una crescente consapevolezza dei valori sottesi al Codice.

Ciononostante, e malgrado l'impegno profuso in varie forme dall'Autorità (ad esempio, attraverso risposte a quesiti, attività di comunicazione, formazione ed informazione svolte; per queste ultime v. i par. 23.1. e ss.) nel sensibilizzare le amministrazioni pubbliche, permane in alcuni contesti una inattuazione (o parziale attuazione) delle disposizioni poste in materia di trattamento dei dati personali, soprattutto con riferimento a quelli sensibili (e giudiziari).

A testimoniare poi l'esistenza di flussi di informazioni personali diversi da quelli sensibili e giudiziari tra enti pubblici, anche in assenza di una norma di legge o di regolamento che li preveda (flussi pur necessari per lo svolgimento delle funzioni istituzionali di uno degli enti coinvolti), stanno le numerosissime comunicazioni pervenute all'Autorità ai sensi degli artt. 19, comma 2 e 39, comma 1, lett. *a*) del Codice (analiticamente menzionate nel successivo par. 2.2).

Il settore pubblico resta uno dei contesti nei quali, per i motivi più vari, persiste la difficoltà di una applicazione piena –che non si risolva nel mero assolvimento di adempimenti puramente formali– dei principi di protezione dei dati personali.

2

Se obiettivo prioritario del Garante è tuttora la "messa in sicurezza" dei trattamenti più delicati (quelli aventi ad oggetto il trattamento dei dati sensibili) o delle modalità più pericolose di trattamento delle informazioni (prime fra tutte le interconnessioni), le pagine a seguire renderanno conto dei mille rivoli nei quali l'Autorità, costantemente sollecitata e pur potendo disporre di risorse assai limitate, è chiamata ad intervenire.

2.2. *Regolamenti sui trattamenti di dati sensibili e giudiziari*

Come è noto, i soggetti pubblici possono trattare i dati sensibili esclusivamente in base ad un'espressa disposizione di legge nella quale siano specificati i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. In presenza di una disposizione primaria che si limiti unicamente a specificare solo la finalità di rilevante interesse pubblico, tali soggetti devono identificare e rendere pubblici i tipi di dati sensibili o giudiziari, nonché le operazioni eseguibili in relazione alle finalità perseguite nei singoli casi, al fine di rendere legittimo il trattamento: a tale scopo, sono tenuti ad adottare o a promuovere l'adozione di un atto di natura regolamentare che sia conforme al parere reso dal Garante sui relativi progetti (parere che, nell'ottica di garantire il principio di semplificazione nell'elevata tutela, può essere fornito anche su schemi-tipo).

Nonostante tale adempimento fosse già contemplato dalla legge n. 675/1996, il Codice, prevedendo un ulteriore periodo transitorio di adeguamento per le amministrazioni, aveva indicato, in un primo tempo, il 30 settembre 2004, termine successivamente prorogato al 31 dicembre 2005, quale scadenza perentoria per l'adozione dei predetti regolamenti previsti dagli artt. 20 e 21 (legge 27 luglio 2004, n. 188, di conversione del decreto-legge 24 giugno 2004, n. 158).

Collaborazioni con le p.a.

Al fine di agevolare l'adozione dei menzionati regolamenti, il Garante ha mantenuto e ampliato le forme di collaborazione con le pubbliche amministrazioni già avviate negli anni passati, finalizzate all'elaborazione dei menzionati schemi-tipo, prestando particolare attenzione ai contenuti delle schede che identificano la tipologia di dati sensibili trattati e le operazioni eseguibili in relazione alle finalità perseguite.

Nel corso dell'anno l'Autorità è stata interpellata sul punto anche da altri soggetti pubblici tra i quali, in particolare, si segnalano la Crui (Conferenza dei rettori delle università italiane), nonché l'Istituto nazionale di fisica nucleare.

Direttiva della Funzione pubblica

L'Autorità ha inoltre collaborato su richiesta alla predisposizione di una direttiva del Dipartimento della funzione pubblica, finalizzata a richiamare l'attenzione delle amministrazioni sulle prescrizioni del Codice che incidono maggiormente nel settore pubblico e che richiedono l'adozione di efficaci scelte organizzative per tradurre sul piano sostanziale le garanzie previste dal legislatore, nonché sulle conseguenze connesse alla loro mancata attuazione.

In chiave di semplificazione, con la direttiva in fase di definitiva formalizzazione, le amministrazioni sono state esortate ad avviare ogni iniziativa utile ad identificare settori di attività, comuni a più enti, per i quali si possa procedere ad un'elaborazione congiunta di schemi tipo da sottoporre all'attenzione del Garante, avvalendosi della collaborazione del Dipartimento della Funzione pubblica medesimo, che intraprenderà a tale scopo le necessarie attività di coordinamento.

In vista della scadenza del 31 dicembre 2005, l'Autorità si riserva di fornire ulte-

riori chiarimenti ed indicazioni di carattere generale in aggiunta a quelle, già dettagliate, del 17 gennaio 2002 (in *Bollettino* n. 24 del 2002, p. 40-45).

Enti locali

Anche la collaborazione avviata dall'Autorità con gli organismi rappresentativi delle autonomie locali (Anci, Upi e Uncem) ha ricevuto un ulteriore impulso nel corso del 2004. La fase della consultazione è altresì proseguita con le regioni, riunite nell'ambito della Segreteria della conferenza dei presidenti delle regioni e delle province autonome di Trento e Bolzano, sotto il coordinamento del Cisis (Centro interregionale per il sistema informatico e il sistema statistico).

Anci

Nel quadro della collaborazione instauratasi, è stata redatta una prima bozza di regolamento per i comuni e le comunità montane contenente la denominazione dei trattamenti effettuati, la fonte normativa, le rilevanti finalità di interesse pubblico perseguite, i tipi di dati trattati e di operazioni eseguibili, nonché la sintetica, ma esauriente, descrizione dei trattamenti e dei flussi informativi.

Lo schema di regolamento per il trattamento dei dati sensibili e giudiziari è stato messo a disposizione delle amministrazioni comunali e delle comunità montane, dal 25 maggio al 15 giugno 2004, sul sito dell'Ancitel (*http://www.ancitel.it/RegolamentoDatiSensibili/*), al fine di stimolare proposte di modifica, suggerimenti, integrazioni ed osservazioni e perfezionare ulteriormente il documento che, una volta approvato dall'Autorità, costituirà lo schema-tipo in conformità al quale gli enti citati potranno adottare –senza dover più richiedere il parere formale del Garante ai sensi dell'art. 20, comma 2, del Codice– i propri atti regolamentari, salvo che debbano procedere a specifici trattamenti non considerati nel contesto generale.

UPI

Analoghe forme di collaborazione sono intercorse con l'Unione delle Province d'Italia (UPI) per la stesura di corrispondenti schemi di regolamento utili per le amministrazioni provinciali: anche in questo caso, è imminente la pubblicazione del modello predisposto sul sito *web* dell'organo rappresentativo, per raccogliere pure in questo ambito, eventuali proposte di integrazione e suggerimenti prima che il Garante esprima il parere di competenza e lo ponga formalmente a disposizione delle province.

Regioni

Con riferimento, invece, alla collaborazione con le regioni, è stato istituito un gruppo di lavoro interregionale, con la partecipazione del Garante, del Ministero della salute, degli assessorati alla sanità e delle aziende sanitarie locali, in considerazione della necessità di includere nello schema di regolamento anche i trattamenti di dati relativi alla salute. Ciò, alla luce della nuova disciplina dettata in argomento dal Codice, che non prevede più una specifica competenza del Ministero della salute a regolamentare tali trattamenti (a differenza dell'art. 23, comma 1-*bis*, della legge n. 675/1996) e demanda tale incombenza all'iniziativa delle diverse amministrazioni.

In considerazione della peculiarità dei trattamenti da parte delle Asl, si è ritenuto opportuno istituire un sottogruppo di esperti, costituito dai rappresentanti degli assessorati in materia, che si è soffermato sui trattamenti di dati sanitari di competenza delle regioni predisponendo lo schema-tipo per i trattamenti di competenza delle aziende sanitarie da inserire nello schema di regolamento regionale.

Pur essendo stata redatta una prima bozza di regolamento nel corso del 2004, la già menzionata proroga al 31 dicembre 2005 del termine per l'adozione degli atti regolamentari (inizialmente prevista per il 30 settembre 2004) ha offerto la possibi-

lità di svolgere ulteriori approfondimenti, potendosi così tenere conto anche delle ulteriori proposte modificative o integrative e delle osservazioni pervenute recentemente al gruppo tecnico e sottoposte successivamente all'attenzione del Garante.

2.3. *Trasparenza dell'attività amministrativa e accesso ai documenti*

Il difficile equilibrio tra la trasparenza dell'attività amministrativa e la tutela della riservatezza ha costituito oggetto di attenta riflessione da parte del Garante che, al pari degli anni passati, è stato interpellato in più circostanze in merito.

Permessi di accesso a zone a traffico limitato

È stata sottoposta al vaglio del Garante la prassi, seguita da alcuni enti locali, di acquisire copia del documento di identità dei soggetti che, a diverso titolo (ad es. residenti e domiciliati in determinate zone), chiedono il rilascio del permesso di accesso/sosta nelle zone urbane a traffico limitato. Tale trattamento dei dati personali è stato ritenuto legittimo –anche in conformità al nuovo Codice della strada (art. 7 del d.lg. 30 aprile 1992, n. 285) e alla normativa in materia di documentazione amministrativa (art. 45 del d.P.R. 28 dicembre 2000, n. 445)– poiché rientra tra le finalità istituzionali dei comuni (art. 18, commi 2 e 3, del Codice) e non contrasta i principi di pertinenza e non eccedenza, di cui all'art. 11, comma 1, lett. *d*), del Codice (*Nota* 28 ottobre 2004).

Albo dei beneficiari di provvidenze economiche

Ulteriori problemi ha sollevato la compatibilità dello specifico regime di pubblicità dell'albo dei beneficiari di provvidenze economiche, istituito ai sensi dell'art. 1 del d.P.R. 7 aprile 2000, n. 118, con le disposizioni in materia di tutela della riservatezza; l'Autorità ha ritenuto lecita la diffusione indifferenziata dei nominativi dei beneficiari unitamente all'indicazione della normativa che autorizza l'erogazione (art. 1, comma 2, del citato d.P.R. n. 118/2000) escludendo, invece, l'indicazione in quella stessa sede di ulteriori dati personali (quali, ad esempio, l'indirizzo, il codice fiscale o l'importo dell'erogazione) ritenuti non pertinenti ed eccedenti rispetto alle finalità perseguite.

In considerazione del divieto di diffondere i dati sulla salute (artt. 22, comma 8, e 68, comma 3, del Codice), è stato precisato che eventuali elenchi di soggetti beneficiari di assegni di cura o di prestazioni sanitarie non devono contenere i nominativi o le iniziali degli interessati, né il puntuale riferimento a disposizioni di legge (come nel caso della legge 5 febbraio 1992, n. 104 in materia di assistenza, integrazione sociale e diritti delle persone handicappate) da cui possano desumersi le cause dell'erogazione: possono essere invece utilizzate, a fini di trasparenza, diciture generiche o codici numerici (*Nota* 2 novembre 2004).

Accesso ai documenti amministrativi

Aspetto importante della tematica relativa alla trasparenza è la conciliabilità del diritto di accesso con il diritto alla riservatezza: permangono in merito numerose le richieste di chiarimenti.

Ostensibilità delle retribuzioni

A tal proposito, tra le questioni maggiormente significative si segnala una richiesta di chiarimenti sull'ostensibilità di documenti amministrativi concernenti l'attività lavorativa dell'*ex* coniuge detenuti dal Servizio ispezione del lavoro (*Nota* 26 aprile 2004). Sul punto il Garante è stato consultato anche da una pubblica amministrazione con riferimento alla richiesta di accesso, presentata da parte dell'*ex* coniuge di un proprio dipendente, volta ad ottenere copia della documentazione contabile relativa alla situazione retributiva del dipendente medesimo al fine di

avviare un'azione giudiziaria per la rideterminazione di un assegno di mantenimento (*Nota* 20 luglio 2004).

In entrambe le occasioni l'Autorità ha evidenziato che la normativa in materia di protezione dei dati personali non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60 del Codice), le quali attribuiscono al cittadino che vi abbia interesse per la tutela di situazioni giuridicamente rilevanti il diritto di accedere ai documenti detenuti dalle amministrazioni pubbliche (artt. 22 e ss. legge 7 agosto 1990, n. 241). È stato quindi sottolineato che spetta all'amministrazione destinataria della richiesta di accesso verificare, caso per caso, l'interesse e i motivi sottesi alla relativa istanza, nonché valutare la sussistenza di una delle ragioni per le quali il documento può essere sottratto alla conoscibilità del richiedente, essendo la stessa in possesso di tutti i necessari elementi di ponderazione della istanza di accesso.

Con riferimento ad una richiesta di accesso ad un rapporto informativo concernente un dirigente scolastico, redatto in seguito ad un accertamento ispettivo, il Garante ha ricordato che il rispetto della normativa in materia di accesso ai documenti amministrativi è requisito di liceità del trattamento. Pertanto, l'Autorità ha ribadito che, qualora il documento sia stato illecitamente reso accessibile, come nel caso specifico, i dati ivi contenuti sono inutilizzabili stante la violazione di una disciplina rilevante in materia di protezione dei dati personali (art. 11, comma 2, del Codice) (*Nota* 16 luglio 2004).

Elenchi delle società concessionarie

L'Autorità è stata chiamata a precisare ulteriormente il rapporto tra il diritto di accesso e quello alla protezione dei dati personali con specifico riferimento alla possibilità per i comuni di accedere ad elenchi dettagliati detenuti dalle società concessionarie dell'erogazione di pubblici servizi contenenti i dati degli intestatari dei contratti di fornitura. In particolare il Garante ha chiarito che ai fini della comunicazione si può prescindere dal consenso dell'interessato nel caso in cui sussistano esigenze di istituzione o completamento del catasto degli impianti termici, alla luce dell'art. 17 del d.P.R. n. 551/1999, il quale ha espressamente previsto che le società distributrici di combustibile comunichino agli enti locali che ne facciano richiesta la titolarità degli impianti da esse riforniti nel corso degli ultimi dodici mesi (*Nota* 1° marzo 2004).

Consiglieri comunali e provinciali

È allo studio dell'Autorità la predisposizione di un documento sulla delicata questione del diritto di accesso dei consiglieri comunali e provinciali, già oggetto di talune pronunce in casi specifici nel corso dell'anno. Con riferimento alla possibilità di consentire ad alcuni consiglieri comunali l'acquisizione di informazioni sui cespiti relativi ad un piano di dismissione del patrimonio immobiliare di un comune, ivi inclusi i nominativi degli utenti assegnatari delle singole unità immobiliari, ed ulteriori dati di carattere sensibile, il Garante ha evidenziato che il Codice non ha abrogato o modificato la specifica disposizione di legge che riconosce ai consiglieri comunali e provinciali il diritto di ottenere dagli uffici del comune, comprese aziende ed enti collegati, informazioni utili all'espletamento del loro mandato, nel rispetto del segreto d'ufficio e del principio di pertinenza e non eccedenza, ai sensi dell'art. 43, comma 2, d.lg. 18 agosto 2000, n. 267 (*Nota* 13 settembre 2004).

Nell'ipotesi in cui l'accesso da parte dei consiglieri comunali riguardi dati sensibili, l'esercizio di tale diritto, ai sensi dell'art. 65, comma 4, lett. *b*), del Codice, è consentito se indispensabile per lo svolgimento della funzione di controllo, di indirizzo politico, di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo.

Resta ferma la necessità, come già accennato nel par. 1.4., che i dati così acquisiti siano utilizzati per le sole finalità connesse all'esercizio del mandato, rispettando in particolare il divieto di divulgazione dei dati idonei a rivelare lo stato di salute. Spetta quindi all'amministrazione destinataria della richiesta accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* del consigliere comunale.

Il medesimo orientamento è stato espresso con riferimento alla possibilità di consentire a un consigliere comunale l'acquisizione di informazioni relative ad una comunità di nomadi Rom coinvolti in un progetto di assistenza ed integrazione sociale intrapreso in loro favore da un comune (*Nota* 10 novembre 2004).

Sindaco

Il Garante ha poi precisato, come in passato, che il diritto di accesso si configura in termini diversi con riferimento ad altri esponenti istituzionali del comune: tale è il caso del diniego opposto ad un sindaco di acquisire copia di tutti i ricorsi proposti dai trasgressori del Codice della strada, corredati dalle deduzioni tecniche redatte dal locale Comando di polizia municipale. Il d.lg. n. 267/2000 dispone, a differenza di quanto previsto per i consiglieri, che il sindaco e i singoli assessori per gli specifici settori ad essi delegati, debbano unicamente sovrintendere al funzionamento degli uffici e dei servizi, non con atti di diretta gestione, ma con direttive generali.

L'ordinamento degli enti locali, infatti, prevede il principio della distinzione tra le funzioni di indirizzo e controllo politico-amministrativo, che spettano agli organi di governo dell'ente, e l'attuazione e gestione amministrativa, che competono ai dirigenti.

Pertanto, nel solo caso in cui la richiesta di informazioni, anche di natura sensibile, sia indispensabile al sindaco 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. Di contro, in assenza delle ricordate finalità di rilevante interesse pubblico, la comunicazione di questi dati, specie se non generalizzata, non è legittima e l'accesso da parte del sindaco non è consentito (*Nota* 22 ottobre 2004).

Difensore civico

Un ulteriore caso particolare è stato portato all'attenzione del Garante da un'associazione, in merito alla richiesta da parte di un difensore civico di conoscere eventuali provvedimenti adottati nei confronti di un educatore (a seguito del rinvio a giudizio di quest'ultimo per maltrattamenti a danno di soggetti disabili affidatigli). Sulla base degli elementi disponibili riguardo ai poteri informativi dello specifico difensore civico richiedente, l'Autorità non ha ravvisato una specifica funzione idonea a consentire l'acquisizione delle informazioni richieste all'associazione, in mancanza del consenso dell'interessato, necessario ai sensi dell'art. 24 del Codice (*Nota* 3 maggio 2004).

Tesserino di riconoscimento

Rispettoso del principio di pertinenza è stato giudicato anche il trattamento dei dati personali riportati nel tesserino di riconoscimento delle guardie ecologiche volontarie di una provincia: al riguardo, la normativa di settore (in particolare il regolamento della provincia in questione) indica espressamente gli elementi identificativi destinati ad essere riportati nel documento (le generalità, la fotografia, i connotati e gli estremi del decreto di guardia particolare giurata), disciplinandone, inoltre, l'uso in caso di esibizione per lo svolgimento dei particolari compiti attribuiti (*Nota* 9 settembre 2004).

2.4. *Il principio del cd. pari rango*

Profili particolari riguardano l'accesso ai documenti amministrativi contenenti dati idonei a rivelare lo stato di salute o la vita sessuale. Infatti, in tal caso il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (art. 60 del Codice).

In proposito, il Garante ha già chiarito che il destinatario della richiesta, al fine di stabilire se il diritto dedotto dal richiedente vada considerato "di pari rango" rispetto a quello della persona cui si riferiscono i dati, deve fare riferimento non al "diritto di azione e difesa" –che pure è costituzionalmente garantito– quanto alla situazione giuridica soggettiva sottostante che il terzo intende far valere (v. già *Provv.* 9 luglio 2003, in *Relazione 2003*, p. 64).

I predetti principi, affermati anche dalla giurisprudenza del Consiglio di Stato, sono stati posti all'attenzione dell'Autorità in varie circostanze. È in avanzato stadio di trattazione la richiesta di chiarimenti di un'amministrazione alla quale un Comando provinciale della Guardia di finanza aveva chiesto copia degli atti relativi al procedimento a carico di un finanziere per l'applicazione della sanzione amministrativa prevista per la fattispecie colposa del reato di atti osceni (art. 527, comma 2, c.p.). La documentazione oggetto della richiesta potrebbe contenere dati sensibili riconducibili, ad esempio, ad informazioni idonee a rivelare la vita sessuale dell'interessato. L'Autorità si è, invece, pronunciata in merito alla richiesta di chiarimenti avanzata da un comune circa la possibilità da parte delle strutture sanitarie di rilasciare ad un consigliere comunale, ai sensi dell'art. 43 del d.lg. n. 267/2000, copia di un referto medico riguardante un terzo (*Nota* 30 settembre 2004).

Ciò comporta, in sintesi, che nella prevalenza dei casi riguardanti solo diritti di credito non sia possibile accogliere l'istanza di accesso e di comunicazione, e che si possa invece valutare, sia pure con cautela e caso per caso, l'effettiva necessità di consentire l'accesso ad una cartella clinica –prima della sua probabile acquisizione su iniziativa del giudice– in caso di controversia risarcitoria per danni ascritti all'attività professionale medica documentata nella cartella stessa.

La questione dei limiti alla comunicazione di dati sulla salute e sulla vita sessuale a persone diverse dall'interessato ha assunto spesso rilevanza nel caso di richieste di accesso a cartelle cliniche detenute presso strutture sanitarie, a volte formulate da un difensore nell'ambito delle cd. indagini difensive (art. 391-*quater* c.p.p.).

Anche in tal caso l'Autorità ha ribadito che le pubbliche amministrazioni non necessitano di una specifica autorizzazione del Garante ai fini dell'accoglimento di richieste di accesso ai documenti o di comunicazione di dati personali formulate ai sensi della disciplina delle indagini difensive introdotta dalla legge 7 dicembre 2000, n. 397. Dal momento che il Codice, come già ricordato, non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (art. 59 del Codice), le disposizioni contenute nell'art. 391-*quater* del c.p.p. vanno ritenute un'idonea fonte normativa per la comunicazione all'esterno di dati personali che va comunque inquadrata sistematicamente (v., ad esempio, art. 71 del Codice). Spetta pertanto all'amministrazione destinataria della richiesta, che dispone di tutti gli elementi a ciò necessari, accertare, caso per caso, la sussistenza dei presupposti per l'esercizio di tale facoltà, compresa la legittimazione del soggetto che ha formulato l'istanza di accesso (*Nota* 15 ottobre 2004).

2

2.5. *Pubblici registri, elenchi, atti e documenti conoscibili da chiunque*

Nel corso dell'anno il Garante si è pronunciato su alcune questioni relative al trattamento dei dati contenuti in pubblici registri, elenchi, atti e documenti conoscibili da chiunque.

Registro quote-latte

In particolare, l'Autorità è stata chiamata a chiarire il regime di pubblicità del registro delle quote-latte tenuto dall'Agenzia per le erogazioni in agricoltura (AGEA) all'interno del Sistema informativo agricolo nazionale (SIAN). Al riguardo, è stata evidenziata la base normativa che consente l'integrale consultabilità (anche in via telematica attraverso il sito Internet del SIAN) del predetto registro da chiunque ne abbia interesse, lasciando invece all'Agenzia la valutazione circa la possibilità di estendere la piena conoscibilità anche alle informazioni relative al periodo antecedente all'istituzione del registro (*Nota* 27 settembre 2004).

ACI

Un'altra questione all'esame dell'Autorità riguarda la possibilità di divulgare tramite il sito *web* dell'ACI l'elenco dei demolitori autorizzati all'esercizio delle operazioni di "rottamazione" dei veicoli fuori uso: in proposito, il Garante ha ribadito le indicazioni già fornite in un'altra occasione (*Nota* 16 giugno 1999), facendo presente che la diffusione del predetto elenco è lecita solo se prevista da apposita disposizione di rango normativo primario o secondario, non essendo sufficiente in tal senso la sola previsione contenuta in un regolamento interno dell'ACI (*Nota* 29 dicembre 2004).

Ipoteche

In sede di ricorso è stata ritenuta infondata, allo stato della normativa all'epoca applicabile, la richiesta di cancellazione dei dati relativi ad un'ipoteca avanzata nei confronti di una società che fornisce informazioni commerciali. Tali dati, relativi alla proprietà immobiliare e detenuti dai competenti uffici dell'Agenzia del territorio competenti erano, infatti, pubblici e quindi accessibili a chiunque ed utilizzabili anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*). Pertanto, la loro estrazione e comunicazione a terzi da parte di società che operano nel settore dell'informazione societaria e commerciale erano, allo stato, lecite (*Provv.* 20 maggio 2004).

Sul punto, tuttavia, è intervenuto da ultimo il legislatore che, con la legge finanziaria 2005, al fine di contrastare fenomeni di elusione fiscale e di tutelare la fede pubblica, ha introdotto una disposizione che, di regola, vieta la riutilizzazione commerciale delle informazioni contenute negli archivi catastali e nei pubblici registri immobiliari tenuti dagli uffici dell'Agenzia del territorio (art. 1, commi 367 e ss., legge 30 dicembre 2004, n. 311). L'eventuale possibilità di riutilizzare per fini commerciali tali informazioni verrebbe subordinata alla stipula di specifiche convenzioni con la stessa Agenzia, le quali dovrebbero disciplinare, a fronte del preventivo pagamento dei tributi dovuti, le modalità ed i termini della raccolta, della conservazione, dell'elaborazione dei dati, nonché il controllo del limite di riutilizzo consentito.

Va però rilevato che l'applicazione di tali disposizioni dovrà essere coordinata con le scelte normative già fatte da Governo e Parlamento nel Codice, anche in attuazione di raccomandazioni del Consiglio d'Europa, tenendo conto, in particolare, del principio di compatibilità con gli scopi per i quali i dati sono stati raccolti, e affidando al Garante la promozione di codici deontologici che dovranno regolare la materia (artt. 61 e 118 del Codice).

2.6. *Documentazione anagrafica e materia elettorale*

A seguito delle modifiche introdotte dal Codice nella materia anagrafica, dello stato civile e delle liste elettorali, sono pervenuti numerosi quesiti volti ad ottenere chiarimenti; più precisamente, il Codice ha integrato la disciplina sull'utilizzo degli elenchi anagrafici da parte delle pubbliche amministrazioni, prevedendo espressamente che rientrano tra gli scopi di pubblica utilità anche quelli relativi all'applicazione della disciplina in materia di comunicazione istituzionale e che può farne uso per tale finalità anche il comune presso il quale è istituita l'anagrafe.

Al riguardo, l'Autorità si è pronunciata su un ricorso relativo all'invio a cittadini minorenni, da parte di un comune, di un invito a partecipare alla sagra patronale ed alla festa di *Halloween* organizzate dall'ente. Il Garante non ha riscontrato, sulla base degli elementi forniti dalle parti, specifiche violazioni in quanto i dati trattati non erano conservati presso il comune e le comunicazioni erano state inviate direttamente dall'ente con la sola intenzione di fare conoscere ai bambini il contenuto delle iniziative ricreative organizzate (*Provv.* 30 gennaio 2004). Sono stati avviati però specifici accertamenti al fine di verificare la liceità del trattamento e la correttezza del comportamento del comune, soprattutto con riferimento all'acquisizione dei dati dei minori.

Scambio di dati Italia-Germania

Significativa è stata anche la collaborazione richiesta al Garante dal Ministero dell'interno per la definizione di una bozza di accordo tra la Repubblica federale tedesca e la Repubblica italiana sullo scambio reciproco di dati tra gli uffici anagrafici nell'ambito dei trasferimenti di domicilio degli abitanti (vale a dire delle persone fisiche sulle quali ricadono obblighi anagrafici ai sensi della normativa statale interna, indipendentemente dalla loro cittadinanza), da e verso i rispettivi territori nazionali.

In proposito il Garante ha evidenziato, con riferimento all'istituzione presso ciascuno Stato contraente di un "ufficio centrale" nazionale competente a gestire il flusso di dati tra i due Paesi, che la disciplina sulle modalità di utilizzazione anche esterna delle banche dati ed il connesso obbligo per gli uffici anagrafici di comunicare dati a tale ufficio centrale, devono essere previsti da norme di legge o di regolamento, in conformità all'art. 19 del Codice. Inoltre, l'Autorità ha rilevato il rischio di vanificare la disciplina anagrafica tramite la previsione contenuta nella bozza di accordo in questione, in quanto i flussi di comunicazioni anagrafiche che si intendono attivare modificano profondamente la specifica normativa di settore (cfr. d.P.R. 30 maggio 1989, n. 223; legge 15 maggio 1997, n. 127). Il Garante ha osservato che simili modifiche potrebbero essere introdotte solo sulla base di una previa disposizione legislativa che le preveda e ne determini i caratteri fondamentali, nel rispetto di necessarie cautele quali, in particolare, la non eccedenza delle informazioni trasmesse rispetto alle finalità perseguite (*Nota* 14 settembre 2004). Alla luce di tali considerazioni, su richiesta del Ministero dell'interno, si è aperto un tavolo di lavoro presso l'Autorità al fine di esaminare congiuntamente i profili più delicati dell'iniziativa ed individuare idonee soluzioni anche nell'ambito della disciplina vigente ed avvalendosi dell'Indice nazionale delle anagrafi (Ina).

Ina-Saia

La collaborazione proficuamente avviata con il Ministero dell'Interno ha trovato conferma anche in altri ambiti: il Garante, infatti, è stato chiamato a prendere parte, assieme ad altre istituzioni, al Comitato tecnico per la predisposizione di uno studio finalizzato alla revisione della normativa anagrafica, alla luce delle innovazioni riguardanti l'Ina ed il Sistema di accesso ed interscambio anagrafico (Saia).

Biografie

Una questione particolarmente delicata in materia è all'esame dell'Autorità, con riferimento alla possibilità di rilasciare ad un istituto enciclopedico privato informazioni sullo *status* di figlio adottivo di un noto imprenditore, al fine di completarne la biografia da inserire nel dizionario degli imprenditori italiani. La normativa fa espresso divieto dell'indicazione della paternità e della maternità nelle attestazioni di stato civile riferite all'adottato (cfr. artt. 26, comma 4, 28, comma 2, e 73, comma 1, della legge 4 maggio 1983, n. 184, in materia di adozioni), negli estratti per riassunto degli atti dello stato civile, nonché nei certificati relativi agli atti di nascita, di matrimonio, di cittadinanza, negli atti attestanti lo stato di famiglia e nelle pubblicazioni di matrimonio esposte al pubblico (art. 1 della legge 31 ottobre 1955, n. 1064, richiamata dall'art. 108, comma 3 del d.P.R. 3 novembre 2000, n. 396). Peraltro, la disciplina in materia di protezione dei dati personali se, da un lato, autorizza, in linea generale, il rilascio degli estratti degli atti dello stato civile una volta decorsi settanta anni dalla loro formazione (cfr. art. 177, comma 3, del Codice), dall'altro fa salve le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di "taluni" dati personali (art. 184, comma 3). Occorre quindi valutare il rilievo dei predetti divieti stabiliti dalla legge sull'adozione.

Ricerche genealogiche

L'Autorità è stata anche interpellata sulla fondatezza della richiesta formulata da uno studio di ricerche genealogiche, volta ad ottenere l'autorizzazione ad effettuare ricerche presso i servizi dello stato civile di alcuni comuni al fine di definire le devoluzioni successorie. Sul punto, il Garante ha ricordato che –a partire dal 1° gennaio 2004, secondo quanto disposto dall'art. 177, comma 3, del Codice– il rilascio degli estratti degli atti dello stato civile è consentito unicamente ai soggetti cui l'atto si riferisce, oppure su motivata istanza comprovante l'interesse personale e concreto del richiedente ai fini di tutela di una situazione giuridicamente rilevante, ovvero decorsi settanta anni dalla formazione dell'atto. Resta ferma la possibilità che l'ufficiale dello stato civile fornisca a richiesta singole notizie che possono essere comunicate ai sensi dell'art. 450 c.c. (*Nota* 12 maggio 2004).

Liste elettorali

Con riferimento, invece, al trattamento dei dati contenuti nelle liste elettorali, il Garante è stato impegnato a fornire chiarimenti alla luce della rilevante modifica introdotta dal Codice che, rispetto al previo regime di piena conoscibilità e pubblicità delle liste elettorali degli enti locali, ora prevede, in applicazione del principio di finalità, che le liste elettorali possano essere rilasciate in copia solo in favore di chi intende perseguire una finalità di attuazione della disciplina in materia di elettorato attivo o passivo, di studio, ricerca scientifica o storica o socio-assistenziale, oppure per perseguire un interesse collettivo o diffuso (art. 177, comma 5, del Codice).

L'Autorità è stata chiamata a pronunciarsi, tra l'altro, in merito al possibile rilascio, da parte delle amministrazioni comunali, di copia delle liste elettorali ai patronati per lo svolgimento delle loro funzioni istituzionali. Il Garante ha chiarito che spetta all'amministrazione destinataria dell'istanza entrare nel merito della richiesta e valutare se la specifica finalità del loro successivo utilizzo dichiarata da parte del richiedente sia conforme all'attività svolta dal soggetto medesimo, nonché se rientri effettivamente tra le ipotesi di cui al citato art. 177. In tale occasione è stato ricordato che il Codice consente agli istituti di patronato e di assistenza sociale, per lo svolgimento delle proprie attività, e solo nell'ambito di un mandato conferito dall'interessato, di accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso dell'interessato (art. 116 del Codice) (*Nota* 28 luglio 2004).

Sportello per il permesso di soggiorno

In materia di immigrazione, è stato adottato un regolamento per la razionalizzazione e l'interconnessione delle comunicazioni fra amministrazioni pubbliche ai fini, in particolare, del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (d.P.R. 27 luglio 2004, n. 242, di attuazione della legge 30 luglio 2002, n. 189), sul quale l'Autorità ha espresso parere il 4 marzo 2004.

Il Dipartimento per le libertà civili e l'immigrazione presso il Ministero dell'interno istituisce e detiene gli archivi automatizzati in materia di immigrazione e di asilo, ai quali accedono le pubbliche amministrazioni interessate, individuate con decreto del Ministro medesimo. Tali archivi sono interconnessi con i sistemi informativi delle pubbliche amministrazioni interessate e con quelli delle regioni, delle province autonome e degli enti locali.

Su richiesta dell'Autorità, i "controlli" sugli accessi al sistema informativo sono stati disciplinati in conformità al principio di proporzionalità, prevedendo che i dati personali concernenti l'identificazione degli utenti e le operazioni di accesso agli archivi possano essere utilizzati solo per finalità di sicurezza e di accertamento di eventuali illeciti.

2.7. *Istruzione*

Esiti scolastici

Anche in materia di pubblicità degli esiti scolastici l'Autorità ha dovuto recentemente ricordare che non è vietata la pubblicazione dei risultati degli scrutini; al contrario, essi devono essere pubblicati, come esplicitamente previsto dalla disciplina in materia (ordinanze ministeriali 13 febbraio 2001, n. 29; 4 aprile 2003, n. 35; 9 febbraio 2004, n. 21).

Voti e interrogazioni

Numerose sono state le richieste di chiarimenti in merito al trattamento dei dati personali nel settore dell'istruzione, con particolare riferimento alla conoscibilità di informazioni riguardanti gli studenti. L'Autorità ha dovuto ancora una volta precisare che non esiste alcuna disposizione del Codice o provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe o delle interrogazioni, né di consegnarli agli alunni in busta chiusa. Così come non esiste alcuna disposizione che proibisca ai medesimi di rendere nota la fede religiosa o che ostacoli le soluzioni da tempo in atto per la partecipazione o meno degli studenti all'ora di religione (*Comunicato stampa* 3 dicembre 2004).

Comunicazioni *ex* art. 39

Sono giunte al Garante numerose comunicazioni ai sensi dell'art. 39, comma 1, lett. *a*), del Codice da parte di istituti scolastici che intendevano comunicare dati personali degli alunni ad altri soggetti pubblici per lo svolgimento di finalità istituzionali, in particolare di natura socio-assistenziale.

In tali occasioni nel ricordare che il trattamento dei dati personali deve essere ispirato ai principi di pertinenza, proporzionalità e necessità, il Garante ha fissato alcuni limiti a tale flusso di dati personali degli alunni, di seguito sintetizzati:

- in merito alla richiesta di una Asl di ricevere dalle strutture scolastiche presenti nella provincia alcuni dati personali dei minori ivi iscritti al fine di realizzare un archivio informatizzato per contattare gli studenti in caso di denuncia di malattie infettive, l'Autorità ha precisato che, pur essendo attribuito a tali enti il compito di provvedere, tra l'altro, all'igiene e alla medicina scolastica negli istituti di istruzione pubblica e privata di ogni ordine e grado (cfr. art. 14, comma 3, lett. *e*), l. n. 833/1978), lo stesso può essere assolto con modalità meno invasive. Ad esempio, sarebbe pos-

sibile individuare un responsabile interno ad ogni istituto scolastico in grado di fornire, qualora si verifichi un evento infettivo, i dati strettamente necessari per assicurare l'opportuno intervento sanitario, senza creare una banca dati informatizzata relativa alla realtà scolastica minorile di un'intera provincia (*Nota* 28 dicembre 2004);

- analogamente, una Asl ha richiesto l'elenco dei nomi e degli indirizzi degli alunni iscritti nelle scuole presenti nel distretto sanitario dell'azienda, al fine di contattare gli stessi all'interno di una campagna contro il morbillo. Il Garante ha osservato che la finalità di promuovere la prevenzione delle malattie infettive attribuita alle Asl può essere utilmente raggiunta anche senza procedere all'invio sistematico alle stesse degli elenchi di tutti gli alunni iscritti agli istituti, mettendo a disposizione delle famiglie il materiale informativo distribuito dal Ministero della salute e dalle Asl presso gli istituti scolastici (*Nota* 17 novembre 2004);
- alcuni istituti scolastici presenti all'interno di uno stesso comune hanno comunicato di voler avviare un progetto di gestione integrato dell'anagrafe scolastica, contenente i dati personali degli alunni iscritti e delle loro famiglie. Da un esame dei dati personali richiesti è risultato che sarebbero state raccolte anche informazioni di carattere sensibile relative ad alunni (es. stato di handicap). In merito a tale progetto, ai sensi degli artt. 20 e ss. del Codice, il Garante sta valutando se –in mancanza di un'espressa previsione di legge o di regolamento che preveda l'interconnessione di banche dati per la gestione integrata dell'anagrafica scolastica comunale e tenendo conto dei principi di indispensabilità, pertinenza e proporzionalità– la finalità di migliorare il percorso formativo degli alunni possa essere raggiunta con altre modalità che non comportino la creazione di archivi contenenti dati sensibili relativi a minori, condivisi da più soggetti pubblici;
- un assessorato regionale alla sanità ha richiesto ad un'università pubblica alcuni dati personali degli iscritti alle facoltà di medicina e di scienze, per inviare agli studenti una lettera di sensibilizzazione in merito alla donazione di sangue e midollo osseo, nonché informazioni sull'autoemoteca dei volontari dell'AVIS. Al riguardo è stato osservato che, pur sussistendo in capo alle regioni ed ad altre amministrazioni pubbliche la funzione di promuovere la donazione del sangue e degli emoderivati (cfr. art. 11, comma 3, legge 4 maggio 1990, n. 107 e Dir. P.C.M. 6 giugno 2003), tale finalità può essere raggiunta con altre modalità, quali, ad esempio, la distribuzione di specifico materiale informativo presso le facoltà universitarie (*Nota* 29 dicembre 2004).

Atti e circolari del dirigente scolastico

L'Autorità ha ricordato che anche nella redazione di atti e circolari interne contenenti dati personali è necessario rispettare i principi di pertinenza e non eccedenza. In seguito ad una segnalazione di un'insegnante il Garante ha ravvisato la non conformità a tali principi del comportamento di un dirigente scolastico che, nell'informare il personale e gli studenti di alcune difficoltà organizzative causate dalla pendenza di procedimenti amministrativi e giudiziari contro l'istituto, aveva specificato anche i nominativi delle insegnanti che li avevano avviati (*Nota* 25 novembre 2004).

Controllo delle presenze

Sono in corso alcuni approfondimenti in merito al progetto di un istituto tecnico industriale volto al controllo elettronico della presenza degli studenti nell'edi-

ficio scolastico, rendendo possibile la verifica della presenza degli alunni da parte dei genitori degli stessi tramite il sito *web* della scuola.

Il Garante è in procinto di definire l'istruttoria in ordine ad un caso di monitoraggio della presenza di allievi stranieri nel territorio provinciale effettuato da un istituto scolastico. Tale attività, che prevede la raccolta di dati sugli alunni tramite questionari distribuiti agli istituti d'istruzione, può comportare il trattamento di dati sensibili dei medesimi (in particolare, di informazioni relative all'origine razziale o etnica), nonché di altre delicate informazioni di carattere personale, come quelle concernenti adozioni o affidamenti.

Comunicazione di dati a privati

A seguito di un ricorso (*Provv.* 29 dicembre 2003), il Garante ha avviato ulteriori accertamenti in merito all'avvenuta comunicazione ad una casa editrice, da parte di un'università statale, di alcuni dati personali dei propri studenti. Al riguardo, è stato rilevato che un determinato decreto rettorale non poteva ritenersi fonte idonea a consentire tale operazione, non individuando in modo puntuale i casi di comunicazione di dati personali degli studenti da parte dell'ateneo a soggetti privati. L'ateneo è stato invitato a sospendere di propria iniziativa il trattamento in questione, nonché ad individuare con esattezza nell'atto regolamentare le singole ipotesi di comunicazione di dati personali degli studenti a soggetti privati, in conformità ai principi di necessità, pertinenza e non eccedenza dei dati rispetto alle finalità perseguite.

L'Autorità in tale occasione ha anche accertato che la stessa università aveva fornito un'informativa incompleta agli studenti, senza individuare le finalità, le modalità del trattamento, nonché l'ambito di comunicazione dei dati personali degli studenti a soggetti privati. Il Garante ha, quindi, contestato all'università la sanzione amministrativa di cui all'art. 161 del Codice (contestazione del 19 novembre 2004, cui è seguito il pagamento in misura ridotta).

2.8. *Notificazioni di atti e comunicazioni*

Notificazioni

Già in passato l'Autorità ha più volte rappresentato alle pubbliche amministrazioni l'esigenza di tutelare in maniera adeguata la riservatezza delle persone alle quali sono notificati atti giudiziari, verbali di contravvenzione, avvisi fiscali o altri atti amministrativi (*Provv.* 22 ottobre 1998 e 26 ottobre 1999).

Molte esortazioni espresse dal Garante sono state tradotte in disposizioni normative dal nuovo Codice, il quale ha modificato le norme processuali interessate (art. 174) seguendo il principio secondo cui, qualora la notificazione non possa essere eseguita nelle mani del destinatario, la copia dell'atto deve essere consegnata in busta sigillata e su questa non devono essere apposte indicazioni da cui possa desumersi il contenuto dell'atto stesso. Tale principio si applica sia nel processo civile, sia in quello penale, nonché per le notificazioni di sanzioni amministrative e di atti e documenti provenienti da organi delle pubbliche amministrazioni, se effettuate a soggetti diversi dagli interessati.

Consegna a mezzo del messo comunale

L'Ufficio del Garante ha inoltre risposto a quesiti relativi alla notifica di violazioni finanziarie o di sanzioni disciplinari, ribadendo che gli addetti al protocollo e il messo comunale tramite il quale viene effettuata la notifica vanno designati quali soggetti incaricati di svolgere le pertinenti operazioni del trattamento; essi possono pertanto accedere al contenuto del documento oggetto di notifica senza che ciò comporti la violazione delle disposizioni sulla comunicazione dei dati personali, essendo peraltro i medesimi incaricati tenuti al segreto d'ufficio in virtù del loro *sta-*

tus di dipendenti pubblici.

Utilizzo del fax

L'Autorità ha ricordato che l'utilizzo del fax come mezzo di comunicazione tra pubbliche amministrazioni è espressamente consentito dalla legge, ed ha fatto anche presente che i dipendenti incaricati dalle amministrazioni di inviare e ricevere comunicazioni tramite fax devono rivestire il ruolo di incaricati del trattamento e, in quanto tali, rispettare le misure di sicurezza e gli obblighi di riservatezza previsti dal Codice (*Nota* 29 dicembre 2004).

Comunicazione di dati sanitari

Il Garante ha precisato che, nel recapitare a mano documenti contenenti dati relativi allo stato di salute (anche qualora il destinatario sia un dipendente del medesimo ente), devono essere prescelte modalità rispettose della riservatezza degli interessati, eliminando ogni occasione di impropria conoscibilità dei dati anche da parte delle persone fisiche incaricate del trattamento, inclusi i messi notificatori (es., allegazione di dati sanitari in busta chiusa; inviti all'interessato a ritirare personalmente un documento presso l'ufficio competente; comunicazione o messa a disposizione telematica o informatica direttamente in favore del solo interessato) (*Provv*. 23 luglio 2004).

Vendite giudiziarie

L'Autorità ha evidenziato in più occasioni che il Codice ha apportato alcune modifiche anche alle disposizioni relative alla pubblicità degli avvisi di vendita giudiziaria. In particolare, con riferimento al processo esecutivo, il nuovo art. 490 c.p.c. prevede che debba essere omessa l'indicazione del debitore qualora l'annuncio sia inserito in quotidiani, oppure divulgato con le forme della pubblicità commerciale. Le informazioni relative al debitore possono essere però fornite dalla cancelleria del tribunale a chiunque vi abbia interesse, unitamente ad ogni altra ulteriore necessaria informazione.

2.9. *Attività fiscale, tributaria e doganale*

Dichiarazioni stragiudiziali

A seguito di numerosi quesiti, segnalazioni e ricorsi, l'Autorità ha giudicato illegittima la prassi delle società concessionarie del servizio per la riscossione dei tributi di chiedere informazioni personali a terzi per ottenerne una dichiarazione stragiudiziale che attesti l'esistenza di crediti del contribuente su cui rivalersi, in quanto nessuna previsione legislativa o regolamentare attribuiva alla stessa il potere di effettuare questo tipo di trattamento senza il consenso del contribuente medesimo (*Provv.* 12 gennaio 2004). Tale procedura, anche in contrasto con il principio di non eccedenza (art. 11 del Codice), poiché sproporzionata rispetto alla finalità di recupero del credito (che può essere comunque perseguita con altri strumenti), risultava, infatti, disciplinata solo da risoluzioni dell'Agenzia delle entrate e da mere circolari ministeriali.

Deve essere tuttavia segnalato che il quadro normativo è stato parzialmente modificato di recente con la legge 30 dicembre 2004, n. 312 (art.1, comma 425, della legge finanziaria 2005), che ha introdotto l'istituto della dichiarazione stragiudiziale. Il nuovo art. 75-*bis* del d.P.R. n. 602/1973 stabilisce, infatti, che il concessionario –anche prima di procedere al pignoramento presso terzi– possa chiedere ai debitori del soggetto che è iscritto a ruolo di indicare per iscritto le cose e le somme dovute al creditore. Poiché la norma prevede che l'indicazione possa avvenire anche solo in modo generico, dovrà essere nuovamente verificato il rapporto tra la novella e il predetto principio di pertinenza e non eccedenza.

Per quanto riguarda il regime di pubblicità dell'elenco dei contribuenti, il Garante ha affermato più volte in passato che, in base al vigente quadro normativo, risultava legittima la pubblicazione presso gli uffici finanziari ed i comuni degli elenchi nominativi dei contribuenti che avevano presentato la dichiarazione dei redditi, unitamente all'indicazione del reddito imponibile. Merita al riguardo segnalare che, recentemente, l'Agenzia delle entrate –nel disporre la pubblicazione degli elenchi per gli anni 2001 e 2002– ha ritenuto, adducendo il rispetto dei principi di pertinenza e non eccedenza, di limitare tale pubblicità al dato relativo alla categoria reddituale prevalente (Provv. dell'Agenzia 29 settembre 2004).

Pubblicità elenco contribuenti

Sono stati avviati approfondimenti con l'Agenzia delle dogane in merito all'applicazione del Codice ai trattamenti effettuati da parte degli uffici centrali e territoriali antifrode che svolgono funzioni di prevenzione, accertamento e repressione delle violazioni della normativa tributaria ed extratributaria. In particolare, l'Autorità ha esaminato anche le collaborazioni avviate dall'Agenzia con gli operatori commerciali e le associazioni di categoria, quali ad esempio la Confindustria.

Agenzia delle dogane

2.10. *Trattamenti svolti da regioni ed enti locali*

Numerosissimi sono stati i casi in cui le regioni e gli enti locali hanno sottoposto all'attenzione del Garante, ai sensi degli artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice, l'intenzione di trasmettere ad altri soggetti pubblici dati personali reputati necessari per lo svolgimento di funzioni istituzionali, anche in assenza di una norma di legge o di regolamento.

Comunicazioni *ex* art. 39

In seguito ad una richiesta di informazioni (*Nota* 15 giugno 2004), ad esempio, il Garante ha ritenuto legittimo il progetto di una regione volto a consentire ai singoli comandanti di polizia locale, in possesso di specifiche *password*, l'accesso all'archivio contenente i dati personali dei propri operatori di polizia locale partecipanti ai corsi di aggiornamento e qualificazione professionale organizzati dalla regione medesima, al fine di poter valutare la partecipazione ai predetti corsi per le esigenze di servizio delle rispettive amministrazioni.

Analogamente, non è stato interdetto alle province l'accesso in rete ai dati contenuti nell'anagrafe venatoria centrale della regione di appartenenza per consentire la vigilanza e la gestione delle opzioni sulle forme di caccia esercitate dagli interessati (*Nota* 30 agosto 2004).

Al contrario, l'Autorità ha precisato che il meccanismo previsto dall'art. 39 non è idoneo a consentire ad un comune di arricchire la propria banca dati sui soggetti che hanno manifestato la propria disponibilità all'affidamento temporaneo di minori con le informazioni relative ai nuclei familiari aspiranti all'adozione trattate dalla Asl. La reciproca comunicazione di dati tra il comune e la Asl avrebbe, infatti, coinvolto anche dati sensibili per i quali sono da osservare le più rigorose garanzie di cui agli artt. 20 e ss. del Codice (*Nota* 13 settembre 2004).

Analoghe problematiche ha sollevato la richiesta della Regione Lazio volta ad ottenere dall'Inps la comunicazione di alcuni dati personali, anche sensibili, per la concessione di benefici economici a favore degli anziani e degli invalidi civili. L'Autorità, interpellata sul punto, ha indicato alle amministrazioni coinvolte le modalità più idonee a garantire il rispetto della normativa in materia di protezione dei dati personali. L'INPS, pertanto, secondo i criteri stabiliti dalla regione, ha individuato direttamente i soggetti beneficiari delle provvidenze economiche. Successivamente, su indicazione della regione, ha consegnato a Poste Italiane S.p.A.,

designata responsabile del trattamento dall'Istituto, l'elenco dei nominativi ed il relativo domicilio dei beneficiari per l'erogazione delle provvidenze economiche.

È stato poi operato un doveroso distinguo tra le ipotesi in cui la comunicazione di dati sia indirizzata da un'amministrazione comunale ad un consorzio, a seconda della natura giuridica, pubblica o privata, di quest'ultimo. L'applicazione degli artt. 19, comma 2, e 39, comma 1, lett. *a*) del Codice è, infatti, ammissibile solo per la comunicazione di dati tra soggetti pubblici, non essendo invece possibile avvalersi della norma in questione ove il consorzio abbia, invece, natura privata. La comunicazione di dati da un soggetto pubblico ad un soggetto privato è ammessa, infatti, dall'art. 19, comma 3, unicamente quando è prevista da norme di legge o regolamento (*Nota* 22 novembre 2004).

Sulla base dei medesimi principi, è stata rappresentata ad un comune l'impossibilità di una trasmissione sistematica di dati relativi a deceduti alle parrocchie, non avendo queste ultime natura di soggetti pubblici (*Nota* 17 gennaio 2005).

Sistema interbibliotecario

Con riferimento allo scambio dei dati dei tesserati nell'ambito dei sistemi bibliotecari provinciali, è stato rilevato che la finalità di assicurare un adeguato servizio pubblico di lettura e di informazione tramite il servizio di prestito interbibliotecario potrebbe essere utilmente conseguita anche riducendo i flussi di dati personali. Ad esempio, nel rispetto dei principi di pertinenza e non eccedenza di cui all'art. 11 del Codice, potrebbero essere trasmesse alle biblioteche collegate le sole richieste dei volumi prive dei dati personali degli utenti, che sarebbero conservati solo presso la biblioteca richiedente (*Nota* 21 dicembre 2004).

Dati anagrafici

È stata ritenuta legittima la comunicazione di dati anagrafici da parte di un comune alla Asl al fine di addivenire, nell'ambito di un piano integrato per l'emergenza estiva, alla campionatura della popolazione anziana per monitorare e prevenire eventuali episodi di grave decadimento psico-fisico e di solitudine. La normativa sugli atti anagrafici prevede, infatti, la possibilità per l'ufficiale dell'anagrafe di rilasciare, anche periodicamente, elenchi degli iscritti nell'anagrafe della popolazione residente alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità, ai sensi dell'art. 34, comma 1, d.P.R. n. 223/1989 (*Nota* 19 luglio 2004).

Diffusione di dati sanitari

In materia di trattamento di dati sensibili da parte degli enti locali, è in istruttoria il caso nel quale un comune ha divulgato sul proprio sito Internet i nominativi di coloro che avevano richiesto la sostituzione nel pagamento della tariffa per la gestione dei rifiuti, affiancati dai motivi della richiesta. In base ad una deliberazione del locale consiglio comunale, la predetta sostituzione può avvenire per "*le utenze domestiche connesse a nuclei familiari ove sussiste la condizione di indigenza o sono presenti portatori di handicap*". La questione involge i diritti dei soggetti portatori di handicap che, sebbene non menzionati con le relative generalità, potrebbero essere indirettamente identificati.

Ausiliari del traffico

Un recente caso in fase di preliminare approfondimento attiene alla richiesta di collaborazione pervenuta da parte della Procura della Repubblica di Roma in relazione ad accertamenti avviati per controllare la liceità dei trattamenti di dati personali relativi alle contestazioni delle sanzioni previste dal Codice della strada effettuate da ausiliari del traffico.

La vicenda riguarda in particolare profili connessi alla verifica dei presupposti richiesti dalla legge in relazione a comunicazioni di dati personali eventualmente inter-

corse tra un ente locale e la società di cui l'ente si avvale per la gestione del servizio.

Censimento nella Provincia autonoma di Bolzano

Nel corso del 2004 è proseguita intensamente l'attività di collaborazione richiesta al Garante in relazione alle modalità di svolgimento del censimento etnico-linguistico nella Provincia di Bolzano. In seguito ad ampi approfondimenti, anche in collaborazione con le istituzioni europee, nazionali e locali, l'Autorità ha ribadito al Governo le considerazioni, già contenute nei due provvedimenti del 2001, in merito al contrasto tra alcuni profili della disciplina sulla "*proporzionale etnica*" e la normativa in materia di protezione dei dati personali sopravvenuta sul piano internazionale comunitario e nazionale. In particolare, è stata evidenziata la necessità di separare dalle operazioni di censimento decennale della popolazione le dichiarazioni individuali nominative di appartenenza o aggregazione linguistica e l'esigenza che le medesime dichiarazioni divengano facoltative, da esercitarsi *una tantum* solo dalle persone interessate ad usufruire dei previsti benefici, senza la necessità di periodici rinnovi. La conservazione di tali dichiarazioni deve avvenire presso un organo pubblico, escludendo la raccolta intermedia presso gli enti locali e, soprattutto, la creazione di banche dati centralizzate. Pur volendo legittimamente prevenire elusioni o utilizzi strumentali, la normativa deve prevedere che, trascorso un adeguato lasso temporale, comunque inferiore all'attuale decennio, l'interessato possa modificare la dichiarazione, semmai con effetti che si producono decorso un congruo periodo di tempo (*Nota* 2 luglio 2004).

Dopo un ampio e serrato confronto, le istituzioni coinvolte hanno siglato un accordo sulle modifiche da apportare alla normativa provinciale, sottoposto nei giorni scorsi al parere del Garante, il quale valuterà prontamente se –come ipotizzato– sono state recepite diverse sue indicazioni, tenendo peraltro conto di alcuni rilievi critici di recente formulati in una nuova segnalazione inviata da parte di associazioni locali.

2.11. *Attività giudiziaria e informatica giuridica*

Processo civile *on-line*

Il Ministero della giustizia ha chiesto all'Autorità un parere in merito allo schema di decreto ministeriale (successivamente approvato con il d.m. 14 ottobre 2004) finalizzato a rendere pienamente operativo il processo civile telematico.

Il decreto prevede che, tramite un complesso sistema informatico (SICI-Sistema informativo civile), magistrati, avvocati, parti e personale giudiziario, collegati in rete, possano intervenire direttamente nel processo, trasmettendo comunicazioni, notifiche, atti sottoscritti con firma digitale e consultando lo stato del procedimento, senza recarsi necessariamente in tribunale.

Nel parere adottato il 23 luglio 2004, l'Autorità, richiedendo maggiori garanzie per i cittadini, ha tra le altre cose invitato il Ministero ad effettuare una rigorosa individuazione dei soggetti abilitati all'accesso al sistema sulla base delle rispettive specifiche competenze. In considerazione della delicatezza della tematica e della complessità del sistema informativo, l'Autorità ha poi sottolineato l'esigenza che i dati e le informazioni trattati dai soggetti pubblici coinvolti nel funzionamento del sistema debbano essere usati solo per le finalità legate allo svolgimento del processo civile *on-line* e in base alle rispettive funzioni e competenze.

Il Garante ha inoltre richiesto un rafforzamento delle misure di sicurezza e l'individuazione di specifici e congrui termini di conservazione dei dati in ragione del tempo necessario a raggiungere gli scopi per i quali essi sono stati raccolti.

Il decreto (pubblicato in *G.U.* n. 272 del 19 novembre 2004) ha tuttavia recepito solo in minima parte le indicazioni fornite dal Garante.

Metodi alternativi di risoluzione delle controversie presso la camera di commercio

Precise garanzie per gli interessati sono state indicate in un progetto avviato da una camera di commercio, un tribunale ed un consiglio dell'ordine degli avvocati nell'ambito dello sviluppo di metodi alternativi di risoluzione delle controversie. Pur essendo il progetto basato sull'adesione libera e volontaria degli interessati, l'Autorità ha individuato alcune prescrizioni da rispettare nella definizione dei moduli operativi. In particolare, i dati personali contenuti nei fascicoli del tribunale non devono essere accessibili ai rappresentanti della camera di commercio e dell'ordine; le parti delle controversie interessate dal tentativo di conciliazione stragiudiziale devono essere preventivamente informate in sede giudiziaria che verranno contattate dagli addetti dello sportello della camera di commercio. L'informativa dovrà essere specifica, con particolare riferimento alle modalità di trattamento ed al periodo di eventuale temporanea conservazione dei dati presso la camera di commercio, anche in caso di insuccesso del tentativo di conciliazione.

Mediazione penale e giustizia riparativa

È in corso un tavolo di lavoro con il Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia nell'ambito dei lavori della Commissione di studio "Mediazione penale e giustizia riparativa". Il Ministero ha infatti avviato un progetto finalizzato all'adozione di modelli di giustizia riparativa nell'ambito dell'esecuzione penale, in particolare con la sperimentazione di percorsi di mediazione penale tra reo e vittima.

Le modalità di attuazione di tale progetto sono al vaglio del Garante nella parte in cui coinvolgono profili che attengono alla tutela della riservatezza, soprattutto per quanto riguarda le esigenze di tutela della vittima del reato.

Pubblicità di sentenze e provvedimenti

Come in passato, il Garante ha più volte ribadito che la normativa in materia di protezione dei dati personali non ha modificato il regime di pubblicità delle sentenze, le quali devono essere redatte secondo le regole ordinarie. Solamente in caso di riproduzione per attività di informazione giuridica il giudice, d'ufficio o su richiesta di parte per motivi legittimi, può disporre l'apposizione sul provvedimento di un'annotazione volta a precludere l'indicazione, nella versione pubblicata, delle generalità e di altri dati identificativi degli interessati. A prescindere dall'annotazione, le generalità e i dati identificativi devono essere comunque omessi nelle decisioni in materia di rapporti di famiglia e di stato delle persone o che coinvolgono minori (artt. 51 e 52 del Codice).

Una distinta questione è stata invece posta all'attenzione del Garante da un ricorso avverso l'Autorità garante per la concorrenza e il mercato, relativamente alla conoscibilità in rete mediante motori di ricerca dei provvedimenti che tale amministrazione deve pubblicare sul proprio bollettino, "riprodotto" anche sul sito *web* istituzionale.

Mezzi di prova

Infine, rispondendo ad alcuni quesiti e segnalazioni relativamente a particolari modalità di acquisizione di mezzi di prova nell'ambito di procedimenti giudiziari, il Garante ha ribadito che resta ferma la competenza del giudice per ogni valutazione circa l'ammissibilità e la rilevanza delle prove; il Codice, infatti, afferma chiaramente che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizione di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (art. 160, comma 6).

3 Sanità

3.1. *Trattamento di dati idonei a rivelare lo stato di salute*

Modifiche al Codice

Come segnalato, nel corso del 2004 sono intervenute alcune modifiche al Codice per quanto riguarda il trattamento dei dati personali in ambito sanitario. In particolare, in materia di trattamenti effettuati da parte dei medici di medicina generale e dei pediatri di libera scelta, il decreto-legge 29 marzo 2004, n. 81, convertito con legge 26 maggio 2004, n. 138, ha introdotto alcune disposizioni in favore di tali soggetti. È stato previsto che ad essi non si applichino le misure organizzative di cui all'art. 83 del Codice (ad es. la distanza di cortesia), purché vengano adottate nell'organizzazione delle prestazioni e dei servizi idonee misure per garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale (art. 83, comma 2-*bis,* del Codice).

Per effetto delle ulteriori modifiche apportate dal citato decreto all'art. 89 del Codice, l'obbligo del medico di medicina generale e del pediatra di libera scelta di apposizione sulla ricetta di un tagliando sopra le generalità e l'indirizzo dell'assistito è ora subordinato ad un'esplicita richiesta di quest'ultimo.

Documentazione clinica abbandonata

Il Garante si è occupato della vicenda, apparsa anche sui mezzi di informazione, del rinvenimento presso un *ex* ospedale psichiatrico in Calabria di documentazione sanitaria abbandonata. Dopo il sequestro della stessa da parte dei carabinieri, l'Autorità ha avviato autonomi accertamenti nei confronti degli enti titolari del trattamento, con particolare riferimento all'adozione delle misure di sicurezza previste dal Codice per la conservazione delle informazioni idonee a rivelare lo stato di salute degli interessati (artt. 11 e 31-35) (*Nota* 13 ottobre 2004). I profili penali della vicenda sono attualmente all'esame della Procura della Repubblica di Catanzaro.

Al di là di quanto più analiticamente segnalato nel par. 20.3, con riferimento ad una vicenda simile l'Autorità ha coordinato un'attività ispettiva in una struttura sanitaria presso cui erano state abbandonate numerose cartelle cliniche per garantire che il recupero e la conservazione della documentazione sanitaria avvenisse con modalità idonee ad evitare accessi non autorizzati ai dati personali in essa contenuti (ispezione presso una *ex* colonia di Santa Maria di Leuca del 12 febbraio 2004). Analogamente, l'Ufficio è intervenuto a seguito di notizie stampa per assicurare la rapida rimozione di numerose ricette e cartelle cliniche rinvenute nel cortile di una biblioteca comunale e nella zona antistante ad una azienda sanitaria in Roma (ispezioni del 10 e 12 gennaio 2004; v. *Comunicato stampa* 24 settembre 2004)

Dati personali dei pazienti

Riguardo alla possibilità di comunicare i dati personali dei pazienti a terzi, ivi compresi i familiari, l'Autorità ha ribadito che gli esercenti le professioni sanitarie sono tenuti ad informare preventivamente in modo adeguato l'interessato ed a richiedere uno specifico consenso scritto sul punto, in conformità a quanto previsto dall'autorizzazione generale del Garante (autorizzazione n. 2/2004, punto 5). Non è, infatti, possibile considerare di per sé equipollente ad una valida prestazione di consenso la presenza del familiare in occasione della visita medica.

Nel caso segnalato all'Autorità, il medico aveva rilasciato alla moglie, senza il con-

senso del marito, un certificato attestante la patologia riscontratagli in occasione di una visita medica. Successivamente, il certificato, che riportava informazioni incomplete ed estranee alle ordinarie esigenze di diagnosi clinica, relative al carattere dell'interessato, era stato prodotto dalla moglie nel procedimento civile di separazione.

Avendo accertato che i dati sulla salute del segnalante erano stati trattati con modalità non conformi alla normativa sulla protezione dei dati personali, il Garante ha intimato al medico di astenersi dall'ulteriore trattamento delle informazioni relative all'interessato; ha poi ricordato che i dati medesimi, essendo stati illecitamente acquisiti, non possono essere ulteriormente utilizzati (art. 11, comma 2, del Codice).

Copia della segnalazione è stata inviata al competente Consiglio dell'Ordine dei medici per le valutazioni del caso (*Nota* 12 agosto 2004).

Contrassegni invalidi

A seguito delle novità introdotte dal Codice, nel corso dell'ultimo anno sono pervenute numerose richieste di parere in merito ai contrassegni per la circolazione e la sosta di veicoli a servizio di persone invalide, regolate, in particolare, dall'art. 188 del Codice della strada (d.lg. 30 aprile 1992, n. 285), dall'art. 381 del relativo regolamento di attuazione (d.P.R. 16 dicembre 1992, n. 495) e, da ultimo, dall'art. 74 del Codice. In relazione al possibile conflitto tra le norme citate, il Garante ha chiarito che, configurandosi l'art. 74 del Codice norma specifica di rango primario, la stessa deve considerarsi prevalente.

Pertanto, i contrassegni da esporre su veicoli devono contenere i soli dati indispensabili ad individuare l'autorizzazione rilasciata e risultare privi di simboli o diciture dai quali possa desumersi la speciale natura dell'autorizzazione.

Per il controllo della regolarità del contrassegno è, quindi, sufficiente porre in evidenza l'indicazione del comune competente e del numero di autorizzazione, informazioni dalle quali si può agevolmente risalire al titolare del permesso, oltre a verificare la validità dello stesso e la correttezza del suo utilizzo (*Note* 21 maggio 2004).

Patologia psichiatrica

È all'attenzione dell'Autorità la richiesta avanzata dal dipartimento di salute mentale di una Ausl di acquisire dalle case di cura private operanti nel territorio di propria competenza i nominativi dei pazienti con patologia psichiatrica. Tale comunicazione avverrebbe in attuazione di quanto previsto da una deliberazione della Giunta della Regione Veneto, in virtù della quale le strutture sanitarie private operanti nella regione, che prendano in cura pazienti psichiatrici, devono comunicare tempestivamente, e comunque entro tre giorni dall'evento, l'avvenuto accoglimento degli stessi.

Al riguardo, il Garante ha precisato che il d.P.R. 10 novembre 1999 (Approvazione del progetto obiettivo "Tutela salute mentale 1998-2000") ha previsto che presso la direzione del Dipartimento di salute mentale (DSM) sia collocato il sistema informativo dipartimentale, il quale raccoglie, elabora ed archivia i dati di struttura, processo ed esito, anche al fine di rilevare il ricorso a strutture di ricovero private degli abitanti del proprio bacino di utenza e i costi relativi. Tuttavia, nessuna disposizione del citato decreto presidenziale impone alle strutture di ricovero private di fornire al DSM competente per territorio l'elenco nominativo dei soggetti che abbiano fatto ricorso alle stesse.

In conformità al citato decreto e al principio di indispensabilità dettato dal Codice, l'Ufficio sta verificando se debbano essere inviati al sistema informativo del DSM solo dati anonimi e aggregati che indichino il numero degli abitanti del bacino di utenza del dipartimento che si siano recati presso la relativa struttura privata e non anche i loro dati identificativi.

Benefici per l'acquisto di sussidi tecnici

Il Garante ha preso in esame la questione, segnalata da un quotidiano, relativa alla documentazione sanitaria da presentare ai rivenditori per beneficiare della riduzione dell'Iva all'atto dell'acquisto di sussidi tecnici e informativi utili a favorire l'autonomia delle persone disabili.

Secondo la disciplina di settore, per usufruire di questa agevolazione occorre presentare al rivenditore una specifica prescrizione rilasciata dal medico specialista della Asl, da cui risulti il collegamento funzionale tra la menomazione e il sussidio che si intende acquistare, insieme ad un certificato (rilasciato dalla Asl) che attesti l'esistenza di un'invalidità funzionale permanente.

L'applicazione di tali disposizioni deve avvenire, però, nel rispetto delle garanzie previste dal Codice per le informazioni sulla salute, secondo le quali è possibile trattare soltanto le informazioni "indispensabili", pertinenti e non eccedenti rispetto alle finalità di volta in volta perseguite, ferme restando ulteriori cautele più severe per il trattamento di talune categorie di dati, quali quelli relativi all'Aids, alla sieropositività o allo stato di disabilità.

Pertanto, è allo studio dell'Autorità la praticabilità di alcune soluzioni alternative rispettose della riservatezza e della dignità delle persone disabili, anche con riferimento alle disposizioni della legge n. 448/1998, che consentano di utilizzare lo strumento dell'autocertificazione per attestare le condizioni personali necessarie al fine di usufruire di una serie di benefici, tra cui le agevolazioni di carattere fiscale.

Sono in corso inoltre ulteriori approfondimenti in merito alle procedure adottate dalle aziende sanitarie locali per il rilascio della tessera di esenzione dal pagamento del *ticket* e dei certificati di invalidità.

Reclami alle Asl e qualità del servizio sanitario

Il Garante è intervenuto in merito ai trattamenti di dati relativi alla gestione dei reclami raccolti dalle Ausl e ai questionari telefonici a domicilio per il rilevamento della qualità sanitaria. Al riguardo, si è precisato che sia l'attività di gestione dei reclami, sia quella di rilevamento della qualità sanitaria, pur essendo considerate di rilevante interesse pubblico dal Codice (artt. 67, comma 1, lett. *b*), 73, comma 2, lett. *g*) e 85, comma 1, lett. *b*), non possono essere effettuate se non dopo aver individuato con atto di natura regolamentare i tipi di dati che possono essere trattati e le operazioni su di essi eseguibili, ai sensi dell'art. 20, comma 2, del Codice (*Nota* 5 ottobre 2004).

Con riferimento alla possibilità di svolgere tali interviste telefonicamente ovvero di contattare al telefono i soggetti che hanno effettuato una prenotazione di un esame clinico al fine di ottenere la conferma o la cancellazione della stessa prenotazione, il Garante ha sottolineato che tali iniziative, seppur lodevoli in quanto dirette ad offrire un servizio migliore agli utenti, presentano profili di criticità. Infatti, in occasione del contatto telefonico, soggetti diversi dall'interessato potrebbero venire a conoscenza di alcuni dati sulla salute di quest'ultimo o più in particolare della sua intenzione di effettuare un determinato esame clinico. Al fine di superare il rischio di tale indebita conoscenza di dati personali dell'interessato, è stato pertanto suggerito di attivare tali servizi solo a seguito di un esplicito assenso dell'utente, previa specifica informativa resa allo stesso ai sensi dell'art. 13 del Codice. Ulteriori, possibili accorgimenti sono stati ipotizzati per l'eventuale uso in occasione di chiamate di conferma da parte dell'azienda sanitaria, specie per ciò che attiene al tipo di indagine medica prenotata o ad altre informazioni di carattere sensibile. Analoghe cautele sono state suggerite in ordine all'attività di refertazione telefonica, effettuata da una casa di cura privata (*Note* 5 ottobre 2004 e 4 gennaio 2005).

Misure organizzative

In materia di consegna dei referti medici, l'Autorità ha appreso da alcune notizie stampa della prassi avviata da un'azienda sanitaria di trasmettere i referti ai pazienti tramite il fax di una tabaccheria. Al riguardo, l'Ufficio ha ricordato che l'art. 84 del Codice prevede che i dati personali inerenti allo stato di salute siano resi noti all'interessato solo per il tramite di un medico designato dallo stesso o dal titolare ed ha quindi invitato la Ausl ad interrompere spontaneamente tale modalità di consegna dei referti, ricevendo subito un positivo riscontro da parte dell'azienda sanitaria (*Nota* 19 ottobre 2004).

L'Autorità è stata interpellata più volte in merito alla possibilità che il personale infermieristico possa essere reso edotto da quello medico delle patologie sofferte dai pazienti in cura. Al riguardo, il Garante ha ricordato che gli organismi sanitari nell'organizzazione delle prestazioni e dei servizi, devono adottare idonee misure per garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati; sono altresì tenuti a sottoporre gli incaricati, che non siano tenuti per legge al segreto professionale, a regole di condotta analoghe (art. 83, comma 2, lett. *i*), del Codice). Il personale infermieristico e di assistenza sanitaria, debitamente designato quale incaricato del trattamento ai sensi dell'art. 30 del Codice, può venire a conoscenza delle informazioni sullo stato di salute dei pazienti strettamente necessarie ad assicurare agli interessati le cure ritenute più idonee e ad adottare le opportune cautele per la propria salute nello svolgimento della prestazione lavorativa. Tali soggetti dovranno, tuttavia, trattare le informazioni sanitarie nel pieno rispetto di quanto indicato nella designazione degli incaricati del trattamento, della normativa in materia di protezione dei dati personali, dell'autorizzazione generale n. 2/2004 e delle regole deontologiche (*Nota* 12 ottobre 2004).

Un'ulteriore problematica sottoposta al Garante riguarda la comunicazione di dati personali di soggetti affetti da una determinata patologia ad una società privata vincitrice di un pubblico appalto per la fornitura di ausili protesici, al fine di consentire alla stessa di provvedere alla consegna di detti ausili direttamente al domicilio dei pazienti.

Carta sanitaria

Il decreto-legge 30 settembre 2003, n. 269, convertito con legge 24 novembre 2003, n. 326, prevede all'art. 50 (*Disposizioni in materia di monitoraggio della spesa nel settore sanitario e di appropriatezza delle prescrizioni sanitarie*) l'introduzione di un modello di ricetta medica a lettura ottica e la costituzione di una banca dati centralizzata (contenente il codice fiscale degli assistiti) in cui confluiscono i dati riguardanti le prescrizioni di farmaci e di prestazioni specialistiche.

Già nel corso dei lavori di conversione del decreto legge, il Garante ha richiamato l'attenzione del legislatore sui delicati problemi sollevati da tale disposizione che, seppur ispirata dall'esigenza di incentivare il monitoraggio della spesa pubblica, è però, allo stato, perseguita attraverso soluzioni che rischiano di compromettere il diritto alla protezione dei dati e, in particolare, di quelli riguardanti lo stato di salute, salvaguardati da particolari garanzie. Attraverso i farmaci prescritti e le prestazioni specialistiche ottenute può essere infatti ricostruita analiticamente la storia sanitaria di ciascun soggetto.

In tale occasione è stato poi rappresentato che le necessarie finalità di controllo della spesa sanitaria potrebbero essere raggiunte anche attraverso altre modalità che non consentano l'identificazione dei soggetti cui si riferiscono le informazioni sanitarie.

Al riguardo, la Camera dei deputati, nella seduta del 19 novembre 2003, ha impegnato il Governo ad intraprendere adeguate iniziative normative al fine di escludere il trattamento dei dati degli assistiti per le finalità sopra descritte.

Tuttavia, in attuazione di quanto previsto dall'art. 50 del decreto-legge

n. 269/2003, sono stati adottati, senza la necessaria consultazione dell'Autorità (prevista dall'art. 154 del Codice), sei atti amministrativi, tra decreti ministeriali e provvedimenti dirigenziali, che individuano con un maggior grado di dettaglio gli aspetti applicativi di tale norma.

Già dal mese di luglio 2004 è stato evidenziato al Governo che per l'adozione di tali atti è mancata la necessaria consultazione del Garante. Il rilievo è stato mosso, tra gli altri, soprattutto nei confronti di un decreto del 30 giugno del 2004, che ha previsto un obbligo –per tutti i cittadini aventi diritto– di dotarsi della tessera sanitaria; obbligo che, per il suo impatto sui diritti delle persone interessate e per le sue caratteristiche, può essere peraltro introdotto solo da una disposizione legislativa e non da un atto amministrativo. Ancora, la connessa sostanziale trasformazione del codice fiscale in un identificativo generale, inserito nella predetta tessera sanitaria, non è allo stato compatibile con la disciplina prevista dalla direttiva 95/46/CE (e con il Codice) nella parte in cui questa dispone che gli Stati membri determinano 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.

Recentemente, il Garante ha nuovamente rappresentato al Governo le ampie riserve in merito alla circostanza che sia stato adottato, con particolare riferimento alla materia sanitaria, un intero pacchetto di atti amministrativi suscettibili di incidere in maniera significativa sui diritti fondamentali garantiti dal Codice, senza il necessario coinvolgimento dell'Autorità in relazione alle proprie specifiche attribuzioni previste dal medesimo Codice, con atti quindi viziati sul piano amministrativo.

Il Ministero della salute ha recentemente sottoposto all'attenzione dell'Autorità l'intenzione di inviare a tutte le famiglie italiane un opuscolo divulgativo dal titolo *"Pensiamo alla salute"*, attraverso Poste italiane S.p.A., designata responsabile del trattamento. L'Autorità, nel prendere atto dell'iniziativa, ha richiamato i criteri indicati nelle precedenti pronunce relative ad importanti casi di comunicazione istituzionale (v., ad esempio, *Provv.* 11 aprile 2002, sull'"euroconvertitore", in *Bollettino* n. 27 del 2002, p. 56), specificando che il titolare di tale trattamento di dati personali, deve essere considerato il Ministero quale entità nel suo complesso, anziché una sua singola articolazione.

3.2. *Trattamento di dati personali in occasione dell'accertamento dell'infezione da Hiv*

L'Autorità è stata più volte sollecitata dalle strutture sanitarie a pronunciarsi in merito alla possibilità di comunicare ai familiari la notizia dello stato di sieropositività di un paziente ricoverato con prognosi grave (anche in caso di decesso). Al riguardo, si è rilevato che il Codice non contiene deroghe alle disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali e ciò anche per quanto riguarda la legge 5 giugno 1990, n. 135 in tema di Aids e Hiv. In tale legge figura, in particolare, l'obbligo di comunicare i risultati di accertamenti diagnostici diretti o indiretti per l'infezione da Hiv alla sola persona cui tali esami si riferiscono (art. 5, comma 4).

Pertanto, deve ritenersi che la comunicazione ai familiari dello stato di sieropositività del paziente non possa prescindere dal consenso dell'interessato. È stata anche valutata l'opportunità che il medico provveda a sensibilizzare la persona sieropositiva e cerchi di persuaderla a comunicare al coniuge la propria sieropositività oppure a manifestare il proprio consenso alla rivelazione da parte dello stesso medico.

Restano infatti da valutare le possibili responsabilità penali del soggetto che, consapevole del proprio stato patologico, ometta di informare il coniuge

(cfr. Cass. pen. n. 30425/2001), nonché le riflessioni in ambito giuridico e scientifico circa i presupposti per l'eventuale applicazione dell'esimente penale dello stato di necessità (art. 54 c.p.) nel caso in cui la sieropositività sia resa nota dal medico senza consenso ad un familiare dell'interessato.

Deve ritenersi peraltro che il difficile bilanciamento dei diversi interessi non possa essere risolto nel senso dell'applicazione –nella fase temporanea in cui il paziente è momentaneamente incosciente– delle recenti disposizioni che prevedono, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, che il consenso possa essere validamente prestato anche da persone diverse da quest'ultimo (art. 82, comma 2, lett. *a*), del Codice), dovendosi considerare anche questa norma in termini sistematici ed omogenei rispetto a tutto il quadro normativo.

Va invece valutato se possa invece giungersi, almeno in parte, a diversa conclusione qualora, in caso di decesso del paziente sieropositivo, il coniuge chieda di accedere alle informazioni che riguardano la persona deceduta. Il diritto di accesso ai dati personali concernenti persone decedute può essere, infatti, esercitato da chiunque abbia un interesse proprio o agisca a tutela dell'interessato o per ragioni familiari meritevoli di protezione (art. 9, comma 3, del Codice).

Sono in corso alcune verifiche volte a controllare se, in occasione del prelievo di sangue per l'accertamento dell'infezione da Hiv, sia fornita al soggetto che si sottopone al test un'idonea informativa, se sia acquisito il suo consenso al trattamento dei dati sensibili, nonché le tipologie di dati raccolti. Dovrà inoltre essere appurato il rispetto delle disposizioni di legge che impongono all'operatore sanitario e ad ogni altro soggetto che viene a conoscenza di un caso di Aids, ovvero di un caso di infezione da Hiv, di adottare in particolare ogni misura o accorgimento necessari alla tutela dei diritti, della dignità e delle libertà fondamentali dell'interessato.

In particolare, l'Autorità si è occupata del caso in cui una paziente era stata sottoposta al test per l'accertamento dell'infezione da Hiv in occasione di un intervento oculistico, senza aver prestato previamente il suo consenso informato. Sebbene la struttura abbia in seguito provveduto alla cancellazione dei dati riguardanti l'interessata, l'Ufficio ha comunque avviato accertamenti sulle modalità con cui vengono generalmente eseguite le analisi in occasione di analoghe prestazioni sanitarie (*Nota* 22 ottobre 2004).

Sono stati, inoltre, avviati alcuni accertamenti volti a verificare la pertinenza e non eccedenza dei dati idonei a rivelare le condizioni di salute dell'interessato (affezione da Aids) contenuti in un verbale di sommarie informazioni assunte *ex* art. 351 c.p.p. dalla Guardia di finanza e successivamente inserito nel fascicolo delle indagini preliminari.

Per quanto concerne la ricerca medica, è avanzato lo studio della questione relativa all'attuazione di un sistema di sorveglianza epidemiologica delle infezioni da Hiv, secondo un progetto della Commissione nazionale per la lotta contro l'Aids e le altre malattie infettive emergenti e riemergenti, sottoposto all'attenzione del Garante, tematica che si collega a precedenti segnalazioni, di cui è ormai ultimata l'istruttoria.

Sull'argomento è stato costituito un gruppo di lavoro in cui, oltre all'Autorità ed alla citata Commissione, sono rappresentate le regioni, la Presidenza del Consiglio dei ministri, l'Istituto superiore di sanità e le associazioni che tutelano l'interesse delle persone affette da Hiv. Nell'ambito di questo gruppo sono stati inizialmente esaminati i presupposti che rendono lecito il trattamento dei dati personali dei sieropositivi, i dati utilizzati, i loro flussi, le modalità con le quali rendere l'informativa agli interessati, nonché le misure di sicurezza da adottare.

L'Ufficio ha poi svolto ulteriori approfondimenti sulla composizione del "codice

identificativo" da assegnare alle segnalazioni delle nuove infezioni e sulla grandezza dell'unità territoriale di rilevazione. Occorre assicurare, infatti, che tale codice sia composto in modo tale, da un lato, da minimizzare il rischio che siano registrate due o più segnalazioni relative ad uno stesso soggetto, e dall'altro, da rispettare l'esigenza, espressa dalla legge 5 giugno 1990, n. 135 e ribadita dal d.m. del 13 ottobre 1995, di non consentire l'identificabilità delle persone cui si riferiscono le singole segnalazioni (artt. 5, l. n. 135/1990 e 178 del Codice, artt. 1 e 2 del decreto citato). Va inoltre individuata la grandezza dell'unità territoriale di rilevazione (macro regioni, regioni, province, macro aree, ecc.) in modo da assicurare l'impossibilità di risalire all'identità degli interessati, in relazione ai tempi e agli strumenti che possono essere ragionevolmente impiegati per compiere tale operazione (v. punto 1, Raccomandazioni del Consiglio d'Europa nn. R (97) 5 e (97) 18).

In proposto, l'Autorità ha anche acquisito un parere tecnico dal Dipartimento per la produzione statistica e il coordinamento tecnico-scientifico dell'Istat, per disporre di idonei elementi di valutazione al fine di formulare le proprie determinazioni all'interno del gruppo di lavoro (*Nota* 19 luglio 2004).

3.3. *Notificazioni in ambito sanitario*

In materia di trattamenti di dati personali in ambito sanitario, il Garante ha adottato un provvedimento nel quale sono individuati i trattamenti di dati idonei a rivelare lo stato di salute esonerati dall'obbligo di notificazione di cui all'art. 37 del Codice (*Deliberazione* n. 1, del 31 marzo 2004).

L'Autorità ha anche chiarito che sono esonerati (dall'obbligo di notificazione) esclusivamente i trattamenti effettuati dai singoli professionisti e dagli altri medici che, in forma associata, condividono il trattamento con altri professionisti, specie all'interno di uno stesso studio medico (*Parere* 26 aprile 2004).

L'esenzione riguarda solo tali soggetti e si riferisce unicamente al trattamento di dati genetici e biometrici, di dati relativi alla procreazione assistita, ai trapianti, alle indagini epidemiologiche, alla rilevazione di malattie mentali, infettive, diffusive e alla sieropositività che siano effettuati nell'ambito degli ordinari rapporti con il paziente. L'esonero non opera, invece, se il trattamento è sistematico ed assume il carattere di costante e prevalente attività del medico come, ad esempio, quello di dati genetici effettuato da un genetista.

Non è previsto esonero neppure per i trattamenti di dati genetici e biometrici effettuati da strutture sanitarie pubbliche o private (ospedali, case di cura e di riposo, aziende sanitarie, laboratori di analisi cliniche, associazioni sportive). Detta misura è stata, infatti, disposta solo in favore di persone fisiche esercenti le professioni sanitarie e non per i trattamenti in quanto tali.

Al riguardo, il Garante ha avviato, con la collaborazione della Guardia di finanza, un ciclo di ispezioni nei confronti di aziende sanitarie locali e di laboratori di analisi privati. Tali accertamenti hanno condotto alla contestazione diretta delle sanzioni amministrative per omessa o ritardata notificazione nei confronti di 14 soggetti sui 15 controllati.

Servizi sanitari *on-line*

Con riferimento alle prestazioni di servizi sanitari per via telematica, il Garante ha precisato che devono essere notificati solo i trattamenti relativi ad una banca dati, ovvero alla fornitura di beni.

Non vanno quindi notificati i trattamenti di dati sanitari nell'ambito della teleassistenza (consultazione di specialisti per via telefonica) e quelli organizzati in banche

dati trattati manualmente (archivi cartacei), ovvero informatizzate ma non collegate ad una rete telematica. Non devono, infine, notificare i medici che usano unicamente un *computer* nel proprio ufficio utilizzando la posta elettronica per dialogare con i pazienti e per effettuare prenotazioni per gli assistiti.

In merito all'attività di monitoraggio della spesa sanitaria è stato precisato che non sono soggetti a notificazione i trattamenti di dati sanitari effettuati da strutture convenzionate con il Servizio sanitario nazionale al solo fine di ottenere il rimborso delle prestazioni specialistiche erogate.

3.4. *Protezione dei dati e procreazione medicalmente assistita*

Per quanto riguarda la materia della procreazione medicalmente assistita, come segnalato nella *Relazione 2003*, l'Autorità è intervenuta in collaborazione col Ministero della salute in ordine alle modalità di attuazione dell'art. 17 della legge n. 40/2004, nella parte in cui prevede che le strutture e i centri in cui si praticano tecniche di procreazione medicalmente assistita trasmettano al Ministero della salute *"un elenco contenente l'indicazione numerica degli embrioni prodotti … nonché, nel rispetto delle vigenti disposizioni sulla tutela della riservatezza dei dati personali, l'indicazione nominativa di coloro che hanno fatto ricorso alle tecniche medesime a seguito delle quali sono stati formati gli embrioni"*.

Il Ministero ha poi specificato che non si sarebbe più sollecitata una comunicazione nominativa di tutti gli interessati che avevano fatto ricorso alla procreazione assistita presso i centri e che, al contrario, si sarebbe proceduto alla sola richiesta di inviare al Ministero una serie di codici numerici indicanti il centro, la regione di riferimento e un numero sequenziale per ogni embrione congelato, in collegamento con i dati identificativi (che rimarranno in possesso dei soli centri).

Nella stessa materia, l'Autorità ha espresso un parere sullo schema di regolamento che disciplina le modalità di manifestazione della volontà degli interessati di accedere alle tecniche di procreazione medicalmente assistita (art. 6, legge 19 febbraio 2004, n. 40). Sebbene la tematica del consenso informato al trattamento medico, oggetto del regolamento, deve ritenersi distinta rispetto a quella del consenso al trattamento dei dati personali, tenuto conto della delicatezza della materia, si è invitato ad adottare la medesima soluzione prevista dal cd. "decreto Di Bella", ovvero quella di acquisire contestualmente entrambe le manifestazioni di volontà, in modo da agevolare l'attività delle strutture e dei centri interessati (*Parere* del 23 luglio 2004).

4 Dati genetici

4.1. *Le informazioni genetiche*

Autorizzazione

Il Garante è in procinto di rilasciare l'autorizzazione generale prevista dal Codice per il trattamento dei dati genetici sentito il Ministero della salute, il quale provvederà una volta acquisito il parere del Consiglio superiore di sanità (art. 90).

Con la nuova autorizzazione si intende precisare la nozione di "dato genetico" e individuare le cautele da adottare in relazione alle informazioni genetiche e ai campioni biologici trattati a fini di tutela della salute dell'interessato o di un terzo appartenente alla stessa linea genetica, a scopi di ricerca scientifica e statistica, nonché per finalità probatorie in un procedimento civile o penale.

Si prevede inoltre di introdurre specifiche garanzie e regole di condotta per lo svolgimento di test e *screening* genetici, nonché di indagini medico-legali (come i test di paternità e/o maternità), soprattutto in relazione al contenuto e alle modalità dell'informativa, alla necessità di fornire all'interessato un'appropriata consulenza genetica e psicologica, al diritto di quest'ultimo di non conoscere i risultati dell'esame (comprese eventuali notizie inattese che lo riguardano), alle modalità di manifestazione del consenso ed al periodo di conservazione dei dati e dei campioni biologici.

Le ricerche dovrebbero essere effettuate secondo le metodologie proprie del pertinente settore disciplinare, sulla base di progetti che indichino le specifiche misure da adottare nel trattamento dei dati per garantire il rispetto dell'autorizzazione, nonché, più in generale, della normativa sulla riservatezza. Gli studi genetici condotti su popolazioni isolate potranno essere attuati soltanto se preceduti da un'ampia attività di informazione volta ad illustrare alle comunità interessate le caratteristiche fondamentali della ricerca.

Particolari limitazioni si applicano, infine, al trattamento di dati genetici da parte di datori di lavoro e di imprese assicurative.

Ricerche genetiche

In risposta ad alcune richieste di autorizzazione al trattamento di dati genetici, l'Ufficio ha precisato che, nel breve periodo che precede il rilascio di tale nuova autorizzazione, il trattamento di queste informazioni resta disciplinato in via transitori dalla precedente autorizzazione generale del Garante che consente di utilizzare i predetti dati soltanto per le finalità in essa individuate e nel rispetto di specifiche prescrizioni, come ad es. il divieto di comunicare le informazioni genetiche a terzi (punto 1.4, dell'autorizzazione generale n. 2/2004, che rinvia al punto 2, lett. *b*), dell'autorizzazione generale n. 2/2002) (*Note* 2 agosto 2004 e 31 agosto 2004).

Sempre in tema di dati genetici, il Garante è intervenuto, a seguito di una segnalazione proveniente dall'estero, rispetto ad una vicenda relativa ad un'articolata ricerca genetica su popolazioni isolate in Alto Adige. L'Autorità, sulla base delle informazioni e dei documenti acquisiti con accertamenti ispettivi *in loco*, anche grazie alla collaborazione dei professionisti preposti alla ricerca, ha accertato la violazione, pur in presenza del rispetto di larga parte dei principi di protezione dei dati, di alcune norme in materia di misure di sicurezza e ha adottato un provvedimento di prescrizione di misure idonee ai sensi dell'art. 169 del Codice.

Su richiesta di una società di ricerca che ha sede in Sardegna, l'Ufficio si è anche

espresso in ordine a un complesso progetto di studio del genoma della popolazione italiana, sottolineando la necessità di tenere conto, nei progetti di medio-lungo periodo come quello esaminato, di alcune garanzie ipotizzate per la autorizzazione.

Sono state quindi anticipate alcune considerazioni in merito alla titolarità del trattamento (la cui individuazione è necessaria anche per determinare il soggetto tenuto ad effettuare la notificazione al Garante ai sensi dell'art. 37 del Codice), alle finalità perseguite, alle modalità di informativa e di manifestazione del consenso, ai diritti che devono essere garantiti agli interessati rispetto alle informazioni che li riguardano, nonché all'ambito di comunicazione dei dati e all'impiego di detti dati per scopi ulteriori rispetto a quelli originari.

In particolare, l'informativa resa deve porre in evidenza il diritto dell'interessato di opporsi per motivi legittimi al trattamento dei dati che lo riguardano e di non conoscere i risultati della ricerca o degli esami genetici effettuati, comprese eventuali notizie inattese.

Nel ricordare che soltanto il perseguimento di altre eventuali legittime finalità di carattere storico, statistico o scientifico, può giustificare una conservazione che si protragga oltre il periodo di tempo necessario al conseguimento degli scopi per i quali i dati sono raccolti o successivamente trattati, l'Ufficio ha segnalato la necessità di individuare con chiarezza le ulteriori finalità scientifica eventualmente perseguite, in modo da determinare un periodo di conservazione dei dati e dei campioni biologici realmente proporzionato rispetto ai medesimi scopi (*Nota* 20 ottobre 2004).

Ricongiungimento familiare

L'Autorità è stata inoltre interpellata dal Ministero degli affari esteri e dal Ministero dell'interno in relazione alla possibilità di utilizzare, nell'ambito delle procedure relative al ricongiungimento familiare dei cittadini dei paesi nei quali non esiste un'autorità statale riconosciuta, l'esame del Dna, già impiegato nei confronti dei cittadini somali, quale strumento di accertamento dell'identità delle persone interessate. In considerazione dei delicati profili incidenti sulla dignità e sulla riservatezza degli interessati, l'Ufficio ha avviato alcuni approfondimenti, anche in collaborazione con i competenti uffici dei predetti dicasteri, per valutare la liceità della procedura impiegata ed, eventualmente, concordare soluzioni idonee a realizzare l'iniziativa prospettata nel pieno rispetto delle garanzie previste dal Codice e dalla nuova autorizzazione sul trattamento dei dati genetici, a tutela dei diritti e delle libertà fondamentali delle persone.

5 Ricerca statistica e scientifica

5.1. *Ricerca statistica*

Dal 1° ottobre 2004 trova applicazione il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici effettuati al di fuori del Sistema statistico nazionale (pubblicato in *G.U.* il 19 agosto 2004 a cura del Garante, e riportato con decreto del Ministro della giustizia del 14 gennaio 2005 nell'allegato A) del Codice).

Tale codice (previsto inizialmente dall'art. 10 del d.lg. 30 luglio 1999, n. 281, e successivamente dall'art. 106, comma 1, del Codice) è il risultato di un lungo lavoro che ha coinvolto, oltre al Garante, la Conferenza dei rettori delle università italiane e numerose associazioni e società scientifiche italiane.

Le norme contenute nel codice deontologico, il cui rispetto è condizione di liceità e correttezza del trattamento, si applicano ai trattamenti di dati personali per scopi statistici e scientifici effettuati da università, altri enti o istituti di ricerca e società scientifiche.

Il codice si ricollega alle garanzie previste dalla normativa che regola i trattamenti effettuati nell'ambito del Sistema statistico nazionale, assicurando particolari cautele per i dati sensibili e giudiziari e per la ricerca medica, biomedica ed epidemiologica, nonché per le ricerche di mercato che non siano connesse alle attività commerciali e di informazione commerciale. Sono previste specifiche regole di condotta e misure di sicurezza soprattutto in relazione alla conservazione dei dati identificativi.

Le ricerche dovranno essere effettuate conformemente agli *standard* metodologici del pertinente settore disciplinare e sulla base di un progetto consultabile per verificare la corretta applicazione della normativa sulla protezione dei dati personali. Le università, gli altri istituti o enti di ricerca e le società scientifiche devono assicurare la diffusione e il rispetto del codice deontologico e segnalano al Garante le violazioni di cui vengono a conoscenza.

Dati reddituali

Per quanto riguarda la concreta applicazione della normativa in materia statistica, il Garante è stato interpellato dall'Agenzia delle entrate in merito alla trasmissione ad una provincia (che aveva avviato un'indagine statistica finalizzata all'individuazione delle differenze socio-economiche tra uomini e donne) dei dati reddituali relativi alla popolazione residente in un comune.

L'Autorità ha specificato in proposito che non devono essere comunicati i dati identificativi diretti degli interessati. I dati possono essere trasmessi, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite dall'indagine, solo a seguito del rilascio di un'idonea informativa agli interessati (*Nota* 1° ottobre 2004).

Ricerca sociologica

Nell'ambito della ricerca sociologica, un'università pubblica ha richiesto ad una scuola i dati personali degli alunni e delle loro famiglie per lo svolgimento di uno studio sull'influenza dell'ambiente scolastico nella valorizzazione del capitale sociale delle famiglie e dei ragazzi. L'Autorità, nell'evidenziare che a tali trattamenti si applica il codice deontologico di recente approvazione, ha precisato che le fina-

lità di ricerca perseguite dall'università potevano essere raggiunte con altre modalità, limitando l'utilizzo di dati personali (art. 12, comma 3, del codice deontologico) (*Nota* 1° dicembre 2004).

Istat

Nel rendere all'Istat il prescritto parere relativo al Programma statistico nazionale per gli anni 2005-2007, l'Autorità ha valutato positivamente l'inserimento nel documento programmatico delle schede relative alle rilevazioni ed elaborazioni che trattano dati personali. Tali schede consentono, infatti, di informare in maniera più chiara gli interessati qualora i dati non siano stati raccolti direttamente presso di loro e il conferimento dell'informativa a ciascuno richieda uno sforzo sproporzionato rispetto al diritto tutelato.

In tale occasione l'Autorità, con riferimento alle cosiddette indagini "multiscopo", ha invitato l'Istat a prestare particolare attenzione nella scelta degli organismi esterni ai quali affidare le fasi di rilevazione, assicurandosi che possiedano requisiti di esperienza, capacità ed affidabilità tali da fornire idonee garanzie del pieno rispetto delle istruzioni ricevute e tenendo conto della delicatezza delle rilevazioni loro affidate. Sono state inoltre fornite indicazioni in relazione a rilevazioni che, seppur non concernenti dati sensibili, riguardino tuttavia informazioni suscettibili di ledere la dignità di chi è chiamato a rispondere.

Per quanto riguarda il quattordicesimo censimento generale della popolazione, sono state sottoposte all'esame dell'Autorità le modalità di diffusione e comunicazione dei dati censuari in favore degli enti della rete di rilevazione, con particolare riferimento ai comuni sprovvisti dell'ufficio di statistica, al fine di contemperare il fabbisogno informativo statistico locale con le disposizioni stabilite a tutela del segreto statistico e della riservatezza dei dati personali.

5.2. *Ricerca medica, biomedica ed epidemiologica*

Nell'ambito della ricerca medica, biomedica ed epidemiologica, oltre all'entrata in vigore del codice deontologico sulla ricerca statistica e scientifica (1° ottobre 2004), occorre più in generale ricordare la disciplina di favore del Codice (art. 110).

Sperimentazioni cliniche

In proposito, con riferimento alla richiesta di una Asl volta ad ottenere l'autorizzazione per l'avvio di una sperimentazione, l'Ufficio ha ricordato che i trattamenti di dati sulla salute effettuati per scopi di ricerca scientifica finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico sono consentiti previa acquisizione del consenso informato delle persone interessate e nel rispetto delle prescrizioni dell'autorizzazione generale n. 2/2004 (*Nota* 30 agosto 2004). Non occorre pertanto un'apposita autorizzazione dell'Autorità laddove il trattamento di queste informazioni venga effettuato in presenza dei presupposti di liceità sopra richiamati e sia altresì conforme alla disciplina sulle sperimentazioni cliniche di medicinali (v. in particolare, il d.lg. 24 giugno 2003, n. 211, ove applicabile).

Comunicazioni *ex* art. 39

Nel corso del 2004 sono pervenute all'Autorità numerose comunicazioni, inoltrate ai sensi dell'art. 39, comma 1, lett. *b*), del Codice. Al riguardo, l'Ufficio ha dovuto precisare in più occasioni che la possibilità di trattare dati sulla salute a prescindere dal consenso degli interessati per scopi di ricerca medica, biomedica ed epidemiologica, è un'ipotesi residuale prevista dal Codice nel caso in cui la ricerca rientri in uno dei programmi di ricerca biomedica o sanitaria. Soltanto in questa evenienza il titolare è

tenuto ad informarne preventivamente il Garante ai sensi dell'art. 39, comma 1, lett. *b*), specificando quali trattamenti intende effettuare senza il consenso degli interessati e la correlazione della ricerca con un programma previsto dall'art. 12-*bis,* d.lg n. 502/1992. Il trattamento potrà poi essere avviato trascorsi 45 giorni da tale comunicazione, a meno che l'Autorità si opponga entro il medesimo termine oppure con successiva determinazione (v., ad esempio, *Nota* 28 ottobre 2004).

In occasione di una comunicazione, ai sensi del medesimo art. 39, comma 1, lett. *b*), concernente la realizzazione di un progetto di ricerca sulla congruità delle prescrizioni farmaceutiche nell'ambito di un programma di ricerca biomedica e sanitaria, l'Autorità ha ricordato che, nel caso in cui le modalità di trattamento previste dal progetto implichino la possibilità di identificare gli interessati, sia pure indirettamente (ad esempio, mediante il riferimento al numero identificativo della cartella detenuta dal medico aderente alla ricerca o anche solo al numero identificativo dello stesso medico), i dati oggetto di trattamento non hanno la natura di "dati anonimi", trattandosi piuttosto di dati personali non direttamente identificativi (art. 4, comma 1, lett. *b*) del Codice).

Quando le informazioni trattate sono idonee a rivelare lo stato di salute degli interessati (poiché, ad esempio, si riferiscono alle patologie che hanno giustificato le prescrizioni mediche), è necessario altresì limitare il trattamento, nelle fasi sia della raccolta sia dell'utilizzo, ai soli dati strettamente indispensabili al raggiungimento delle finalità perseguite, in armonia con i principi di indispensabilità, necessità, pertinenza e non eccedenza dei dati (artt. 3, 11 e 22 del Codice) (*Nota* 28 ottobre 2004).

In un'altra vicenda sottoposta all'esame dell'Autorità, l'Ufficio ha specificato che, nel caso in cui siano coinvolti nella ricerca vari soggetti, occorre indicare nella comunicazione inoltrata all'Autorità ai sensi dell'art. 39 del Codice quali, tra questi, è il titolare del trattamento. Il titolare e, se designato, il responsabile del trattamento devono essere inoltre indicati nell'informativa specifica resa agli interessati ai sensi degli artt. 13, 78, comma 5, e 79 del Codice (*Nota* 14 dicembre 2004).

Registri tumori

Prosegue l'esame delle questioni relative al trattamento dei dati effettuato per la tenuta e la gestione dei registri tumori. Al riguardo, sono stati curati ulteriori approfondimenti al fine di verificare in quale misura le operazioni connesse alla tenuta ed alla gestione di tali banche dati possano considerarsi comprese tra le attività di rilevante interesse pubblico individuate dal Codice (in particolare, dall'art. 98).

In un caso riguardante il trattamento dei dati sulla salute dei pazienti coinvolti in un programma di prevenzione dei tumori sono stati avviati accertamenti nei confronti di una Asl e dell'associazione che, per suo conto, ha svolto le attività di gestione delle visite mediche e delle schede dei pazienti, con particolare riferimento al rispetto delle cautele poste dal Codice in materia di informativa, consenso e adozione delle misure di sicurezza (*Nota* 24 novembre 2004).

Sorveglianza epidemiologica

L'Autorità ha avviato anche approfondimenti volti a verificare l'idoneità delle disposizioni di una legge della Regione Piemonte a legittimare, ai sensi dell'art. 20 del Codice, il trattamento dei dati sulla salute necessario per la gestione di un sistema di sorveglianza epidemiologica delle malattie sessualmente trasmissibili, anche in considerazione della mancanza di attribuzioni regionali a disciplinare, sia pure indirettamente, la materia della protezione dei dati personali e tenuto conto che, per alcune delle patologie interessate dal sistema di sorveglianza regionale, è già operativo un sistema nazionale di sorveglianza epidemiologica sulle malattie infettive e diffusive che prevede soltanto la rilevazione di dati anonimi (artt. 253 e 254, r.d. n. 1265/1934; d.m. 5 luglio 1975 e 15 dicembre 1990).

5

Su richiesta del Ministero della difesa, l'Autorità si è pronunciata sul flusso di dati necessario all'attuazione delle disposizioni legislative che hanno previsto la realizzazione di una "campagna di monitoraggio" sulle condizioni sanitarie dei cittadini italiani operanti a qualunque titolo in Bosnia-Herzegovina e in Kosovo (art. 4-*bis*, decreto-legge 29 dicembre 2000, n. 393, convertito, con modificazioni, dalla legge 28 febbraio 2001, n. 27). La questione concerne profili particolarmente delicati attinenti ai diritti della personalità dei soggetti inclusi nel monitoraggio sui quali l'Autorità non è stata coinvolta in sede di emanazione del d.m. 22 ottobre 2002 del Ministro della salute che dà attuazione alle citate disposizioni legislative.

Al riguardo, pur comprendendo la rilevanza delle finalità perseguite dall'iniziativa, il Garante ha rilevato che, in considerazione dei delicati aspetti su cui essa incide, il quadro normativo deve essere perfezionato al fine di garantire i diritti delle persone interessate.

La norma di legge che ha previsto il monitoraggio non individua, infatti, gli obiettivi dell'iniziativa, né fissa i criteri generali sulle relative modalità di attuazione. In base a tale previsione sarebbe consentita una semplice rilevazione dei dati numerici dei casi eventualmente accertati, senza alcun riferimento ai dati personali. Laddove, invece, l'utilizzo di dati sulla salute sia ritenuto indispensabile per svolgere l'attività di monitoraggio, non essendo sufficiente il trattamento di dati anonimi o di dati personali di natura diversa (art. 22, comma 3, del Codice), è necessario tenere presente il sistema di garanzie previsto dal Codice per il trattamento dei dati sensibili da parte dei soggetti pubblici (attraverso i regolamenti di cui all'art. 20 del medesimo Codice). Inoltre, devono essere introdotte specifiche cautele volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, avendo cura, in particolare, di fornire un'idonea informativa agli interessati e di conservare i dati nel rispetto delle rigorose misure di sicurezza previste per il trattamento dei dati sanitari.

6 Attività di polizia

6.1. *Il controllo sul Centro elaborazione dati del Dipartimento di p.s.*

Anche nel 2004 l'Autorità ha ricevuto alcune segnalazioni, talvolta presentate direttamente al Garante o adesso a seguito di istanze di accesso rivolte al Dipartimento della pubblica sicurezza, con le quali gli interessati hanno fatto presente la registrazione nel Centro elaborazioni dati (C.e.d.) di dati inesatti, incompleti ovvero non aggiornati, per lo più in riferimento a provvedimenti giudiziari o amministrativi adottati e non registrati (art. 10, legge 1° aprile 1981, n. 121, modificato dall'art. 42, l. n. 675/1996 e, da ultimo, dall'art. 175, comma 3, del Codice).

In più occasioni l'Autorità ha sottolineato che anche 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 nel rispetto dei principi di liceità, pertinenza e non eccedenza. L'Autorità ha richiamato l'attenzione degli uffici sulla necessità di verificare con cadenza periodica la rispondenza dei dati trattati a tali principi, apportandovi le modifiche richieste e necessarie o cancellando i dati detenuti, specie in ragione degli esiti processuali a volte documentati dagli stessi interessati.

Dal 1° gennaio 2004, con l'entrata in vigore del Codice, tali indicazioni hanno trovato ulteriore rafforzamento, in linea con quelle fornite dal Garante.

Interrogazioni di altre banche dati

Il Codice ha previsto che il C.e.d. del Dipartimento della pubblica sicurezza debba assicurare, in misura più incisiva rispetto al passato, l'aggiornamento periodico e la pertinenza e non eccedenza dei dati trattati anche attraverso interrogazioni di altre banche dati, come il casellario giudiziale e quello dei carichi pendenti del Ministero della giustizia, al fine di garantire il costante "allineamento" delle informazioni registrate nel C.e.d. con quelle conservate in altri archivi (art. 54, comma 3, del Codice).

L'obbligo di verificare periodicamente il rispetto dei principi descritti nell'art. 11 del Codice è previsto anche per i singoli organi e uffici di polizia, i quali potranno avvalersi delle risultanze del C.e.d. e dovranno, in caso di trattamenti di dati effettuati con mezzi diversi da quelli elettronici, annotare o integrare i documenti cartacei che li contengono (art. 54, comma 4, del Codice).

L'importanza attribuita dal Codice a tali garanzie è testimoniata dalla previsione di un regolamento governativo che dovrà sviluppare l'applicazione dei descritti principi ai trattamenti effettuati per finalità di polizia, prevedendo, fra l'altro, più precisi termini di conservazione dei dati e specifiche modalità di aggiornamento periodico e di verifica della pertinenza dei dati stessi rispetto alla finalità perseguita (art. 57 del Codice).

In considerazione della particolare importanza che assume la corretta applicazione dei principi di protezione dei dati personali in tale settore, l'Autorità intende fornire in materia altre utili indicazioni al Governo, anche in occasione del rilascio del parere sullo schema di regolamento che dovrà essere richiesto al Garante ai sensi dell'art. 154, comma 4 del Codice.

Accesso ai dati conservati nel C.e.d.

Il Codice ha ulteriormente valorizzato le garanzie per l'interessato in materia di accesso ai dati personali che lo riguardano, in riferimento alla circostanza che la disciplina vigente per l'accesso ai dati conservati nel C.e.d. si applica anche ai dati comunque trattati da organi o uffici di polizia con l'ausilio di strumenti elettronici, nonché a quelli –già espressamente considerati in passato– destinati a confluire nel C.e.d. medesimo (art. 10, commi 3, 4 e 5, l. n. 121/1981 e art. 56 del Codice).

A fronte dell'accresciuto quadro di garanzie, il Garante, nell'esaminare alcune segnalazioni pervenute, ha non di rado constatato l'inadeguatezza del riscontro fornito dal competente ufficio della pubblica sicurezza alle richieste di accesso, di rettifica o di cancellazione dei dati registrati nel C.e.d. presentate dall'interessato.

In alcuni casi, infatti, contrariamente a quanto chiaramente previsto dallo stesso art. 10 della l. n. 121/1981, l'ufficio competente non ha fornito all'interessato la "comunicazione in forma intellegibile" dei dati registrati nel C.e.d.; in altri, la richiesta di modifica o di cancellazione dei dati, benché supportata da documentati esiti processuali, è stata riscontrata con la sola, generica comunicazione che la posizione dell'interessato nella banca di dati risultava aggiornata o che erano state apportate le richieste modifiche ai dati. L'Autorità intende avviare un ciclo generale di accertamenti e verifiche presso gli archivi del C.e.d. tenendo conto del numero ingente di casi per i quali il riscontro fornito dal Dipartimento non è risultato soddisfacente, al fine di verificare l'effettiva corrispondenza delle operazioni compiute dal Dipartimento della pubblica sicurezza alle richieste di rettifica o di cancellazione dei dati presentate dagli interessati e, più in generale, affinché i trattamenti effettuati nell'ambito del C.e.d. si svolgano nel tempestivo e sostanziale rispetto delle garanzie previste dal Codice.

Particolari tecnologie

Sempre nel quadro delle più ampie garanzie previste dal Codice, deve essere prestata particolare attenzione a taluni trattamenti effettuati per finalità di polizia che presentano maggiori rischi per l'interessato in quanto riferiti a dati genetici, biometrici o effettuati mediante tecniche basate su dati relativi all'ubicazione.

Per tali trattamenti l'Autorità intende prescrivere, anche su comunicazione degli organi interessati, particolari misure ed accorgimenti a garanzia dell'interessato (artt. 55 e 17, del Codice) ed ha già segnalato la necessità di individuare tali misure in relazione alla raccolta dei rilievi dattiloscopici effettuata in occasione del rilascio o del rinnovo del permesso di soggiorno agli stranieri e all'eventuale inserimento dei dati biometrici nel documento di soggiorno elettronico.

6.2. *Controllo sui trattamenti effettuati dai servizi di informazione e di sicurezza*

Il Garante ha svolto anche nel periodo di riferimento l'attività di verifica su specifici trattamenti di dati personali effettuati presso gli organismi competenti in materia di informazioni e di sicurezza (SISMI, SISDE e CESIS), disciplinati ora dall'art. 58 del Codice.

Questa disposizione, oltre a specificare quali regole del Codice sono applicabili a tali trattamenti, stabilisce che, con decreto del Presidente del Consiglio, si provveda ad individuare le misure minime di sicurezza e le modalità di applicazione a tali trattamenti delle pertinenti disposizioni del Codice. La previsione di tali decreti assume particolare importanza per assicurare, anche in sintonia con orientamenti giurisprudenziali internazionali in materia di tutela dei diritti dell'uomo, trasparenza ai trattamenti effettuati per tali finalità, in relazione ai tipi di operazioni e di dati trattati, l'aggiornamento e la corretta conservazione dei dati mede-

simi. L'Autorità si accinge quindi a prestare la propria collaborazione a partire dai profili relativi alle misure di sicurezza.

Il Garante ha effettuato gli accertamenti rispetto alle segnalazioni presentate dai soggetti interessati, in conformità a quanto previsto dal Codice (art. 160) e con le modalità già osservate nel corso dei precedenti anni.

I controlli, che hanno fatto seguito a quelli effettuati nel marzo 2003, sono stati concentrati nel quinto gruppo di verifiche effettuate dal Garante a decorrere dalla sua istituzione (per un totale di circa 40 persone che hanno chiesto accertamenti) e si sono svolti con la piena collaborazione dei predetti organismi, permettendo di fornire un riscontro dell'attività svolta agli interessati nei particolari termini previsti dal Codice all'esito degli accertamenti.

6.3. *Il controllo sul Sistema di informazione Schengen*

Il Codice ha introdotto importanti modifiche alle modalità di esercizio del diritto di accesso al Sistema di informazione Schengen (SIS) e degli altri diritti connessi (rettifica, integrazione o cancellazione), che possono ora essere esercitati direttamente nei confronti dell'autorità di polizia (c.d. accesso "diretto") e non più solo "per il tramite" del Garante (c.d. accesso "indiretto").

Accesso diretto

Come riportato più diffusamente nella *Relazione 2003*, il Codice ha stabilito (in linea con le scelte effettuate da gran parte dei paesi di "area Schengen") che l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del Sis, ossia il Dipartimento della pubblica sicurezza, fermo restando il diritto di proporre una segnalazione o un reclamo al Garante in caso di mancata o incompleta risposta.

In vista dell'entrata in vigore della nuova normativa il Garante, sulla base dell'esperienza, ha suggerito al Ministero dell'interno e all'Ufficio visti del Ministero degli affari esteri accorgimenti idonei ad assicurare ai richiedenti l'accesso un riscontro completo e tempestivo, anche attraverso il ricorso a moduli prestampati. A seguito delle indicazioni fornite dall'Autorità, il Dipartimento della pubblica sicurezza ha designato la Divisione N-SIS dell'Ufficio coordinamento e pianificazione delle forze di polizia quale ufficio preposto a ricevere le richieste di accesso, mentre il Ministero degli affari esteri ha comunicato alle ambasciate e alle cancellerie le necessarie misure operative, riformulando l'informativa da inserire sui provvedimenti di diniego di visto in modo da orientare più correttamente l'esercizio del diritto di verifica delle segnalazioni.

Il Garante ha reso nota al pubblico la nuova procedura (anche mediante *Newsletter*) pubblicando sul proprio sito *web*, in italiano e in inglese, una breve informativa con alcune indicazioni volte ad agevolare l'inoltro delle richieste di verifica, consultabile nella *home-page* del sito dell'Autorità (*www.garanteprivacy.it*); ad essa ha fatto riferimento anche il Ministero degli affari esteri nell'ambito delle direttive impartite agli uffici consolari.

Delle novità introdotte dal Codice l'Autorità ha poi informato le autorità nazionali di controllo sulla protezione dei dati, con le quali è stata instaurata una significativa collaborazione nell'ambito della procedura di coordinamento prevista dall'art. 114 della Convenzione di Schengen al fine di definire le indicazioni che tali autorità possono fornire agli interessati che richiedano assistenza per l'inoltro di richieste di accesso al SIS.

In proposito, l'Autorità ha registrato la fattiva collaborazione della Divisione N-SIS

del Dipartimento della pubblica sicurezza nell'applicazione della nuova normativa.

Su specifica indicazione fornita dall'Autorità, la Divisione N-SIS informa per conoscenza il Garante su ogni richiesta di accesso ricevuta e sul relativo riscontro fornito, in modo da consentire all'Autorità un efficace monitoraggio e controllo di tutte le richieste di accesso presentate. Quest'ultima, a sua volta, trasmette al predetto ufficio le richieste di semplice verifica dei dati che continuano a pervenire assai numerose probabilmente a causa di una ancora incompleta conoscenza (specie in paesi terzi) delle nuove modalità di accesso "diretto" introdotte dal Codice (dal 1° gennaio 2004 al 31 dicembre 2004 risultano pervenute al Garante circa 300 richieste).

Si tratta in gran parte di domande presentate a seguito di diniego del rilascio di visti, per lo più in conseguenza di segnalazioni dovute alla 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 altri casi si tratta di asserite usurpazioni d'identità o di omonimie in relazione alle quali è stata ulteriormente rafforzata la collaborazione con il Centro visti del Ministero degli affari esteri e con la Direzione centrale per l'immigrazione e la polizia delle frontiere del Dipartimento della pubblica sicurezza.

Valutazione Schengen in Italia

Nei mesi di settembre e ottobre, l'Italia è stata oggetto della visita di valutazione da parte di gruppi di esperti del Consiglio dell'Unione europea. Il Consiglio ha infatti costituito da alcuni anni un gruppo per la valutazione Schengen che sta procedendo ad un esame, paese per paese, del funzionamento di tutti gli elementi che compongono il sistema: visti, frontiere esterne, SIS e SIRENE.

Una delle visite era espressamente dedicata alla verifica del rispetto delle norme italiane in materia di protezione dei dati personali; in particolare, ha riguardato le modalità di inserimento dei dati nel SIS nazionale, quelle di accesso ai dati contenuti nel sistema, le misure di protezione da accessi indesiderati e le misure di sicurezza dei sistemi e delle reti.

Attenzione è stata anche dedicata all'incontro con il Garante nella sua qualità di autorità nazionale di controllo sul SIS; dopo la presentazione svolta dal segretario generale dell'Autorità, sono state soddisfatte diverse domande tese a verificare il grado di effettiva indipendenza dell'Autorità (come, ad esempio, in merito a: disponibilità di una sede idonea, adeguatezza delle risorse finanziarie, possibilità di scelta del proprio personale e numero di persone in servizio) e le modalità di esercizio del suo ruolo di controllo sulla correttezza dei trattamenti.

Il rapporto redatto dagli esperti al termine della visita esprime una valutazione positiva pur contenendo alcuni inviti agli uffici di polizia che gestiscono il sistema informativo a migliorare la protezione dei dati da accessi non autorizzati e a controllare, in particolare, i dati inseriti dall'Italia nel SIS, numericamente superiori a quelli di qualsiasi altro paese Schengen, verificando la necessità del loro mantenimento nel sistema. Su questo aspetto il Garante stà eseguendo un dettagliato lavoro di verifica concordato con l'Autorità comune di controllo Schengen.

6.4. *Altri casi di intervento del Garante in relazione a diverse attività svolte dalle forze di polizia*

Foto segnaletiche

L'Autorità è nuovamente intervenuta in merito alla diffusione da parte di organi di polizia di immagini e, specialmente, di foto segnaletiche di persone coinvolte in attività di polizia (in particolare con riferimento ad una vicenda giudiziaria che ha coinvolto anche alcuni personaggi del mondo dello spettacolo). Il Garante ha sot-

tolineato –in linea con quanto già avvenuto in precedenti occasioni– che la diffusione di immagini di persone coinvolte in indagini o altri accertamenti è consentita agli organi di polizia solo per finalità di giustizia o di polizia e comunque nel rispetto della dignità della persona arrestata o altrimenti detenuta (cfr. art. 97, legge 22 aprile 1941, n. 633 sul diritto d'autore e art. 42-*bis*, legge 26 luglio 1975, n. 354). A seguito dell'intervento del Garante, le amministrazioni interessate hanno nuovamente richiamato il personale di polizia al rispetto della normativa vigente e delle cautele indicate dall'Autorità.

L'orientamento dell'Autorità ha trovato da ultimo conferma in una pronuncia della Corte europea dei diritti dell'uomo.

Trasmettere agli organi di stampa fotografie di una persona accusata in un procedimento penale costituisce infatti una violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo.

Il principio è stato affermato in una recente sentenza della Corte europea (50774/99, 11 gennaio 2005) originata dal ricorso di un'insegnante italiana –fermata e posta agli arresti domiciliari con l'accusa di associazione a delinquere, evasione fiscale e falso in bilancio– la cui fotografia, scattata durante le indagini, era stata diffusa nel corso di una conferenza stampa delle forze dell'ordine e quindi pubblicata su diverse edizioni di due quotidiani locali.

I giudici hanno messo in evidenza che, rispetto ad altri casi oggetto di precedenti pronunce della Corte (cfr. von Hannover/Germania, 59320/00, 24 giugno 2004), la fattispecie in esame presentava alcune peculiarità: essa, in primo luogo, non riguardava un personaggio pubblico; inoltre, la foto pubblicata proveniente dal fascicolo d'inchiesta era stata fornita ai giornali da agenti della Guardia di finanza.

Il fatto che nel caso di specie la ricorrente non fosse un personaggio pubblico giustifica –secondo la Corte– una contrazione della legittima "zona di interazione tra l'individuo e i terzi" (più ampia, evidentemente, nel caso di persone note) che non può espandersi in ragione del coinvolgimento della donna in un procedimento penale.

I giudici, inoltre, ravvisando l'inapplicabilità al caso di specie dell'art. 329 c.p.p. (obbligo del segreto per gli atti d'indagine), non hanno riscontrato la presenza di previsioni normative nell'ordinamento italiano che nella fattispecie in esame giustificassero, ai sensi del secondo comma dell'art. 8 della Convenzione, l'ingerenza nella vita privata della ricorrente.

Osservatorio appalti nel Mezzogiorno

Nell'ambito dei trattamenti svolti per finalità di polizia, il Ministero dell'interno ha sottoposto all'esame dell'Autorità la realizzazione di un sistema automatizzato di supporto alle decisioni per garantire trasparenza e sicurezza degli appalti nel Mezzogiorno che comporta l'acquisizione di dati da numerose altre pubbliche amministrazioni. Il Garante ha proposto l'avvio di un tavolo di lavoro finalizzato all'individuazione di una soluzione idonea a realizzare tale iniziativa nel pieno rispetto delle garanzie previste dal Codice (*Nota* 4 ottobre 2004).

L'Autorità ha altresì avviato specifici accertamenti in merito ad un progetto finanziato dall'Unione europea volto alla prevenzione ed alla repressione da parte delle forze di polizia del traffico di stupefacenti tra alcuni porti dell'Adriatico attraverso l'utilizzo di tecnologie informatiche di ultima generazione.

Cessione di fabbricati

Il Ministero dell'interno e la Questura di Genova hanno chiesto al Garante se i dati contenuti nelle comunicazioni di cessione di fabbricati di cui al decreto-legge 21 marzo 1978, n. 59, convertito in legge, con modificazioni, dalla legge 18 maggio 1978, n. 191, delle quali il sindaco è destinatario ai sensi dell'art. 15, comma 2, della l. n. 121/1981, potessero essere utilizzati dal comune per lo svol-

gimento di controlli di natura fiscale e tributaria.

L'Autorità ha chiarito che la disciplina da ultimo menzionata consente l'utilizzo delle informazioni contenute nel C.e.d. del Dipartimento di pubblica sicurezza esclusivamente per finalità di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità e ne vieta la circolazione all'interno della pubblica amministrazione (*Nota* 5 ottobre 2004).

Collaborazione con il Ministero dell'interno

L'Autorità è stata contattata dal Ministero dell'interno per approfondire le modalità di attuazione della normativa in materia protezione dei dati personali nell'ambito delle prefetture, con particolare riferimento ai trattamenti non finalizzati alla tutela della sicurezza e dell'ordine pubblico ovvero alla prevenzione, accertamento e repressione dei reati e, quindi, soggetti all'integrale applicazione del Codice.

Accesso ai dati anagrafici

Alcuni quesiti riguardano ancora le richieste delle autorità di pubblica sicurezza e delle forze di polizia volte ad acquisire informazioni e documenti riguardanti cittadini detenuti dagli uffici comunali. In proposito è stato in più occasioni ricordato che, fermo restando il divieto per le persone estranee all'ufficio di anagrafe di accedere all'ufficio stesso e, quindi, di procedere alla consultazione diretta degli atti anagrafici, le persone appositamente incaricate dall'autorità giudiziaria e gli appartenenti alle forze dell'ordine ed al Corpo della Guardia di finanza possono legittimamente consultare tali informazioni. In tal caso, tuttavia, i nominativi delle persone autorizzate ad effettuare la consultazione diretta degli atti anagrafici devono figurare in apposite richieste dell'ufficio o del comando di appartenenza, da esibire all'ufficiale di anagrafe unitamente ad un documento di riconoscimento (art. 37, d.P.R. 30 maggio 1989, n. 223).

Inoltre, il Codice prevede che, in conformità alla legge ed ai regolamenti, tale acquisizione possa altresì essere realizzata per via telematica attraverso convenzioni, anche con schemi tipo adottati dal Ministero dell'interno su conforme parere del Garante, a condizione che le modalità di collegamento previste assicurino un accesso selettivo ai soli dati necessari al perseguimento delle finalità di sicurezza ed ordine pubblico, nonché di prevenzione, accertamento e repressione dei reati (artt. 3, 11 e 54, del Codice).

Monitoraggio della spesa sanitaria

Prosegue, infine, l'attività di verifica dell'Autorità sui protocolli di intesa sottoscritti tra le regioni, le Asl e la Guardia di finanza ai fini del coordinamento dei controlli e dello scambio di informazioni in materia di spesa sanitaria che presentano diversi elementi critici sul piano della proporzionalità e liceità delle modalità di trattamento previste.

7 Attività giornalistica e mezzi di informazione

7.1. *Profili generali*

Il Codice in materia di protezione dei dati personali ha confermato il principio in base al quale chi esercita l'attività giornalistica o altra attività comunque riconducibile alla libera manifestazione del pensiero (inclusa l'espressione artistica e letteraria, come ora precisato dall'art. 136 del Codice) può trattare dati personali anche prescindendo dal consenso dell'interessato e, con riferimento ai dati sensibili e giudiziari, senza una preventiva autorizzazione di legge o del Garante. A fronte di queste esenzioni e deroghe si pone, tuttavia, l'obbligo di rispettare alcune condizioni: i limiti al diritto di cronaca già individuati in passato da una consolidata giurisprudenza; il requisito dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice); i principi previsti dal codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (adottato con provvedimento del Garante del 29 luglio 1998, all. A1 al Codice).

A distanza di sei anni dall'entrata in vigore del codice deontologico è stato costituito un gruppo di lavoro tra l'Autorità e l'Ordine nazionale dei giornalisti che si è occupato di analizzarne i principali profili applicativi. Per rispondere ai quesiti posti in quella sede, il 6 maggio 2004 il Garante ha approvato un documento *("Privacy e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti")* con il quale sono state fornite ulteriori precisazioni in merito al corretto utilizzo dei dati personali da parte dei giornalisti, specie in riferimento ad aspetti di particolare problematicità, quali la diffusione di fotografie, la pubblicazione dei nomi delle persone coinvolte in vicende giudiziarie, la diffusione di dati relativi allo stato di salute e alla vita sessuale, i margini di accessibilità da parte dei giornalisti alle informazioni detenute dalle pubbliche amministrazioni.

7.2. *Tutela dei minori*

La particolare tutela accordata ai minori dal Codice è stata richiamata dal Garante con interventi incisivi anche nel corso del 2004.

Si tratta di un settore in cui la vigente normativa in materia di tutela dei dati individua più chiaramente le coordinate entro cui il giornalista (o un soggetto ad esso equiparato ai sensi dell'art. 136 del Codice) è tenuto ad operare.

Il codice deontologico e la Carta di Treviso (da questo richiamata) stabiliscono con nettezza che il diritto del minore (anche quando si trovi coinvolto in fatti di cronaca che non costituiscono reato) alla riservatezza prevale sul diritto di critica e di cronaca. Il Codice ha rafforzato tali garanzie estendendo il divieto di pubblicare con qualsiasi mezzo notizie e immagini idonee a consentire l'identificazione di un minore (già affermato con l'art. 13, d.P.R. 22 settembre 1988, n. 448) anche nel caso in cui esso sia coinvolto a qualunque titolo in procedimenti giudiziari in materie diverse da quella penale (art. 50).

Il Garante ha adottato in proposito specifici provvedimenti di divieto della diffusione di dati idonei a rendere il minore, anche solo indirettamente, identificabile

(si pensi al caso, ad esempio, della pubblicazione di informazioni idonee ad identificare i genitori o afferenti al contesto ambientale e sociale in cui vive). Il divieto di diffusione del resto è posto, in caso di abusi sessuali subiti dal minore, anche da altre norme dell'ordinamento (*Provv.* 12 marzo 2004 e 6 aprile 2004).

Può inoltre rivelarsi necessaria l'adozione di cautele anche nella divulgazione dei dati identificativi di soggetti che risultano indagati per reati di siffatta natura pur quando non operino in tal senso specifiche limitazioni di legge (*Newsletter* 8-11 novembre 2004).

Come è stato chiarito nel documento del 6 maggio 2004, i limiti posti alla diffusione dei dati e delle immagini riguardanti i minori non sono assoluti; essa, infatti, può avvenire in casi particolari in cui un servizio giornalistico ritrae il minore in momenti di svago e di gioco o dà comunque positivo risalto a sue qualità e/o al contesto familiare in cui va formandosi, sempre che i dati siano stati raccolti nel rispetto del principio di correttezza. In linea con i principi generali della normativa in materia di tutela dei dati, il giornalista dovrà tuttavia valutare, anche in queste specifiche ipotesi, l'eventuale opposizione al trattamento manifestata dal minore o da chi ne esercita la potestà genitoriale.

7.3. *Cronache giudiziarie*

Come è noto, i dati giudiziari possono formare oggetto di trattamento per finalità di giornalismo (art. 137, comma 1, lett. *b*) del Codice), anche se nei limiti indicati dall'art. 12 del codice deontologico il quale, a sua volta, rinvia al principio di essenzialità dell'informazione. Tale disposizione va letta alla luce del Codice che estende ora la nozione di dati giudiziari, includendovi anche i dati idonei a rivelare la qualità di imputato e di indagato (art. 4, comma 1, lett. *e*), del Codice.

Continuano ad essere numerosi i reclami e le segnalazioni in relazione al trattamento di tali informazioni da parte degli organi di informazione. In questo ambito, indicazioni utili sono state fornite dal citato documento del 6 maggio 2004 che ha fornito chiarimenti sulle condizioni di liceità della diffusione di dati identificativi di persone arrestate o indagate, di foto segnaletiche e di altre immagini che documentano operazioni di arresto o altre attività processuali (ad es., la traduzione degli imputati), anche alla luce di norme diverse da quelle contenute nella normativa sulla protezione dei dati. Entro questi limiti è affidata alla responsabilità del giornalista la valutazione, caso per caso, dell'essenzialità della notizia (contenente il dato personale) in relazione all'interesse pubblico, ferma restando la completezza della medesima con riferimento alla corretta indicazione della fase del procedimento giudiziario di cui si dà notizia.

Non di rado i profili sollevati dai segnalanti in questo settore attengono alle modalità con cui vengono riportate le notizie, evidenziando possibili lesioni dell'onore e della reputazione dell'interessato piuttosto che problematiche attinenti alla protezione dei dati personali. Merita di essere segnalato a tal proposito il caso sottoposto all'attenzione del Garante (e in corso di accertamento) relativo alla diffusione del contenuto di intercettazioni telefoniche che consentivano l'accostamento del nome dell'interessato a quello dei componenti di un'organizzazione criminale. L'Autorità, ravvisata la liceità della raccolta dei dati dell'interessato in quanto desunti da atti conoscibili (ordinanza regolarmente depositata), ha ricordato nelle more che, fermo restando il diritto di chiedere la pubblicazione di una rettifica nei casi previsti dalla legge, la valutazione del carattere diffamatorio della notizia e dell'eventuale richiesta di risarcimento dei danni rimane di competenza dell'autorità giudiziaria ordinaria.

7.4. *Dati idonei a rivelare lo stato di salute*

Anche quest'anno l'Autorità ha richiamato i mezzi di informazione al rispetto della dignità e della libertà di autodeterminazione delle persone malate. In particolare, nel comunicato del 3 febbraio 2004 è stato stigmatizzato l'accanimento dei giornali sulla vicenda della donna che aveva espresso un rifiuto all'operazione di amputazione della gamba, ritenuta dai medici necessaria per salvarle la vita.

I medesimi principi sono alla base di un recente provvedimento con cui il Garante –al fine di prevenire il rischio di un possibile pregiudizio per l'interessato e in attesa di procedere ad ulteriori approfondimenti sul caso (art. 154, comma 1, lett. *d*), del Codice)– ha disposto il blocco temporaneo dell'ulteriore diffusione televisiva di immagini particolarmente invasive relative ad un uomo indigente, senza dimora, la cui identità sembrava corrispondere a quella di uno straniero assente da diversi anni dal proprio paese e di cui alcuni familiari avevano di recente intrapreso nuove ricerche (*Provv*. 8 novembre 2004).

7.5. *Libertà di informazione e personaggi pubblici*

Come più volte ricordato in passato, esistono alcuni margini più ampi per la diffusione di dati personali relativi a persone che godono di particolare notorietà (eventualmente anche in ambito locale), in ragione del ruolo o della funzione ricoperti. Questo diverso approccio opera solo quando l'informazione si riferisce al ruolo e alla vita pubblica di tali personaggi e non vengano diffuse informazioni relative a terzi. Tali principi, consolidatisi negli anni di applicazione del codice deontologico (artt. 10 e 11), sono stati ripresi nel documento del 6 maggio 2004, anche alla luce di quanto precisato dal Consiglio d'Europa (Dichiarazione del 12 febbraio 2004).

Questa "giurisprudenza" del Garante va ora misurata sulla recente sentenza della Corte europea dei diritti dell'uomo (von Hannover/Germania del 24 giugno 2004, citata nel par. 6.4) che si è pronunciata sulla controversa pubblicazione di una foto della principessa di Monaco ritratta in un momento della sua vita privata. La pronuncia conferma per un verso alcuni principi già espressi nella normativa italiana e ribaditi dal Garante in varie occasioni in merito ai presupposti di liceità per la raccolta (correttezza e trasparenza) e la diffusione delle fotografie nell'ambito di servizi giornalistici (tutela della dignità della persona; pertinenza e non eccedenza di eventuali dettagli fotografici). La decisione della Corte introduce però un'inedita distinzione tra trattamenti concernenti personaggi politici nell'esercizio delle loro funzioni e individui che, pur essendo figure pubbliche, non esercitano tali funzioni, invitando gli organi di informazione ad una maggiore cautela con riferimento alla diffusione di immagini e altri particolari che riguardano la vita privata di questi ultimi.

7.6. *Esercizio dei diritti e diritto all'oblio*

I diritti riconosciuti all'interessato dall'art. 7 del Codice trovano applicazione anche con riferimento ai trattamenti effettuati nell'ambito dell'attività giornalistica: al riguardo il Garante ha accolto due ricorsi presentati *ex* art. 145 del Codice in relazione a istanze di opposizione per motivi legittimi al trattamento rimaste insoddisfatte. La prima concerne la pubblicazione, da parte di un giornale locale, di dati idonei a rendere indirettamente identificabile una minore, vittima di reati sessuali

(*Provv*. 6 aprile 2004 sopra citato con cui, alla luce della speciale tutela accordata ai minori, è stato disposto il divieto di ulteriore trattamento dei dati). La seconda riguarda la ripetuta rievocazione, da parte di giornali a diffusione locale, di un episodio di grave aggressione subita in passato da una donna, ponendolo in connessione ad altri simili e più recenti fatti di cronaca. Il Garante, reputata fondata l'istanza dell'interessata, ha ritenuto ingiustificata la pubblicazione dei dati che la riguardavano (dati identificativi, residenza, particolari relativi allo stato di salute, fotografie) in ragione della loro eccedenza nonché dell'ampio lasso di tempo trascorso dall'episodio che aveva portato l'interessata all'attenzione della cronaca. L'Autorità ha così disposto il divieto di ulteriore trattamento dei dati della ricorrente e la cancellazione dei medesimi dalle pagine *web* delle relative testate giornalistiche (*Provv*. 15 aprile 2004).

Quest'ultima decisione ha riproposto la delicata tematica del cosiddetto "diritto all'oblio" su cui pure diversi quesiti, segnalazioni e reclami pervenuti al Garante hanno sollecitato un'ulteriore riflessione: in questo quadro giova ricordare le indicazioni contenute nel più volte citato documento del 6 maggio volte a sollecitare, da parte del giornalista, un'attenta ponderazione dell'essenzialità dell'informazione e del (rinnovato) interesse pubblico con riferimento a cronache di casi giudiziari risalenti nel tempo, con riguardo a persone condannate o assolte e, a maggior ragione, a soggetti estranei al processo rievocato (in questo senso possono segnalarsi alcuni accertamenti avviati dal Garante con riferimento a casi riproposti a distanza di tempo da una trasmissione televisiva).

Questo tema non può essere disgiunto dall'analisi dell'incidenza sul punto delle nuove tecnologie dell'informazione, in particolare nel caso di diffusione di informazioni tramite la rete Internet e conseguente utilizzo di motori di ricerca. Il nodo è venuto al pettine a proposito del ricorso proposto nei confronti dell'Autorità garante della concorrenza e del mercato cui si è già fatto cenno (v. par. 2.11).

8 Associazioni, movimenti politici e partiti

8.1. *Associazioni*

Con riferimento alle strutture associative, il trattamento dei dati personali non sensibili degli altri associati, o di soggetti che hanno contatti regolari con le associazioni, è consentito anche senza il consenso dell'interessato qualora riguardi il perseguimento di finalità lecite e sulla base di quanto previsto dall'atto costitutivo o dallo statuto dell'associazione, o in presenza di uno degli ulteriori presupposti di liceità previsti dalla normativa sul trattamento dei dati personali (ad es., per obblighi di legge o per esigenze di difesa in sede giudiziaria).

Sindacati, patronati e Caaf

Nell'ambito delle diverse iniziative dell'Autorità sul tema del trattamento di dati personali da parte delle realtà associative è da ricordare, tra l'altro, l'incontro avuto con i rappresentanti delle principali organizzazioni sindacali, e degli enti di patronato e dei "Centri autorizzati assistenza fiscale" (Caaf) ad essi collegati, finalizzato alla revisione dei testi di informativa e consenso inseriti nelle tessere di adesione al sindacato. I soggetti intervenuti hanno chiesto il supporto dell'Ufficio del Garante allo scopo di sciogliere alcuni nodi interpretativi circa l'applicazione delle norme del Codice, con particolare riferimento alla possibilità di adottare un'informativa semplificata e di trattare in alcuni casi (in presenza di idonee garanzie) i dati senza il consenso degli interessati.

Con riferimento al trattamento dei dati all'interno delle strutture territoriali in cui si articolano le organizzazioni sindacali, il Garante ha richiamato la novità introdotta dal Codice riguardo alla facoltà di designare gli incaricati non solo nominativamente, ma anche mediante atti di preposizione a specifiche funzioni interne o unità organizzative che effettuano particolari trattamenti di dati, nell'ambito e a cura di titolari di strutture organizzative complesse che abbiano però chiarito per iscritto quali trattamenti di dati possono essere effettuati presso le singole articolazioni.

L'Autorità ha inoltre confermato l'obbligo, per i sindacati e per gli enti cd. collaterali (patronati e Caaf) di adottare le misure minime di sicurezza previste dal Codice e dal disciplinare tecnico, incluso il Documento programmatico per la sicurezza.

CONI

L'Ufficio ha anche reso un parere in ordine alla possibilità per il CONI di richiedere ad un ente di promozione sportiva riconosciuto a livello nazionale i dati relativi agli iscritti delle società affiliate all'ente. In proposito, nel richiamare le previsioni in materia di trattamento dei dati personali degli aderenti da parte delle associazioni, si è precisato che i soggetti pubblici, quale è il CONI, non devono richiedere il consenso degli interessati per il trattamento di dati personali effettuato nello svolgimento delle proprie funzioni istituzionali (*Nota* 24 maggio 2004).

Consorzi

È peculiare il caso esaminato dall'Autorità, su richiesta di un consorzio al fine di fornire alcuni chiarimenti in merito alle modalità di trattamento di taluni dati personali: si trattava di informazioni relative alla denominazione e alla sede del macello e delle aziende dove è avvenuto l'ingrasso, da riportare nell'etichettatura cd. facoltativa delle carni bovine, la quale contiene informazioni ulteriori rispetto a quelle

obbligatoriamente prescritte, allo scopo di migliorare la trasparenza delle condizioni di produzione e di commercializzazione delle carni bovine. In proposito, l'Autorità ha fatto presente che l'adesione al consorzio da parte delle singole imprese era avvenuta su base contrattuale e che, pertanto, la diffusione dei dati riprodotti nelle etichette (facoltativi rispetto alla normativa, ma obbligatori per gli aderenti al consorzio) non richiede il consenso degli interessati in quanto necessaria per eseguire obblighi derivanti dal contratto (qui consortile) (art. 24, comma 1, lett. *b*), del Codice) (*Nota* 1° luglio 2004).

8.2. *Movimenti politici e propaganda elettorale*

Il Garante –specie in prossimità di tornate di consultazioni elettorali– ha analizzato diverse questioni legate al trattamento dei dati personali effettuato da partiti e singoli candidati nell'ambito della propaganda politica.

In particolare, con un provvedimento di carattere generale (*Provv.* 12 febbraio 2004, pubblicato in *G.U.* 24 febbraio 2004, n. 45 e riprodotto anche in *Documentazione* par. 38) adottato in vista delle elezioni europee ed amministrative indette per il 12 e 13 giugno 2004, l'Autorità ha indicato i casi in cui partiti, movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare dati personali a fini di propaganda informando gli interessati, ma senza richiedere il loro consenso, e i casi in cui, al contrario, il consenso è necessario.

In tale occasione il Garante ha sottolineato che si può prescindere dal consenso nelle ipotesi in cui i dati utilizzati siano estratti da registri, elenchi, atti o documenti detenuti da un soggetto pubblico e accessibili liberamente in base ad un'espressa disposizione di legge o di regolamento.

Il candidato o l'organismo politico, sia quando acquisisca direttamente i dati sia allorché si avvalga dei servizi offerti da un privato, rivestendo comunque la qualifica di "titolare del trattamento", ha l'onere di verificare che gli interessati siano stati adeguatamente informati e abbiano prestato un consenso idoneo, validamente espresso solo se manifestato specificamente e se è stata resa all'interessato una previa informativa.

A tal proposito, merita di essere altresì ricordato il più recente provvedimento del 12 ottobre 2004, relativo all'invio di messaggi a contenuto propagandistico effettuato da una società per conto di una formazione politica. In tal caso l'Autorità ha sottolineato che, anche se l'invio di messaggi è avvenuto a nome di quest'ultima ad opera di un terzo, è la formazione politica medesima che è, e rimane, titolare del trattamento in questione; ciò in quanto essa assume le decisioni di fondo su finalità e modalità del trattamento preordinato all'invio del messaggio propagandistico.

Alla luce di tale principio, il Garante ha quindi prescritto alla formazione politica, a nome della quale la società aveva inviato *e-mail* per finalità promozionali senza aver acquisito il previo consenso dell'interessato, di fornire un idoneo riscontro alle richieste presentate ai sensi degli artt. 7 ed 8 del Codice.

Il Garante è stato anche interpellato in ordine alla liceità dell'invio di messaggi di posta elettronica a fini di propaganda elettorale da parte di società concessionarie di pubblicità ad utenti che avevano invece precedentemente conferito il loro esplicito consenso a ricevere solo comunicazioni di carattere commerciale e informativo. A tal proposito è stato rilevato che l'inserzione di messaggi di propaganda, in particolare nelle *Newsletter* tematiche richieste da soggetti cui è stata fornita una specifica informativa collegata al solo fine commerciale, non permette di considerare autorizzata anche la propaganda politica elettorale, poiché ciò contrasterebbe

con le particolari garanzie che il Codice prevede in tema di posta elettronica, differenti da quelle previste per la propaganda cartacea basata sull'utilizzo di registri ed elenchi pubblici accessibili a chiunque. È comunque praticabile (in luogo dell'inserzione di messaggi di propaganda all'interno di *Newsletter* tematiche) richiedere agli abbonati una manifestazione integrativa del consenso basata su un supplemento di informativa riferito alla propaganda politico-elettorale (*Nota* 25 marzo 2004).

Sempre a tale riguardo, e in linea con il predetto orientamento, in una successiva nota è stato precisato che non è sostenibile un accostamento tra le inserzioni pubblicitarie su quotidiani acquistati in modo anonimo presso un'edicola e i contenuti dei messaggi inviati nominativamente ad indirizzi di posta elettronica ad utenti che abbiano ricevuto un'informativa specifica riguardante solo attività commerciali o specifiche attività informative che nulla hanno a che vedere con la sfera politico-elettorale (*Nota* 7 aprile 2004).

9 Attività economiche

9.1. *Trattamenti in ambito bancario e finanziario*

Accesso ai dati personali in ambito bancario

Gli strumenti di tutela offerti dal Codice vengono utilizzati sempre più ampiamente nel settore bancario e finanziario: una problematica ricorrente è rappresentata dal rapporto tra il diritto di accesso ai dati personali detenuti da istituti di credito, specificamente disciplinato dagli artt. 7 e seguenti del Codice, ed il (diverso) diritto di ottenere copia della documentazione relativa ad operazioni bancarie, riconosciuto dall'art. 119, comma 4, d.lg. n. 385/1993 (T.U. in materia bancaria e creditizia).

In proposito, rispondendo anche ad alcune segnalazioni pervenute, nonché, in particolare, ad un quesito della Banca d'Italia, l'Autorità ha confermato l'alterità delle due figure in quanto il diritto di accesso previsto dal Codice si riferisce solo ai dati personali e non agli atti o documenti che li contengono, diversamente dal diritto, accordato dal menzionato art. 119, comma 4, d.lg. n. 385/1993, in base al quale il cliente, o colui che gli succede a qualunque titolo o colui che subentra nell'amministrazione dei suoi beni, possono *"ottenere, a proprie spese, entro un congruo termine e comunque non oltre novanta giorni, copia della documentazione inerente a singole operazioni poste in essere negli ultimi dieci anni"* (*Nota* 6 agosto 2004).

Si è così ribadita la posizione consolidata dell'Autorità, precisando anche che il diritto di accesso ai dati personali comporta l'obbligo per il titolare del trattamento (in questi casi, le banche) di estrarre i dati e di trasporli, se vi è richiesta, su un supporto cartaceo o informatico, ma non l'obbligo di esibire o consegnare, anche in copia, gli atti e documenti che li contengono (a meno che risulti particolarmente difficoltosa l'estrazione dei dati dai medesimi atti o documenti e non sia parimenti possibile la loro trasmissione per via telematica: art. 10, comma 4, del Codice).

Il diritto di accesso riguarda, di norma, unicamente i dati riferiti all'interessato. Soltanto in casi particolari, nei quali risulti impossibile per la banca estrarre o trasporre singoli dati, può rendersi necessario far visionare o trasmettere, in tutto o in parte, atti o documenti che possono riguardare anche terzi: si tratta però di ipotesi eccezionali, ricorrenti solo quando i dati relativi al richiedente e ai terzi siano tra loro collegati in maniera tale che la scomposizione degli stessi o la privazione di alcuni elementi ne renderebbe incomprensibile la lettura (v. art. 10, comma 5, del Codice).

In base a tali disposizioni l'Autorità ha definito, ad esempio, il procedimento con il quale si è segnalata l'avvenuta consegna, da parte di un istituto di credito, della documentazione relativa ad estratti di un conto corrente, cointestato anche alla segnalante, agli eredi legittimi del genitore deceduto (contitolare di quel conto) che ne avevano fatto richiesta (*Nota* 24 marzo 2004).

Al di là dei più consueti rapporti di conto corrente, al diritto di accesso si fa ricorso anche in funzione prodromica a possibili azioni di responsabilità nei confronti degli istituti di credito: il Garante ha esaminato, ad esempio, il ricorso presentato da un cliente di una banca colpito da un'ingente perdita finanziaria dopo aver sottoscritto un investimento erroneamente reputato a basso rischio; il ricorrente intendeva accedere ai dati personali che lo riguardavano e, in particolare, a quelli contenuti nei documenti che ne evidenziavano obiettivi e propensione al rischio. Nel definire il procedimento, l'Autorità ha ribadito che il cliente può cono-

scere tutti i dati personali che lo riguardano detenuti da un istituto di credito e, in caso di operazioni finanziarie, può conoscere anche le informazioni eventualmente riportate nei documenti in cui sono indicati i rischi dell'investimento (*Provv*. 12 marzo 2004, v. *Newsletter* n. 209 del 5-25 aprile 2004). Come già riconosciuto in passato, le informazioni personali devono essere comunque comunicate in modo chiaro e intellegibile, fornendo altresì i criteri e i parametri per la comprensione dei codici eventualmente utilizzati.

Nella nozione di dato personale rientra *"ogni informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"* (art. 4, comma 1, lett. *b*), del Codice). Il Garante ha pertanto accolto un ricorso (*Provv*. 23 luglio 2004) avente ad oggetto l'accesso ai dati relativi alle registrazioni telefoniche degli ordini di negoziazione effettuati dal ricorrente, secondo le disposizioni di cui al regolamento Consob n. 11522/1998. Anche in tali fattispecie viene infatti effettuato un trattamento di dati personali (qui la voce del cliente) e sono pertanto proponibili le istanze *ex* art. 7 del Codice.

In ordine ai trattamenti effettuati da società emittenti carte di credito è stata poi esaminata una vicenda nella quale l'interessato aveva espressamente chiesto di conoscere anche i "criteri di selezione" adottati per valutare la richiesta della carta (*Provv*. del 10 giugno 2004); al riguardo l'Autorità ha sottolineato l'obbligo per il titolare del trattamento di comunicare all'interessato tutti i dati che lo riguardano, eventualmente detenuti anche in forma di punteggi negativi. Si sono ritenute inammissibili, invece, le richieste volte a conoscere alcune notizie attinenti a criteri organizzativi e gestionali del titolare del trattamento.

Accesso ai dati da parte di eredi dell'interessato

Un particolare profilo applicativo del diritto di accesso ai dati personali, che si presenta di frequente specialmente in ambito bancario e assicurativo, riguarda la possibilità che, nel caso di dati concernenti persone decedute, i diritti dell'interessato siano esercitati anche *"da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione"* (art. 9, comma 3, del Codice).

Si tratta di tematica delicata e complessa rispetto alla quale si è più volte richiamata la necessità di distinguere fra richieste, inammissibili dal punto di vista della protezione dei dati, volte ad ottenere specificamente e direttamente dati personali relativi a terzi (ad esempio, i nominativi dei beneficiari di contratti di assicurazione a favore di terzo o di destinatari di rimesse bancarie: v. già il *Provv*. 3 aprile 2002, in *Bollettino* n. 27 del 2002, p. 20 e ss.) ed istanze, fondate, dirette invece a conoscere dati e informazioni riferite al defunto: la banca è quindi tenuta a comunicare agli eredi in modo chiaro e comprensibile i dati relativi alla consistenza patrimoniale del defunto, a movimentazioni bancarie, saldi, depositi "al portatore", anche se estinti da terzi dopo la data del decesso, usando però l'accortezza di oscurare eventuali informazioni personali riferite a terzi (*Provv*. 20 maggio 2004; v. *Newsletter* 21-27 giugno 2004).

Nelle diverse decisioni assunte in tema di accesso, il Garante ha ribadito la natura essenzialmente gratuita dell'esercizio dei diritti previsti dall'art. 7 del Codice. Peraltro, la complessità e l'estensione di alcune richieste di accesso in ambito bancario, sottolineata da diversi titolari, potrebbe portare in futuro l'Autorità, all'esito di un'adeguata istruttoria, ad adottare un provvedimento generale in tema di eventuali contributi spese forfettari a carico dell'interessato (contributo che, secondo quanto disposto dall'art. 10, comma 8, del Codice e in base ad una previa decisione generale del Garante, può essere chiesto dal titolare del trattamento, ad esempio qualora il riscontro alle richieste di accesso degli interessati comporti un notevole impiego

di mezzi in relazione all'entità o complessità delle istanze o comunque sia fatta richiesta della riproduzione dei dati cui si richiede l'accesso su speciali supporti).

Profili di liceità e correttezza

Attenzione particolare merita di essere attribuita ad un fenomeno relativo a modalità improprie di comunicazione talora adottate da banche, società finanziarie o società di recupero crediti, e consistenti nel contattare telefonicamente soggetti terzi –ad esempio abitanti nello stesso stabile– affinché riferiscano agli interessati di rivolgersi all'istituto per comunicazioni urgenti che li riguardano.

Si tratta di modalità di comunicazione che possono risultare lesive della riservatezza e della dignità degli interessati; l'Autorità ha pertanto richiamato l'attenzione di alcune banche sulla necessità di conformare le operazioni di trattamento ai principi di liceità e correttezza (art. 11, comma 1, lett. *a*), del Codice). In applicazione di tali principi, non dovranno essere effettuate comunicazioni alla clientela (relative anche a semplici richieste a terzi di riferire all'interessato di contattare la banca) per il tramite di condomini dello stesso stabile o vicini di casa, recando peraltro disturbo alla tranquillità di soggetti estranei al rapporto tra la banca e l'interessato; le banche e le società interessate, inoltre, sono state invitate a fornire apposite istruzioni in tal senso alle proprie strutture e dipendenti (*Note* 30 marzo 2004 e 25 ottobre 2004).

In un altro caso, l'Autorità ha rilevato un trattamento non corretto di dati personali da parte di una banca e di una società finanziaria, in occasione dell'addebito della rimessa interbancaria diretta (Rid) su un conto corrente diverso da quello indicato dal segnalante nell'ambito di una operazione di finanziamento (*Nota* 28 settembre 2004). La società finanziaria aveva infatti comunicato all'istituto di credito i dati indicati dal segnalante per la domiciliazione del Rid in modo inesatto ed incompleto, non fornendo né il numero di conto corrente prescelto per l'addebito, né il nominativo del terzo effettivamente intestatario di tale conto corrente (coobbligato per lo stesso rapporto di finanziamento). La banca, pur rilevando un'incompletezza dei dati comunicati, ha poi autonomamente proceduto, senza interpellare l'interessato, a domiciliare il Rid su un altro conto corrente non indicato a tal fine (cointestato al segnalante e ad un suo familiare), salvo poi sospendere l'addebito delle somme a seguito delle contestazioni del cliente.

Anche in questo caso, l'Autorità ha richiamato l'attenzione delle due società sulla necessità di impartire adeguate istruzioni al personale incaricato del trattamento per ridurre la probabilità che si verifichino errori analoghi e, comunque, per assicurare il pieno rispetto dei principi sanciti dal Codice in tema di correttezza del trattamento, di esattezza e di completezza dei dati.

9.2. *Trattamenti effettuati nell'ambito dei sistemi di informazione creditizia*

Conclusisi i lunghi e complessi lavori per la redazione del codice di deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti, il testo preliminare del codice è stato dapprima sottoposto ad una consultazione pubblica e all'attenzione delle associazioni dei consumatori riunite nel Consiglio nazionale dei consumatori e utenti (Cncu) (recependone poi varie osservazioni) e, quindi, approvato dal Garante il 16 novembre 2004. Suscettibile di applicazione dal 1° gennaio 2005 (con d.m. 14 gennaio 2005 il Ministro della giustizia ha disposto l'allegazione al Codice), il codice è stato sottoscritto dalle associazioni rappresentative del settore creditizio e introduce un quadro articolato di garanzie per i soggetti che chiedono prestiti, mutui, dilazioni di pagamento, *leasing* e carte di credito.

Tra le novità, al di là della (significativa) nuova dizione –abbandonandosi la tradizionale denominazione *"centrali rischi private"* a vantaggio della locuzione *"sistemi di informazioni creditizie"* (Sic)–, merita segnalare le principali regole di comportamento che costituiscono condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali da parte delle società che li gestiscono e che li consultano (banche, società finanziarie e società di *leasing*), precisando che il codice deontologico non riguarda nella sua interezza i sistemi informativi gestiti da soggetti pubblici e, in particolare, il servizio di centralizzazione dei rischi gestito dalla Banca d'Italia (al quale continua ad applicarsi la specifica normativa di settore).

Per quanto riguarda, invece, il sistema centralizzato di rilevazione dei rischi di importo contenuto istituito con deliberazione Cicr del 3 maggio 1999 e attualmente gestito da Sia S.p.A. (Società interbancaria per l'automazione), relativo agli affidamenti di importo inferiore al limite minimo di censimento previsto per la Centrale della Banca d'Italia e superiore al limite massimo fissato per le operazioni di credito al consumo (cd."centralina"), con esclusione dei crediti in sofferenza, trovano applicazione, in quanto compatibili, alcuni principi stabiliti dal codice. Al riguardo, l'Autorità ha già avuto occasione di pronunciarsi precisando che quest'ultimo sistema (e il relativo trattamento di dati personali) non rientra nel campo di applicazione dell'art. 8, comma 2, lett. *d*), del Codice, per cui gli interessati possono esercitare i diritti di cui al precedente art. 7 (*Provv*. 27 luglio 2004).

Questi i principi basilari contenuti nel codice di deontologia:

- la fissazione delle finalità esclusive per le quali i sistemi di informazioni creditizie potranno essere utilizzati e consultati (tutela del credito e contenimento dei relativi rischi), con la contestuale preclusione del perseguimento di scopi ulteriori (ad esempio, relativi all'attività di *marketing* o ricerche di mercato);
- la precisazione delle categorie di dati che potranno essere trattate in questi sistemi; in particolare, si conferma la distinzione tra i sistemi, più diffusi, che registrano e forniscono informazioni su richieste e rapporti di finanziamento (ossia informazioni "di tipo positivo-negativo") e quelli che raccolgono solo dati "di tipo negativo", come i ritardi nei pagamenti (le cd. morosità) o situazioni più gravi di mancato rimborso del credito;
- la necessità di fornire idoneo preavviso al cliente prima di effettuare una segnalazione a contenuto negativo al sistema d'informazione creditizia;
- l'individuazione di precise regole per la segnalazione delle morosità;
- maggiore trasparenza nei confronti dei consumatori attraverso una completa informativa inserita in una modulistica più chiara: in allegato al codice deontologico vi è un modello unico per l'informativa –predisposto dal Garante ai sensi dell'art. 154, comma 1, lett. *c*), del Codice– basato su espressioni che aspirano ad essere chiare, semplici e di agevole comprensione, e che dovrà essere adottato da tutti gli operatori economici;
- la fissazione di tempi massimi di conservazione, distinti a seconda della natura della segnalazione effettuata. In particolare, per i dati di tipo "negativo": un anno per gli inadempimenti, poi regolarizzati, relativi a ritardi fino a due rate; due anni per ritardi superiori poi sanati; tre anni per inadempimenti non regolarizzati. Per i dati "positivi": ventiquattro mesi dalla cessazione del rapporto o dalla scadenza del contratto;
- la previsione che, in caso di ritardo nel fornire la risposta al consumatore che abbia esercitato il diritto d'accesso, la visualizzazione dei dati sia sospesa e che, in caso di controversie relative al rapporto sottostante la richiesta di finanziamento (riguardanti ad esempio inadempimenti del

venditore/fornitore dei beni o servizi oggetto del contratto), ne verrà fatta opportuna annotazione.

Tra i partecipanti ai sistemi non figurano le società di telefonia, che avevano iniziato a collaborare con le centrali rischi in termini che il Garante aveva già considerato illegittimi. Il principio è stato ribadito anche in un provvedimento a seguito di ricorso (v. *Newsletter* 20-26 dicembre 2004), nel quale è stato precisato che nei sistemi di informazioni creditizie (Sic) potranno figurare solo dati relativi al vero e proprio rischio creditizio e non informazioni relative a bollette telefoniche non pagate e contratti di telefonia.

Il bilanciamento di interessi

Il trattamento dei dati personali nei sistemi di informazione creditizia richiede, secondo le previsioni del Codice, il consenso libero e informato degli interessati (art. 23) o la sussistenza degli altri presupposti di liceità alternativi rispetto ad esso (art. 24).

In proposito, l'Autorità ha ritenuto opportuno dare attuazione all'istituto del bilanciamento di interessi (previsto all'art. 24, comma 1, lett. *g*), del Codice), individuando i casi in cui il predetto trattamento potrà avvenire anche a prescindere dal consenso dell'interessato ed al solo fine di perseguire i legittimi interessi del titolare del trattamento o dei terzi destinatari dei dati (*Provv*. 16 novembre 2004, in *Documentazione* par. 40).

Il provvedimento del Garante riguarda in particolare i trattamenti relativi a:

- ritardi nel pagamento di un credito (che possono essere conservati, a seconda dei casi, per dodici o ventiquattro mesi dalla loro regolarizzazione);
- rapporti di credito per i quali si sono verificati ritardi o inadempimenti non regolarizzati (che possono essere conservati per non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto, o comunque dalla data di cessazione del rapporto). In quest'ultimo caso, possono essere conservati ulteriormente anche i dati personali relativi ad informazioni creditizie di tipo positivo eventualmente presenti nel sistema informativo, anche se riferiti ad altri rapporti di credito riguardanti il medesimo interessato.

In questi casi, il trattamento dei dati personali da parte dei soggetti che gestiscono o consultano sistemi di informazioni creditizie, è lecito ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, anche in assenza del consenso degli interessati.

Dati provenienti da fonti pubbliche

Secondo un principio recepito anche nel nuovo codice di deontologia, i dati trattati nell'ambito dei sistemi di informazioni creditizie devono essere in ogni caso di tipo obiettivo, strettamente pertinenti e non eccedenti rispetto alle finalità perseguite, oltre che relativi ad una richiesta/rapporto di credito. Non è sufficiente, a tal riguardo, che le informazioni vengano acquisite da fonti pubbliche (che comunque, se registrate, dovranno figurare in banche dati separate dal sistema di informazioni creditizie).

Al riguardo, si segnala un ricorso presentato da un cittadino relativamente alla mancata cancellazione, da parte del gestore del sistema di informazioni creditizie, di dati personali relativi alla trascrizione di una sentenza di divisione ereditaria e contenuti nella banca dati denominata "Atti pubblici". Il gestore giustificava il proprio diniego adducendo la perfetta coincidenza tra le informazioni censite nella propria banca dati e quelle risultanti dalla conservatoria dalla quale erano tratte, non ritenendo quindi di poter procedere alla cancellazione perché si era limitato a *"veicolare quanto contenuto nelle banche dati pubbliche consultate"* (*Provv*. 18 ottobre 2004). L'Autorità ha ritenuto il ricorso fondato in quanto, pur non contestandosi l'esattezza dell'informazione, il suo inserimento in una banca dati relativa a "dati pregiudizievoli" ha dato luogo ad un trattamento non corretto ai sensi dell'art. 11, comma 1,

lett. *a*), del Codice, per il fatto di aver descritto arbitrariamente come dato negativo un'informazione neutra quale quella connessa ad un'ordinaria operazione di scioglimento di una comunione ereditaria.

È stato al contrario ritenuto lecito il trattamento relativo ad un pignoramento immobiliare in quanto l'informazione, ancora presente nel pubblico registro dal quale era stata tratta, risultava pertinente e necessaria, trovando applicazione nel caso di specie la disposizione del Codice per cui, nel caso di informazioni provenienti da pubblici registri, i soggetti privati possono effettuare il relativo trattamento anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*), *Provv*. 29 aprile 2004).

Contributo spese

Nel quadro dei lavori relativi ai sistemi di informazione creditizia l'Autorità ha poi adottato il 23 dicembre 2004 una prima deliberazione di applicazione dell'art. 10, comma 8, del Codice, per il solo 2005, su istanza di una società che ha chiesto di riconoscere la facoltà di esigere dagli interessati un contributo spese per l'esercizio di alcuni diritti, in relazione alla situazione straordinaria che, presso quella società (Crif S.p.A.), si è temporaneamente determinata in ragione del notevole impiego di mezzi connessi alla complessità ed entità delle ricerche conseguenti alla richieste (*Deliberazione* 23 dicembre 2004, n. 15).

9.3. *Archivio degli assegni bancari e postali e delle carte di pagamento irregolari*

Anche il contenzioso relativo alle segnalazioni effettuate da soggetti pubblici (autorità giudiziaria e Ministero dell'interno) e privati (banche, uffici postali, società emittenti carte di credito) all'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (Cai-Centrale d'allarme interbancaria) ha registrato un notevole incremento, con la proposizione di numerosi ricorsi da parte di privati cittadini concernenti la mancata cancellazione o rettifica dei dati.

Come ricordato nelle precedenti relazioni, l'archivio risponde alla finalità di interesse generale di assicurare il regolare funzionamento del sistema dei pagamenti e in esso vengono segnalati i provvedimenti o le segnalazioni riguardanti persone che hanno emesso assegni senza autorizzazione o provvista, titolari di carte di pagamento revocate (per mancato pagamento o costituzione di fondi), nonché assegni o carte di pagamento sottratti, smarriti o bloccati. Gli enti che effettuano tali segnalazioni vi sono obbligati da precise norme di legge (v. legge 15 dicembre 1990, n. 386, legge 25 giugno 199, n. 205, d.lg. 30 dicembre 1999, n. 507) che non consentono ai segnalanti alcuno spazio di valutazione personale.

Con alcune decisioni il Garante ha esaminato taluni profili relativi al trattamento dei dati effettuato presso tale archivio, riconoscendo la possibilità di esercitare il complesso dei diritti previsti dall'art. 7 del Codice sia nei confronti degli intermediari segnalanti sia della Banca d'Italia, soggetti che agiscono entrambi in qualità di titolari dei trattamenti rispettivamente effettuati (*Provv*. 27 settembre 2004 e 4 ottobre 2004).

L'Autorità ha altresì dichiarato l'infondatezza di diverse richieste volte ad ottenere la cancellazione di alcuni dati personali dall'archivio Cai relativi alla revoca di carte di credito o dell'autorizzazione ad emettere assegni, in quanto tali segnalazioni risultavano essere state effettuate nel rispetto della vigente normativa che disciplina il funzionamento del Cai (art. 10-*bis*, l. n. 386/1990; v. *Provv*. 4 e 12 ottobre 2004).

Anche un pagamento tardivo ritenuto satisfattivo dal creditore, ma non documentato nelle forme puntualmente previste dalla legge (art. 8, l. n. 386/1990), deve essere infatti segnalato nell'archivio una volta decorso il termine di legge indicato nel preavviso di revoca dell'autorizzazione ad emettere assegni a causa del mancato

pagamento per difetto di provvista. Resta in ogni caso salva, per effetto del Codice, la possibilità per gli interessati di richiedere ed ottenere la rettifica della segnalazione a loro carico, allorché siano in grado di dimostrare l'avvenuto pagamento nelle forme idonee, attraverso, ad esempio, un'integrazione della documentazione richiesta dalla legge (*Provv.* 4 ottobre 2004).

In applicazione di questi principi, è stato ritenuto fondato il ricorso di un imprenditore che era stato privato dell'autorizzazione ad emettere assegni per non essere riuscito a dimostrare alla banca, seguendo le prescritte formalità, di aver pagato un assegno. L'Autorità, pur riconoscendo la sussistenza dei presupposti per l'inserimento del nominativo dell'imprenditore nell'archivio informatizzato, ha tuttavia ordinato la cancellazione dei dati inseriti nell'archivio, in quanto gli stessi documentavano una situazione non più corrispondente alla realtà: l'interessato figurava infatti come un soggetto che non aveva provveduto al pagamento, neppure tardivo, dell'assegno, mentre lo stesso era stato effettuato per intero, anche se la documentazione in grado di dimostrarlo non era stata inizialmente accettata e, infine, era giunta con lieve ritardo (*Provv.* 27 settembre 2004). Non si è ritenuta, quindi, giustificata la tesi sostenuta dai titolari del trattamento di dover conservare i dati nella Cai per il periodo di efficacia del provvedimento di revoca dell'autorizzazione ad emettere assegni (sei mesi) sulla base di un regolamento (d.m. n. 458/2001), normativa peraltro di rango secondario rispetto al Codice, che disciplina in termini generali la conservazione dei dati.

9.4. *Trattamenti in ambito assicurativo*

Accesso alle perizie medico-legali

Nel contesto assicurativo il tema delle perizie medico-legali è da tempo al centro di un intenso contenzioso e continua ad essere oggetto di numerose decisioni del Garante.

La questione dell'accesso ai dati personali contenuti in perizie medico-legali redatte da professionisti incaricati dalle compagnie assicurative di stimare i danni denunciati dagli assicurati –rispetto alla quale in passato si erano registrate alcune difformità di posizioni tra Garante e taluna giurisprudenza di merito– è ora oggetto di una apposita e dettagliata disposizione del Codice (art. 8, comma 4) in base alla quale *"l'esercizio dei diritti di cui all'art. 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento"*.

In alcune decisioni su ricorsi, il Garante ha ricordato che, come molti altri documenti, anche le perizie medico-legali in ambito assicurativo contengono di regola dati personali del paziente interessato, sia nella parte nella quale sono riportati dati identificativi dello stesso, nonché riscontri di visite mediche e dei cd. esami obiettivi, sia all'interno della parte che comprende valutazioni e giudizi del perito fiduciario. Informazioni personali riferite all'interessato possono essere ugualmente presenti nelle relazioni investigative eventualmente predisposte su incarico delle imprese di assicurazione. Si tratta infatti di informazioni comunque relative all'interessato che devono essere considerate "dati personali" ai sensi dell'art. 4, comma 1, lett. *d*), del Codice.

È possibile comunque che il titolare del trattamento invochi il temporaneo differimento dell'esercizio dei diritti di cui all'art. 7 del Codice, per il solo periodo durante il quale potrebbe derivarne un pregiudizio per lo svolgimento di cd. "inda-

gini difensive" o, più in generale, per far valere o difendere un diritto in sede giudiziaria (art. 8, comma 2, lett. *e*) del Codice); la valutazione dell'esistenza del pregiudizio deve essere effettuata caso per caso e sulla base di elementi concreti. Cessate tali circostanze, il diritto di accesso ai dati personali può essere nuovamente esercitato (*Provv*. 19 aprile 2004).

Per quanto riguarda le modalità del riscontro alle richieste di accesso relative ai dati inerenti allo stato di salute, contenuti nella perizia medico-legale, esso deve essere fornito direttamente agli interessati (a differenza di quanto previsto dalla normativa precedente, in base alla quale il riscontro doveva invece provenire da un medico di fiducia designato dal titolare o dall'interessato: v. l'art. 23, comma 2, della legge n. 675/1996, abrogato). L'art. 84 del Codice prevede ora l'obbligo del loro inoltro per il tramite del medico di fiducia solo a carico di esercenti le professioni sanitarie e di organismi sanitari.

Liceità e correttezza del trattamento in ambito assicurativo

Sempre in ambito assicurativo, ulteriori interventi dell'Autorità hanno riguardato alcuni profili relativi al trattamento di dati sensibili degli assicurati o di terzi.

In particolare, valutando la modulistica predisposta da una compagnia assicurativa, è stato affrontato il profilo dell'informativa. In tale occasione, il Garante, oltre a ribadire che la disciplina sulla protezione dei dati personali rende comunque necessaria la raccolta da parte dell'impresa di assicurazione del consenso scritto dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute (v. art. 26, del Codice, nonché le autorizzazioni del Garante nn. 2 e 5 del 2004), ha richiamato l'attenzione della società sulla necessità che il modello di informativa sottoposto ai clienti, e più in generale agli interessati, specifichi con chiarezza le caratteristiche del trattamento. In particolare, anche in considerazione del fatto che il consenso dell'interessato deve essere prestato *"specificamente in riferimento ad un trattamento chiaramente individuato"* (art. 23, comma 3, del Codice), l'informativa deve contenere un'indicazione puntuale e non esemplificativa dei titolari in favore dei quali il consenso potrebbe valere, eventualmente allegando un elenco, nonché delle principali caratteristiche degli ulteriori trattamenti effettuati (finalità, modalità e ambito di comunicazione dei dati).

La società è stata inoltre invitata a valutare la praticabilità di una designazione del professionista che effettua le visite medico-legali su incarico della stessa, in qualità di "responsabile del trattamento" ai sensi dell'art. 29 del Codice, specificando analiticamente per iscritto i compiti e le istruzioni cui attenersi. In tal modo il professionista potrebbe rendere l'informativa all'interessato precisando che i dati rientreranno nell'ambito del più generale trattamento effettuato dall'impresa di assicurazioni. In mancanza di tale designazione il professionista deve essere considerato un autonomo titolare del trattamento, anche relativamente ai dati sensibili rilevati nel contesto della visita medico-legale, e deve pertanto effettuare una autonoma informativa all'interessato e riceverne il consenso formulato per iscritto.

L'Autorità ha esaminato, inoltre, una segnalazione relativa ad un contratto di assicurazione riguardante il rimborso della penale prevista per l'annullamento di un viaggio; nel caso di specie, la compagnia di assicurazioni non ha proceduto al rimborso perché non ha reputato sufficiente il certificato medico inviato dal segnalante e riferito ad un congiunto impossibilitato a partecipare al viaggio, richiedendo, invece, copia della cartella clinica attestante la ragione dell'addotta impossibilità.

In tale occasione, il Garante non ha ritenuto ammissibile l'acquisizione, da parte del segnalante o di altri soggetti (la compagnia assicuratrice), della cartella clinica detenuta dalla struttura ospedaliera presso cui la persona interessata era stata ricove-

9

rata. Si è infatti rilevato che, quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il medesimo è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale o inviolabile (art. 60 del Codice; si vedano anche i chiarimenti sul concetto di "diritto di pari rango" forniti dal Garante con provvedimento del 9 luglio 2003, con cui è stato precisato che, quantomeno "nella prevalenza dei casi", i diritti di credito non rientrano tra i "diritti di rango almeno pari" a quello della persona cui si riferiscono i dati).

Preso atto che il diritto fatto valere dal segnalante nei confronti della società assicuratrice aveva natura di mero diritto di credito (rimborso della penale pagata al *tour operator* in seguito all'annullamento del viaggio), l'Autorità ha concluso per l'impossibilità per la struttura ospedaliera di accogliere una sua eventuale richiesta di ottenere, a scopo di tutela di tale diritto, un accesso ai dati sanitari contenuti nella cartella clinica del terzo ricoverato.

Già in precedenti occasioni il Garante aveva considerato giustificati i trattamenti di dati relativi alla salute degli assicurati effettuati da imprese di assicurazione al fine della gestione e dell'esecuzione di polizze infortuni e malattie, previa acquisizione del consenso scritto dell'interessato (nel caso di specie, peraltro, estraneo al contratto). Tra questi trattamenti può rientrare anche la raccolta di dati sanitari contenuti in cartelle cliniche degli assicurati, quando tali dati siano strettamente necessari per fornire le specifiche prestazioni richieste dagli interessati con questa tipologia di contratti, in relazione –ad esempio– ad attività di accertamento dei sinistri denunciati e di rimborso delle spese mediche sostenute dall'assicurato (cfr. *Provv*. 12 aprile 1999, in *Bollettino* n. 8 del 1999, p. 42).

È stato sottolineato, anzi, che anche per il trattamento dei dati contenuti nella certificazione sanitaria già inviata dal segnalante la società assicuratrice avrebbe dovuto comunque acquisire il consenso scritto della persona interessata. Inoltre, la raccolta ed il trattamento dei dati sanitari devono comunque essere effettuati in conformità ai principi di indispensabilità, di pertinenza e di non eccedenza dei dati rispetto alle finalità perseguite (v. l'art. 11 del Codice) oltre che ai requisiti indicati dalle citate autorizzazioni generali, con particolare riguardo alla stretta necessità per la società di assicurazione di acquisire copia integrale di una cartella clinica ai fini della liquidazione di un sinistro. L'acquisizione dell'intera cartella clinica può infatti rivelarsi non rispettosa dei principi ora richiamati poiché tale documento, insieme ad elementi strettamente necessari ai fini delle verifiche effettuate dall'impresa di assicurazione per procedere al rimborso (riguardo, ad esempio, ad informazioni che permettono di stabilire la natura della malattia), contiene ulteriori dati di carattere sanitario che possono non avere alcuna rilevanza ai fini delle suddette verifiche e che devono essere quindi omesse.

Oltre ad aver rilasciato nuove autorizzazioni generali, alcune delle quali di diretto rilievo per il settore assicurativo (v. in particolare le autorizzazioni nn. 2 e 5 del 2004), il Garante ha autorizzato con un provvedimento *ad hoc* una società cooperativa di assicurazioni che ne aveva fatto richiesta, a trattare i dati relativi alla convinzione religiosa dei propri soci (*Newsletter* 4-10 ottobre 2004). L'autorizzazione riguarda i dati e le operazioni strettamente indispensabili per l'applicazione di una specifica norma dello statuto della compagnia di assicurazioni, alle stesse condizioni previste dalla citata autorizzazione generale n. 5/2004 (che la società deve già rispettare per il trattamento degli altri dati personali dei propri assicurati).

Nell'accogliere la richiesta dell'assicurazione, il Garante ha tenuto conto anche dello scopo mutualistico della società che offre ai propri soci contratti di assicura-

zione a condizioni economiche particolari. La società cooperativa di assicurazioni si trova, secondo quanto stabilito dallo statuto, nella condizione di raccogliere e conservare anche dati dei soci che dichiarano di professare la religione cattolica e manifestano sentimenti di adesione alle opere cattoliche. A differenza degli altri clienti, tali soci possono essere assicurati a particolari condizioni di favore.

Nel caso in esame, l'intervento specifico a tutela del dato "religioso" dei soci si è reso necessario, non essendo prevista nelle autorizzazioni generali una disposizione che regoli espressamente il trattamento di questo tipo di informazioni da parte delle imprese di assicurazioni.

9.5. Marketing

Il settore del *marketing* è stato oggetto di costante attenzione da parte del Garante, in special modo a seguito dei numerosi ricorsi, segnalazioni e reclami relativi ad episodi di ricezione di lettere, telefonate, fax ed altre comunicazioni indesiderate effettuate da operatori del settore.

Una parte cospicua del contenzioso ha riguardato, ad esempio, l'invio di corrispondenza pubblicitaria relativa a proposte di abbonamento a riviste o all'acquisito di alcuni prodotti editoriali.

In proposito, il Garante ha valutato il ricorso di un cittadino che, avendo ricevuto un invito ad abbonarsi ad una rivista pubblicata da una casa editrice italiana (tra l'altro in collaborazione con un editore straniero), non aveva ricevuto riscontro alla richiesta di sapere in che modo la società avesse ottenuto i suoi dati personali, con quali modalità essi venissero utilizzati e per quali scopi. L'Autorità ha pertanto ordinato alla casa editrice di dare completo riscontro alle richieste del ricorrente (*Provv*. 25 maggio 2004; v. *Newsletter* 21-27 giugno 2004).

L'Autorità ha altresì avviato accertamenti nei confronti di una società che offre alcuni servizi aggiuntivi ai clienti che si registrano nel proprio sito *web*. Il Garante, in particolare, intende accertare se gli utenti, al momento della registrazione *on-line*, ricevano un'informativa idonea e se il consenso, che la società chiede di manifestare obbligatoriamente, sia espresso liberamente dagli utenti; ulteriore profilo che l'Autorità intende valutare è se il consenso richiesto faccia riferimento ad un trattamento ben individuato di dati personali o sia, invece, un consenso "*omnibus*" che autorizzi anche l'invio di materiale pubblicitario, vendita diretta, ricerche di mercato o comunicazioni commerciali.

Al vaglio del Garante è altresì la prassi, ormai diffusa fra gli istituti bancari, di raccogliere e trattare dati personali ai fini di *marketing* diretto per la promozione di carte di credito. In merito a tale vicenda l'Autorità ha compiuto accertamenti sulle modalità dei trattamenti effettuati, al fine di verificare la loro conformità al Codice. In particolare, sono state acquisite notizie sull'adempimento degli obblighi di informativa e la raccolta dell'eventuale consenso dell'interessato, nonché sull'origine dei dati personali utilizzati per la promozione delle predette carte.

Al riguardo, tenuto conto della tendenza degli operatori commerciali ad attingere dati personali da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per intraprendere operazioni di *marketing*, il Garante ha ribadito nuovamente, nell'ambito dei menzionati accertamenti, il divieto dell'ulteriore utilizzo per finalità pubblicitarie dei dati estratti dalle liste elettorali, in relazione a quanto previsto dall'art. 177, comma 5 del Codice (che ha modificato l'art. 51 del d.P.R. n. 223/1967). Alla luce di tale quadro legislativo, infatti, le liste elettorali, pur avendo natura di elenchi pubblici, non possono essere più utilizzate da terzi per scopi commerciali o

pubblicitari, a differenza della previgente disciplina che consentiva a chiunque di copiare, stampare o mettere in vendita tali liste.

Con parere del 15 luglio 2004, l'Autorità ha inoltre stabilito che a partire dalla seconda metà del 2005 non potranno più essere adoperati i nominativi contenuti negli elenchi telefonici per realizzare operazioni di *marketing* diretto nei confronti di chi non lo abbia espressamente consentito. Sono state così individuate le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati (ed ai titolari di carte prepagate) negli elenchi cartacei o elettronici disponibili al pubblico, anche con riferimento al diritto dell'interessato di decidere se ricevere o meno pubblicità per corrispondenza o per telefono. Infatti, sarà possibile inviare pubblicità soltanto a chi avrà scelto liberamente, in forma specifica e documentata per iscritto (tramite la compilazione del modello messo a punto dal Garante ed allegato al provvedimento menzionato), di ricevere informazioni commerciali o promozionali; la scelta da parte dell'utente di voler ricevere tali comunicazioni sarà evidenziata da un simbolo associato, a seconda dei casi, all'indirizzo e/o al numero telefonico (cfr. ulteriori considerazioni in merito nel par. 15.3).

L'attività dell'Autorità nella tematica in questione ha riguardato anche l'illecito utilizzo, per finalità pubblicitarie, di fax inviati da altri Stati dell'Unione europea. Grazie ad un sistema di cooperazione tra le istituzioni competenti nei vari stati membri, il quale prevede una procedura di trasmissione delle segnalazioni e dei reclami riguardanti la possibile violazione dell'art. 13 della direttiva 2002/58/CE, è stato possibile intervenire, per il tramite della omologa autorità britannica, anche nei confronti di una società che effettuava dal Regno Unito un invio massivo di fax pubblicitari nel nostro paese.

Infine, nel più ampio contesto dell'autoregolamentazione promossa dall'Autorità, particolare rilevanza riveste per il settore in esame la definizione del codice di deontologia relativo al trattamento dei dati personali a scopo di *marketing* diretto e di invio di materiale pubblicitario, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale. Il codice dovrà tra l'altro prevedere, anche per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale opposizione all'invio di determinate comunicazioni commerciali.

Sono già pervenute all'Autorità alcune richieste di partecipazione ai prossimi lavori preparatori per l'adozione del predetto codice. Il Garante sta valutando tali richieste al fine di individuare i soggetti rappresentativi del settore in esame che prenderanno parte ai lavori.

9.6. *Carte di fidelizzazione*

Già in passato l'Autorità è stata chiamata a pronunciarsi sul tema delle cd. "carte di fedeltà" o tessere di "fidelizzazione" della clientela: si tratta di tessere, spesso rilasciate gratuitamente presso punti di vendita, centri o esercizi commerciali, che consentono ai consumatori di usufruire di sconti o premi. Il rilascio delle predette carte è di regola subordinato alla compilazione di questionari sulle abitudini e le scelte di consumo dei clienti e delle loro famiglie e alla raccolta di ulteriori dati personali in ordine ai volumi di spesa e alle tipologie di prodotti acquistati dal consumatore al fine di consentire alle società titolari del trattamento di compiere operazione di cd. profilazione della clientela. Dalla documentazione acquisita è emerso che spesso gli interessati non hanno una piena consapevolezza di tali operazioni e dei rischi implicati, in quanto non ricevono preventivamente idonee informazioni sulle caratteristi-

che del trattamento dei dati che si accingono a fornire e sugli strumenti posti a difesa dei loro diritti.

L'Autorità ha ritenuto opportuno avviare una consultazione pubblica sul tema volta ad acquisire ulteriori elementi di informazione e documentazione da parte degli operatori dei settori della grande distribuzione e del *marketing*, degli organismi rappresentativi degli operatori dei predetti settori, delle associazioni dei consumatori e di ogni altro soggetto interessato. I quesiti che hanno formato oggetto della consultazione hanno riguardato in particolare: l'individuazione delle prassi seguite in sede di rilascio delle carte, con particolare riferimento alla (necessaria) richiesta del consenso della clientela al trattamento dei dati per la fruizione di benefici di varia natura (premi, sconti o buoni, speditezza e dilazione nei pagamenti ecc.); le modalità e finalità del trattamento dei dati dei clienti e l'individuazione della loro tipologia; gli adempimenti degli obblighi di informativa e consenso; l'eventuale uso in tale ambito delle tecniche di profilazione e classificazione della clientela; i tempi di conservazione delle informazioni raccolte; le misure adottate per agevolare l'esercizio dei diritti degli interessati, nonché l'ambito di comunicazione di tali dati.

9.7. *Flussi transfrontalieri*

Il trasferimento all'estero di dati personali da parte di una società o di una pubblica amministrazione è consentito dalla normativa comunitaria ed italiana solo se il livello di protezione garantito dal Paese di destinazione è adeguato. Si possono, invece, trasferire i dati verso Paesi che non garantiscono tale livello di protezione solo con il consenso degli interessati o sulla base di altri presupposti di liceità indicati all'art. 43 del Codice (esecuzione di obblighi derivanti da un contratto di cui è parte l'interessato, esigenza di salvaguardia della vita e dell'incolumità di un terzo, investigazioni difensive ecc.) oppure con l'autorizzazione del Garante. Al di fuori di questi casi il trasferimento verso Paesi terzi di dati personali è vietato.

Questi principi sono stati ribaditi anche in occasione di una richiesta di intervento urgente del Garante, trasmessa da alcune associazioni a tutela dei diritti dei consumatori, relativamente al trasferimento in Argentina di dati personali di soggetti intestatari di titoli obbligazionari (nell'ambito di una Offerta pubblica di scambio volontaria promossa dalla Repubblica Argentina). Si è precisato, in particolare, che il trasferimento dei dati personali degli investitori che intendono aderire all'offerta della Repubblica Argentina –paese che la Commissione europea ritiene fornisca un adeguato livello di tutela dei dati personali (Decisione 30 giugno 2003, in *G.U.C.E.* 5 luglio 2003)– è lecito solo se necessario per l'esecuzione di obblighi contrattuali o in presenza di uno specifico consenso informato che individui le istituzioni argentine come destinatarie dei dati (art. 43 del Codice).

L'Autorità, a seguito dell'esame della documentazione relativa alla predetta operazione, ha ritenuto che il trasferimento di dati personali degli investitori sia consentito solo in base ai requisiti sopra indicati, fermo restando che i dati, una volta trasferiti, potranno essere poi utilizzati soltanto per le finalità specificate nel rapporto contrattuale (e che potranno essere trasferiti, altresì, solo i dati pertinenti e non eccedenti rispetto a tale rapporto).

Il Garante ha svolto un attento monitoraggio in relazione ad operazioni di "esportazioni" di dati da parte di operatori italiani e al tipo di garanzie e strumenti adottati per tutelare i diritti degli interessati. Nel 2004 è stata portata a conclusione l'indagine (v. *Relazione 2003*, p. 96) presso cinquanta tra le principali società e gruppi industriali che operano in Italia, incentrata sull'analisi dei presupposti, delle

finalità e modalità del trasferimento di dati all'estero, delle categorie di dati trasferiti e delle persone interessate (cittadini, lavoratori, professionisti, imprenditori ed altre società), delle attività dei soggetti importatori, nonché degli strumenti utilizzati per la tutela dei dati personali in rapporto a ciascuna tipologia di trasferimento.

Dall'indagine svolta è emerso che l'oggetto prevalente dei trasferimenti di dati all'estero effettuati dalle società è rappresentato dai dati personali dei dipendenti ed in misura minore, ma sempre rilevante, dalle informazioni relative a clienti, società concorrenti e fornitori. Di regola i flussi di dati sono effettuati dopo aver acquisito lo specifico consenso degli interessati. In alcune limitate ipotesi, quando la gestione delle risorse umane avviene negli Stati Uniti, le società che "importano" i dati personali hanno aderito all'accordo del cosiddetto "*Safe Harbor*". È emersa, inoltre, una diffusa tendenza a predisporre contratti, anche "multilaterali" nel caso di gruppi societari, da sottoporre al parere preventivo del Garante, e a fare uso delle clausole contrattuali *standard* indicate dalla Commissione europea (cfr. *Newsletter* 17 maggio 2004).

Nel corso del 2004 si è assistito, altresì, ad un aumento di richieste di pareri ed informazioni da parte di imprese e gruppi societari, operanti a livello internazionale, in merito alla corretta applicazione della normativa in materia di trasferimento dei dati personali.

In particolare, è attualmente all'esame dell'Autorità una richiesta di parere relativa ad un sistema informativo costituito da una banca dati elettronica e centralizzata –allo stato non più aggiornata, in attesa di verificare appunto la compatibilità del sistema con la normativa sulla protezione dei dati personali– la cui gestione e manutenzione è affidata ad una società che ha sede nel Regno Unito e nella quale confluiscono informazioni trasmesse da istituti di credito, relative a presunte condotte fraudolente tenute da esercenti commerciali convenzionati con un circuito internazionale.

Il *server* che ospita la predetta banca dati è fisicamente collocato al di fuori dell'Ue, in particolare negli Stati Uniti, mentre la consultazione del sistema da parte degli istituti di credito aderenti al circuito avviene su base nazionale.

Da una prima analisi dei quesiti formulati dalla società richiedente, l'Autorità ha potuto rilevare che il trattamento di dati personali effettuato da parte di quest'ultima nell'ambito del sistema descritto potrebbe non essere soggetto alla normativa italiana sulla protezione dei dati personali, trattandosi di un sistema gestito direttamente da un titolare del trattamento stabilito fuori dal territorio dello Stato. In tal caso, infatti, in base al principio di stabilimento previsto dal Codice (art. 5), il trattamento dei dati non ricadrebbe nell'ambito di applicazione della legge italiana. Per quanto riguarda, invece, la trasmissione dei dati al sistema da parte degli istituti bancari italiani, nonché il successivo trasferimento degli stessi al *database* situato negli Usa, il Garante si è riservato di esaminare i profili inerenti la materia di trasferimento dei relativi dati personali all'estero al fine di individuare la disciplina applicabile.

Sempre nel settore dei flussi transfrontalieri di dati riguardanti presunte condotte irregolari connesse all'uso di carte di credito, il Garante ha partecipato attivamente ad un gruppo di lavoro istituito presso il *Working Group* di cui all'art. 29 della direttiva 95/46/CE, insieme a rappresentanti di altre autorità nazionali di protezione dei dati, della Commissione europea, e dell'industria delle carte di credito, con l'obiettivo di individuare alcune linee-guida affinché questi flussi di dati –talvolta limitati all'interno dello spazio comune europeo, talaltra invece su base globale– avvengano nel rispetto dei diritti e delle libertà delle persone interessate. Il documento, in versione non ancora definitiva, è adesso al vaglio del *Working Group* che dovrà tenere conto delle osservazioni formulate in merito da alcune autorità nazionali (tra queste, il Garante).

Sono inoltre giunte all'attenzione dell'Autorità alcune richieste di autorizzazione al trasferimento dei dati all'estero da parte di società di revisione contabile che, in base alla normativa di settore vigente negli Usa (in particolare il recente *Sarbanes-Oxley Act*), per svolgere prestazioni professionali a favore di società quotate nei listini americani sono tenute a registrarsi presso un apposito elenco, detenuto da un organismo americano istituito per monitorare le società che operano nel mercato finanziario. Le società richiedenti hanno infatti evidenziato che, ai fini della relativa registrazione, devono raccogliere e trasmettere all'organismo menzionato informazioni personali relative alle stesse società, ai soci e ai dipendenti, nonché ai consulenti che assistono le società di revisione nello svolgimento dei relativi incarichi. Tali informazioni, peraltro, includono dati giudiziari e fanno altresì riferimento a procedimenti civili, amministrativi e disciplinari o arbitrati in cui sono stati coinvolti i predetti soggetti.

Al riguardo, il Garante sta valutando se siano applicabili al caso descritto i presupposti di liceità richiesti dall'art. 43 del Codice e, più in generale, la compatibilità di tali trattamenti di dati con la normativa italiana e comunitaria.

Con riferimento all'attività svolta dall'Autorità al fine di dare attuazione ad alcune decisioni comunitarie relative al settore in esame, come anticipato nella *Relazione 2003*, è in procinto di essere resa operativa in Italia anche la decisione della Commissione europea n. 2003/490/CE del 30 giugno 2003, pubblicata sulla *G.U.C.E.* L 168 del 5 luglio 2003, riguardante l'adeguatezza del livello di tutela dei dati personali esistente in Argentina. Va specificato, inoltre, che il 28 aprile 2004 la Commissione europea, con decisione 2004/411/CE, ha stabilito che il livello di protezione dei dati personali esistente nell'Isola di Man, su cui si era già espresso in senso favorevole, con il parere n. 6 del 21 novembre 2003, il Gruppo art. 29, è parimenti "adeguato" ai fini del trasferimento di dati personali dall'Ue verso soggetti ivi residenti. È, infine, in fase di pubblicazione sulla Gazzetta Ufficiale la deliberazione con la quale il Garante ha dato attuazione alla Decisione comunitaria del 21 novembre 2003, n. 2003/821/CE recante il riconoscimento del Baliato del Guernsey tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali.

10 Libere professioni

10.1. *Ordini e collegi professionali*

Anche nel corso del 2004 sono pervenuti quesiti sul trattamento dei dati personali relativi a soggetti iscritti ad albi e collegi professionali. Rispondendo ad essi, il Garante ha avuto occasione di ribadire le significative innovazioni introdotte in questa materia dal Codice e di fornire alcune precisazioni in merito alla divulgazione delle informazioni relative a provvedimenti disciplinari.

Al riguardo, si ricorda che, ai sensi dell'art. 61 del Codice, in armonia con le disposizioni sulla comunicazione e diffusione di dati personali da parte dei soggetti pubblici, gli ordini e i collegi professionali possono ora più agevolmente comunicare pure a privati e diffondere, anche mediante reti di comunicazione elettronica, i dati (diversi da quelli sensibili e giudiziari) che, secondo le disposizioni legislative o regolamentari di settore, devono essere necessariamente inseriti nei rispettivi albi per legge o regolamento.

In merito alla divulgazione delle informazioni relative a provvedimenti atti ad incidere sull'attività dell'iscritto all'albo, su richiesta del Consiglio nazionale degli ingegneri, è stato specificato che nelle comunicazioni a soggetti pubblici o privati, o in sede di diffusione, anche per via telematica, di dati inseriti nell'albo professionale, può essere resa nota l'esistenza di provvedimenti disciplinari che dispongono la sospensione dalla professione, ma non il provvedimento nella sua integralità, fermo restando il dovere di porre in circolazione informazioni corrette, complete ed aggiornate, specie con riguardo ad eventuali sviluppi favorevoli per gli interessati.

D'altra parte, in base alla nuova disciplina (art. 61, comma 3, del Codice) gli ordini ed i collegi professionali possono integrare i dati contenuti negli albi con ulteriori informazioni che l'iscritto richieda di aggiungere, purché pertinenti e non eccedenti in relazione alla sua attività professionale (*Nota* 17 agosto 2004).

In risposta ad un quesito di un consiglio notarile distrettuale, l'Ufficio ha poi precisato che, ai sensi dell'art. 61 del Codice, l'esistenza e l'esito del provvedimento di sospensione possono essere comunicati a soggetti privati che abbiano presentato un esposto, ferma restando, peraltro, l'applicazione nel caso concreto delle disposizioni della legge n. 241/1990 in tema di accesso ai documenti amministrativi (*Nota* 17 agosto 2004).

10.2. *Liberi professionisti*

Avvocati

In ossequio ai principi di semplificazione ed efficacia, il Garante, in un articolato parere indirizzato al Consiglio nazionale forense, ha fornito alcuni chiarimenti per una corretta applicazione della disciplina sulla protezione dei dati nell'esercizio dell'attività forense che, per alcuni aspetti, possono valere anche per altri liberi professionisti (*Nota* 3 giugno 2004).

In relazione alla titolarità del trattamento è stato chiarito che, quando l'attività è svolta individualmente, titolare del trattamento è lo stesso avvocato, cui spettano quindi le decisioni sull'uso dei dati, sugli strumenti impiegati e sul profilo della sicu-

rezza, mentre sono contitolari del medesimo trattamento due professionisti che operino congiuntamente. Se l'attività è invece svolta in forma societaria o associata, il titolare è l'entità nel suo complesso e gli adempimenti previsti dal Codice devono essere attuati unitariamente per evitare frammentazioni o ripetizioni da parte dei singoli professionisti. La designazione del responsabile del trattamento è facoltativa e nelle grandi organizzazioni ne possono essere designati anche diversi. Chiunque abbia accesso interno ai dati (praticanti, personale amministrativo ecc.), deve essere designato quale incaricato del trattamento, indicando per iscritto i compiti affidatigli.

Per quanto riguarda gli adempimenti, la maggior parte dei trattamenti effettuati dagli avvocati non sono soggetti a notificazione, mentre resta fermo l'obbligo di informativa all'interessato, che può essere resa anche oralmente e in forma sintetica, purché completa.

Il titolare deve inoltre adottare le misure di sicurezza idonee e preventive per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta. Contrariamente a quanto ipotizzato in alcuni quesiti formulati da singoli professionisti, il Garante ha precisato che, per quanto riguarda l'organizzazione del lavoro quotidiano di studio, non si deve affatto eliminare il nome delle parti dalla copertina dei fascicoli cartacei. È invece sufficiente seguire adeguate modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti.

I dati comuni e sensibili possono essere trattati senza il consenso degli interessati solo se il loro uso è necessario per svolgere indagini difensive o far valere un diritto in sede giudiziaria. Se tra i dati sensibili vi sono anche informazioni relative a salute e vita sessuale, è necessario seguire il cd. principio del pari rango, in ragione del quale il diritto difeso o fatto valere in giudizio deve essere un diritto della personalità o un altro diritto o libertà fondamentale o inviolabile (art. 26, comma 4, lett. *c*), del Codice).

Per quanto riguarda il trattamento dei dati giudiziari, purché esso avvenga nel rispetto dell'autorizzazione generale n. 4/2004, non è richiesto il consenso dell'interessato.

L'esercizio dell'attività stragiudiziale (arbitrati, conciliazioni, ricorsi amministrativi) è soggetto, invece, a regole differenti, in base alle quali il trattamento dei dati comuni di soggetti diversi dal cliente deve generalmente avvenire con il consenso dell'interessato, a meno che sia applicabile uno dei presupposti indicati dall'art. 24 del Codice (ad esempio, nel caso di trattamento di dati "pubblici"). Nel caso di dati sensibili, il consenso, sempre necessario, deve essere scritto.

Notai

Nel corso dell'anno, con un parere reso al Consiglio nazionale del notariato, l'Autorità ha precisato le modalità con le quali i notai, in qualità di titolari del trattamento, devono dare applicazione alla normativa in materia di protezione dei dati personali, assumendo un formale impegno a redigere a breve un agevole e sintetico "decalogo", in cooperazione con il Consiglio.

L'Ufficio ha nel frattempo ribadito che la disciplina sulla protezione dei dati personali non pone in discussione la peculiarità della funzione notarile e si affianca alle regole generali sul segreto professionale per assicurare l'integrità e la disponibilità dei dati, indicando come gli stessi debbano essere custoditi e trattati in concreto.

Analogamente a quanto previsto per gli avvocati, il Garante ha chiarito le modalità di applicazione delle misure minime di sicurezza e degli obblighi di informativa all'interessato. Tuttavia, è stato precisato che, data la peculiarità e gli obblighi della funzione notarile, il dare conoscenza o pubblicità ad alcuni dati e documenti trat-

10

tati dal notaio non concreta la fattispecie della "diffusione" prevista dal Codice.

È stato ricordato, ferme restando le particolari garanzie per i dati sensibili, che il consenso è solo uno dei presupposti del trattamento dei dati comuni: si può, infatti, fare riferimento agli altri presupposti indicati nell'art. 24 del Codice, come, ad esempio, l'adempimento di obblighi di legge o l'esecuzione di obblighi contrattuali (*Nota* 3 dicembre 2004).

11 Rapporto di lavoro e previdenza

11.1. *Dati trattati nel corso del rapporto di lavoro*

Il Garante ha proseguito la valutazione, già iniziata nel 2003, degli effetti delle disposizioni di attuazione della cd. riforma Biagi del mercato del lavoro (l. n. 30/2003 e d.lg. n. 276/2003) con riguardo al trattamento dei dati personali in ambito lavorativo.

L'Autorità, anche con le autorizzazioni generali al trattamento dei dati sensibili, ha ribadito la necessità che il trattamento di taluni dati sensibili sia effettuato nel rispetto delle regole e dei principi generali dettati dal Codice ed entro i limiti fissati dall'art. 8 dello Statuto dei lavoratori (legge 20 maggio 1970, n. 300, che vieta indagini sulle opinioni e trattamenti discriminatori).

La Borsa continua nazionale del lavoro

Il principio è stato altresì indicato in un parere reso il 3 settembre 2004 sullo schema di decreto interministeriale di attuazione della Borsa continua nazionale del lavoro, nel quale il Garante ha sottolineato l'esigenza che il richiamo all'art. 10 del d.lg. n. 276/2003 ivi contenuto sia interpretato in armonia con l'art. 8 della legge n. 300/1970.

Con il citato parere, le cui indicazioni sono state solo in parte recepite nel testo definitivo del decreto del 13 ottobre 2004, sono stati affrontati ulteriori importanti profili in materia di protezione dei dati personali nel sistema della Borsa continua nazionale del lavoro: in particolare, su specifica richiesta dell'Autorità, il regolamento reca ora l'indicazione dei titolari dei trattamenti, al fine di definirne compiutamente le relative responsabilità. Per assicurare il rispetto del principio di proporzionalità del trattamento dei dati, l'indicazione dei dati da far confluire nella Borsa (in particolare, delle informazioni minime ed essenziali relative alle candidature e alle richieste di personale), contenuta negli allegati, è ora esaustiva e si prevede che eventuali ulteriori dati possano essere inseriti solo su base volontaria e non possano essere oggetto, in ogni caso, di utilizzazione a fini discriminatori, specie qualora abbiano natura di dati sensibili, come l'"appartenenza a liste speciali"; è stato altresì precisato nel regolamento che i soggetti che fruiscono della Borsa possono trattare solo i dati pertinenti all'instaurazione del rapporto di lavoro.

Videosorveglianza in ambito lavorativo

Sono stati definiti alcuni procedimenti già istruiti in materia di controllo a distanza dei lavoratori a mezzo di apparecchiature di videosorveglianza e sono state fornite prescrizioni ai titolari del trattamento con particolare riferimento al rispetto dell'art. 4 della legge n. 300/1970, oltre che dei principi generali posti dal Codice a garanzia degli interessati.

Il controllo del lavoratore attraverso videocamere è stato oggetto anche di alcuni ricorsi sottoposti al Garante.

I casi affrontati nel corso dell'anno (concernenti impianti di ripresa video installati da soggetti privati) hanno permesso di dare applicazione ai precetti di legge ed alle indicazioni specifiche contenute nel provvedimento generale del Garante del 29 aprile 2004 (v. par. 12.1).

In particolare, nelle decisioni del 16 giugno 2004 e dell'11 ottobre 2004, è stato sottolineato che i trattamenti in questione violavano i presupposti di liceità, propor-

zionalità, correttezza e trasparenza in relazione, tra l'altro, all'angolo di ripresa delle telecamere, all'assenza di idonea informativa o all'invasività dell'impianto stesso di videosorveglianza, nonché alle finalità perseguite che potevano essere raggiunte anche con accorgimenti diversi (nel caso di specie, installazione di cancelli o provvedimenti per regolare gli accessi).

Profili di liceità e correttezza del trattamento in ambito lavorativo

L'Autorità è poi intervenuta su ulteriori temi specifici, tra i quali: adeguatezza della modulistica di informativa e richiesta del consenso dei lavoratori predisposta dai datori di lavoro; accesso dei lavoratori ai dati personali che li riguardano; modalità di conservazione e custodia dei dati dei dipendenti a cura dei datori di lavoro.

È stato esaminato il caso di un dipendente di banca che ha contestato la formula di manifestazione del consenso al trattamento dei dati personali riportati nell'estratto conto certificativo della sua posizione contributiva (cd. "Ecocert") inserita dal datore di lavoro in un modulo con il quale chiedeva all'interessato la delega all'acquisizione di tali dati presso l'ente previdenziale. L'Autorità (*Nota* 7 luglio 2004) ha rilevato che, nel caso di specie, la richiesta del consenso era superflua, in quanto i dati non sensibili erano trattati per adempiere a specifici obblighi fissati dalla normativa vigente (artt. 4 e 24, legge 23 luglio 1991, n. 223) e dagli accordi contrattuali al fine di avvalersi di procedure di riduzione collettiva del personale.

Anche con riferimento agli eventuali dati sensibili contenuti nel modulo "Ecocert", l'acquisizione del consenso dell'interessato è stata ritenuta superflua, dal momento che il segnalante aveva già manifestato alla banca il consenso al trattamento dei dati personali, anche sensibili, per le finalità e nei termini indicati nelle informative già fornite a suo tempo dalla banca e nel cui ambito potevano essere ricomprese anche le operazioni necessarie per adempiere agli obblighi appena richiamati. Si è poi fatto presente che, in base alle nuove disposizioni del Codice, non è più necessario il consenso scritto dell'interessato quando il trattamento dei dati sensibili occorra in rapporto a specifici obblighi o compiti previsti dalla legge per la gestione del rapporto di lavoro, nel rispetto dell'autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro e delle regole che saranno individuate mediante il codice di deontologia in materia di lavoro e previdenza (art. 26, comma 4, lett. *d*), del Codice).

L'Autorità ha pertanto prescritto alla banca di precisare agli interessati, ad integrazione delle informative fornite in passato, che il conferimento dei dati contenuti nel modulo "Ecocert" è necessario per l'adempimento dei predetti obblighi, con l'indicazione delle conseguenze in caso di mancato rilascio di tali dati, e di invitare i lavoratori a produrre direttamente l'estratto conto della propria posizione contributiva in alternativa al rilascio di una delega a tal fine alla banca, tenuto conto che comunque è loro facoltà accedere personalmente ai dati in questione presso gli enti previdenziali (art. 54, legge 9 marzo 1989, n. 88).

Rapporto di lavoro e tutela della dignità e della riservatezza del lavoratore

In numerose ipotesi il Garante è dovuto intervenire a tutela della dignità e della riservatezza dei lavoratori, specialmente se interessati da delicate vicende personali e familiari attinenti allo stato di salute e alla vita sessuale.

Si segnala, al riguardo, l'accoglimento del ricorso della dipendente di una società per una seria violazione della propria riservatezza personale e familiare (*Provv.* 27 luglio 2004, v. *Newsletter* 11-17 ottobre 2004). La dipendente, che occupava temporaneamente la scrivania di un collega, aveva trovato la fotocopia di una lettera da lei stessa inviata al direttore dell'ufficio, nella quale erano riportate anche delicate informazioni sulla condizione di salute della figlia minore disabile.

L'Autorità ha rilevato che la presenza di tale fotocopia contenente dati sensibili

della dipendente e della figlia minore, al di fuori del fascicolo personale e comunque in un contesto inappropriato, contrastava con le prescrizioni e le cautele indicate nell'autorizzazione generale che disciplina il trattamento dei dati sensibili nei rapporti di lavoro, nonchè con le disposizioni del Codice in materia di misure di sicurezza; ha ricordato che i dati sensibili devono essere conservati in una sezione separata del fascicolo personale ed essere accessibili solo al personale autorizzato.

Il Garante, riconosciute le ragioni della dipendente, ha imposto alla società di adottare tutte le misure di sicurezza idonee a prevenire il ripetersi di eventi del genere, comunicandone il contenuto all'Autorità.

La società, che non ha contestato la ricostruzione della vicenda fatta dalla dipendente, ha avviato una indagine interna i cui esiti dovranno essere comunicati al Garante per la valutazione di altre eventuali violazioni o responsabilità.

Cartellini identificativi e mutamento del sesso

L'Autorità ha inoltre affrontato la delicata questione relativa alla possibilità di ottenere la rettificazione degli atti dello stato civile solo a seguito di una sentenza del tribunale passata in giudicato che attribuisca alla persona un sesso diverso da quello enunciato nell'atto di nascita, in ragione delle intervenute modificazioni esteriori dei suoi caratteri sessuali. Tale previsione, pur corrispondendo ad una scelta normativa specifica, che solo il Parlamento ha il potere di modificare, mostra alcuni elementi di criticità in merito alla difesa dei diritti dei soggetti coinvolti nel procedimento di rettificazione del sesso, specie nella fase transitoria di tale procedimento. La lunga durata dei procedimenti di rettificazione di attribuzione di sesso ha reso quindi necessario richiamare l'attenzione sull'esigenza di porre allo studio la possibilità di introdurre nell'ordinamento specifiche misure provvisorie volte a tutelare l'identità personale e la dignità dell'interessato nel periodo preliminare al passaggio in giudicato della sentenza. Spetta al Governo e al Parlamento valutare anche la possibile applicazione di tali misure in eventuali altri procedimenti giudiziari in cui si presentino analoghe esigenze (*Nota* 11 agosto 2004).

Con riferimento all'uso sul luogo di lavoro del nome di battesimo, nell'intervallo di tempo necessario al passaggio in giudicato della sentenza di rettificazione di sesso, l'Autorità ha avuto modo di precisare che, in applicazione dei principi di pertinenza e non eccedenza, sui cartellini identificativi dei dipendenti devono essere presenti unicamente i dati sufficienti ad assicurare la trasparenza dei rapporti tra il personale e tra questi e gli utenti (ad es. l'immagine fotografica, la definizione del ruolo ricoperto ed eventualmente un numero o una sigla) e non anche altri dati non necessari per perseguire tale finalità (es. dati anagrafici). Analogamente, con riferimento alla prassi di indicare il nome di battesimo nell'indirizzo di posta elettronica, nei moduli di richiesta di ferie e/o permessi e nelle comunicazioni personali e domiciliari, l'Autorità ha ricordato che l'interessato che non desidera che su tali atti compaia il suo dato anagrafico non ancora rettificato ha il diritto di richiedere, per motivi legittimi, l'adozione di specifiche misure che, in armonia con la disciplina dettata dal Codice, tengano conto della sua delicata posizione meritevole di tutela (art. 7, comma 4, del Codice). Il datore di lavoro ha l'obbligo di valutarle tempestivamente; l'interessato che ritenga di aver ricevuto una risposta insoddisfacente ha il diritto di adire l'autorità giudiziaria ordinaria o, in alternativa, il Garante con gli strumenti di tutela previsti dal Codice.

Accesso in ambito lavorativo

Diverse ipotesi esaminate hanno avuto origine da richieste da parte del lavoratore di accedere ai dati che lo riguardano detenuti dal datore di lavoro, richieste talvolta estese alla conoscenza di tutte le informazioni utilizzate dallo stesso datore di lavoro in relazione alla carriera professionale dell'interessato (comprese relazioni

valutative periodiche, documentazione relativa a ferie, permessi e malattie, o tabulati contenenti le registrazioni delle presenze in servizio) (*Provv*. 12 maggio 2004).

Il Garante ha ribadito che il riscontro alle richieste di accesso deve essere completo e deve comprendere tutti i dati relativi all'interessato comunque trattati dal titolare, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali (art. 10, comma 3, del Codice). Ciò, anche nel caso in cui il conferimento all'interessato di determinate qualifiche e ruoli sia ricavabile da atti societari custoditi in archivi aziendali diversi da quelli contenenti i dati connessi alla gestione del rapporto. L'Autorità, nel caso esaminato, ha rilevato che l'interessato aveva dapprima formulato un'istanza in termini tali da potersi ritenere riferita esclusivamente ai dati conservati nel suo fascicolo personale, mentre una richiesta successiva comprendeva, di fatto, tutti i dati personali che lo riguardavano trattati dall'*ex* datore di lavoro. A fronte di questa seconda richiesta, la società era comunque tenuta a individuare tutti i dati personali del lavoratore, a prescindere dalla circostanza che fossero custoditi nel fascicolo personale del lavoratore stesso (*Nota* 9 agosto 2004).

In risposta ad una richiesta di parere presentata da una società, il Garante ha per altro verso sottolineato che, in linea di principio, non può escludersi la necessità di esibire o consegnare al richiedente copia di interi atti o documenti, o parte di essi, riguardanti anche terzi, purché ciò avvenga nel solo caso in cui i dati relativi al richiedente e ai terzi siano intrecciati al punto da risultare incomprensibili o snaturati nel loro contenuto, se privati di alcuni elementi o scomposti rispetto alla loro originaria collocazione (*Nota* 23 novembre 2004).

In merito all'ammissibilità della richiesta dell'interessato di accedere a dati già in suo possesso, l'Autorità ha ricordato che alla richiesta di accesso ai dati deve essere fornito riscontro anche nell'ipotesi in cui le medesime informazioni, in tutto o in parte, siano state comunicate all'interessato o siano comunque dallo stesso detenute. Ciò, al fine di consentire all'interessato di poterne controllare l'esattezza e di chiederne, se del caso, l'aggiornamento, l'integrazione o la correzione. Si è inoltre fatto presente che il diritto di accesso è a volte esercitato chiedendo legittimamente di conoscere anche origine dei dati, finalità, modalità e logica del trattamento, ovvero gli estremi identificativi del titolare e del responsabile del trattamento, ove nominato, nonché dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati (art. 7, comma 2, lett. *e*), del Codice).

Sempre sul tema dell'accesso ai dati personali relativi a dipendenti (in particolare, dati valutativi o contenuti in note di qualifica, dati relativi ad assenze dal servizio per malattia ed altri dati contenuti nei fascicoli personali), sono state numerose anche le decisioni adottate a seguito di ricorso. Unitamente a tali richieste di accesso è stata talvolta manifestata l'opposizione per motivi legittimi al trattamento dei dati: in particolare, in un caso l'istanza era motivata dall'illecita comunicazione di dati riferiti alla carriera professionale del lavoratore ad altre società, in assenza del consenso informato dell'interessato (*Provv*. 3 giugno 2004).

Al termine del 2004 il Garante ha avviato un ciclo di ispezioni per accertare la posizione di alcune *ex* società di fornitura di lavoro interinale e società di ricerca e selezione del personale in materia di notificazione dei trattamenti di taluni dati personali (cfr. par. 20.3)

11.2. *Rapporto di lavoro in ambito pubblico*

Dati sensibili

Nel settore del pubblico impiego, l'Autorità è stata chiamata ad intervenire in vicende in cui, nelle comunicazioni concernenti l'adozione di provvedimenti di gestione interna del personale (trasferimenti o avvicendamenti), sono riportati dati di carattere sensibile riguardanti, in particolare, la salute di dipendenti. Il trattamento di queste informazioni, per perseguire una rilevante finalità d'interesse pubblico di gestione di rapporti di lavoro, può in generale ritenersi lecito. Occorre, tuttavia, che siano rispettati anche i principi di proporzionalità, necessità, pertinenza e non eccedenza dei dati, limitando il trattamento, in ogni sua fase, alle sole informazioni strettamente indispensabili al raggiungimento di tale finalità (artt. 11 e 22 del Codice).

Non è stata così ritenuta rispondente al principio di necessità l'indicazione, nelle comunicazioni indirizzate alle sedi interessate, dei gravi motivi di salute su cui era fondato il provvedimento di trasferimento di un dipendente. Il trasferimento, infatti, avrebbe potuto essere comunicato a tali uffici mediante una nota contenente, in sintesi, il testo del provvedimento originario e gli estremi di riferimento del provvedimento. Tale accorgimento, peraltro, non pregiudica l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, l. n. 241/1990), né la facoltà delle persone a ciò legittimate di accedere ad eventuali altri dati, anche di tipo sensibile, contenuti in tali atti, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa.

In materia di trattamento di dati sensibili, l'Autorità ha ritenuto che la disciplina sulla protezione dei dati personali non ponesse ostacoli di fondo ad un'iniziativa del Ministero degli affari esteri consistente nell'identificare i dipendenti portatori di handicap ai fini di esercitazione per evacuazioni antincendio in conformità alla disciplina sull'igiene e la sicurezza del lavoro. Tale attività rientra infatti tra quelle che, sulla base del Codice, possono giustificare il trattamento di dati sensibili (artt. 86, comma 1, lett. *c*) e 112, comma 2, lett. *e*) del Codice).

Nel ricordare, anche in questo caso, che l'amministrazione può effettuare il trattamento delle informazioni relative allo stato di disabilità dei dipendenti soltanto se esse sono realmente *"indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa"* (art. 22, comma 3, del Codice), dovendo altresì rispettare le regole di proporzionalità, indispensabilità, pertinenza e non eccedenza, si è fatto presente al Ministero che, per questa ed altre attività di trattamento di dati sensibili, è necessario provvedere con atto regolamentare ad individuare i tipi di dati che possono essere trattati e le operazioni eseguibili (art. 20, comma 2, del Codice).

Con specifico riferimento al trattamento dei dati sensibili nell'ambito della gestione del personale delle forze armate e di polizia, su richiesta della Guardia di finanza, l'Autorità si è espressa in merito all'utilizzo di test psico-attitudinali nelle procedure concorsuali di reclutamento (*Nota* 3 giugno 2004).

Test psico-attitudinali

Si è precisato, in primo luogo, che il divieto di trattare informazioni sensibili nell'ambito di test psico-attitudinali previsto dal Codice (art. 22, comma 10) si riferisce anche alla raccolta di questi dati mediante questionari volti a costruire il profilo o la personalità dell'interessato. Va pertanto espunta dai questionari utilizzati sia per gli esami psico-attitudinali, sia per quelli psichiatrici, ogni domanda idonea a rivelare profili particolarmente delicati della sfera privata dell'interessato, quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere.

A seconda degli esiti di tali esami è invece possibile procedere ad ulteriori accer-

tamenti, ove ritenuto indispensabile, purché questi non consistano nella somministrazione ai candidati di test psico-attitudinali volti a definire il loro profilo o la loro personalità mediante il trattamento di dati sensibili. In questo caso occorre rendere all'interessato una previa e specifica informativa, in modo da consentirgli di non sottoporsi alla prosecuzione della procedura concorsuale e, quindi, a tali ulteriori accertamenti (artt. 13 e 7 del Codice).

Nei ricorsi presentati da alcuni sottufficiali della Guardia di finanza, il Garante ha ritenuto illecita la procedura utilizzata da un comando regionale di stilare un elenco nominativo di tutti i militari in licenza per convalescenza o in aspettativa al fine di regolare l'accesso alla caserma dei dipendenti assenti dal servizio (*Provv.* 7 luglio 2004).

Contrariamente a quanto sostenuto dal comando, l'indicazione del dato relativo all'assenza per "convalescenza" dà luogo ad un trattamento di dati sensibili dal momento che questa informazione, pur non facendo riferimento a specifiche patologie, è comunque suscettibile "di rivelare lo stato di salute del dipendente". Pur non essendo in discussione il potere-dovere della Guardia di finanza di perseguire gli obiettivi di sicurezza della caserma, il trattamento in questione è stato giudicato illecito dal momento che, per disciplinare l'accesso dei militari che si assentano per servizio, non è indispensabile specificare la ragione di tale assenza attinente allo stato di salute, essendo invece sufficiente la sola indicazione dei relativi nominativi.

Nel trattamento di queste informazioni l'amministrazione deve rispettare comunque il principio di indispensabilità, valutando specificamente il rapporto tra i dati sensibili e gli adempimenti legati a compiti e obblighi espletati (artt. 20 e 22 del Codice). Il mancato rispetto di tali garanzie rende il trattamento illecito, anche se effettuato nello svolgimento di funzioni istituzionali o ritenute giustificate da norme di servizio e regolamenti interni.

Visite medico-legali

Non è risultata, invece, contraria alla disciplina sul trattamento dei dati personali la trasmissione alla questura e alla prefettura da parte di un comune (finalizzata all'adozione dei provvedimenti di competenza) dell'esito di alcune visite medico-legali cui era stato sottoposto un dipendente, essendo l'interessato, un agente di pubblica sicurezza, abilitato al porto di pistola, nonché in possesso del porto d'armi per uso di caccia (*Provv.* 22 gennaio 2004). Il caso va visto in connessione con un altro, esaminato da questa Autorità, oggetto di una valutazione parzialmente difforme dell'autorità giudiziaria presso cui è stato impugnato il provvedimento del Garante, in considerazione dell'ulteriore documentazione prodotta dall'interessato, invece non presentata in sede di ricorso all'Autorità (v. par. 19.4). Nel ricorso, il dipendente di una questura aveva lamentato che i dati relativi al proprio stato di salute, accertati nel corso di una visita medica cui era stato sottoposto per verificare la sua idoneità al servizio, erano stati comunicati ad altri soggetti al fine del ritiro cautelativo dell'arma in dotazione e del tesserino di servizio. Nella decisione del ricorso, sulla base degli elementi prodotti dalle parti, il Garante aveva ritenuto che tali comunicazioni fossero avvenute lecitamente, in quanto effettuate in conformità alle norme sulle autorizzazioni di polizia per la detenzione ed il porto d'armi e finalizzate all'adozione dei relativi provvedimenti (*Provv.* 15 gennaio 2004). L'Ufficio, invece, ha avviato specifici accertamenti per verificare se all'interessato sia stata fornita un'idonea informativa anche in relazione ai flussi di dati necessari ai fini dell'adozione dei provvedimenti sull'arma di servizio.

Sempre in materia di trattamento di dati del personale in servizio presso le questure, è stato oggetto di una decisione su ricorso il trattamento di dati sensibili di un funzionario amministrativo. In proposito, il Garante ha segnalato alla questura

la necessità di adottare ogni misura idonea a dare compiuta applicazione alla disciplina relativa agli incaricati del trattamento e a quella concernente le misure minime di sicurezza. Ciò, tenendo anche presente che, in base all'art. 11, comma 2, del Codice, i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati (*Provv.* 7 luglio 2004).

Particolari comunicazioni: in special modo, nell'ambito del procedimento disciplinare

L'utilizzo del fax come mezzo di comunicazione tra amministrazioni è consentito dalla legge e, in linea generale, non è in contrasto con i principi in materia di protezione dei dati personali. Il Garante ha tuttavia evidenziato che per talune circostanze occorre rispettare le specifiche modalità eventualmente previste dalla normativa di settore. Ad esempio, è all'attenzione dell'Autorità una questione relativa alle modalità di trasmissione delle comunicazioni nell'ambito del procedimento disciplinare, per alcune delle quali la normativa prevede la consegna personale all'interessato o, qualora questa non sia possibile, l'invio di una raccomandata (artt. 111 e 104, d.P.R. n. 3/1957). Nel caso in esame, il fax era stato utilizzato anche per le convocazioni dei componenti del Consiglio di disciplina che contenevano il nominativo della persona sottoposta al procedimento, anche se, in ossequio ai principi di pertinenza e non eccedenza, sarebbe stato probabilmente sufficiente anticipare soltanto il tipo di intervento per il quale si richiedeva la presenza del consigliere.

È di nuovo all'esame dell'Autorità la questione dell'indicazione di dati personali dei lavoratori nei buoni pasto (in particolare, i nominativi dei singoli beneficiari e la loro sede di servizio), accanto alle informazioni sul datore di lavoro, nonché dei presupposti di liceità per comunicare i dati dei dipendenti al soggetto tenuto all'erogazione del servizio.

Diritto al lavoro dei disabili

Per quanto riguarda la normativa sul diritto al lavoro dei disabili, è pervenuta una segnalazione con la quale si lamentava che la graduatoria del collocamento obbligatorio, contenente i nominativi di circa tredicimila disabili, era stata pubblicata sul sito *web* del servizio per le politiche del lavoro di una provincia. All'esito degli accertamenti e degli ulteriori approfondimenti effettuati, è stato previsto il blocco del trattamento, visto l'ingente numero di soggetti interessati dalla diffusione indiscriminata di dati idonei a rivelare il loro stato di salute e tenuto conto che le disposizioni di settore (art. 8, legge 12 marzo 1999, n. 68) non definiscono le modalità per garantire la pubblicità degli elenchi e delle graduatorie degli aventi diritto al collocamento obbligatorio.

Anche a tale proposito occorre sottolineare che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti.

Un'amministrazione provinciale ha poi informato il Garante, nell'ambito di una comunicazione ai sensi dell'art. 39 del Codice, dell'intenzione di trasmettere ad un comune i dati identificativi degli iscritti ad una lista del collocamento obbligatorio per consentire lo svolgimento di un'indagine sui bisogni dei cittadini disabili. In proposito, l'Autorità ha precisato che, trattandosi di informazioni idonee a rivelare lo stato di disabilità degli interessati, occorre far riferimento alla distinta e più stringente disciplina prevista per il trattamento dei dati sensibili (artt. 20 e 22 del Codice) (*Nota* 21 settembre 2004). Nel corso degli ulteriori approfondimenti, avviati in collaborazione con gli enti pubblici coinvolti, sono state poi fornite indicazioni idonee a realizzare l'iniziativa nel pieno rispetto delle garanzie poste dal Codice a tutela della riservatezza e degli altri diritti dei disabili interessati dall'indagine.

11

Sciopero nei servizi pubblici essenziali

Con riferimento alla disciplina sullo sciopero nei servizi pubblici essenziali, l'Autorità si è occupata della prassi, seguita da alcune amministrazioni pubbliche, di comunicare al Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e all'apposita Commissione di garanzia gli elenchi nominativi di dipendenti che hanno esercitato, in specifici casi, il diritto di sciopero.

In proposito, considerando la chiarezza del dettato normativo della legge n. 146/1990, che pone in capo alle amministrazioni e alle imprese erogatrici di detti servizi l'obbligo di rendere pubblico "il numero dei lavoratori che hanno partecipato allo sciopero, la durata dello stesso e la misura della trattenuta effettuata secondo la disciplina vigente" (art. 5), si è rilevato che talune amministrazioni potevano essere state indotte ad effettuare siffatte comunicazioni da una espressione utilizzata nella circolare del 18 giugno 2002 del Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, con riferimento alle rilevazioni delle adesioni allo sciopero.

Per prevenire altri equivoci, l'Ufficio ha pertanto invitato la Presidenza e la Commissione di garanzia a valutare l'opportunità di impartire specifiche istruzioni chiarificatrici sul punto (*Nota* 18 agosto 2004). In proposito, la Commissione ha assicurato al Garante di aver sempre richiesto i soli dati numerici dei lavoratori partecipanti alle astensioni collettive dal lavoro, salvo le ipotesi in cui l'individuazione dell'aderente allo sciopero fosse indispensabile per l'applicazione delle sanzioni previste dalla disciplina di settore.

Concorsi

Il Ministero degli affari esteri ha sottoposto all'attenzione del Garante l'intenzione di consentire ai candidati interessati a partecipare ai concorsi banditi dall'amministrazione di inviare direttamente *on-line* all'ufficio competente la domanda di partecipazione, corredata di dati personali. Poiché la questione attiene alla più generale tematica dell'informatizzazione dell'amministrazione pubblica, il Garante, nelrilevare che l'iniziativa in esame di per sé non era in contrasto con i principi del Codice, ha evidenziato al Ministero che, tuttavia, la disciplina dell'accesso agli impieghi nelle pubbliche amministrazioni e dello svolgimento dei concorsi pubblici (art. 4, d.P.R. n. 487/1994) esclude espressamente l'utilizzo di strumenti diversi dalla diretta presentazione all'ufficio competente delle domande di ammissione al concorso o dal loro invio tramite raccomandata con avviso di ricevimento (*Nota* 25 agosto 2004).

Poiché il trattamento di dati personali da parte di soggetti pubblici è ammesso soltanto per lo svolgimento delle funzioni istituzionali dell'ente, nei limiti stabiliti dalla legge e dai regolamenti, si è quindi indicato all'amministrazione di operare una nuova valutazione dell'iniziativa prospettata, ma in riferimento alla specifica disciplina dei concorsi, piuttosto che rispetto al Codice.

Sempre in tema di trattamento di dati personali nell'ambito di concorsi pubblici, si è precisato che non costituisce violazione della disciplina sulla riservatezza la richiesta, rivolta dalle amministrazioni pubbliche agli aspiranti, di una dichiarazione sostitutiva dei carichi pendenti. Tale procedura tiene conto dell'esigenza dell'amministrazione di verificare l'eventuale presenza di cause ostative all'accesso al pubblico impiego (art. 85, d.P.R. 10 gennaio 1957, n. 3 e art. 2, d.P.R. 9 maggio 1994, n. 487); esigenza quest'ultima espressamente riconosciuta dall'art. 71 del d.P.R. n. 445/2000 e dalla recente riforma del casellario giudiziale, che prevede anche una forma di accesso diretto alla banca dati da parte delle amministrazioni (d.P.R. 14 novembre 2002, n. 313).

11.3. *Previdenza*

Su richiesta di un'associazione di difesa dei diritti dei cittadini, sono all'esame del Garante alcuni moduli adottati dall'Inps con la circolare n. 103 dell'11 maggio 2001, utilizzabili dai lavoratori per presentare le domande di congedo per maternità e di congedo parentale.

In proposito, è necessario valutare alla luce dei principi di indispensabilità, pertinenza e non eccedenza dei dati trattati, la raccolta di informazioni ulteriori rispetto a quelle che, secondo la disciplina sulla tutela delle lavoratrici madri, devono essere necessariamente riportate nel certificato medico di gravidanza (art. 14 d.P.R. 25 novembre 1976, n. 1026).

Maggiori garanzie nelle modalità di raccolta, peraltro, non pregiudicano l'eventuale successiva acquisizione di ulteriori informazioni, anche sensibili, da parte dell'istituto previdenziale o dei medici dei servizi ispettivi del Ministero del lavoro e delle politiche sociali, qualora emerga la reale necessità di svolgere gli accertamenti amministrativi e i controlli previsti (artt. 76 e 77, d.lg. n. 151/2001).

Non è invece in contrasto con i principi di pertinenza e non eccedenza la raccolta, sul modulo di domanda per congedo parentale, dei dati relativi all'altro genitore o affidatario (dati anagrafici, periodi di congedo eventualmente fruiti, tipologia dell'attività lavorativa svolta, ecc.). Tali informazioni sono infatti pertinenti rispetto alla necessità di quantificare il periodo di congedo e la relativa indennità che il datore di lavoro e l'istituto previdenziale devono accordare al genitore richiedente (artt. 32, 33 e 34, d.lg. n. 151/2001) e non risultano eccedenti rispetto alla medesima finalità, non facendo alcun riferimento specifico al tipo di rapporto che intercorre tra i soggetti beneficiari.

L'Autorità, pertanto, è in procinto di definire la questione al fine di invitare l'Inps a riesaminare i moduli per la presentazione delle domande di congedo per maternità, in modo da garantire la riservatezza delle lavoratrici che intendono usufruire dei benefici previsti dalla legge a tutela della maternità.

Dati sanitari dei dipendenti

A seguito di una segnalazione relativa al trattamento dei dati sanitari, l'Autorità si è pronunciata circa le informazioni che devono essere contenute nelle denunce di malattia professionale che i datori di lavoro sono tenuti a trasmettere all'Inail. In tali atti devono essere indicate solo informazioni sanitarie relative o collegate alla patologia denunciata, anziché dati sulla salute inerenti a semplici malesseri accusati o ad assenze registrate nel corso del rapporto di lavoro, non rilevanti per la malattia professionale.

Con un provvedimento del 15 aprile 2004, il Garante ha così vietato all'Inail di utilizzare i dati sanitari di un'assicurata ed ha disposto il blocco di alcune informazioni relative allo stato di salute presenti negli archivi del datore di lavoro e ricavabili dalle diagnosi contenute nei certificati dei lavoratori. All'amministrazione è stato, inoltre, imposto di adottare opportuni accorgimenti per non rendere visibili le diagnosi sulle certificazioni sanitarie detenute.

L'attuale disciplina in materia prevede che il lavoratore assente per malattia sia tenuto a presentare al datore di lavoro solo l'attestazione della prognosi. Può capitare, però, che il certificato contenga un'indicazione non necessaria della diagnosi: in questo caso l'amministrazione non è legittimata a trattare ulteriormente questi dati, e deve adottare opportune misure affinché lavoratori e medici rispettino tali cautele nella redazione dei certificati.

Nel 2004 è stata allo studio dell'Autorità la questione relativa alla trasmissione per via telematica all'Inps dei certificati di malattia predisposti da medici di medi-

cina generale. Al riguardo, il Garante aveva avviato un tavolo di lavoro con i rappresentanti dell'Istituto, al fine di evidenziare gli aspetti relativi alla tutela dei dati personali degli assistiti coinvolti da tale progetto. In particolare, l'Ufficio aveva rappresentato che tale modalità di trasmissione doveva essere prevista da norma di legge o di regolamento essendo difforme da quella prevista dalla disciplina vigente.

Da ultimo, con la legge finanziaria 2005 (art. 1, comma 149, l. n. 311/2004), è stato però stabilito che, a decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante trasmetta all'Inps per via telematica il certificato di diagnosi sull'inizio e sulla durata presunta della malattia. La definizione delle specifiche tecniche e delle modalità procedurali è demandata ad un apposito decreto interministeriale sul quale l'Autorità dovrà fornire il proprio parere ai sensi dell'art. 154, comma 4, del Codice per garantire, in particolare, il rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati trattati.

12 Videosorveglianza

12.1. *Protezione dei dati e videosorveglianza*

Nel corso degli ultimi anni si è constatato un forte incremento dell'impiego di sistemi a circuito chiuso, di telecamere e di altri sofisticati strumenti di rilevazione di immagini da parte sia di soggetti pubblici, sia di soggetti privati. Nel corso del 2004 il Garante è ripetutamente intervenuto, intensificando altresì la propria attività ispettiva, a fronte delle sempre più frequenti segnalazioni di cittadini per presunte violazioni della normativa sulla protezione dei dati determinate dall'installazione di impianti di videosorveglianza.

Nel periodo in esame sono stati anche ribaditi i chiarimenti, a più riprese forniti in passato, relativi all'uso privato di telecamere. In particolare, in occasione di un ricorso, l'Autorità ha constatato la mancanza dei presupposti di applicazione del Codice al trattamento dei dati personali effettuato per mezzo di un impianto di videosorveglianza installato da alcuni soggetti presso il cancello di ingresso della propria abitazione (*Provv.* 25 febbraio 2004). Le telecamere così attivate, infatti, configuravano un trattamento effettuato per fini esclusivamente personali. Su questo tipo di trattamenti occorre peraltro verificare quanto richiamato nel citato provvedimento del 29 aprile 2004, sia in relazione alle finalità perseguite, sia in riferimento alla necessità che i dati personali così registrati non siano destinati alla comunicazione sistematica o alla diffusione (in merito v. pure par. 13.1).

Il provvedimento generale sulla videosorveglianza: i principi

Alla luce dell'evoluzione tecnologica, dei nuovi documenti elaborati in sede comunitaria ed internazionale (in particolare, il parere n. 4/2004 dell'11 febbraio 2004 fornito dai Garanti europei, nonché le linee guida espresse dal Consiglio d'Europa il 20-23 maggio 2003) e, soprattutto, delle innovazioni contenute nel Codice, si è reso necessario aggiornare ed integrare il "decalogo" sulla videosorveglianza del novembre 2000, adottando un nuovo provvedimento di carattere generale che stabilisce regole più precise a garanzia dei cittadini (*Provv.* 29 aprile 2004).

Con tale provvedimento sono stati richiamati i principi generali enucleati dal Codice (validi in ambito pubblico e privato) il cui rispetto assicura un equo contemperamento tra le esigenze di sicurezza ed il rispetto della normativa sulla protezione dei dati personali nella rilevazione di immagini e suoni.

Il trattamento deve ovviamente avvenire nel rispetto, oltre che della citata normativa, anche delle prescrizioni contenuti in altre disposizioni di legge che possono interessare l'installazione di apparecchi audiovisivi (come, ad es., in materia di interferenze illecite nella vita privata, tutela della dignità, dell'immagine e del domicilio, tutela dei lavoratori e intercettazioni di comunicazioni e conversazioni).

Con riferimento al principio di necessità, i sistemi di videosorveglianza e il relativi programmi informatici non possono utilizzare dati riferiti a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

Viene inoltre ribadito che, nel rispetto del principio di proporzionalità, il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare se il suo impiego sia realmente proporzionato agli scopi perseguiti; l'utilizzo di tali

strumenti può essere giustificato, allora, solo quando altre misure (sistemi d'allarme, altri controlli fisici o logistici, misure di protezione agli ingressi ecc.) siano insufficienti o inattuabili.

In applicazione del principio di finalità, il titolare che attiva telecamere deve perseguire scopi determinati, espliciti e legittimi e, non ultimo, di sua pertinenza. È invece emerso che finalità di pubblica sicurezza, prevenzione e accertamento dei reati, pur competendo solo ad organi giudiziari o a forze armate o di polizia, sono state indicate quali finalità perseguite da parte di soggetti pubblici e privati.

Attività dei comuni

È stata ritenuta in contrasto con il principio di finalità l'attivazione da parte di un comune di impianti di videosorveglianza per propaganda turistica, nonché per rendere visibili le condizioni meteorologiche di porti e spiagge. In particolare, l'Autorità ha considerato del tutto ingiustificata l'attività di rilevazione di immagini con finalità promozionali e pubblicitarie, peraltro realizzata attraverso *web cam* dotate di *zoom*, successivamente diffuse sul sito *web* del comune, se in grado di rendere identificabili i cittadini ripresi (*Nota* 15 giugno 2004).

Non sono invece stati rilevati profili di illiceità nell'installazione, da parte di alcuni comuni, di apparecchi in grado di scattare fotografie in prossimità di semafori, al fine di monitorare il traffico e rilevare infrazioni. L'installazione di tali apparecchi che, peraltro, se hanno la finalità di controllare gli accessi ai centri storici, sono disciplinati da un apposito regolamento che ha recepito alcune indicazioni del Garante, non deve essere autorizzata caso per caso dall'Autorità.

Nel recente provvedimento generale sono stati confermati anche gli adempimenti cui sono soggetti tutti i titolari di impianti di videosorveglianza pubblici e privati.

Informativa

I cittadini che si trovano o che transitano in una zona videosorvegliata devono poter essere resi edotti dell'esistenza di sistemi di videosorveglianza, anche attraverso un modello semplificato di informativa "minima", messo a disposizione dal Garante (art. 13, comma 3, del Codice), consistente in un cartello con un simbolo che rappresenta una telecamera, valido per la videosorveglianza posta in essere in aree esterne. In tutte le altre ipotesi, devono essere altresì indicati gli elementi di cui all'art. 13 con particolare riguardo alle finalità e all'eventuale conservazione dei dati.

Prior checking

Nel citato provvedimento generale, il Garante ha anche ricordato che, di regola, l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo dell'Autorità e che non si applica il principio del silenzio-assenso. Pertanto, non può desumersi alcuna approvazione implicita dalla semplice trasmissione al Garante di progetti relativi alla intenzione di installare sistemi di videosorveglianza, peraltro spesso incompleti o comunque privi di quegli elementi che consentirebbero di valutare il rispetto del principio di proporzionalità.

La verifica preventiva da parte dell'Autorità è invece obbligatoria per le tecnologie particolarmente invasive, come quelle che prevedono intrecci, interconnessioni, collegamenti delle immagini con altri particolari dati personali (ad es. biometrici) o in caso di digitalizzazione o indicizzazione delle immagini o di videosorveglianza cd. dinamico-preventiva, che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi, caratteristiche fisionomiche o eventi improvvisi.

Bilanciamento

Per quanto riguarda il settore privato, con il provvedimento in questione ha trovato applicazione anche la disciplina che prevede il bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice) individuando i casi in cui è possibile effet-

tuare la rilevazione di immagini anche senza il consenso dell'interessato, ritenendosi prevalente il legittimo interesse del titolare, con un impiego circoscritto dei sistemi di videosorveglianza nei limiti previsti dal provvedimento.

Notificazione

I trattamenti di dati nell'ambito di un'attività di videosorveglianza devono essere notificati al Garante solo se rientrano in una delle ipotesi previste dall'art. 37 del Codice; in ogni caso, non devono essere notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio (v. *Provv*. 31 marzo 2004, relativo ai casi da sottrarre all'obbligo di notificazione, nonché il *Parere* 23 aprile 2004, recante chiarimenti sui trattamenti da notificare al Garante).

Numerose segnalazioni e reclami sul trattamento di dati effettuato tramite sistemi di videosorveglianza installati da studi professionali, esercizi commerciali, società, enti *no-profit*, hanno reso necessario effettuare accertamenti *in loco* spesso in collaborazione con la Guardia di finanza. In alcuni di questi casi, precedenti all'adozione del nuovo provvedimento generale, è stato necessario contestare gli illeciti di omessa notificazione al Garante del trattamento effettuato mediante impianti di videosorveglianza e/o di mancata adozione di un'idonea informativa agli interessati circa la presenza dei predetti sistemi, comprovata dall'assenza di avvisi o cartelli recanti le indicazioni prescritte dalla vigente normativa in materia di protezione dei dati personali. I relativi titolari del trattamento sono stati, inoltre, richiamati al rispetto delle precise garanzie fissate nel provvedimento del 29 aprile e a fornire un riscontro al riguardo (*Note* 27 ottobre 2004). Anche a seguito dell'adozione del predetto provvedimento del 29 aprile, sono state accertate *in loco* e contestate alcune violazioni dell'obbligo di informativa, che i titolari del trattamento non hanno reso neanche nella forma semplificata suggerita dal Garante con il modulo allegato al provvedimento (v., al riguardo, par. 20.3). In altri casi in cui gli elementi acquisiti in sede ispettiva hanno consentito di escludere la commissione di illeciti da sanzionare, l'Autorità ha comunque richiamato i titolari al rispetto delle prescrizioni contenute nel provvedimento medesimo (*Nota* 29 novembre 2004).

Impianti di videosorveglianza su treni e stazioni

In relazione ad un progetto sperimentale di Trenitalia S.p.A., relativo all'installazione di sistemi di videosorveglianza su taluni vagoni dei treni che transitano su specifiche tratte ferroviarie oggetto di ripetuti atti vandalici e di episodi di microcriminalità a danno dei passeggeri, l'Autorità (v. *Note* 11 novembre 2003 e 25 novembre 2004), preso atto di taluni accorgimenti adottati spontaneamente dalla società a protezione dei dati (effettuazione delle riprese con modalità volte ad escludere l'ingrandimento dell'immagine e la ripresa degli scompartimenti dei passeggeri; memorizzazione delle immagini riprese in forma criptata; predisposizione di un'informativa agli interessati), ha prescritto l'adozione di alcune misure: in particolare, individuare i responsabili e gli incaricati del trattamento; ridurre al minimo, ove tecnicamente possibile, i tempi di conservazione giornaliera delle immagini prima della loro cancellazione; adottare idonee misure di sicurezza dei sistemi e dei dati raccolti. Trenitalia S.p.A. ha recentemente comunicato al Garante che, per ragioni tecnico-organizzative, la sperimentazione non avrebbe avuto inizio prima della fine del 2004, impegnandosi a fornire, entro il primo semestre del 2005, una relazione dettagliata sullo stato di avanzamento del progetto.

Sempre in relazione all'impiego di impianti di videosorveglianza nel settore del trasporto ferroviario, va segnalato un parere che il Garante ha reso ad una società del gruppo Ferrovie dello Stato circa un'iniziativa sperimentale da avviare con la colla-

borazione di una società telefonica (v. *Nota* 29 ottobre 2004). Il progetto consiste nell'installazione presso tre stazioni (Roma Fiumicino, Anzio, Taormina) di alcune telecamere con inquadratura panoramica e rilevazione di immagini a bassa definizione da trasmettere via Internet attraverso il portale *web* della società per finalità di carattere pubblicitario. Gli impianti, inoltre, permettono la visualizzazione delle immagini solo in presa diretta, senza possibilità per l'utente di accedere a registrazioni, né di scaricare le informazioni sul proprio *computer*, o di effettuare variazioni di inquadratura o di dimensioni dell'immagine visualizzata. Il Garante, confermando quanto aveva già precisato con un provvedimento del 14 giugno 2001, ha fatto presente che questo tipo di sistema di videosorveglianza non si pone in contrasto con quanto affermato nel provvedimento del 29 aprile 2004, poiché le telecamere installate non consentono di identificare (neanche indirettamente) gli interessati, in ragione della distanza dal luogo ripreso o delle altre caratteristiche tecniche.

La società ha inoltre sommariamente descritto le caratteristiche di un diverso sistema di videosorveglianza, costituito da telecamere ad alta risoluzione e utilizzato dalla Polizia ferroviaria per finalità di tutela dell'ordine e della sicurezza pubblica. Con lo stesso parere, quindi, l'Autorità ha precisato che quest'ultimo sistema rientra invece nell'ambito applicativo del Codice; e ha altresì sottolineato che il trattamento di dati personali effettuato attraverso l'impianto deve essere pienamente conforme ai principi di necessità, finalità e proporzionalità richiamati nel citato provvedimento generale, e che occorre rispettare, pur in presenza di pericoli concreti o dell'esigenza di prevenzione di specifici reati, le competenze che le leggi assegnano a tali scopi solo ad organi giudiziari e di polizia giudiziaria.

Recentemente l'Autorità ha avuto comunicazione da Trenitalia S.p.A. della messa in servizio, dal 9 settembre 2004, dei treni regionali "Minuetto", dotati di particolari sistemi di videosorveglianza. Si tratta di un'iniziativa scaturita da indicazioni emerse nel corso dei lavoro del Comitato interministeriale sulla sicurezza dei trasporti (Cist) che, ai fini di tutela dell'ordine e sicurezza pubblica, ritiene che tra le misure prioritarie da adottare vi sia anche la videosoveglianza sui treni. L'Autorità è in procinto di definire i termini della propria eventuale attivazione.

12.2. *Videosorveglianza in ambito pubblico*

Frequenti sono stati gli interventi del Garante con riferimento a sistemi di videosorveglianza posti in essere da comuni, da istituti scolastici o da luoghi di cura pubblici.

Ambiti sanitari

A questo riguardo, l'Autorità ha espresso il proprio avviso in ordine alla liceità dell'uso di telecamere presso alcune Asl al fine di assicurare un livello adeguato di sicurezza all'interno dei locali e fronteggiare episodi di aggressione a danno di guardie mediche (*Note* 15 luglio 2004).

L'Autorità ha così precisato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti od ambienti, stante la natura sensibile di alcuni dati che possono essere in tal modo raccolti, devono essere circoscritti ai soli casi di stretta indispensabilità e limitando le riprese a determinati locali e a precise fasce orarie. Deve inoltre essere adottato ogni ulteriore accorgimento necessario per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione delle misure che il Codice prescrive per le strutture sanitarie.

È stato ribadito, inoltre, che il titolare deve assicurare che l'accesso alle immagini sia limitato solo ai soggetti specificamente autorizzati, evitando che siano visionate

da estranei. Rigorose cautele sono state indicate anche in relazione alla possibilità di accedere alle riprese da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione). In tali ipotesi, i familiari possono comunque visionare, con gli adeguati accorgimenti tecnici, l'immagine del proprio congiunto. Stante il divieto di divulgazione dei dati idonei a rivelare lo stato di salute, deve essere prevenuto il rischio di diffondere immagini di persone malate su *monitor* accessibili al pubblico.

Esigenze di sicurezza

L'Autorità ha fornito ancora chiarimenti in risposta a quesiti posti da alcuni comandi provinciali dei vigili del fuoco e dall'Istat circa la possibilità di installare sistemi di videosorveglianza presso l'ingresso, l'atrio e il vano scala della sede degli edifici, per ragioni di sicurezza e tutela del patrimonio dell'ente (*Nota* 30 novembre 2004), nonchè per controllare l'accesso del pubblico, onde evitare che utenti esterni possano accedere ad aree vietate (*Note* 15 luglio 2004).

In particolare è stato evidenziato, sulla scorta di precedenti provvedimenti dell'Autorità, che le riprese potrebbero riguardare anche i lavoratori dipendenti e configurare, pertanto, un controllo a distanza nei confronti dei medesimi. A tal proposito, si è richiamata nuovamente l'attenzione sulle garanzie da osservare nell'ambito dei rapporti di lavoro anche quando gli impianti siano utilizzati per esigenze organizzative e dei processi produttivi, ovvero siano richiesti per la sicurezza del lavoro, con particolare riguardo al principio contenuto nell'art. 4 della l. n. 300/1970 che sancisce il divieto di controllo a distanza dell'attività dei lavoratori.

Istituti scolastici

Con riferimento agli istituti scolastici, è stata sottoposta all'attenzione dell'Autorità la questione riguardante l'installazione di telecamere presso alcuni istituti (*Note* 18 agosto 2004 e 24 dicembre 2004) al fine di controllare gli accessi all'edificio e dissuadere dal compimento di atti di vandalismo.

Al riguardo, è stato evidenziato che l'installazione di sistemi di videosorveglianza può essere giustificata nelle sole aree interessate, soltanto se strettamente indispensabile (ad esempio in caso di ripetuti atti vandalici) e, comunque, al di fuori dell'orario scolastico, quando gli edifici sono chiusi.

È necessario, in ogni caso, rispettare il diritto alla riservatezza dello studente (art. 2, comma 2, d.P.R. n. 249/1998), anche in considerazione del fatto che, frequentemente, lo studente è un minore.

In applicazione di questi principi, l'Autorità è intervenuta a proposito dell'installazione, secondo quanto segnalato da alcune notizie di stampa, di numerose telecamere all'interno e all'esterno di un edificio scolastico. L'Ufficio ha invitato l'istituto a conformarsi alle citate prescrizioni e a produrre ogni documento utile a sostegno delle iniziative assunte (*Nota* 10 settembre 2004), ricevendo un tempestivo riscontro sul quale sono stati però attivati ulteriori accertamenti.

Luoghi di culto

Il Garante è altresì intervenuto al fine di assicurare l'intimità di chi accede a luoghi di culto, quali chiese od altri luoghi di ritrovo dei fedeli, invitando i titolari ad un uso particolarmente prudente dei mezzi di ripresa in ragione del potenziale discriminatorio dei trattamenti riguardanti tali informazioni sensibili, relative alla sfera religiosa dell'individuo, e a limitare l'utilizzo di telecamere nei luoghi di sepoltura ai casi in cui via sia concreto rischio di atti vandalici.

Camere ardenti

Ciononostante, a seguito di un ciclo ispettivo, è stata rilevata l'installazione da parte di un comune di un sistema di videosorveglianza presso un edificio all'interno del quale vengono allestite camere ardenti per la veglia dei defunti. Tali telecamere

12

non erano segnalate mediante le necessarie informative previste dal Codice, ed anzi erano celate alla vista del pubblico. A seguito di un invito da parte dell'Autorità ad effettuare il blocco spontaneo del trattamento, gli uffici comunali hanno sospeso le attività di videosorveglianza, sulla cui complessiva liceità e sull'eventuale applicazione di sanzioni l'Autorità si esprimerà a breve.

13 Condomìni e multiproprietà

13.1. *Protezione dei dati e condomìni*

Diversi profili di protezione dei dati personali in ambito condominiale, approfonditi negli anni precedenti, sono stati ripresi nel corso del 2004 per rispondere al rilevante numero di segnalazioni e quesiti pervenuti in materia all'Autorità.

In particolare, sono stati posti –sia da parte degli interessati, sia da amministratori di condominio– numerosi quesiti in merito alla diffusione di dati personali riguardanti eventuali situazioni di morosità di singoli condòmini. Ciò, allo scopo di verificare se le modalità di volta in volta utilizzate in concreto, in quanto potenzialmente idonee a rendere tali informazioni accessibili ad un numero indeterminato di soggetti esterni al condominio, fossero compatibili, ed in quali limiti, con le disposizioni contenute nella normativa sulla tutela dei dati personali. Su tale argomento, l'Autorità ha confermato la posizione già assunta in provvedimenti e decisioni adottate nel corso degli anni precedenti.

Il Garante ha avuto modo di precisare che il singolo condòmino può avere conoscenza dei dati disponibili presso l'amministratore, relativi anche agli indirizzi degli altri condòmini, poiché gli indirizzi, così come i nominativi degli interessati, oltre a rendere possibile l'individuazione di ciascun proprietario, sono utili per consentire il regolare svolgimento della vita condominiale (ad esempio, in caso di convocazione dell'assemblea da parte dei condomini o per la comunicazione di avvisi).

L'Autorità ha specificato, inoltre, che i principi in materia di condominio sono applicabili anche nei confronti della gestione di edifici in multiproprietà a scopo residenziale e, con riferimento agli indirizzi di comproprietari che abbiano domicilio o residenza diversi dall'immobile in multiproprietà, qualora ciò sia necessario per particolari e reali esigenze collegate alla gestione della cosa e interessi comuni (*Nota* 11 agosto 2004).

Per contro, in un altro caso sottoposto alla sua attenzione, il Garante ha ribadito che il condominio deve adottare, anche tramite l'amministratore, tutte le cautele necessarie per evitare che terzi non legittimati vengano indebitamente a conoscenza dei dati relativi ai condomini (*Nota* 20 ottobre 2004).

Impianti di videosorveglianza nei condomìni

In relazione al frequente impiego di sistemi di videosorveglianza nei condomìni, il provvedimento del 29 aprile 2004 ha precisato che i videocitofoni sono utilizzabili per identificare coloro che si accingono ad entrare in luoghi privati e che la loro installazione, quando non sono predisposti da persone fisiche per fini esclusivamente personali (art. 5, comma 3, del Codice), deve essere resa nota attraverso un'informativa agevolmente rilevabile.

Quanto all'installazione di vere e proprie telecamere ad iniziativa di singoli condòmini all'interno di edifici in condominio e loro pertinenze (es. posti auto, *box*), il Garante ha precisato che l'impiego di tali sistemi, pur non rientrando nell'ambito di applicazione delle disposizioni del Codice, a meno che i dati siano comunicati sistematicamente o diffusi (art. 5, comma 3, del Codice), richiede comunque l'adozione di cautele a tutela dei terzi. In particolare, l'angolo visuale delle riprese deve essere rigorosamente limitato ai soli spazi di propria esclusiva per-

13

tinenza, ad esempio antistanti l'accesso alla propria abitazione, escludendo ogni forma di ripresa anche senza registrazione di immagini relative ad aree comuni (cortili, pianerottoli, corridoi, scale, garage comuni) o antistanti l'abitazione di altri condomini; ciò, anche al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.).

Il Codice si applica, invece, in caso di installazione di sistemi di ripresa di aree condominiali da parte di più proprietari o condòmini oppure ad iniziativa di un condominio o della relativa amministrazione (comprese le amministrazioni di *residence* o multiproprietà). In questi casi, l'installazione di impianti è ammissibile a condizione che ricorrano determinate finalità, quali l'esigenza di preservare la sicurezza di persone e la tutela di beni in presenza di concrete situazioni di pericolo (di regola costituite da illeciti già verificatisi); la valutazione di proporzionalità, da effettuare anche nei casi di utilizzazione di sistemi di videosorveglianza che non prevedano la registrazione dei dati, va effettuata in rapporto ad altre misure già adottate o che è possibile adottare (es. sistemi comuni di allarme, blindatura o protezione rinforzata di porte e portoni, cancelli automatici).

Un caso particolarmente delicato ha riguardato l'installazione da parte di un condominio di un impianto di videosorveglianza finalizzato a garantire la sicurezza dei condòmini in seguito ad un grave delitto verificatosi in uno stabile vicino. L'Autorità ha ritenuto che, nel caso di specie, trovassero applicazione le prescrizioni e i principi richiamati nel citato provvedimento del 29 aprile, ed ha invitato l'amministrazione del condominio a fornire un riscontro dettagliato su finalità e proporzionalità del trattamento, tempi di conservazione delle immagini registrate, nonché sull'eventuale designazione del responsabile dell'impianto come "responsabile" o "incaricato" del trattamento delle immagini, il quale potrebbe accedere ai dati solo attenendosi alle istruzioni del condominio (*Nota* 5 ottobre 2004).

14 Dati biometrici

14.1. *Protezione dei dati e biometria*

L'impiego di sistemi di rilevazione di impronte digitali comporta chiaramente un trattamento di dati personali, intendendosi in tal senso "*ogni informazione relativa a persona fisica,…, identificat[a] o identificabil[e], anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" (art. 4, comma 1, lett. *b*), del Codice). Tale trattamento di dati personali può avvenire solo se proporzionato rispetto alle finalità che si vogliono perseguire: il titolare, prima ancora di dare inizio al trattamento, deve quindi valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione di un sistema di rilevazione delle impronte digitali sia in concreto realmente proporzionata, anche nelle modalità prescelte, rispetto agli scopi prefissi e legittimamente perseguibili.

In questo ambito, sono pervenute all'Ufficio numerose richieste di cittadini relative all'installazione, da parte di alcune banche, di sistemi di rilevazione biometrica per l'accesso alle filiali associati ad apparecchiature di videosorveglianza. In un caso del tutto particolare, originato dalla segnalazione relativa all'utilizzo di un sistema di rilevazione dell'impronta digitale per l'accesso ad una banca, l'Autorità (*Nota* 29 ottobre 2004), ribadendo il chiaro orientamento già espresso che delimita l'uso a casi del tutto eccezionali, valuterà quanto dichiarato dalla banca circa le specifiche e concrete esigenze di sicurezza che hanno giustificato l'installazione dell'impianto (nell'Agenzia segnalata si erano verificati due episodi di rapina). Nel frattempo, ha segnalato interlocutoriamente alla banca la necessità di adottare talune misure: predisporre meccanismi che, in caso di libera indisponibilità dell'utente al rilascio dei propri dati biometrici, gli permettano comunque di accedere alla banca; abbinare il sistema di rilevazione ai comuni dispositivi d'ingresso già in uso, evitando il ricorso a meccanismi complicati ed ulteriori rispetto a quelli già comunemente utilizzati per l'ingresso in banca.

Sul tema dell'impiego da parte delle banche di dati biometrici, eventualmente in associazione a sistemi di videosorveglianza, è in corso un approfondimento con l'Associazione bancaria italiana che, anche a seguito di alcuni incontri con l'Ufficio, si è impegnata a far pervenire gli elementi necessari per consentire all'Autorità di esprimersi nuovamente in materia a seguito di una completa valutazione dell'entità e rilevanza del fenomeno. Uno specifico approfondimento si è avuto, inoltre, in occasione di un convegno organizzato presso la Confindustria.

Il Garante, infine, sta effettuando accertamenti specifici a seguito di alcune segnalazioni circa l'impiego, da parte di talune società, di tecniche di autenticazione biometrica (impronta palmare o facciale) per la rilevazione delle presenze del personale dipendente, in considerazione del fatto che il trattamento di dati biometrici in tale ambito è in molti casi eccedente e ingiustificato alla luce dei principi di necessità e proporzionalità.

Dati biometrici in ambito pubblico

Ulteriori interventi hanno riguardato l'installazione di impianti di rilevazione delle impronte digitali per il controllo degli accessi ai luoghi di lavoro o a servizi di mensa universitaria.

In merito all'iniziativa di un ente regionale per il diritto allo studio, volta ad

installare lettori di impronte digitali in ristoranti e pizzerie convenzionati al fine di controllare che l'accesso al servizio di ristorazione avvenisse esclusivamente da parte degli aventi diritto, l'Autorità aveva già avuto modo di chiarire nei primi mesi del 2004 che tale sistema era sproporzionato rispetto alle finalità di controllo della spesa perseguite (*Newsletter* 12-18 gennaio 2004).

In seguito, il Garante ha accertato che tale ente regionale per il diritto allo studio ha nuovamente manifestato la concreta volontà di installare tali sistemi di rilevazione delle impronte digitali per l'accesso ai servizi di ristorazione convenzionati, avendo riscontrato un aumento degli ingressi a tali esercizi di ristorazione da parte di soggetti non autorizzati. L'Autorità ha quindi disposto il blocco del trattamento di dati personali degli studenti effettuato tramite tale sistema di rilevazione delle impronte digitali, riaffermando il principio secondo cui la raccolta generalizzata di dati biometrici di un gruppo selezionato di individui (tutti gli studenti universitari iscritti ad un ateneo) risulta sproporzionata rispetto ad un generico bisogno di "regolare l'utilizzo del servizio ristorazione" in assenza di reali esigenze di sicurezza determinate da concrete e gravi situazioni di rischio (*Provv.* 16 dicembre 2004).

In tale occasione, è stato anche ribadito che i sistemi di rilevazione di impronte digitali rappresentano una *extrema ratio,* potendo essere attivati solo quando, dopo matura riflessione, altre misure (nel caso esaminato, la vigilanza all'ingresso delle mense, ovvero l'esibizione del tesserino di riconoscimento da parte degli studenti) siano valutate del tutto insufficienti o inattuabili, e non quando tale scelta risulti semplicemente meno costosa o di più rapida attuazione ovvero risponda a mere esigenze di apparenza o di "prestigio".

Sono in corso, inoltre, vari approfondimenti in merito a diversi progetti attivati da enti pubblici diretti a sostituire il normale controllo degli accessi al luogo di lavoro (foglio firme, *badge* magnetico) con sistemi di rilevazione delle impronte digitali o di altri dati biometrici come la geometria della mano.

15 Reti di comunicazione elettronica

15.1. *Notazioni introduttive*

Il rapido sviluppo tecnologico degli ultimi anni ha reso sempre più urgente l'individuazione a favore degli utenti dei servizi di comunicazione elettronica di un elevato livello di protezione dei diritti della personalità, con particolare riguardo alla protezione dei dati e del segreto nelle comunicazioni.

Anche in considerazione della crescente convergenza fra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione, l'Autorità è intervenuta, cooperando talora con altri soggetti istituzionali (come riferito nel par. 21.4) e con i diversi operatori del settore, svolgendo un'ampia serie di attività: adozione di provvedimenti, attività istruttorie ed ispettive (in taluni casi a seguito di ricorsi decisi dall'Autorità); intense, inoltre, le attività di studio e monitoraggio che in alcuni casi, come si vedrà più avanti, sono giunte ad uno stadio avanzato, con l'apertura di procedure di consultazione pubblica.

15.2. *Dati di traffico*

Si è già dato conto (v. *Relazione 2003*) delle modifiche apportate all'art. 132 del Codice, in materia di conservazione di dati di traffico per finalità di accertamento e repressione di reati (*ex* art. 3, decreto-legge 24 dicembre 2003 n. 354, convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45). Si può qui brevemente ricordare che, nella sua formulazione originaria, l'art. 132 prevedeva che, per le predette finalità, i fornitori di servizi di comunicazione elettronica dovessero conservare i dati relativi al traffico telefonico per trenta mesi; il citato decreto legge, approvato a ridosso dell'entrata in vigore del Codice, aveva prolungato il periodo di conservazione ad un periodo massimo di cinque anni, estendendolo anche al traffico su Internet.

Tale soluzione suscitò forti preoccupazioni anche al di fuori del circuito istituzionale; il Garante manifestò forti riserve, soprattutto alla luce della prevista estensione delle nuove regole al traffico su Internet, che avrebbe determinato una forte compressione delle garanzie della persona, anche in relazione ai principi costituzionali in materia di libertà delle comunicazioni e segretezza della corrispondenza.

La soluzione adottata in sede di conversione del decreto-legge ha portato a sopprimere ogni riferimento ai dati di traffico diversi da quello telefonico (in particolare Internet), determinando in complessivi quattro anni i tempi di conservazione dei soli dati di traffico telefonico.

Analoghe preoccupazioni, con espresso riferimento all'ipotesi di conservazione dei dati di traffico telematico, sono state ribadite dall'Autorità –nell'audizione in Commissione giustizia della Camera dei Deputati il 24 novembre 2004– in sede di esame del disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (del quale si è riferito nel par. 1.2).

In questa occasione sono stati richiamati, oltre al quadro normativo europeo e nazionale e alla giurisprudenza costituzionale in materia di segretezza delle comuni-

15

cazioni, anche le conclusioni cui è pervenuto lo stesso Parlamento, in particolare nel corso della discussione del decreto-legge n. 354/2003 (cfr. par. 1.2). Nell'ambito dei dati di traffico telematico è stata altresì sottolineata la difficoltà di distinguere, anche sul piano tecnico, i dati "esteriori" (tutelati anch'essi dalla garanzia costituzionale, ma acquisibili sulla base di un ordine di esibizione da parte dell'autorità giudiziaria, senza le garanzie previste dal codice di procedura penale in materia di intercettazioni) da quelli di "contenuto". Infatti, vi sono diversi casi in cui dati apparentemente "esteriori" sono idonei a rivelare il contenuto della comunicazione (ad esempio, i messaggi allegati alle *e-mail*, i contenuti di *chat* e *newsgroup*), le scelte della persona e, in alcuni casi, anche dati sensibili (è il caso di dati di accesso ai siti *web*).

Fermo restando il potere-dovere dell'autorità giudiziaria e di polizia di accedere a fonti di prova eventualmente disponibili in base alla legge (ad es. i dati di traffico telefonico), è stato evidenziato il rischio che un eventuale obbligo di (indiscriminata) conservazione di tutti i dati di traffico telematico configuri già, esso stesso, una sostanziale limitazione della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione.

Con riferimento alla conservazione dei dati di traffico telefonico, il Garante, conformemente alla previsione dell'art. 132, comma 5, del Codice, ha avviato i lavori necessari a individuare le misure e gli accorgimenti al cui rispetto è subordinato il trattamento per le finalità di accertamento e repressione dei reati. A tale scopo sono stati acquisiti elementi utili nel corso di incontri con diversi operatori telefonici, al fine della verifica preliminare dei sistemi attualmente utilizzati, in conformità con quanto stabilito dall'art. 17, comma 2, del Codice, cui l'art. 132, comma 5, fa espresso richiamo.

Accesso ai dati di traffico

Per quanto concerne l'accesso ai dati personali relativi alle comunicazioni telefoniche "in entrata", l'Autorità ha più volte sottolineato (v., da ultimo, *Provv.* 18 febbraio 2004) come il Codice realizzi al riguardo un primo bilanciamento tra il diritto dell'interessato di conoscere i dati che lo riguardano e il diritto alla riservatezza di terzi (utenti chiamanti e soggetti chiamati diversi dall'abbonato), circoscrivendo il diritto del chiamato di accedere ai dati identificativi di telefonate in entrata alle sole informazioni la cui mancata conoscenza possa comportare "*un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397*" (art. 8, comma 2, lett. *f*), del Codice).

L'Autorità ha ricordato che l'interessato può presentare la propria richiesta di accesso anche prima che sia instaurato un procedimento penale: l'attività investigativa può essere svolta, ai sensi dell'art. 391-*nonies* c.p.p., anche dal difensore che ha ricevuto apposito mandato dalla persona offesa dal reato, per l'eventualità che si instauri un procedimento penale (*Provv.* 15 aprile 2004). Il Garante, pertanto, ha accolto una richiesta di accesso a dati personali relativi al traffico telefonico "in entrata", avendo ritenuto che sussistesse un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive che poteva derivare al ricorrente dalla mancata identificazione del numero telefonico chiamante.

Come evidenziato già nella *Relazione* 2003, il diritto d'accesso ai dati relativi al traffico telefonico può essere esercitato dall'interessato soltanto nei confronti dei dati che lo riguardano, risultando inammissibile la richiesta volta a identificare utenze diverse da quella dell'interessato medesimo.

In relazione a ciò, e in particolare all'accesso ai dati relativi alle chiamate nella telefonia mobile, l'Autorità ha valutato con esito positivo la risposta fornita da un operatore ad una richiesta formulata ai sensi dell'art. 157 del Codice. Il Garante, in particolare, aveva chiesto di conoscere la procedura predisposta dalla società e le

misure di sicurezza adottate al fine di identificare i soggetti che richiedono l'accesso stesso utilizzando il telefono mobile o i servizi *on-line*.

15.3. *I nuovi elenchi telefonici*

La disciplina degli elenchi è stata oggetto di significative modifiche. Scopo peculiare degli elenchi è di consentire la ricerca degli abbonati per le comunicazioni interpersonali; ciò è ora previsto espressamente dall'art. 129, comma 2, del Codice che sancisce, in relazione a tale finalità, il principio della massima semplificazione per l'inserimento degli abbonati negli elenchi e, per le finalità ulteriori, la necessità del preventivo consenso specifico ed espresso degli interessati.

In applicazione di tale principio, e in esito ad un'intensa attività svolta anche in collaborazione con l'Autorità per le garanzie nelle comunicazioni, il Garante ha individuato le modalità da osservare per il corretto inserimento e successivo utilizzo dei dati personali degli abbonati nei nuovi elenchi telefonici (*Provv*. 15 luglio 2004).

Nei nuovi elenchi telefonici possono essere pubblicati anche i dati relativi alle utenze mobili, nonché informazioni ulteriori quali l'indirizzo di posta elettronica, la professione e il titolo di studio. Nel caso in cui l'interessato abbia manifestato il proprio consenso a ricevere informazioni commerciali o promozionali, l'indirizzo o il numero telefonico saranno contrassegnati da uno speciale simbolo: in tal modo l'abbonato potrà ricevere pubblicità telefonica tramite operatore o materiale pubblicitario a domicilio. Diversamente, nel caso di iniziative pubblicitarie realizzate mediante sistemi automatizzati (fax, chiamate senza operatore, messaggi *sms* o di posta elettronica), è comunque necessario raccogliere a parte il consenso specifico dell'interessato. Le scelte espresse dagli interessati possono essere modificate in ogni momento e senza alcun onere.

Il Garante ha altresì predisposto, con la cooperazione dell'Autorità per le garanzie nelle comunicazioni e la collaborazione delle associazioni dei consumatori, un modulo di informativa e richiesta di consenso che gli operatori telefonici devono inviare ai propri clienti entro il 31 gennaio 2005.

Successivamente all'adozione del provvedimento, si sono svolti presso l'Autorità ulteriori incontri con rappresentanti degli operatori telefonici e delle associazioni di consumatori. Nel corso di tali incontri, e principalmente dall'esame dei primi moduli predisposti dalle diverse compagnie, sono emersi alcuni elementi che hanno reso necessario un nuovo intervento del Garante, volto a fornire agli operatori stessi prescrizioni integrative di quelle già impartite, nonché a dare l'avvio alla campagna informativa prevista nel provvedimento stesso.

L'Autorità ha curato una prima campagna di informazione attraverso un apposito *depliant*, che, su sua autorizzazione, verrà inviato dai gestori al domicilio degli abbonati. Un'apposita conferenza stampa si è tenuta il 26 gennaio 2005.

15.4. Spam

È costantemente all'attenzione dell'Autorità il fenomeno dell'invio ad indirizzi di posta elettronica di comunicazioni non sollecitate, non solo di contenuto commerciale, ma anche riconducibili all'ambito del cd. *marketing* politico (cfr. *Provv*. 12 febbraio 2004, oltre al più recente provvedimento del 12 ottobre 2004, presi in considerazione nel par. 8.2).

Gli utenti della Rete hanno manifestato un'accresciuta sensibilità in relazione al

fenomeno *spam*, desumibile dall'intenso contenzioso che ha investito l'Autorità anche nel 2004 (come ricordato nel par. 18.3), oltre che dalle azioni proposte dinanzi all'autorità giudiziaria ordinaria.

Sono proseguite le attività di controllo e verifica effettuate presso i fornitori di servizi di comunicazione elettronica (individuati grazie alle segnalazioni pervenute) al fine di accertare eventuali violazioni dell'art. 130 del Codice e delle prescrizioni contenute nel provvedimento di carattere generale emanato dal Garante il 29 maggio 2003.

Per arginare il fenomeno, il Garante ha partecipato ad alcuni incontri tenuti presso il Ministero delle comunicazioni, cui sono intervenuti operatori di telefonia fissa e mobile, e associazioni di fornitori dei servizi Internet e dei consumatori.

In tali incontri si è lavorato alla possibile stesura di un codice di autoregolamentazione in relazione al quale è stata chiesta la collaborazione di questa Autorità, che fornirà il proprio contributo tenendo però presente il valore cogente delle norme che saranno contenute nel codice di deontologia e di buona condotta per Internet (v. par. 15.8).

Proprio in questo settore, grande rilievo sugli organi di informazione ha avuto la vicenda relativa all'indagine giudiziaria curata dalla Guardia di finanza nei confronti di una società quotata in borsa in relazione all'utilizzo di migliaia di indirizzi *e-mail* per finalità di *marketing*, in assenza del consenso informato degli interessati.

Sulla vicenda, per la quale sono indagati due responsabili della società per reati che vanno dall'illecito trattamento dei dati personali alla frode informatica ed all'accesso abusivo a sistemi informatici, il Garante ha ricevuto di recente copia di alcuni atti e valuterà a breve l'eventuale adozione dei provvedimenti di competenza.

15.5. Sms *istituzionali*

In occasione delle elezioni del 12 e 13 giugno 2004, gli utenti di telefonia mobile hanno ricevuto *Sms* "firmati" dalla Presidenza del Consiglio dei ministri con i quali si comunicavano orari e modalità di voto delle imminenti consultazioni elettorali.

A seguito di più di 4500 reclami e segnalazioni il Garante, al fine di acquisire ogni elemento idoneo a valutare la questione, ha richiesto informazioni al Ministero dell'interno (che aveva disposto l'invio degli *Sms* con proprio d.m. del 9 marzo 2004) ed agli operatori di telefonia mobile.

Pur prendendo atto dell'esistenza nel caso specifico di un formale provvedimento del Ministro che ravvisava ragioni contingibili e urgenti, l'Autorità ha sottolineato in termini generali il rischio che impropri riferimenti all'eccezionalità, all'emergenza e alle calamità possano condurre ad una "banalizzazione" dell'invio di messaggi *Sms* da parte di diversi soggetti istituzionali, anche a livello locale (*Provv*. 7 luglio 2004).

Il Garante aveva peraltro già individuato nella eccezionalità e straordinarietà delle circostanze le condizioni per l'invio di comunicazioni via *Sms*, anche in mancanza di previo consenso dell'interessato (*Provv*. 12 marzo 2003).

In relazione alla decisione del Ministero dell'interno di indicare la Presidenza del Consiglio dei ministri come firmataria del messaggio, l'Autorità ha rilevato come nel caso di specie non operasse una disposizione della legge n. 150/2000 sulla comunicazione istituzionale, che riguarda l'invio di messaggi da parte della concessionaria del servizio pubblico radiotelevisivo (art. 3). Con riferimento all'invio di *Sms* in caso di disastri o calamità naturali o per ragioni di tutela dell'ordine pubblico, il soggetto istituzionale "mittente" delle comunicazioni deve poi essere sempre identificabile.

Nel medesimo provvedimento è stata altresì evidenziata la necessità per gli operatori telefonici di integrare l'informativa fornita ai cittadini inserendo la previsione dell'eventualità che, tra i vari trattamenti di dati legati alle utenze, vi sia quello dell'invio di *Sms* istituzionali per effetto di provvedimenti d'urgenza. Tutte le compagnie telefoniche interessate hanno integrato il modello di informativa come richiesto dal Garante.

È stata da ultimo richiesta la cooperazione del Garante da parte della Presidenza del Consiglio dei ministri e del Ministero degli affari esteri ai fini dell'acquisizione dalle compagnie di telefonia di alcuni dati relativi all'utenza mobile di cittadini italiani che si trovavano nelle zone colpite dal maremoto in Asia del 26 dicembre 2004; ciò, in particolare, al fine di consentire al Ministero di inviare un *Sms* agli interessati, invitandoli a dare notizie di sé (cfr. anche par. 1.3 e 15.10).

15.6. *Videochiamate*

Ha formato oggetto di esame da parte dell'Autorità il fenomeno delle cd. videochiamate, ossia le chiamate –realizzate attualmente tramite la rete *Umts*– nel corso delle quali vengono trasmesse, oltre ai suoni, anche immagini dei soggetti coinvolti nella conversazione. La caratteristica peculiare dei trattamenti realizzati in occasione delle videochiamate consiste nel fatto che, a differenza di quanto accade con l'invio degli *Mms* (in relazione al quale si veda il *Provv*. 12 marzo 2003), le immagini vengono trasmesse contestualmente all'effettuazione della chiamata e coinvolgono il chiamante, il chiamato ed eventuali persone situate nelle loro vicinanze.

Ferma restando la generale liceità dell'utilizzo di tali nuove applicazioni tecnologiche, sono di tutta evidenza anche i potenziali pericoli insiti nelle stesse: le videocamere, infatti, oltre ad essere normalmente di dimensioni assai ridotte, il più delle volte non sono dotate di dispositivi acustici o visivi atti a rivelarne il funzionamento all'esterno.

Al fine di acquisire ulteriori elementi di valutazione, il Garante ha attivato una consultazione pubblica preordinata ad un provvedimento che fornirà indicazioni di carattere generale sul corretto utilizzo dei nuovi telefoni mobili c.d. di terza generazione.

15.7. *Servizi di comunicazione elettronica offerti a titolo gratuito*

Non di rado viene rappresentata da parte di utenti dei servizi gratuiti di accesso ad Internet ed alla posta elettronica l'impossibilità di esprimere un consenso specifico e differenziato con riferimento alle diverse finalità del trattamento operato dai fornitori dei medesimi servizi. In particolare, viene talvolta negata la stessa opportunità di usufruire dei predetti servizi nel caso in cui l'utente non presti il consenso al trattamento dei dati per finalità pubblicitarie e commerciali.

In occasione della trattazione di uno specifico ricorso (*Provv*. 12 ottobre 2004) il Garante ha chiarito che è improprio richiedere un ampio e generalizzato consenso –peraltro anche quando lo stesso Codice permette di prescindere da esso, come, ad esempio, per l'eventuale comunicazione dei dati all'autorità giudiziaria (cfr. art. 24, comma 1, lett. *a*), del Codice)– associandovi finalità pubblicitarie e di profilazione per le quali non è lasciata all'utente alcuna libertà nella manifestazione di volontà. La mancata richiesta di consensi differenziati (e limitatamente ai casi in cui sono necessari) determina un quadro confuso che non permette all'utente di esprimere scelte libere, consapevoli e non contraddittorie fra loro.

In questa prospettiva, l'Autorità ha riaffermato la necessità che il consenso sia realmente espresso senza condizionamenti che ne influenzino sotto vari profili la libera manifestazione (art. 23, comma 3, del Codice).

Quanto all'eventuale trattamento dei dati dell'interessato per finalità di profilazione, è stato precisato che tale trattamento potrebbe risultare lecito in determinate circostanze qualora, per i rapporti contrattuali, la società preveda l'assegnazione di un accesso gratuito ad Internet dietro "corrispettivo" di una profilazione lecita, corretta e proporzionata dell'interessato medesimo.

15.8. *Il codice deontologico*

Nell'ambito delle iniziative promosse in vista della predisposizione del codice deontologico e di buona condotta sui trattamenti dei dati personali effettuati dai fornitori dei servizi di comunicazione ed informazione offerti per via telematica (art. 133 del Codice), è stata avviata la consultazione delle organizzazioni rappresentative degli operatori del settore e dei consumatori che hanno aderito all'invito a partecipare formulato in precedenza dall'Autorità. Ciò è stato ritenuto opportuno al fine di identificare, congiuntamente ai soggetti a vario titolo interessati, gli aspetti che presentano particolari criticità sotto il profilo della protezione dei dati.

Alla luce dei primi contributi pervenuti, nonché degli studi da tempo avviati dalla stessa Autorità, sono state individuate alcune specifiche questioni che potranno essere oggetto di disciplina nell'adottando codice. Tra queste si ricordano, ad esempio, le modalità ed i contenuti dell'informativa; i profili relativi all'acquisizione del consenso ed ai diritti degli interessati; l'adozione di particolari misure di sicurezza; gli strumenti tecnici e giuridici di contrasto del fenomeno dello *spamming*, ivi compresa l'adozione di procedure di filtraggio o altre misure praticabili; l'individuazione di bollini di qualità per il trattamento dei dati posti in essere dagli operatori del settore; i problemi relativi alla registrazione dei nomi a dominio.

La definizione del codice in questione potrà fornire, sia agli operatori, sia agli utenti delle reti di comunicazione elettronica, riferimenti più precisi per assicurare il rispetto della normativa sulla protezione dei dati personali e, in particolare, dei principi generali di cui all'art. 11 del Codice.

15.9. *La televisione digitale: i servizi interattivi*

L'Autorità ha ultimato uno specifico studio sulle caratteristiche della televisione satellitare e interattiva individuando alcuni primi aspetti di rilevanza per la normativa sulla protezione dei dati personali.

Grazie allo sfruttamento delle potenzialità offerte dalla tecnologia digitale, è possibile offrire attraverso la televisione anche servizi caratterizzati dall'interattività: attraverso il collegamento di un apposito apparecchio (*decoder*) alla linea telefonica, l'utente può, ad esempio, partecipare a sondaggi, giochi, test o usufruire di particolari servizi di pubblica utilità erogati dalle amministrazioni pubbliche (cd. *T-government*), o ancora, usufruire di servizi cd. transattivi, previa identificazione ed autorizzazione, grazie all'inserimento nel *decoder* medesimo di particolari "carte identificative" (*smart card*).

Agli indubbi vantaggi derivanti da questa tecnologia, si affiancano, tuttavia, alcune criticità con riguardo alla tutela della sfera privata degli utenti: l'uso dei servizi e programmi interattivi può determinare un'esposizione, anche inconsapevole,

dei gusti, delle abitudini ed in generale della personalità dell'utente. Questi dati, opportunamente raccolti e trattati, potrebbero dare luogo al monitoraggio delle preferenze e dell'attività dell'utente medesimo. La circostanza che la raccolta dei dati avvenga in un ambito tipicamente "privato" (come quello familiare, nel quale l'individuo nutre la ragionevole aspettativa di essere al riparo da forme di controllo esterne) suscita ulteriori preoccupazioni. Inoltre, ad uno stesso apparecchio televisivo corrispondono di regola più fruitori (appartenenti o estranei al nucleo familiare dell'abbonato), i quali debbono essere messi in grado di compiere liberamente le proprie scelte in merito al trattamento dei dati personali che li riguardano.

Proprio al fine di approntare idonee cautele onde evitare che siano svolte illecite operazioni di profilazione ed invasive forme di controllo sulle abitudini delle persone, l'Autorità ha avviato una consultazione pubblica in vista della predisposizione di un provvedimento a carattere generale.

15.10. *Dati relativi all'ubicazione*

Negli ultimi anni si è assistito ad una rapida diffusione dei servizi basati sull'ubicazione. Tali servizi, pur presentando aspetti di indubbia utilità, possono comportare seri rischi per le libertà civili dell'interessato, potendo determinare un'esposizione, anche inconsapevole, dello stesso ad un controllo sistematico dei suoi spostamenti ovvero dei gusti e delle abitudini manifestati in occasione di specifiche richieste.

In questa prospettiva assume una particolare importanza il fatto che l'interessato sia pienamente a conoscenza delle caratteristiche del trattamento di dati che lo riguarda, nonché dei soggetti che svolgono il trattamento medesimo; ciò, anche al fine di prestare un consenso libero, specifico ed informato.

Proprio in ragione della particolare delicatezza di tali trattamenti, l'Autorità intende offrire indicazioni e chiarimenti ai soggetti che vogliano fornire tali tipologie di servizi. Al riguardo si segnala che il Garante sta ultimando la predisposizione di un provvedimento di carattere generale a completamento di quanto già disposto in materia dall'art. 126 del Codice.

Uno sviluppo di queste problematiche si è avuto con la menzionata richiesta della Presidenza del Consiglio dei ministri di acquisire dai vari gestori di telefonia mobile i dati di cittadini italiani che, in relazione alle informazioni sull'ubicazione dell'apparecchio disponibili presso i gestori stessi, risultavano trovarsi negli stati colpiti dal maremoto in Asia (v. par. 1.3 e 15.5).

Ferma restando la necessità di bilanciare la tutela della riservatezza con esigenze di salvaguardia della vita e dell'incolumità delle persone, questa vicenda pone (su un piano più generale) l'interrogativo se i dati relativi all'ubicazione degli apparecchi di telefonia mobile (e quindi, indirettamente, delle persone che li detengono), allorché siano diversi dai dati relativi al traffico telefonico –assistiti, questi ultimi, dalle garanzie costituzionali di libertà e segretezza della corrispondenza– godano comunque di una tutela costituzionale, e quale, anche alla luce del principio della libertà di circolazione (art. 16 Cost.).

15.11. Radio Frequency Identification

Il Garante ha seguito con grande attenzione lo sviluppo delle tecniche di identificazione via radiofrequenze (*Radio Frequency Identification-Rfid*).

Tali tecnologie si fondano sull'utilizzo di micro-processori che, collegati ad

15

un'antenna ed impiegati come etichette di riconoscimento (*cd. etichette intelligenti*), sono in grado di trasmettere –attraverso onde radio– segnali leggibili da appositi lettori dotati di un'antenna di attivazione/ricezione.

La *Rfid* rappresenta uno strumento utile in numerosi settori e per diverse finalità: essa può essere impiegata, ad esempio, per il "tracciamento" di singole unità di prodotto nella catena di distribuzione dell'industria; per la prevenzione di furti e di contraffazioni dei prodotti; per garantire una maggiore rapidità nelle operazioni commerciali; per il controllo degli accessi ad aree riservate. L'utilizzo di questa tecnologia può, in alcuni casi, comportare un trattamento di dati personali rendendo necessaria l'applicazione della relativa normativa. Attraverso le cd. "etichette intelligenti" si possono trattare, anche senza che l'interessato ne sia a conoscenza, innumerevoli dati personali che lo riguardano, compresi quelli di natura sensibile; raccogliere dati sulle abitudini del medesimo ai fini di profilazione attraverso l'aggregazione con altre informazioni di carattere personale; verificare prodotti (vestiti, accessori, medicine, ecc.) indossati o trasportati; tracciare i percorsi effettuati.

Il Garante ha svolto una prima attività di approfondimento della materia in questione, rivolgendo l'attenzione al possibile impatto che le tecniche di identificazione via radio possono già avere sulle condizioni di esercizio delle libertà delle persone e alle problematiche che la loro introduzione è destinata a sollevare relativamente all'applicazione della normativa sulla tutela dei dati personali.

Tutto questo anche in vista del fatto che, se attualmente il terreno di elezione della *Rfid* appare ancora il settore industriale (soprattutto all'interno della catena di distribuzione, dove però la sua applicazione non comporta, il più delle volte, un trattamento di dati personali), tale tecnologia presenta enormi potenzialità: in prospettiva, anche in vista dell'ulteriore sviluppo tecnologico, dell'abbattimento dei costi di produzione, della possibilità di integrazione con altre infrastrutture di rete (telefonia, Internet, ecc.), le tecniche di identificazione via radio-frequenza potranno avere un impiego sempre maggiore e nei più diversi settori.

Occorre tenere altresì presente che più gravi pericoli per gli interessati possono derivare dal prevedibile incremento della potenza dei sistemi di *Rfid* (i quali potrebbero rendere fattibile una "lettura" delle etichette a maggiori distanze) nonché –specie in ragione dell'adozione di *standard* tecnici comuni– dalla possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, "riscrittura").

L'attività istruttoria compiuta dall'Autorità in merito al trattamento dei dati nell'ambito della *Rfid* si è svolta anche attraverso contatti in Italia e all'estero con alcuni operatori del settore, che hanno portato ad un proficuo scambio di informazioni.

Consultazione pubblica

Al medesimo scopo è stata indetta una specifica consultazione pubblica cui è stata data ampia visibilità anche attraverso il sito *web www.garanteprivacy.it*. A completamento delle informazioni già acquisite, l'Autorità si è così potuta avvalere degli ulteriori elementi di valutazione provenienti da osservazioni e commenti inviati dalle associazioni di utenti, consumatori, operatori dei settori interessati e singoli cittadini.

Impianto sottocutaneo di etichette *Rfid*

Uno dei più recenti ambiti di utilizzo di questa tecnologia riguarda l'impianto sottocutaneo di dispositivi *Rfid* anche su persone. Si ha già notizia dell'avvio, anche in Italia, di tecniche di inserimento di *microchip* nel corpo umano per diverse finalità: ad esempio, allo scopo, di conservare e rendere all'occorrenza disponibili informazioni sullo stato di salute del paziente; al fine di verificare l'accesso a determinati luoghi riservati; ancora, per garantire pagamenti rapidi in transazioni commerciali di vario tipo.

La delicatezza di tali interventi è di tutta evidenza, sì da sollevare interrogativi circa le ripercussioni che i relativi trattamenti possono avere sulla dignità della persona (art. 2, comma 1, del Codice).

15

16 Sicurezza dei dati e dei sistemi

16.1. *Le misure minime di sicurezza*

L'Autorità –a seguito di numerose richieste di proroga e di chiarimenti pervenute circa il nuovo quadro normativo in materia di misure minime di sicurezza introdotto dal Codice– ha precisato che l'applicazione delle misure minime (artt. 33-35 del Codice e allegato B), la cui omessa adozione costituisce reato (art. 169 del Codice), va graduata a seconda che i trattamenti di dati personali, sensibili e giudiziari, siano effettuati con o senza l'ausilio di strumenti elettronici. Queste misure rappresentano, però, solo i requisiti minimi ai quali tutti i titolari del trattamento (anche a mezzo del responsabile, ove designato) devono attenersi nella protezione dei dati. Vi è, infatti, il dovere più generale di adottare misure preventive idonee (art. 31 del Codice), la cui mancata predisposizione può esporre il titolare a responsabilità civile per eventuali danni cagionati a terzi (*Nota* 22 marzo 2004).

Nella stessa sede il Garante ha ricordato anche che la redazione del Documento programmatico sulla sicurezza (Dps) rientra tra le misure minime di sicurezza e che qualsiasi titolare pubblico o privato deve redigerlo se effettua un trattamento di dati sensibili e/o giudiziari con strumenti elettronici.

Inoltre, le misure minime già previste dal d.P.R. n. 318/1999 e riprodotte nell'allegato B) restano obbligatorie senza differimenti. Il termine transitorio, di recente nuovamente prorogato al 30 giugno 2005 (decreto-legge 9 novembre 2004, n. 266, convertito, con modificazioni, con legge 27 dicembre 2004, n. 306; salva l'ulteriore proroga al 30 settembre 2005, da riferire al solo caso in cui obiettive ragioni tecniche non consentano di adottare subito alcune misure) riguarda, infatti, solo le "*nuove*" misure minime che non erano già previste dal citato d.P.R. n. 318/1999 (art. 180, comma 1 e 3, del Codice).

L'Autorità ha inoltre precisato che è sostenibile ipotizzare che la redazione del Dps sia una "nuova" misura minima, con la conseguenza che, anche per questo adempimento, vale il termine del 30 giugno 2005. Il Garante ha poi messo a disposizione degli operatori, sul proprio sito *web*, una guida utilizzabile per agevolarne la redazione soprattutto presso le realtà medio-piccole.

Gli stessi principi sono stati tra l'altro confermati dall'Autorità nel già richiamato parere reso al Consiglio nazionale forense (*Nota* 3 giugno 2004) sui principali adempimenti in materia di protezione di dati personali nello svolgimento dell'attività forense, con il quale si è anche precisato che, per quanto riguarda l'organizzazione del lavoro quotidiano di studio, non occorre affatto depennare il nome delle parti dalla copertina dei fascicoli cartacei ed utilizzare solo numeri identificativi. Resta invece necessario seguire opportune modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti.

L'orientamento del Garante è stato inoltre ribadito con un recente parere, anch'esso già menzionato (*Nota* 3 dicembre 2004), in materia di trattamento dei dati personali da parte dei notai rilasciato al Consiglio nazionale del notariato (v. pure par. 10.2).

Su richiesta di un dipendente di un ufficio legale comunale, l'Autorità ha rilevato i limiti entro i quali un dirigente può utilizzare la *password* del dipendente per accedere ai dati contenuti nel suo *computer* in caso di assenza di quest'ultimo.

L'adozione di un sistema di "autenticazione informatica" per gli incaricati del trattamento effettuato con strumenti elettronici rientra tra le misure "minime" di sicurezza aggiornate dal Codice. Secondo le modalità tecniche specificate nell'allegato B) del Codice, tale sistema deve basarsi sull'attribuzione all'incaricato di credenziali di autenticazione che possono consistere anche in un codice per l'identificazione associato ad una parola chiave riservata conosciuta solamente a quest'ultimo (regole nn. 1 e 2).

In particolare, quando i dati sono accessibili soltanto attraverso l'uso di parole chiave è possibile rendere disponibili le medesime informazioni solo in caso di prolungata assenza o impedimento dell'incaricato, sempre che l'intervento si rilevi indispensabile e indifferibile e sia altresì esclusivamente motivato da esigenze di operatività o di sicurezza del sistema. Proprio in vista di tali evenienze, è necessario individuare con chiarezza le modalità attraverso le quali il titolare può assicurare la disponibilità dei dati mediante idonee e preventive indicazioni fornite per iscritto. In tal caso, l'incaricato deve essere tempestivamente informato dell'intervento effettuato (regola n. 10 dell'allegato B).

Tali accorgimenti, oltre a consentire di proteggere i dati personali contenuti nella memoria dell'elaboratore dalla possibile intrusione di soggetti non autorizzati –specie se si tratta di dati giudiziari, come del caso sottoposto all'esame dell'Autorità–, permettono contestualmente di renderli disponibili in particolari casi di necessità e urgenza per trattamenti consentiti ed effettuati secondo modalità predeterminate chiaramente per iscritto dal titolare (*Nota* 16 luglio 2004).

A conclusione degli accertamenti svolti in seguito ad alcune segnalazioni relative alla raccolta e al trattamento di dati personali di clienti effettuato da una società nell'ambito di un servizio sperimentale di gestione *on-line* di polizze assicurative, l'Autorità ha ritenuto soddisfacente il riscontro fornito circa le misure tecniche ed organizzative adottate a protezione delle transazioni effettuate sul proprio *server web*. Gli accessi alle banche di dati personali relativi alle polizze assicurative, consentiti solo ad utenti registrati in apposite aree riservate del sito *web* della società, sono risultati protetti tramite specifiche misure di sicurezza (cd. protocollo *https*).

Si è comunque ricordato alla società che, per il trattamento di dati personali sensibili e/o giudiziari effettuato con strumenti elettronici, devono essere comunque adottate preventivamente idonee misure di sicurezza (art. 31 del Codice), oltre a quelle minime prescritte dal Codice (*Nota* 22 ottobre 2004).

L'Autorità sta concludendo accertamenti a seguito di un reclamo con il quale si è segnalata la diffusione di dati personali causata dall'asserito abbandono di documenti, da parte di una filiale della banca, in occasione del rilascio dei locali ove si svolgeva la sua attività (*Nota* 29 luglio 2004).

Il Garante si è inoltre pronunciato sul reclamo di un lavoratore che contestava le modalità di consegna di una lettera di sanzione disciplinare da parte del datore di lavoro (*Nota* 23 novembre 2004). Il dipendente aveva ricevuto una comunicazione di sanzione disciplinare contenuta in un foglio non spillato, né racchiuso in busta sigillata, consegnatogli a mano e recante la chiara indicazione dell'oggetto della lettera e della sanzione comminata. Dando attuazione ai principi di proporzionalità, pertinenza e non eccedenza dei dati, è stato chiesto alla società di prevedere che la comunicazione della sanzione all'interessato venga in ogni caso inserita in busta chiusa e sigillata; è stato inoltre prescritto di impartire precise istruzioni a tutti gli uffici e dipendenti formalmente incaricati di tali trattamenti di dati, volte all'ado-

16

zione di modalità e misure idonee a garantire la sicurezza e la riservatezza di comunicazioni contenenti dati relativi ai lavoratori interessati e ad evitare un accesso, anche casuale, da parte di terzi non autorizzati ai dati riportati al loro interno.

Ricevuta la segnalazione di un dipendente di una società che, alla ripresa del servizio dopo un prolungato periodo di assenza dal lavoro, non aveva trovato alcuni documenti personali lasciati in un armadio aziendale, l'Autorità dovrà valutare se sussistono o meno profili di violazione della normativa di protezione dei dati, anche in relazione alla circostanza che i documenti in questione siano relativi a trattamenti effettuati per ragioni di servizio.

17 Registro dei trattamenti

17.1. *La notificazione*

Linee normative

La nuova modalità di notificazione del trattamento dei dati personali al Garante (disciplinata dagli artt. 37, 38, 181, comma 1, lett. *c*), del Codice) presenta profondi cambiamenti sia nei contenuti, sia nelle modalità di compilazione, rispetto alla precedente normativa (artt. 7, 16 e 28, l. n. 675/1996): basti qui ricordare che, mentre quest'ultima prescriveva un obbligo di carattere generale di notificazione per un numero consistente di trattamenti –salve, comunque, le varie eccezioni previste dalla legge–, il Codice reca ora un più ristretto "elenco positivo" di trattamenti soggetti ad obbligo di notificazione, che il Garante può peraltro sviluppare attraverso un proprio provvedimento, il che attesta la conformità della soluzione innovativa ora prescelta dal legislatore italiano alla direttiva europea.

Il provvedimento di esonero

Il Garante si è già avvalso del potere di esonerare dal predetto obbligo alcuni trattamenti rientranti nelle generali previsioni di cui all'art. 37, ma in concreto ritenuti non suscettibili di recare specifico pregiudizio ai diritti e alle libertà dell'interessato (art. 37, comma 2). In base a tale disposizione con il provvedimento n. 1 del 31 marzo 2004 (v. *Documentazione* par. 39), l'Autorità ha individuato diverse ipotesi di trattamento sottratte all'obbligo di notificazione: è stato previsto, ad esempio, un esonero per il trattamento di dati genetici e biometrici trattati in maniera non sistematica da esercenti la professione sanitaria, purché non organizzati in banche dati accessibili da terzi; o, ancora, per il trattamento dei medesimi dati da parte degli avvocati, purché necessario a condurre investigazioni difensive o a far valere o difendere un diritto anche da parte di terzi in sede giudiziaria. È altresì possibile che, all'esito di questa prima fase di applicazione del Codice, si possano individuare, anche in collaborazione con le categorie interessate, ulteriori esoneri dall'obbligo di notificazione.

Il Garante ha poi ritenuto, allo stato, di non individuare ulteriori trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in aggiunta alla lista figurante nell'art. 37, comma 1, e pertanto da sottoporre all'obbligo di notificazione.

Ulteriori chiarimenti del Garante

Dopo il provvedimento che ha espressamente escluso la notificazione per alcuni trattamenti di dati personali, l'Autorità ha fornito numerosi chiarimenti per il settore privato (imprese, banche, assicurazioni, professionisti, enti *no-profit*) su alcuni trattamenti che devono ritenersi comunque sottratti all'obbligo di notificazione in base ad una corretta interpretazione delle disposizioni del Codice (*Nota* 23 aprile 2004; v. anche *Newsletter* n. 209 del 5-25 aprile 2004); ulteriori chiarimenti sono stati forniti in risposta a quesiti presentati dalla FnomCeo, dalla Fimmg e dall'Anisap, circa l'esatta individuazione dei trattamenti da notificare al Garante in ambito sanitario (*Nota* 26 aprile 2004; v. anche *Newsletter* n. 210 del 26 aprile-2 maggio 2004, consultabili sul sito *web* dell'Autorità).

La nuova notificazione

Accanto alla forte riduzione del numero dei trattamenti, è stata operata contemporaneamente, alla luce dell'esperienza, una drastica semplificazione dei contenuti e delle

17

modalità di compilazione del modello informatico. La nuova notificazione può avvenire anzitutto solo in via telematica e accompagnata dalla firma digitale; gli elementi richiesti sono pochi, ma significativi, di immediata comprensione e di facile redazione.

Il nuovo sistema ha così prodotto solo un numero limitato di notificazioni (circa 10.000 rispetto alle oltre 330.000 pervenute precedentemente ai sensi della legge n. 675/1996), circoscrivendo l'istituto alle sole ipotesi di trattamento "rischioso" per gli interessati, come prescritto dalla normativa comunitaria, e azzerando i casi di notificazione irregolare che avevano comportato in passato un onere assai rilevante per l'Ufficio del Garante.

Risoluzione di inconvenienti tecnici

Alcune temporanee e iniziali difficoltà tecniche dovute all'enorme traffico telematico registrato a ridosso della scadenza del termine per adempiere all'obbligo di notificazione fissato per il 30 aprile 2004 hanno indotto il Garante, avvalendosi delle facoltà previste dall'art. 38 del Codice, a riconoscere ulteriori quindici giorni a coloro che avevano tempestivamente intrapreso le operazioni di notificazione e che, per impossibilità tecniche a loro non imputabili, non erano riusciti a concludere la procedura. Alcuni interventi sulla stampa di dirigenti dell'Ufficio hanno ricostruito i punti estremamente interessanti di questo primo riuscito esperimento generalizzato nella p.a. di utilizzo della firma digitale per la produzione di un atto a rilevanza giuridica anche penale.

Il consistente potenziamento della banda trasmissiva utilizzata anche da molti visitatori interessati ad analizzare la procedura pur non dovendo notificare in concreto, e il breve differimento al 15 maggio 2004 del termine per concludere la notificazione hanno offerto agli utenti idonee opportunità di completare le operazioni di notificazione senza ulteriori problemi.

I vantaggi della procedura telematica

La procedura per la notificazione in via telematica ha dato ottima prova anche sotto l'aspetto della facilità d'uso. Il fatto che la medesima possa essere avviata e portata a termine nella sua interezza da una qualsiasi postazione, in qualunque momento e con l'assistenza *on-line* da parte del personale dell'Autorità durante l'orario d'ufficio, costituisce un indubbio vantaggio per l'utente.

Le procedure telematiche di notificazione si sono rivelate di qualità elevata per celerità nell'effettuare adempimenti e ricerche, affidabilità del programma di gestione, correttezza dei dati inseriti e puntualità nei riscontri.

Ulteriori prospettive

Permane tra gli obiettivi del Garante quello di mantenere alta la qualità del sistema di notificazione arricchendolo nel tempo di ulteriori elementi e procedure anche al fine di tenerlo al passo con lo sviluppo tecnologico e le prospettive di miglioramento complessivo delle attività dell'Autorità.

Accanto al perfezionamento dell'attuale versione, non va esclusa nel medio periodo la possibilità che, in conformità a quanto verrà deciso a livello europeo sulla standardizzazione della notificazione nei vari paesi, siano apportate modifiche al registro dei trattamenti e ai contenuti della notificazione. Una delle modifiche potrebbe, ad esempio, riguardare la redazione del modello anche in lingua inglese.

Nel corso dell'anno 2005 il Dipartimento registro dei trattamenti sarà comunque impegnato già nella predisposizione e messa a disposizione del modello di notificazione in lingua tedesca (come già avvenuto per la provincia di Bolzano con il vecchio modello di notificazione su carta).

Doppia notificazione

Nonostante il sistema di notificazione risulti agevole anche a fronte delle istruzioni esaustive e replicate in diversi passaggi della procedura, si sono riscontrati

pochi casi (limitati a qualche decina) di doppia notificazione da parte dello stesso titolare o di richiesta di annullamento di quella già inviata in quanto non dovuta.

L'orientamento dell'Ufficio è stato quello di restituire l'importo dei diritti di segreteria a coloro che, pur avendo iniziato la notificazione, non avevano ancora proceduto all'invio della medesima al Garante. Nei casi di doppia notificazione, invece, su dichiarazione del titolare, l'Ufficio ha provveduto ad "oscurare" una delle due, restituendo i diritti di segreteria pagati in eccesso.

Annullamento di notificazione inviata

Non sono state accolte, invece, le richieste di semplice "annullamento" della notificazione da parte di coloro che l'avevano validamente inviata, nonostante fosse a posteriori ritenuta non dovuta secondo il giudizio sopravvenuto del (solo) titolare del trattamento. Questo diverso orientamento si giustifica con il fatto che in tali casi la notificazione è regolarmente inserita nel registro (pubblico) dei trattamenti e ha dispiegato i suoi effetti (tenuto conto, tra l'altro, che l'inserimento nel registro non produce conseguenze negative sul titolare).

Assistenza agli utenti

Come già detto, il Garante ha fornito –e continua a fornire– ai soggetti tenuti alla notificazione un'attività di assistenza che si sostanzia in diverse forme: risposta ai numerosi quesiti e dubbi sulla notificazione, comunque formulati; controlli costanti dei messaggi inoltrati via *web* dagli utenti in caso di sospensione della notificazione e immediato riscontro via posta elettronica; effettuazione di controlli richiesti dai vari dipartimenti del Garante in occasione di istruttorie, attività ispettive e ricorsi.

17.2. *Il registro dei trattamenti e futuri sviluppi*

Le notificazioni regolarmente presentate sono confluite nel registro dei trattamenti.

Tale registro si è rivelato di maggiore utilità ed efficacia rispetto al precedente, non solo al fine di predisporre interventi ispettivi nei confronti di soggetti tenuti alla notificazione. Ulteriori benefici provenienti dal *database* riguardano, infatti, la possibilità di elaborare più efficacemente varie statistiche: esse costituiscono un importante strumento di comprensione dei fenomeni che ruotano intorno a trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà degli interessati; forniscono, inoltre, al Garante un significativo quadro di insieme in merito ai trattamenti effettuati; danno impulso, infine, alle attività di controllo assistite dal nucleo della Guardia di finanza.

In tale prospettiva, il Garante intende procedere all'affinamento di specifiche statistiche e alla creazione di sistemi che prevedano l'invio di una segnalazione automatica nel caso in cui la notificazione contenga elementi che si ritiene debbano essere sottoposti ad approfondimento.

Particolare cura verrà posta nel riscontro automatico dei pagamenti dei diritti di segreteria effettuati mediante banca e uffici postali, con la collaborazione della banca tesoriera e di Poste S.p.A.

Controlli a campione e audizioni in caso di contestazioni amministrative

Esaurita la fase di immissione della maggior parte delle notificazioni alla scadenza del 30 aprile 2004, sono stati effettuati diversi controlli a campione sulla congruenza dei dati dichiarati, sul ritardo o l'omissione della notificazione. A richiesta, il notificante viene ammesso ad un'audizione nella quale un funzionario del dipartimento stila una relazione sullo stato della notificazione.

Notificazione dei trattamenti e direttiva 95/46/CE

Nell'ambito dell'attività del Gruppo dei Garanti europei istituito dall'art. 29 della direttiva 95/46/CE, l'istituto della notificazione si avvia ad una possibile fase di revisione in chiave europea che ne conferma tuttavia l'utilità e la persistente necessità, soprattutto nell'innovativa connotazione che assume quella italiana.

In ragione del margine di discrezionalità che ciascuno Stato membro ha nel dare attuazione alla direttiva, nei diversi paesi sono stati infatti realizzati nel tempo sistemi (in parte) differenti con riferimento a taluni aspetti attinenti ai contenuti, alle modalità, ai provvedimenti di esonero e al diverso utilizzo delle tecnologie. Tali peculiarità non agevolano un pronto confronto tra le applicazioni nei vari Stati e possono comportare qualche difficoltà applicativa nel caso in cui il trattamento sia effettuato da aziende con stabilimenti in più paesi.

Si è pertanto proceduto ad uno studio congiunto con le autorità degli altri 24 paesi per omogeneizzare l'istituto e semplificare gli adempimenti. Ciò dovrebbe portare, per quanto possibile, all'eliminazione di notizie ritenute meno utili e ad elaborare un insieme condiviso di informazioni.

L'Italia, che tra gli ordinamenti europei dispone di una modalità esecutiva della notificazione progredita, ha svolto la funzione di relatore sugli aspetti di semplificazione ed omogeneizzazione dell'istituto e ha assunto un ruolo attivo nella predisposizione di un *vademecum* illustrativo delle diverse modalità di notificazione da pubblicare sul sito *web* della Commissione europea.

Il precedente registro generale dei trattamenti

Il precedente registro generale dei trattamenti viene temporaneamente utilizzato per alcuni riscontri, confrontando quanto il titolare abbia dichiarato all'epoca e quanto contenuto nella nuova notificazione.

Come evidenziato nella *Relazione 2003*, gran parte dell'attività del Dipartimento registro dei trattamenti ha riguardato in passato la regolarizzazione delle numerose notificazioni pervenute su modello cartaceo; operazione, questa, risultata piuttosto lunga e faticosa, nonostante l'utilizzo di strumenti a scansione ottica dell'intero archivio.

Il complesso archivio cartaceo è stato distrutto e memorizzato in dischi Dvd.

17.3. *Alcuni dati statistici*

Al 31 dicembre 2004 risultano pervenute poco più di 10.000 notificazioni.

Rinviando, per quanto riguarda la rappresentazione grafica alle tabelle riprodotte al par. 25 –nel quale sono rinvenibili i dati statistici relativi alla tipologia di trattamento notificato (tabella e grafico 14), alla distribuzione delle notificazioni per aree geografiche (grafico 15) o per tipologia di soggetto notificante, pubblico o privato (tabella e grafico 16); da ultimo si rappresentano le modalità di invio della notificazione (grafico 17)– si segnala qui che per il versamento dei diritti di segreteria, gli utenti si sono avvalsi, per il 80% circa dei casi, di forme tradizionali di pagamento (mediante conto corrente postale o bonifico bancario); una percentuale significativa (20%) ha preferito, tuttavia, il pagamento *on-line* mediante carta di credito.

Notificazioni pervenute tramite intermediari

Oltre il 46% delle notificazioni è pervenuto tramite intermediari, il che conferma l'utilità dell'iniziativa di stipulare convenzioni con organismi privati e pubblici per l'invio della notificazione con firma digitale.

Dei quattro intermediari con i quali il Garante ha stipulato la convenzione, Poste S.p.A. è stato quello più utilizzato dagli utenti privi di dispositivo di firma digitale.

18 Esercizio dei diritti e trattazione dei ricorsi

18.1. *Considerazioni generali*

Il ricorso al Garante come "*passepartout*". Questa immagine può dar conto in modo efficace del ruolo e del significato che lo strumento di tutela disciplinato negli artt. 145 e ss. del Codice è andato assumendo nel pur ampio spettro di quelli offerti dall'ordinamento.

A sei anni dall'entrata in vigore delle disposizioni applicative contenute nel d.P.R. 31 marzo 1998, n. 501 che, nel febbraio 1999, hanno dato concretezza e piena possibilità di esplicazione a questo meccanismo di tutela (originariamente previsto dall'art. 29 della legge n. 675/1996), il bilancio relativo al suo concreto utilizzo è senza dubbio positivo.

Dopo una necessaria fase di "rodaggio", la riflessione sulla portata e sull'estensione della nozione "dato personale", definita ora all'art. 4, comma 1, lett. *b*), del Codice (e sulle connesse possibilità di tutela) ha fatto sì che venissero pienamente apprezzate le potenzialità contenute nell'elenco di diritti di cui all'art. 7 del Codice (i soli in ordine ai quali può essere proposto un ricorso).

Di conseguenza, al più consueto esercizio del diritto di accesso ai dati personali (che, peraltro, si è andato estendendo dalla sfera dei comuni dati oggettivi, ai dati personali contenuti in giudizi ed alle informazioni di tipo valutativo: si vedano i provvedimenti del 19 aprile 2004 e 29 aprile 2004), si è affiancato l'utilizzo delle altre situazioni giuridiche soggettive contemplate dal medesimo art. 7: in particolare, per menzionare le ipotesi presentatesi più di frequente, il diritto di conoscere l'origine dei dati, le finalità e le modalità del trattamento come pure la logica applicata alle operazioni effettuate con strumenti elettronici; il diritto di ottenere l'aggiornamento, la rettificazione o l'integrazione dei dati, oltre alla possibilità di ottenere la cancellazione dei dati trattati in violazione di legge o di opporsi per motivi legittimi al loro trattamento, ancorché pertinenti allo scopo della raccolta.

Ma il vero punto di svolta, del quale la casistica dell'ultimo anno offre ampia prova, è l'utilizzo sempre più esteso dei diritti previsti dal Codice nell'ambito di più ampie e complesse vicende giudiziarie. Il ricorso tende quindi a trasformarsi da isolato (per quanto significativo) meccanismo di tutela, a strumento propedeutico o complementare (a volte anche strumentale) per rafforzarne altri già offerti dall'ordinamento ad ogni interessato. Ecco quindi che sempre più spesso si affaccia, nell'ambito della complessiva strategia processuale, l'utilizzo del ricorso in procedimenti giudiziari di tipo risarcitorio, in controversie di lavoro (volte alla ricostruzione di lunghi periodi di vita professionale) o relative al consapevole utilizzo di strumenti finanziari (v. *Provv.* 16 settembre 2004).

I dati statistici sono la migliore prova degli assunti precedenti: nell'anno solare 2004, con un incremento ancora più sensibile rispetto agli anni passati, sono stati esaminati e decisi dall'Autorità più di 700 formali ricorsi spesso piuttosto complessi. (cfr. par. 25.2).

Contributo spese per l'accesso ai dati

Con riferimento all'esercizio dei diritti dell'interessato, non sussistono differenze di fondo rispetto a quanto messo in evidenza in passato, avendo il Codice sostanzialmente riprodotto le previsioni normative in materia già contenute nelle previ-

gente disciplina, pur integrate con alcuni principi fissati dalla "giurisprudenza" del Garante in merito alle modalità di esercizio.

Al riguardo, occorre tuttavia sottolineare che l'Autorità, con il provvedimento del 23 dicembre 2004 (v. *Documentazione* par. 41), ha determinato i criteri per la fissazione del contributo spese relativo all'esercizio del diritto di accesso dell'interessato ai dati che lo riguardano; ciò, tenendo conto della tendenziale gratuità –confermata dal Codice, (art. 10, comma 8)– dell'esercizio di tale diritto, della normativa e della situazione in ambito comunitario e internazionale.

18.2. *Profili procedurali*

Novità introdotte dal Codice

Il 2004 ha visto la prima applicazione delle nuove disposizioni del Codice relative alle modalità di esercizio dei diritti di cui all'art. 7 e alla proposizione dei ricorsi: si tratta, in particolare, della possibilità di proporre ricorso dopo quindici giorni dalla ricezione dell'interpello preventivo da parte del titolare del trattamento; della durata del procedimento per la decisione del ricorso (ora di sessanta giorni); della possibilità di proroga di quaranta giorni di tale termine, anche su decisione dell'Ufficio; della previsione (contenuta nell'art. 150, comma 6, del Codice) secondo cui, in caso di mancata opposizione, il provvedimento, nella parte relativa all'ammontare delle spese e dei diritti, costituisce titolo esecutivo ai sensi degli artt. 474 e 475 del c.p.c.

Tali interventi, sia in ragione della loro limitata portata innovativa, sia in quanto rispondenti ad esigenze di razionalizzazione e di migliore gestione del procedimento, non hanno generato particolari problemi. Al contrario, la maggiore durata del procedimento (pur sempre assai contenuta) ha consentito di seguire in modo più accurato l'istruttoria dei ricorsi: sotto questo profilo, l'Ufficio e, in particolare, l'Unità ricorsi, ha potuto esercitare un ruolo più attivo, con frequenti richieste di integrazione della documentazione, preordinate ad assicurare il corretto svolgersi del contraddittorio, procedendo altresì all'assunzione di informazioni anche presso terzi.

Nei limitati casi in cui è stato segnalato un iniziale ritardo nella corresponsione della somma liquidata dal Garante a titolo di rimborso spese, l'Ufficio si è attivato al fine di accertare che il provvedimento non fosse stato impugnato ai sensi dell'art. 152 del Codice, con il conseguente pagamento da parte del soccombente.

Regolarizzazione e profili di inammissibilità

Negli ultimi mesi del 2004 è diminuito il numero dei ricorsi che formano oggetto di richiesta di regolarizzazione da parte dell'Ufficio per irregolarità o carenze sotto il profilo formale (con riferimento ai requisiti prescritti dall'art. 147 del Codice). A parte le informazioni quotidianamente fornite dall'Autorità attraverso l'Ufficio relazioni con il pubblico o il sito Internet *www.garanteprivacy.it*, si riscontra il diffondersi di moduli ed istruzioni (veicolate anche dalle associazioni dei consumatori) che facilitano l'accesso a questo strumento di tutela –e il suo corretto utilizzo– anche da parte dei singoli interessati (che, come noto, possono proporre il ricorso senza l'assistenza di un legale). Un nuovo modello per l'esercizio dei diritti è stato predisposto dall'Ufficio e pubblicato sul sito *web*, anche al fine di indurre gli interessati a concentrare l'attenzione sulle specifiche richieste di loro concreto interesse, caso per caso, nell'ambito della vasta gamma prevista dall'art. 7, semplificando anche i tempi per il riscontro e per la successiva tutela.

Continuano a pervenire, seppure in numero sempre più limitato, richieste di informazioni in ordine alla necessità di autenticazione della firma del ricorrente in calce al ricorso. In proposito si conferma l'obbligatorietà di tale requisito –ora spe-

cificamente previsto dall'art. 147, comma 4, del Codice– che non può essere sostituito dall'autocertificazione dell'interessato. L'Autorità ha recentemente ribadito tale necessità, rispondendo ad una richiesta di parere formulata dal Ministero dell'interno, Dipartimento per gli affari interni e territoriali.

Va infine ricordato che il Garante ha adottato, il 23 dicembre 2004 (e disposto la sua pubblicazione sulla Gazzetta Ufficiale), una nuova deliberazione concernente i casi di regolarizzazione dei ricorsi (art. 148, comma 2, del Codice), in sostituzione della delibera del 1° marzo 1999 adottata in occasione dell'entrata in vigore delle disposizioni del citato d.P.R. n. 501/1998.

In due occasioni, l'Autorità si è pronunciata in ordine a quanto disposto dall'art. 145, comma 2, del Codice in base al quale *"il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria"*. Con decisione del 4 ottobre 2004, è stato dichiarato inammissibile il ricorso proposto da un soggetto che aveva precedentemente prospettato la medesima questione innanzi ad una commissione tributaria provinciale. Al contrario, non si è ritenuta sussistente la fattispecie di cui all'art. 145, comma 2, in una decisione adottata il 21 ottobre 2004, ritenendosi ammissibile un ricorso al Garante avanzato a seguito del diniego opposto ad un'istanza di accesso ai dati formulata da un lavoratore già coinvolto in una controversia dinanzi al giudice del lavoro. Nel corso del procedimento giudiziario era stata avanzata una richiesta di esibizione di documenti (sulla quale il giudice si era riservato di decidere) ai sensi dell'art. 210 c.p.c. che, almeno in parte, potevano contenere alcuni dei dati personali poi richiesti con l'istanza *ex* art. 7. In proposito, l'Autorità ha rilevato l'ammissibilità del ricorso dal momento che –nonostante l'ipotetica coincidenza di alcuni documenti oggetto della domanda giudiziale rivolta al giudice con quelli contenenti le informazioni richieste ai sensi della normativa sulla protezione dei dati personali– i presupposti (*petitum*, *causa petendi*) sulla base dei quali il ricorrente aveva agito nel corso del giudizio erano diversi rispetto a quelli fatti valere innanzi al Garante.

Diritti di segreteria e determinazione delle spese del procedimento

A far data dal 15 gennaio 2005 è stata adeguata la misura dei diritti di segreteria che devono essere corrisposti per la presentazione di un ricorso all'Autorità.

I motivi di tale adeguamento, oltre al lungo tempo trascorso dalla prima deliberazione che li prevedeva (*Deliberazione* n. 1 del 18 febbraio 1999), sono solo in parte legati alla valutazione (ed alla connessa esigenza di parziale recupero) delle spese che l'Ufficio affronta per l'ordinaria gestione di tali procedimenti; procedimenti che comunque, come si è visto, presentano istruttorie maggiormente articolate, determinando oneri economici più elevati per l'Autorità e non compensati da correlativi aumenti di bilancio.

Da tale esborso, peraltro, l'interessato può essere tenuto indenne: va infatti ricordato che, su istanza di parte, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso posti a carico della parte soccombente (art. 150, comma 3).

18.3. *Brevi cenni sulla casistica*

Al di là dei riferimenti alle singole decisioni del Garante assunte in sede di ricorso e rinvenibili nell'intera *Relazione* in ragione della materia sulla quale sono andate ad incidere, si ritiene utile fornire qui un quadro d'insieme delle tematiche affrontate con i provvedimenti resi *ex* art. 150 del Codice, con particolare riguardo a quelle che sono state oggetto del maggior numero di ricorsi (rinviando, per la sintetica trat-

tazione del loro contenuto, alle diverse sezioni della presente *Relazione*).

Se gli ambiti interessati dai ricorsi sono stati i più vari –solo a fini esemplificativi, si menzionano qui le materie delle perizie medico-legali in ambito assicurativo, del rapporto di lavoro (pubblico e privato) e della videosorveglianza– non di rado le decisioni che ne sono scaturite hanno delineato un primo quadro di riferimento per provvedimenti più organici o rappresentato il punto di partenza per lo svolgimento di attività ispettive.

Settore bancario e finanziario

Dal punto di vista tipologico, si è registrato un elevato numero di decisioni nel settore bancario e finanziario, specie in riferimento a richieste di accesso riferite a tutti i dati e le informazioni di carattere personale detenute da un istituto di credito. Ad esso deve essere aggiunto il settore dei sistemi di informazione creditizia (Sic), già noti con la locuzione *"centrali rischi (private)"*, che ha registrato nel corso del 2004 una vera e propria esplosione del contenzioso. Ciò, anche a seguito della più ampia conoscenza del provvedimento generale adottato in materia dal Garante il 31 luglio 2002 (che ha costituito il primo tentativo di articolare i principi di protezione dei dati personali in un settore, quello appunto dei sistemi di informazione creditizia, sviluppatosi in Italia in assenza di uno specifico quadro normativo di riferimento) ed in relazione allo sviluppo dei lavori che hanno portato alla redazione ed all'adozione del codice deontologico di settore (pubblicato in *G.U.* 23 dicembre 2004, n. 300 in merito al quale v. par. 9.2.).

Nei numerosi provvedimenti adottati –oltre a rilevarsi l'esistenza di dati errati, incompleti o non aggiornati, o di constatare l'esistenza di dati comunicati ai Sic in assenza dei requisiti di liceità del trattamento (informativa e consenso espresso dell'interessato)– sono stati messi a fuoco tutti i principali problemi che la prassi operativa delle banche e delle società finanziarie (che consultano quotidianamente i predetti archivi) ha sollevato.

Si sono invece nettamente distinte dai dati trattati in riferimento alle operazioni di credito al consumo (oggetto di specifica tutela nel menzionato codice di deontologia) le informazioni (generalmente riferite a mutui ipotecari) presenti in altri archivi (cd. banche dati "Atti pubblici") che, parimenti, sono rese disponibili dai soggetti che gestiscono i sistemi di informazioni creditizie: si tratta di dati desunti dai pubblici registri immobiliari che i soggetti privati possono trattare anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*), del Codice). Sono trattamenti, questi ultimi, che allo stato non possono ritenersi illeciti, ma rispetto ai quali (con particolare riguardo alla pertinenza e alla completezza delle informazioni e alla conservazione dei dati stessi) saranno fornite a breve più specifiche indicazioni in sede di adozione dei codici di deontologia di cui agli artt. 61 e 119 del Codice.

Va infine ricordato il provvedimento del 16 settembre 2004 nel quale, per la prima volta, il Garante ha accolto la richiesta di cancellazione dall'archivio di un sistema di informazioni creditizie di dati riferiti ad una richiesta di abbonamento telefonico. Tali trattamenti sono stati infatti ritenuti incompatibili e non pertinenti con le funzioni specifiche delle centrali rischi volte, come detto, alla tutela del credito e al contenimento dei relativi rischi nel solo settore del credito al consumo.

Trattamenti effettuati da pubbliche amministrazioni

Fra gli altri profili affrontati nel corso dell'anno vanno sinteticamente ricordate, tra le tante, la decisione del 27 settembre 2004 relativa alla possibilità del ricorrente di accedere ai dati personali che lo riguardano contenuti in un esposto presentato a suo carico presso l'ente locale titolare del trattamento (ente presso il quale il ricorrente aveva prestato servizio) ed il provvedimento del 21 ottobre 2004, concernente la rettificazione dei dati di un insegnante detenuti da un istituto scolastico, con par-

ticolare riferimento a quelli contenuti nei certificati relativi al servizio prestato nei precedenti anni scolastici.

Trattamenti in rete

Al di là di singoli interventi nel settore delle comunicazioni elettroniche –si pensi, fra le altre, alla decisione del 24 marzo 2004 concernente la divulgazione a mezzo degli elenchi cartacei e *on-line* dei dati dell'interessato riferiti ad un'utenza telefonica che doveva rimanere "riservata"– merita segnalare la persistenza di un intenso contenzioso in ordine all'invio di comunicazioni pubblicitarie non sollecitate dirette a indirizzi di posta elettronica senza che risulti acquisito il previo consenso dell'interessato.

Trattamenti degli operatori telefonici

Va sottolineato anche il provvedimento del 25 maggio 2004 con il quale è stata accolta la richiesta dell'interessato di conoscere i dati personali relativi alle numerose carte telefoniche illecitamente attribuite al ricorrente per la dolosa condotta di un *dealer*.

19 Contenzioso giurisdizionale

19.1. *Considerazioni generali*

L'entrata in vigore del Codice ha avuto ripercussioni sull'attività dell'Autorità anche riguardo al contenzioso giurisdizionale, sia quello direttamente concernente provvedimenti del Garante, sia, più in generale, quello relativo all'applicazione del Codice stesso.

Quest'ultimo infatti, all'art. 152, da un lato, ha confermato l'originaria impostazione della legge n. 675/1996 relativamente alla procedura per l'impugnazione degli atti del Garante (specificando alcuni aspetti che avevano dato luogo ad incertezze negli anni passati) e, dall'altro, ha previsto un'apposita procedura per il coinvolgimento dell'Autorità in tutte le cause in materia di protezione dei dati personali.

In particolare, sotto il primo profilo, ribadito che tutte le controversie riguardanti l'applicazione del Codice sono devolute all'autorità giudiziaria ordinaria, l'art. 152, comma 2, precisa che l'azione deve proporsi con ricorso da depositarsi *"nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento"*.

Con tale formulazione si è confermata la scelta della giurisdizione e del foro competente, superandosi, fra l'altro, definitivamente il dubbio circa la possibilità di adire il giudice di pace, che risulta ora evidentemente esclusa.

I commi da 7 a 11 dell'art. 152 descrivono poi le fasi processuali, in buona parte mutuate da quelle previste in materia di depenalizzazione dall'art. 23 della legge n. 689/1981.

Nel definire tale procedura, il legislatore delegato ha previsto (art. 152, comma 7) che i ricorsi presentati all'autorità giudiziaria vengano notificati anche al Garante. Tale disposizione non riguarda solo i casi in cui sia proposta opposizione avverso i provvedimenti dell'Autorità, ma tutte le controversie concernenti l'applicazione del Codice.

Per tale secondo aspetto la modifica legislativa è di sicuro rilievo in quanto consente all'Autorità, da un lato, di essere utilmente informata per intervenire anche in quei procedimenti nei quali, pur non essendo essa direttamente coinvolta, sono in discussione profili di carattere generale; dall'altro, di venire a conoscenza, comunque, di controversie concernenti l'applicazione della disciplina in materia di protezione dei dati personali.

Quest'ultima attività d'informazione, di primaria importanza anche in relazione all'adozione di eventuali provvedimenti amministrativi e all'attività di segnalazione al Parlamento ed al Governo degli interventi normativi necessari per la tutela del diritto alla protezione dei dati (art. 154, comma 1, lett. *f*), è formalizzata nell'ultimo comma del citato art. 154, il quale, riproducendo quanto originariamente previsto dall'art. 40 della legge n. 675/1996, stabilisce che copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica sia trasmessa, a cura della cancelleria, al Garante.

Le modifiche introdotte, nell'ottica di un maggior coinvolgimento dell'Autorità nel contenzioso giudiziario, hanno indotto il Garante ad istituire, con decorrenza 1° gennaio 2004, un'unità temporanea di primo livello per gli "Affari legali", ai fini di un approccio più strutturato ed organico nell'enucleazione delle linee di difesa e intervento dell'Autorità e nei rapporti con le competenti avvocature dello Stato.

19.2. *Profili procedurali*

Con riferimento al contenzioso giurisdizionale, appare opportuno ricordare almeno i più significativi interventi in materia, sotto il profilo procedurale e di merito, richiamando anche alcuni utili precedenti che, seppur relativi ad anni passati, spiegano ancora rilievo.

Riguardo al primo aspetto, vanno senz'altro segnalate le pronunce in tema di giurisdizione che già la legge n. 675/1996 (art. 29, comma 8) aveva individuato nel giudice ordinario e che ora il Codice –come si è detto– indica specificamente nel tribunale.

Sulla base della formulazione del 1996, il Tribunale amministrativo del Lazio ha dovuto dichiarare la propria carenza di giurisdizione in merito ad un ricorso ad esso presentato dalla Congregazione cristiana dei Testimoni di Geova che aveva impugnato l'autorizzazione n. 3/1999 del Garante.

Per analoghe ragioni, nel 2004, nel fornire alla Presidenza del Consiglio dei ministri –Dipartimento per il coordinamento amministrativo– gli elementi necessari a predisporre le valutazioni su due ricorsi straordinari al Capo dello Stato, l'Autorità ha dovuto eccepire il difetto di giurisdizione.

Il Garante ha rivolto ulteriori osservazioni relativamente alla possibilità di adire il giudice di pace anziché il tribunale ordinario; tema, questo, che si è posto in particolare evidenza nel 2004 anche a seguito di più decisioni del Giudice di pace di Napoli che, investito di alcune azioni contro lo *spamming*, ha condannato, nel caso più noto, una società a cancellare i dati dell'interessato dai propri archivi e a pagare allo stesso 1.000,00 euro (oltre interessi legali e spese di giudizio) a titolo di risarcimento del danno.

La decisione da parte di tale giudice si è resa possibile solo in quanto la causa era stata instaurata prima dell'entrata in vigore del Codice, sebbene sul piano mediatico sia stata erroneamente commentata da alcuni come sentenza-pilota per (improprie) azioni dinanzi al giudice di pace.

In merito al foro competente, non sono mancate decisioni volte a far valere quanto disposto dall'art. 29, comma 6, della legge n. 675/1996 (prima) e dell'art. 152 del Codice (ora), che individuano nel tribunale del luogo ove risiede il titolare del trattamento la sede presso la quale proporre l'azione per tutte le controversie riguardanti l'applicazione del Codice.

In tal senso, con riguardo all'art. 29 della legge, si era espresso già nel passato il Tribunale di Firenze con decisione depositata in cancelleria il 15 aprile 2003; analogamente, il Tribunale di Napoli, con ordinanza del 29 luglio 2004, ha dichiarato la propria incompetenza su un ricorso proposto contro un titolare del trattamento avente sede legale in Bologna, con la contestuale dichiarazione di manifesta infondatezza della questione di legittimità costituzionale sollevata dal ricorrente sulla scelta effettuata dal legislatore con il citato art. 152.

Sulla stessa linea il Tribunale di Barcellona Pozzo di Gotto, con ordinanza n. 3694 del 31 luglio 2004, ha dichiarato manifestamente infondata la questione di legittimità costituzionale connessa alla mancata previsione della competenza del giudice del luogo di residenza del ricorrente quale foro alternativo a quello del luogo ove ha sede il titolare del trattamento.

Sempre in tema di competenza territoriale, ma sotto un diverso profilo, può essere ricordata la decisione con la quale il Giudice di pace di Amantea, cui un titolare si era rivolto opponendosi ad un'ordinanza di applicazione di sanzione amministrativa comminata dal Garante (ai sensi di quanto previsto dalla l. n. 689/1981), si è dichiarato incompetente, ma qui con riferimento all'ambito territoriale. Nel caso di specie, infatti, si doveva far riferimento al *"luogo in cui è stata commessa la*

violazione" (art. 22, comma 1, l. n. 689/1981), coincidente, secondo quanto affermato della giurisprudenza costituzionale e di legittimità, con quello nel quale la violazione era stata accertata (Roma).

Ancora, con riferimento agli aspetti procedurali, la giurisprudenza ha consentito di chiarire il dubbio relativo alla legittimazione passiva del Garante e, quindi, alla possibilità per esso di costituirsi innanzi ai tribunali o alla Corte di cassazione per difendere le ragioni giuridiche dei provvedimenti oggetto di impugnazione.

Su tale questione il Garante aveva chiesto in passato l'avviso dell'Avvocatura generale dello Stato, la quale, con parere del 29 ottobre 1999, si era espressa in termini favorevoli, ritenendo essenziale che l'Autorità potesse far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni.

A questo indirizzo l'Autorità stessa si è attenuta costantemente nel corso degli anni, intervenendo a difesa di decisioni il cui rilievo, andando ben oltre il singolo caso di specie, aveva riflessi su un'ampia platea di interessati e coinvolgeva rilevanti profili interpretativi della disciplina sulla protezione dei dati.

Sul punto la giurisprudenza –dopo la sentenza della Corte di cassazione (Sez. I Civ. 30 giugno 2001, n. 8889) che, dichiarando inammissibile un ricorso incidentale proposto dal Garante, non aveva affermato principi contrastanti con la sua prospettata legittimazione passiva– ha registrato un netto chiarimento con la sentenza n. 7341/2002 della prima sezione civile della Corte di cassazione.

Con tale pronuncia la Suprema Corte 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 il Garante agisce.

A seguito di tale pronuncia, il Tribunale di Roma, cui erano stati nuovamente trasmessi gli atti per l'esame della controversia, si è dovuto anche esprimere sulla questione di costituzionalità sollevata dal ricorrente in merito alla possibile violazione della regola del "giusto processo". La parte, infatti, sosteneva che la possibilità di impugnare la decisione del giudice di primo grado sull'opposizione al provvedimento del Garante solo tramite ricorso per cassazione sarebbe stata in contrasto con la regola del doppio grado di giudizio. Il Tribunale, con sentenza del 17 luglio 2003, dichiarando la questione manifestamente infondata ha riconosciuto che ragioni di speditezza possono giustificare l'esistenza di procedimenti giurisdizionali semplificati in cui è previsto un unico sindacato di merito, in quanto nella Costituzione non è contenuta alcuna norma che garantisca espressamente il doppio grado di giudizio.

Sempre con riferimento alla legittimazione passiva dell'Autorità, nel corso del 2004, la Suprema Corte (Sez. I Civ., sent. 22 marzo-25 giugno 2004, n. 11864), nel rigettare un'opposizione proposta contro una decisione del Garante, ha ritenuto quest'ultimo (sollevando con ciò qualche perplessità in dottrina) privo di interesse ad impugnare, nel caso di specie, il provvedimento giurisdizionale che, sebbene avesse ingiustamente negato la sua legittimazione processuale, aveva però confermato la decisione adottata dall'Autorità.

19.3. *Profili di merito*

Relativamente agli aspetti di merito, i primi anni di applicazione della disciplina sulla protezione dei dati personali hanno visto un numero assai esiguo di giudizi di

impugnazione dei provvedimenti del Garante; giudizi che, comunque, si sono risolti in una generale conferma dei principi di diritto affermati dall'Autorità. L'ingresso ormai consolidato della protezione dei dati personali nel circuito giudiziario rende opportuno compiere, come nei paragrafi precedenti, una sintetica ricognizione di alcune decisioni giurisprudenziali che hanno finora riguardato l'applicazione della normativa sulla tutela dei dati.

Al riguardo (omettendo una panoramica integrale anche di casi particolarmente significativi come quelli all'esame, all'epoca, del Tribunale di Bergamo in materia di investigazione privata), giova ricordare, tra l'altro, le vicende relative alla riconducibilità delle valutazioni alla nozione di "dato personale" fornita dalla legge n. 675/1996 e confermata dal Codice.

In tal senso già il Tribunale di Bologna, con decreto del 2 luglio 2002, concluse nel senso che anche i giudizi valutativi riferiti ai dipendenti contengono di regola dati personali.

Sulla medesima linea e discostandosi da alcuni circoscritti precedenti (Tribunale di Fermo, 26 ottobre 1999), il Tribunale di Roma ha riconosciuto che, anche con riferimento a dati valutativi (e in particolare sulle valutazioni espresse nelle perizie medico-legali), l'interessato può esercitare il diritto di accesso e alcuni altri diritti previsti dalla normativa in materia di protezione dei dati, ad esclusione di quelli di rettificazione o integrazione. Al riguardo, merita di essere sottolineato che della questione della riconducibilità delle valutazioni alla nozione di "dato personale" si è infine fatto carico il legislatore adottando un'equilibrata soluzione nell'art. 8, comma 4, del Codice.

Con riferimento alla possibilità di ottenere l'integrazione dei dati personali, il Tribunale di Padova, con decisione del 26 maggio 2000, aveva confermato il provvedimento con il quale il Garante, respingendo il ricorso dell'interessato che chiedeva la cancellazione dei propri dati personali dal registro dei battesimi di una parrocchia, aveva affermato comunque il suo diritto a veder aggiornato il medesimo dato.

Sempre in materia di esercizio dei diritti ora disciplinati dagli artt. 7 e ss. del Codice, restano attuali i principi affermati dalla già citata sentenza della Corte di cassazione (Sez. I Civ. 30 giugno 2001, n. 8889) che, ribadendo la piena applicazione delle disposizioni della legge n. 675/1996 anche agli archivi ed ai trattamenti svolti in ambito giornalistico, ha riconosciuto la possibilità di esercitare detti diritti (con particolare riguardo al diritto di accesso, integrazione ed eventuale correzione di dati inesatti) anche nei confronti di dati personali trattati a tal fine.

19.4. *Opposizione ai provvedimenti del Garante*

Il 2004 ha registrato dodici opposizioni ad altrettanti provvedimenti del Garante (tutte decisioni adottate su ricorso).

Tale numero può essere considerato in linea con quello degli anni precedenti, sia in relazione all'aumentata attività decisoria dell'Autorità, sia in considerazione del fatto che ben sette di queste opposizioni sono state presentate da un unico titolare (Crif S.p.A.) nelle more dell'approvazione del codice deontologico sui sistemi di informazioni creditizie, successivamente alla quale, per le medesime opposizioni, è stata chiesta la cessazione della materia del contendere.

Per quanto riguarda le ulteriori opposizioni presentate nel corso del 2004 e quelle pendenti degli anni precedenti, si è registrata la conferma di due decisioni relative alla produzione in giudizio (rispettivamente, in una causa civile ed in una

penale) di documenti contenenti dati personali, con le quali il Garante aveva ricordato i limiti di applicazione della disciplina in materia di tutela della riservatezza nei casi di trattamenti svolti per fini di giustizia.

Hanno avuto invece esito favorevole ai ricorrenti due opposizioni ad altrettante decisioni dell'Autorità relative, rispettivamente, ad una comunicazione di una relazione medica fra uffici periferici della stessa amministrazione ed alla pubblicazione di fotografie di persone arrestate.

Relativamente alla prima, considerato che la diversa valutazione del giudice si è basata soprattutto su una documentazione non prodotta dall'interessato in sede di ricorso all'Autorità e che la stessa è apparsa condivisibile nella sostanza, il Garante, su conforme avviso dell'Avvocatura generale, ha deciso di prestare acquiescenza.

Decisione diversa è stata invece stata assunta con riferimento alla seconda decisione, la quale, annullando il provvedimento dell'Autorità che aveva ritenuto illegittima la pubblicazione di fotografie di persone in stato di arresto, è invece apparsa censurabile sotto diversi profili. Relativamente ad essa è stato pertanto proposto ricorso per cassazione.

Sono ancora alle prime fasi del giudizio due ulteriori opposizioni presentate nel corso del 2004 da altrettante amministrazioni locali contro le decisioni con le quali l'Autorità ha censurato, in termini di mancato rispetto del principio di pertinenza, la pubblicazione di notizie relative all'attività istituzionale e coinvolgenti direttamente i ricorrenti.

Allo stesso stadio processuale si trovano anche l'opposizione presentata dalla RCS S.p.A. contro il provvedimento del 26 novembre 2003, con cui il Garante ha vietato l'ulteriore diffusione di fotografie di persone sottoposte a misure restrittive della libertà personale, e quella proposta da un interessato avverso la decisione con cui l'Autorità ha dichiarato infondato il ricorso in materia di rilascio di certificati del casellario giudiziale.

Sono parimenti in attesa di decisione due ricorsi straordinari al Capo dello Stato, relativamente ai quali il Garante ha chiesto di far valere in primo luogo il difetto di giurisdizione; si è conclusa la fase istruttoria e dovrebbe essere imminente la decisione in merito alle opposizioni a suo tempo proposte da RAI S.p.A. e dall'Agenzia per le entrate contro il provvedimento del 5 dicembre 2001 in materia di canone televisivo.

19.5. *Intervento del Garante in giudizi relativi all'applicazione del Codice*

Nel corso del 2004 si è registrata la notifica al Garante, ai sensi di quanto ora prescritto dall'art. 152, comma 7, del Codice, di trentadue ricorsi all'autorità giudiziaria non coinvolgenti direttamente pronunce dell'Autorità.

A tal proposito, occorre evidenziare che il Garante, conformemente agli indirizzi giurisprudenziali ed al già riferito parere dell'Avvocatura generale dello Stato, ha deciso di delimitare la propria attiva presenza ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto, pur continuando a seguire con attenzione tutti questi contenziosi.

In questo quadro, il Garante, laddove non ha ritenuto opportuno intervenire, ha pregato le avvocature distrettuali dello Stato di seguire periodicamente le vicende, provvedendo invece direttamente per le questioni sollevate presso il foro della Capitale.

Per sette dei ricorsi notificatile, l'Autorità ha ritenuto opportuno costituirsi. Si è trattato, in particolare, di due casi concernenti l'applicazione delle regole in materia di trattamento dei dati da parte delle cd. "centrali rischi", per i quali l'intervento è stato ritenuto essenziale alla luce dei lavori allora in corso di svolgimento per il codice deontologico.

Due ulteriori costituzioni del Garante si sono avute in cause riguardanti la violazione della riservatezza in ambito condominiale (nella specie, si trattava dell'affissione nella bacheca di un condominio di vari atti relativi al ricorrente) e per una notificazione, senza busta ed in mani di terzi, di atti contenenti dati sensibili, entrambe questioni sulle quali l'Autorità è intervenuta in passato con proprie pronunce di carattere generale.

L'Autorità ha poi ritenuto necessario costituirsi, in ragione della questione di diritto sottostante, in una causa relativa al rifiuto di consegna di una perizia medica per una vicenda giudiziaria in corso, nonché in due ulteriori casi, per far valere l'incompetenza territoriale del foro prescelto dal ricorrente.

In questo primo anno di attività la nuova unità Affari legali ha coordinato gli interventi dell'Autorità alla luce anche del suo aumentato, e probabilmente crescente, coinvolgimento nei procedimenti innanzi all'autorità giudiziaria, anche in relazione alle controversie che un'aumentata attività ispettiva e, soprattutto, sanzionatoria del Garante potrà comportare.

20 Attività ispettive e applicazione di sanzioni amministrative

20.1. *Profili generali*

Al fine di dare concreta attuazione al diritto alla protezione dei dati personali, la legge ha dotato il Garante di veri e propri poteri ispettivi, tramite i quali è possibile richiedere informazioni e documenti al titolare, ai responsabili ed incaricati del trattamento, agli interessati ed a terzi (art. 157 del Codice), anche inviando personale per rilevare le informazioni e i documenti, acquisendole *in loco*. L'Autorità può, inoltre, accedere a banche dati e archivi ed effettuare ispezioni e verifiche nei luoghi in cui si svolge il trattamento o dove occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento di dati personali (art. 158). Nel solo caso in cui tali attività debbano svolgersi in abitazioni, in altri luoghi di privata dimora o nelle relative appartenenze, l'accesso è subordinato all'autorizzazione dell'autorità giudiziaria o, in alternativa, all'assenso informato del titolare o del responsabile del trattamento dei dati.

In generale, le ispezioni possono originare da segnalazioni o reclami ricevuti dal Garante, nonché da esigenze di approfondimenti ulteriori emerse nell'ambito dell'esame di ricorsi. L'Autorità ha un potere di iniziativa autonomo in relazione, ad esempio, all'esigenza di verificare gli adempimenti di determinate categorie di titolari di trattamenti, ovvero sulla base di notizie comunque direttamente acquisite dal Garante. Talvolta vengono effettuati controlli a campione per verificare lo stato di attuazione della legge in determinati settori, spesso in concomitanza con scadenze imposte dal Codice (quali, per esempio, quelle previste per le notificazioni e per il Documento programmatico di sicurezza).

La scelta dello strumento potestativo da utilizzare per l'esercizio dell'attività di controllo è 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), nonché la disponibilità e la collaborazione del soggetto controllato per lo svolgimento delle verifiche.

Nell'ambito degli accertamenti ispettivi, il personale del Dipartimento vigilanza e controllo del Garante riveste la qualifica di ufficiale o di agente di polizia giudiziaria. Ciò comporta che, qualora nel corso dell'ispezione emergano violazioni penalmente rilevanti (artt. 167-171 del Codice), il personale addetto al Dipartimento possa procedere utilizzando i poteri investigativi che il codice di procedura penale attribuisce agli ufficiali ed agenti di polizia giudiziaria (eseguendo per esempio perquisizioni o sequestri, anche di iniziativa).

Al termine del procedimento amministrativo di controllo, del quale le attività ispettive rappresentano una fase, l'Autorità può segnalare ai titolari o responsabili del trattamento dei dati le modificazioni necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti e contestare le violazioni amministrative eventualmente rilevate; nei casi più gravi, previsti dalla legge, il Garante è tenuto ad inviare una comunicazione di notizia di reato all'autorità giudiziaria per l'accertamento delle violazioni costituenti illecito penale.

20.2. *Procedure*

Gli accertamenti di cui all'art. 157 del Codice (richiesta di informazioni ed esibizione di documenti) hanno una valenza marcatamente collaborativa. Il Garante adotta la predetta procedura nei confronti di soggetti e in relazione a materie per le quali ritiene di non dover procedere all'accesso, oppure quando sono necessarie informazioni analitiche che titolare e responsabile potrebbero avere difficoltà a fornire in modo esaustivo, nonché quando devono essere effettuati controlli incrociati rispetto a trattamenti di dati personali che interessano più titolari. Il carattere collaborativo di queste attività è evidenziato anche dalla prassi, seguita spesso dall'Autorità, di preannunciare le iniziative. I soggetti interpellati sono comunque tenuti a fornire informazioni non mendaci od omissive e ad esibire documenti genuini, al fine di non incorrere nella sanzione penale prevista dall'art. 168 del Codice (*Falsità nelle dichiarazioni al Garante*) o in quella amministrativa di cui all'art. 164 (*Omessa informazione o esibizione al Garante*).

Gli accertamenti previsti dall'art. 158 sono invece disposti quando, per acquisire gli elementi necessari alla compiuta definizione del contesto, non sia ritenuto sufficiente procedere con una mera richiesta di informazioni o di esibizione di documenti, ovvero nei casi in cui le informazioni o i documenti richiesti non siano pervenuti o siano ritenuti incompleti o non veritieri.

A differenza di quanto stabilito dall'art. 157, l'art. 158 conferisce al Garante una potestà di tipo inquisitorio ed *"i soggetti interessati agli accertamenti sono tenuti a farli eseguire"* (art. 159, comma 2, del Codice). L'accertamento è effettuato anche in caso di rifiuto e le eventuali spese sono poste a carico del titolare.

Il Codice prevede che le attività effettuate durante l'ispezione siano verbalizzate, registrando tutti gli elementi rilevanti emersi nell'operazione; agli accertamenti possono eventualmente assistere anche persone indicate dal titolare o dal responsabile (collaboratori interni, consulenti o legali) (art. 159).

20.3. *I casi più rilevanti*

Operatori sanitari

I trattamenti di dati sensibili effettuati da operatori sanitari sono stati oggetto di numerose ispezioni sia per quanto riguarda le modalità di conservazione dei dati e le connesse misure di sicurezza (anche in relazione ad episodi di gravi inadempienze che hanno avuto vasta eco attraverso gli organi di informazione), sia per quel che attiene all'osservanza dell'obbligo di notificazione.

In questo settore, i soggetti ispezionati sono stati ventidue, comprendendo Asl, ospedali e laboratori di analisi. Gli accertamenti si sono conclusi con l'invio di quattro notizie di reato per violazione dell'art. 169 (*Mancata adozione delle misure minime di sicurezza*) del Codice e con la contestazione di tredici sanzioni amministrative.

Uno dei casi più rilevanti ha riguardato un intervento effettuato presso un'azienda sanitaria a seguito della notizia apparsa su alcuni quotidiani che evidenziava la circostanza secondo la quale un'ingente quantità di documentazione sanitaria contenente dati idonei a rivelare lo stato di salute degli interessati (certificati medici, referti di analisi, registri di ricovero ecc.) era stata dispersa in un'area aperta al pubblico e abbandonata per giorni alla portata di chiunque. Durante l'accertamento è emerso che il fatto era da mettere in relazione ad un incendio, occorso circa quindici giorni prima, in un prefabbricato adibito ad archivio dove era conservata documentazione sanitaria relativa ad annualità molto risalenti nel tempo e in attesa di essere distrutta. Le operazioni di spegnimento dell'incendio avevano comportato la parziale demolizione del prefabbri-

20

cato e lo spostamento all'esterno di tutta la documentazione cartacea in esso contenuta.

Terminata l'emergenza, l'azienda sanitaria, pur avviando le procedure burocratiche per affidare ad una ditta specializzata la distruzione della documentazione, non aveva adottato alcun adempimento volto a ripristinare le misure di sicurezza, doverose in considerazione anche del fatto che i documenti si trovavano su un piazzale dal quale si accedeva peraltro ad una biblioteca comunale assiduamente frequentata (rendendo così accessibili a chiunque dati sensibili di migliaia di cittadini). L'Autorità, attraverso l'attività ispettiva, non solo ha provveduto ad accertare le responsabilità, ma ha anche disposto l'immediata attuazione di alcune misure di sicurezza.

In un altro caso l'Ufficio, raccogliendo la segnalazione di un programma televisivo trasmesso da una rete nazionale, si è recato in una struttura a suo tempo adibita a colonia per la cura delle malattie respiratorie infantili, attualmente dismessa, dove erano state abbandonate cartelle cliniche e altri documenti sanitari relativi ai pazienti della colonia. Anche in questo caso, gli enti che nel tempo avevano avuto in gestione l'immobile avevano dimostrato una totale inosservanza delle misure minime di sicurezza (art. 31 del Codice).

L'Ufficio si è anche occupato di un ulteriore caso di cattiva gestione della documentazione cartacea contenente dati sensibili dei cittadini, questa volta da parte di un'azienda ospedaliera della capitale. Anche in questa circostanza, una consistente quantità di documentazione sanitaria, concernente in particolare risultanze del laboratorio di analisi, era stata rinvenuta nel centro della città in prossimità di cassonetti dell'immondizia collocati su una pubblica via.

I casi sopra citati evidenziano una scarsa consapevolezza della delicatezza dell'attività di gestione della documentazione, anche di natura cartacea, contenente dati sensibili e della necessità che le misure di sicurezza previste per la conservazione di tali informazioni siano mantenute fino alla materiale distruzione della stessa. Appare irragionevole porre in essere complesse e onerose misure di conservazione e sicurezza degli archivi cartacei se poi lo smaltimento dei documenti non più necessari viene effettuato semplicemente gettandoli integri in un cassonetto dell'immondizia.

Gli episodi dimostrano inoltre, da una parte, la necessità di un "approccio sostanziale" alla legge; dall'altro, l'importanza che la documentazione contenente dati personali sia sempre conservata *"in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati"* (art. 11, comma 1, lettera *e*), del Codice).

Sempre in ambito sanitario, l'Ufficio ha svolto una serie di accertamenti per verificare la correttezza dei trattamenti di dati personali effettuati da un'associazione senza scopo di lucro nell'ambito di un progetto di ricerca realizzato con un'amministrazione comunale e con la collaborazione di una Asl. Il caso riguardava il rilevamento di dati personali attraverso la compilazione di minuziosi questionari, successivamente smarriti, che rivelavano anche le abitudini sessuali degli interessati. Anche in questo caso, tutte le operazioni di trattamento dei dati erano state effettuate in assenza di misure minime di sicurezza; tale circostanza è stata quindi oggetto di una comunicazione di reato alla competente autorità giudiziaria.

Anche le ispezioni effettuate nei confronti di due grosse aziende ospedaliere hanno evidenziato gravi deficienze nell'adozione delle misure di sicurezza per il trattamento dei dati sanitari mediante reti telematiche, debitamente segnalate alle competenti procure della Repubblica.

A fattor comune si evidenzia che nel caso di omessa adozione delle misure minime di sicurezza, il Garante, una volta segnalata la violazione all'Autorità giudiziaria, provvede ad impartire all'autore del reato una prescrizione fissando un termine per la regolarizzazione.

Se allo scadere del termine risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dall'Autorità a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato.

Dati genetici

Un altro dei settori oggetto di attenzione ispettiva è stato quello relativo alla raccolta e al trattamento di dati genetici.

In particolare, in relazione ad un delicato progetto di ricerca genetica, l'Ufficio ha svolto un'intensa attività ispettiva e di verifica nei confronti dei soggetti presso i quali tali dati erano stati raccolti e, pur mettendo in luce la generale correttezza sostanziale e liceità dei trattamenti effettuati, ha evidenziato ancora una volta un'inadeguatezza delle misure di sicurezza adottate che è stata segnalata all'autorità giudiziaria.

***Test* del Dna**

In un altro caso, l'ispezione è stata effettuata nei confronti di un'azienda che stava avviando la commercializzazione, via Internet, di un *test* del Dna "fai-da-te" che avrebbe consentito agli interessati di ottenere un responso mediante l'invio di campioni di materiale organico (saliva). L'intervento dell'Ufficio, avvenuto prima che la vera e propria commercializzazione del *test* avesse inizio, ha consentito di far emergere tutti i profili estremamente delicati legati alla gestione di un'attività che comporta il trattamento di dati genetici. L'Autorità ha infatti indotto l'azienda a valutare con maggiore attenzione tutte le implicazioni di carattere giuridico connesse con l'operazione prima di avviare materialmente l'iniziativa.

Informazioni sui sinistri stradali

Un'altra questione sottoposta all'attenzione del Garante (e sfociata poi in una verifica ispettiva) ha tratto origine da numerose segnalazioni di cittadini coinvolti in sinistri stradali. Gli stessi lamentavano di essere stati contattati da un'agenzia di pratiche automobilistiche che promuoveva i propri servizi volti a far ottenere il risarcimento dei danni patiti a seguito degli incidenti. Secondo i segnalanti, il contatto sarebbe avvenuto (in alcuni casi tramite lettera, in altri casi tramite visite a domicilio da parte di incaricati, in altri ancora tramite telefono), nei giorni immediatamente successivi l'incidente (in alcuni casi addirittura il giorno successivo) senza che gli interessati avessero mai comunicato i dati personali che li riguardavano all'agenzia segnalata.

Gli accertamenti hanno consentito di verificare che l'agenzia aveva organizzato un sistema informativo che le consentiva di conoscere, a distanza di poche ore dal verificarsi dei sinistri, gli elementi identificativi delle persone coinvolte, riuscendo così a proporre i propri servizi con grande anticipo rispetto alle imprese concorrenti.

Il trattamento illecito di dati personali effettuato dall'agenzia è stato segnalato alla competente autorità giudiziaria. Si è ritenuto in particolare che la causa obiettiva di punibilità prevista dall'art. 167 del Codice ("*se dal fatto deriva nocumento*") si configurasse sia per il modo in cui, immediatamente a ridosso di un evento, in taluni casi anche psicologicamente estremamente traumatico, le persone coinvolte sono state contattate, sia nella sofferenza morale che spesso deriva alle persone che si accorgono che dati personali riguardanti la salute escono dal circuito proprio nell'ambito del quale devono essere trattati.

Notificazione

Decorsi i termini utili per la presentazione della notificazione (30 aprile 2004), è stata avviata una serie di ispezioni nei confronti di trenta soggetti pubblici e privati, tra cui dodici aziende sanitarie locali e dodici società di lavoro interinale. Gli accertamenti, delegati al "Nucleo speciale funzione pubblica e *privacy*" della Guardia di finanza, hanno portato, in sedici casi, alla contestazione di violazioni per omessa o ritardata notificazione.

L'attività di vigilanza in materia di notificazione proseguirà, con modalità analo-

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.

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-

20

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.

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

nella sua comunicazione del 22 gennaio 2004 e la definizione di elementi per una cooperazione tra le autorità nazionali incaricate dell'attuazione dell'art. 13 (per l'Italia, il Garante) attraverso la rete *spam* Cnsa, cui si è fatto riferimento, e l'adozione di regole comuni per la trattazione di casi di *spam* transfrontaliero.

Il Consiglio dell'Unione, proprio in considerazione del grande impegno da assumere per contrastare lo *spam,* ha adottato nel mese di novembre alcune conclusioni che impegnano gli Stati ad un recepimento puntuale della direttiva 2002/58/CE ed in particolare del suo art. 13; ha richiesto poi alla Commissione di valutare se alcune disposizioni nazionali introdotte in attuazione della direttiva possano ritenersi confliggenti con l'applicazione armonizzata del principio del consenso preliminare (*opt-in*) da parte del destinatario e pertanto incidere sull'efficacia delle misure di contrasto allo *spam* transfrontaliero.

Analoga attenzione è stata posta all'intensificazione della collaborazione internazionale –in particolare, come ricordato, in sede Ocse ed *International Communication Union* (Itu)– finalizzata alla presentazione, attraverso la Commissione europea, di una posizione unitaria dei Paesi dell'Unione. Infatti, in altri Paesi la legislazione vigente si fonda sul diverso principio del cd. *opt-out* (la possibilità, cioè, per il destinatario di chiedere di non ricevere le comunicazioni commerciali) e pertanto quello che nell'Unione europea dall'entrata in vigore della direttiva 2002/58/CE (e nei singoli Paesi dalla data di trasposizione) è assoggettato a sanzione, in altri paesi può non costituire un comportamento vietato.

In questo quadro, il contributo del Gruppo art. 29 assume una notevole rilevanza. In particolare, il parere n. 5/2004 del 27 febbraio 2004 offre indicazioni su specifici elementi che riguardano le nozioni di "posta elettronica", "previo consenso" da parte degli abbonati e "commercializzazione diretta"; si prendono altresì in considerazione l'eccezione alla norma del previo consenso e il regime per le comunicazioni indirizzate alle persone giuridiche.

22.3. *Le conferenze tra autorità di protezione dei dati a livello europeo*

La Conferenza di primavera dei Garanti europei si è svolta a Rotterdam dal 21 al 23 aprile 2004 ed è stata dedicata alle politiche finalizzate a garantire l'efficacia della protezione dei dati. I temi al centro dell'incontro hanno riguardato il ruolo e l'azione di intervento delle autorità, le comunicazioni elettroniche, il rispetto delle norme sulla protezione dei dati personali e la cooperazione giudiziaria a livello europeo.

Il segretario generale dell'Autorità ha affrontato il tema delle strategie da mettere in atto per garantire l'effettiva attuazione delle norme in materia di *privacy*, non solo attraverso verifiche e controlli, ma anche mediante una costante azione di sensibilizzazione. Per quanto riguarda in particolare l'attività di verifica, soprattutto alla luce della direttiva 95/46/CE, si è altresì evidenziata l'opportunità di potenziare la collaborazione fra le autorità nazionali della protezione dei dati, anche in considerazione del carattere transnazionale delle problematiche che investono il settore della *privacy* (esempio tipico lo *spam*).

22.4. *Conferenze delle autorità su scala internazionale*

La 26ª Conferenza internazionale dei Garanti per la protezione dei dati personali, che si è tenuta a Wroclaw dal 14 al 16 settembre, è stata dedicata al binomio società della *privacy* società e della dignità.

Il Garante ha partecipato all'incontro attraverso quattro interventi nelle differenti sessioni di lavoro:

Mauro Paissan ha svolto una relazione sul delicato rapporto tra libertà di informazione e diritti della persona, evidenziando come il diritto di sapere, la libertà di comunicare e la trasparenza non possano cancellare il bisogno di intimità e il diritto di sviluppare liberamente la personalità;

Gaetano Rasi si è soffermato sugli aspetti economici della *privacy*, sottolineando come la tutela dei dati personali sia destinata a svolgere una funzione fondamentale per disegnare i futuri assetti del rapporto tra imprese e consumatori; in particolare, il trattamento –da parte delle aziende– di informazioni relative alla clientela improntato ai criteri di correttezza e trasparenza può sensibilmente migliorare la qualità del rapporto tra azienda e cliente;

Giovanni Buttarelli è intervenuto nella sessione dedicata al *marketing* politico, evidenziando gli aspetti legati alla necessità di ottenere un consenso preventivo, da parte degli interessati, all'invio di materiale propagandistico. Ciò, soprattutto perché la "pubblicità" elettorale, fondata sul trattamento di dati che riguardano identità personale e convinzioni politiche, tocca una sfera particolarmente delicata dell'individuo. Le nuove tecnologie utilizzate anche nella propaganda politica comportano la necessità di salvaguardare ancora più attentamente il diritto alla riservatezza. Ferma restando la libera circolazione delle idee e delle proposte politiche, è opportuno promuovere –anche in questo settore– un *marketing* responsabile. La proposta del segretario generale di operare in vista di una possibile risoluzione in occasione della prossima conferenze mondiale è stata condivisa.

Al Presidente Stefano Rodotà è stato affidato il compito di chiudere i lavori della Conferenza. Nella sintesi conclusiva, il prof. Rodotà ha affermato che fra i concetti di *privacy*, libertà e dignità esiste un legame sempre più stretto, in ragione del fatto che il trattamento di dati personali può determinare discriminazioni sulla base di convinzioni politiche, credenze religiose, condizioni di salute: la *privacy,* non più riconducibile al solo diritto ad essere lasciati soli, costituisce un elemento essenziale della società dell'uguaglianza. In particolare, il Presidente ha evidenziato quattro temi che –per le loro implicazioni rispetto ai valori fondanti di una società democratica e al rispetto della persona– necessitano di una riflessione approfondita: i rischi del progressivo passaggio da forme di sorveglianza mirata verso soggetti pericolosi ad una sorveglianza "generalizzata"; le trasformazioni del corpo –utilizzato come *password* attraverso i dati biometrici– determinate dall'impiego di strumenti elettronici che rendono possibile localizzare e seguire l'individuo in modo permanente; la conservazione di dati per periodi troppo lunghi che rende ciascuno "prigioniero" del proprio passato e dei controllori delle grandi banche dati; la necessità di una protezione integrale della persona anche nella dimensione elettronica. Questi temi proiettano la tutela dei dati al di là della semplice protezione della sfera privata, per farla divenire un elemento essenziale della cittadinanza del nuovo millennio.

Al termine dei lavori sono state approvate tre risoluzioni riguardanti l'aggiornamento automatico dei *software*, l'istituzione di un *forum* comune per le questioni attinenti alla cooperazione giudiziaria e di polizia e la definizione di uno standard-quadro ISO in materia di *privacy* (v. *Documentazione* par. 75).

Nella risoluzione sull'aggiornamento automatico dei *software* i Garanti hanno preso atto con preoccupazione che le società produttrici di *software* fanno sempre più ricorso a meccanismi non trasparenti che permettono una serie di operazioni: trasferire nel *computer* degli utenti, a loro insaputa, aggiornamenti di *software* per raccogliere i dati personali memorizzati; assumere il controllo, almeno parziale, del *computer* terminale limitando la capacità dell'utente, quale titolare del trattamento, di

22

far fronte agli obblighi ed alle responsabilità previsti dalla legge per garantire la sicurezza dei dati trattati; modificare o provocare malfunzionamenti nel *software* installato senza la possibilità di individuarne la causa. I Garanti hanno, pertanto, invitato le aziende produttrici di *software* a prevedere che le procedure per il rilascio dei dati da parte degli utenti Internet, finalizzate anche all'aggiornamento *on-line* del *software*, siano trasparenti ed associate ad un'informativa adeguata. Tale aggiornamento dovrebbe avvenire, inoltre, solo dopo aver ottenuto il consenso dell'utente, impedendo nel contempo che possano verificarsi accessi non controllati al *computer*.

La risoluzione sulla cooperazione giudiziaria e in materia di polizia chiede l'istituzione di un *forum* comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia, nell'ambito, cioè, del cosiddetto Terzo Pilastro del Trattato di Amsterdam. Tale risoluzione poggia sulla necessità, avvertita nelle diverse sedi istituzionali europee, che gli Stati membri dell'Unione europea intensifichino ulteriormente la cooperazione giudiziaria e di polizia in ambito penale per assicurare un livello elevato di sicurezza in un'area di libertà, sicurezza e giustizia, garantendo al contempo un equo bilanciamento fra l'esigenza di sicurezza e la difesa delle libertà civili, compresi i diritti di protezione dei dati, la cui tutela è sancita dalla Carta dei diritti fondamentali dell'Unione europea. Tuttavia, le autorità per la protezione dei dati personali si trovano nella situazione di non poter esercitare la loro attività consultiva in materia a causa dell'assenza di una struttura di coordinamento. I Garanti hanno pertanto invitato il Consiglio e la Commissione, da un lato ad incorporare l'attività consultiva in materia di protezione dei dati nella struttura del Consiglio dell'Unione europea, dotandola delle necessarie risorse umane ed organizzative prima della fine del 2004 e, dall'altro, a creare i presupposti giuridici per l'armonizzazione delle attività di controllo nell'ambito del Terzo Pilastro.

Con la terza risoluzione, la Conferenza ha invece raccomandato all'Organizzazione internazionale per la standardizzazione (ISO), la definizione di uno o più *standard* globali in materia di protezione dei dati e *privacy*. I Garanti hanno chiesto, in particolare, l'individuazione di uno *standard* tecnologico fondato sulle prassi di leale informazione e sui principi di parsimonia, necessità ed anonimizzazione nell'uso dei dati, tale da supportare l'attuazione di norme di legge in materia di *privacy* e protezione dei dati, se già esistenti, e la formulazione di tali norme ove esse non siano ancora definite. Lo *standard*, si legge nella risoluzione, dovrebbe poggiare sul rispetto di tre parametri. In primo luogo, offrire criteri di valutazione e verifica che facilitino il rispetto delle normative nazionali ed internazionali da parte dei titolari. In secondo luogo, indicare se le misure volte alla tutela della *privacy* impiegate da sistemi utilizzati per la gestione di dati personali siano realmente efficaci. Infine, garantire che i dati personali siano trattati sempre nel rispetto dei parametri in base ai quali sono stati inizialmente raccolti, indipendentemente dai passaggi e dal numero di soggetti che possono intervenire nella gestione e nell'interscambio di tali dati personali. La Conferenza ha, inoltre, sottoposto all'ISO le sue preoccupazioni; le medesime sono state recepite, conducendo alla sospensione delle iniziative in corso miranti alla definizione di "*standard privacy*" per le tecnologie dell'informazione, avviate senza consultare le autorità di protezione dati.

La Conferenza internazionale che, nel 2005, tornerà a riunire le autorità garanti dei diversi Paesi, avrà ad oggetto le sfide legate alla protezione dei dati personali nel mondo globalizzato.

In particolare, la discussione si concentrerà sul carattere universale del diritto alla *privacy* pur nel necessario rispetto delle diversità. Ciò, ponendosi in una linea di continuità con le riflessioni iniziate nel corso della Conferenza internazionale *"One*

world, One privacy" (Venezia, settembre 2000) che hanno portato all'adozione della "Carta di Venezia". Già in tale occasione, infatti, le autorità –alla luce del riconoscimento della *privacy* come diritto fondamentale della persona e quale elemento costitutivo della libertà del cittadino– hanno evidenziato la necessità di perseguire regole comuni universalmente condivise per la salvaguardia di tale diritto.

22.5. *La cooperazione tra autorità garanti nell'Unione europea: il Gruppo* ex *art. 29*

Nel 2004 l'attività del Gruppo *ex* art. 29 si è incentrata, come nel passato, su tematiche attinenti agli ordinari ambiti di applicazione delle direttive 95/46/CE e 2002/58/CE soffermandosi, in particolare, su iniziative che, alla luce delle esigenze rappresentate dalle autorità giudiziaria e di polizia al fine di migliorare la raccolta e lo scambio di informazioni per la lotta al terrorismo ed alla criminalità, hanno potenzialmente un grande impatto sulla tutela della riservatezza e sul diritto alla protezione dei dati personali affermato solennemente come diritto fondamentale (già dalla Carta dei diritti fondamentali e ora) dal Trattato che adotta una Costituzione per l'Europa, firmato a Roma il 29 ottobre 2004 (articoli I-51 e II-68).

Il Gruppo, proprio per tener adeguatamente conto dei cambiamenti legati, da un lato, all'allargamento dell'Unione europea con l'adesione di dieci nuovi Stati e, dall'altro, al riconoscimento del diritto alla protezione dei dati come diritto fondamentale, ha deciso di avviare una riflessione approfondita sul proprio ruolo e sulle prospettive di lavoro futuro. Si è giunti così all'adozione di un documento di ampio respiro che disegna un programma di lavoro di medio-lungo termine e si affianca al programma di lavoro del Gruppo, che ha cadenza annuale. A giudizio delle autorità europee, i due binari da percorrere sono il miglioramento dell'attuazione dei principi comunitari in materia di protezione dei dati attraverso iniziative concrete, in parte già in corso, e la definizione ed il potenziamento della cooperazione fra il Gruppo stesso e le istituzioni comunitarie (in particolare la Commissione europea, il Parlamento europeo e il Consiglio dell'Unione), oltre che con le autorità chiamate a far rispettare le regole poste a garanzia di tale diritto (il Garante europeo per la protezione dei dati e, in particolare, le autorità comuni di controllo Europol, Schengen, Dogane ed Eurojust).

Il Gruppo ha chiesto di essere pienamente informato riguardo alle iniziative in corso di predisposizione (da parte delle istituzioni comunitarie) che possono avere un impatto sulla protezione dei dati personali, in modo da poter fornire il proprio contributo di conoscenza e competenza sin dalle fasi iniziali di formazione delle proposte di azione comunitaria. Ha in parallelo considerato opportuno sollecitare un miglioramento della cooperazione delle autorità di protezione dei dati per affrontare tematiche non più limitate agli aspetti tipici del mercato interno, ma che coinvolgano altri settori e politiche comunitarie sì da richiedere un esame ed un'azione comune da parte delle diverse autorità. Quest'ultimo punto, in particolare, riveste crescente importanza alla luce del rilievo assunto dalle questioni cosiddette di Terzo Pilastro anche in rapporto al difficile contesto internazionale. Il Gruppo è infatti intervenuto prendendo posizione con sempre maggiore frequenza anche su queste tematiche (ad esempio l'obbligo per i vettori aerei di fornire i dati *Passenger Name Record* (*Pnr*) dei passeggeri dei voli transoceanici (sul quale più compiutamente si sofferma il par. 22.6), quello di conservazione dei dati concernenti comunicazioni elettroniche, pur parzialmente sottratte all'ambito comunitario, nonché di introdurre in passaporti, visti, permessi di soggiorno elementi biometrici, foto digitalizzata ovvero scannerizzata del volto, impronte digitali).

22

Il programma di lavoro annuale per il 2004 ha, a sua volta, concentrato molte iniziative d'azione sui temi evidenziati dalla Commissione europea nel rapporto sull'applicazione della direttiva 95/46/CE e, segnatamente, in materia di semplificazione dei requisiti delle notificazioni, armonizzazione dei requisiti in materia di informativa, semplificazione dei trasferimenti internazionali, migliore e più coordinata attuazione di alcuni principi della direttiva.

Come illustrato in dettaglio nel par. 22.6, il Gruppo ha continuato a dedicare speciale attenzione alle richieste degli Stati Uniti di ottenere da parte delle compagnie aeree i dati personali dei passeggeri in viaggio da e verso il loro territorio. Alle richieste degli Stati Uniti si sono aggiunte quelle di alcuni altri Stati, segnatamente il Canada e l'Australia.

Sono stati al riguardo adottati, in rapida successione, cinque pareri, 3 rivolti alle richieste USA (pareri 2/2004, 6/2004 ed 8/2004) e due, rispettivamente a quelle australiane e canadesi (pareri 1/2004 e 3/2004).

In tema di trasferimento dei dati personali verso Paesi terzi, si segnala altresì la decisione adottata il 28 aprile dalla Commissione europea, sulla scorta del parere espresso in precedenza dal Gruppo, in merito all'adeguatezza della protezione dei dati personali nell'Isola di Man. Nel corso del 2004 è stata effettuata, sempre da parte della Commissione, la valutazione del funzionamento delle due decisioni di adeguatezza adottate nel 2000, relative alla Svizzera ed al cd. *Safe Harbor* (concernente il trasferimento dei dati verso gli Stati Uniti).

Entrambe le valutazioni sono state fatte precedere da uno studio affidato a consulenti esterni e le relative conclusioni sono state adottate il 20 ottobre 2004. I documenti di lavoro e gli studi su cui si fondano sono stati resi pubblici.

Per quanto riguarda il particolare il funzionamento dell'accordo sul *Safe Harbor*, il documento della Commissione conclude che, a suo avviso, pur evidenziandosi talune difficoltà applicative, non vi sono ragioni per rivedere la decisione del 2000. La Commissione ritiene apprezzabile l'aumento del numero delle società che hanno aderito al *Safe Harbor*, anche se considera necessario acquisire in futuro elementi sulla loro consistenza. Lo studio al quale la Commissione ha fatto riferimento per formulare le proprie valutazioni, svolto dal Crid (Centro di ricerca su informazione e diritto) dell'Università di Namur sotto la guida del prof. Poullet, fornisce un'approfondita ed articolata valutazione del funzionamento del sistema ed evidenzia vari aspetti problematici che vanno dal ruolo, non sempre pienamente svolto, delle autorità statunitensi preposte alla verifica del rispetto dei principi da parte delle società aderenti, alla mancanza di *privacy policy* sui siti delle stesse società, con la sensazione di una scarsa conoscenza delle implicazioni che l'adesione all'accordo determina e, quindi, di una ancora più scarsa informazione degli interessati in merito alla possibilità di far valere i loro diritti di accesso, di verifica, di rettifica e cancellazione. Altro aspetto messo in luce dallo studio consiste nella possibilità che in taluni casi la legislazione adottata negli Stati Uniti a seguito degli eventi dell'11 settembre abbia introdotto obblighi di comunicazione dei dati per le società aderenti.

Un caso segnalato specificamente dallo studio riguarda anche il possibile conflitto tra le normative statunitense ed europee con riguardo all'invio delle comunicazioni commerciali (*opt-out* vs. *opt-in*).

Alla luce di queste riflessioni, il Gruppo ha deciso nella sua ultima riunione del novembre 2004 di affidare ad un gruppo ristretto l'analisi attenta delle valutazioni offerte dallo studio del Crid.

Il Gruppo ha inoltre continuato ad approfondire il lavoro sulle cd. "soluzioni contrattuali", che consentono alle imprese di trasferire dati personali nel rispetto dei principi della direttiva anche quando il Paese di destinazione non abbia una legisla-

zione adeguata, prevedendo le idonee garanzie attraverso lo strumento contrattuale.

Da un lato, anche sulla scorta di un precedente parere del Gruppo, è stato approvato dalla Commissione europea un ulteriore modello di clausole contrattuali *standard* (in *Documentazione* par. 46). Le imprese saranno libere di scegliere se utilizzare l'uno o l'altro gruppo di regole. Il modello cd. "alternativo", cui si è fatto cenno anche nella *Relazione 2003*, è stato presentato dalla Camera di commercio internazionale e da altre organizzazioni commerciali ed è stato successivamente modificato in più parti su suggerimento del Gruppo, al fine di assicurare che le clausole contrattuali tipo proposte offrano un livello di tutela paragonabile a quelle approvate in virtù della decisione della Commissione n. 497/2001/CE.

Dall'altro lato, sono proseguiti i lavori per il riconoscimento e la possibile introduzione di un diverso sistema che consenta, in particolare, il trasferimento fra società appartenenti ad uno stesso gruppo multinazionale. Questo sistema, basato su ipotizzate "norme vincolanti d'impresa" (cd. *binding corporate rules*) era stato già analizzato dal Gruppo in un documento di lavoro (WP del 3 giugno 2003) al fine di valutare in quali termini e in base a quali condizioni questi speciali "codici di condotta" possano offrire, appunto, le "garanzie sufficienti" menzionate dall'art. 26(2) della direttiva.

Le "norme vincolanti d'impresa" sarebbero infatti veri e propri codici di condotta elaborati nell'ambito di un gruppo di imprese e validi per tutte le società che di tale gruppo fanno parte.

Basandosi sull'esperienza maturata in alcuni Stati membri e sugli approfondimenti scaturiti nel corso di un seminario internazionale svoltosi a l'Aja, il Gruppo ha recentemente adottato un documento in cui si individuano gli elementi essenziali per presentare ad una autorità di protezione dei dati la richiesta di autorizzazione (*model checklist*). Giova ricordare che, a differenza delle clausole contrattuali, sulla base delle disposizioni della direttiva la Commissione europea non è competente ad adottare una decisione vincolante in materia ed i singoli Stati (più precisamente le autorità nazionali di protezione dei dati) restano liberi di rendere o meno operanti le "norme vincolanti d'impresa" sul proprio territorio.

Dopo l'adozione di uno specifico documento di lavoro sull'uso dei sistemi biometrici (WP 80 del 1° agosto 2003), il Gruppo ha adottato l'11 agosto 2004 un parere sull'inclusione di elementi biometrici nei visti e permessi di soggiorno, che esprime dubbi sulla proporzionalità delle misure proposte rispetto alle finalità individuate dai proponenti e forti preoccupazioni in relazione al quadro più ampio in cui la proposta si colloca.

Come già evidenziato, infatti, occorre guardare in modo unitario ad una congerie di proposte formulate da Consiglio e/o Commissione, che prevedono un crescente impiego della biometria (impronte digitali e scannerizzazione del volto in particolare) rendendone obbligatorio l'inserimento nei documenti rilasciati a stranieri e cittadini (passaporti, carte d'identità, visti, permessi di soggiorno), prevedendo la creazione a livello europeo di grandi basi di dati in cui anche questi elementi vengono inseriti (Sis II, Sistema informazione visti-Vis) ed intensificando la possibilità di scambiare queste informazioni con una pluralità di Stati ed organismi esteri (in proposito si veda in allegato, anche il Regolamento (CE) n. 2252/2004 del Consiglio sulle caratteristiche di sicurezza e gli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri).

Il Gruppo, nel suo parere, ricorda che tali proposte hanno un forte impatto sui diritti umani fondamentali ed in particolare sul diritto alla protezione dei dati personali; pertanto, richiama l'attenzione sulla necessità di esserne preliminarmente informato e che le stesse proposte siano adeguatamente rese pubbliche nei confronti

22

dei Parlamenti e della società civile e che ai relativi lavori sia data trasparenza, anche attraverso il coinvolgimento delle autorità di protezione dei dati. Nel parere, infatti, il Gruppo ricorda l'obbligo di rispettare in particolare il principio di proporzionalità e la necessità di definire con chiarezza le finalità del trattamento dei dati biometrici. Il parere individua anche le cautele da adottare al fine di rendere "affidabile" il trattamento di tali dati e richiede precise garanzie in ordine allo stesso; chiede inoltre di ricevere informazioni approfondite sulla sicurezza del sistema scelto e sulle modalità di incorporazione dei dati nel *chip*.

Esprime infine forti preoccupazioni riguardo alla previsione della possibile creazione di un *database* centralizzato a livello europeo e ricorda che il ruolo delle autorità di supervisione deve essere mantenuto adeguato alle novità che si vogliono introdurre per evitare un abbassamento del livello di tutela.

Come già segnalato nella *Relazione* 2003, il Gruppo ha adottato il parere 4/2004 (WP 89 del 11 febbraio 2004) sul trattamento dei dati effettuato attraverso la videosorveglianza, che individua regole e garanzie precise sull'installazione di telecamere fornendo un quadro uniforme e armonizzato in materia a livello europeo. Il parere contiene un "decalogo" sulle cautele ed i principi da osservare, principi che si applicano anche ai trattamenti non soggetti espressamente alle disposizioni della direttiva europea (ad esempio, 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).

È stato altresì adottato un parere in tema di comunicazioni commerciali non richieste (parere 5/2004 WP 90 del 27 febbraio 2004), al fine di fornire una interpretazione comune dell'art. 13 della direttiva 2002/58/CE riguardo ad alcuni aspetti che potrebbero dare luogo a soluzioni divergenti in sede di recepimento o di applicazione della normativa nei diversi Stati membri.

Altro importante parere del Gruppo (parere 9/2004 del 9 novembre 2004) riguarda una proposta legislativa presentata da quattro Stati dell'Unione il 28 aprile 2004 (Doc. 8958) tendente ad imporre ai fornitori di servizi di comunicazione elettronica l'obbligo di conservazione dei dati di traffico trattati ai fini della fornitura del servizio o comunque disponibili.

La proposta, in discussione presso il Consiglio dell'Unione, nella sua forma attuale prevede la conservazione preventiva in maniera indiscriminata, per un periodo di tempo limitato solo nel minimo, di tutti i dati di traffico (telefonico, Internet, comprensivo della posta elettronica).

I Garanti hanno ritenuto tale proposta in contrasto con i principi fondamentali in materia di protezione dei dati e con la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Il Gruppo ha richiamato i precedenti pareri espressi, ha rinnovato la richiesta che sia previamente valutato, come previsto dalla stessa Convenzione, se l'ipotizzata interferenza nella vita privata abbia un'adeguata base giuridica e se risponda a criteri di necessità nel quadro di una società democratica, rammentando la necessità del rispetto dei principi in materia di protezione dei dati –in particolare dei principi di proporzionalità, pertinenza, finalità– per la conservazione dei dati di traffico anche per finalità giudiziarie e di polizia (v. art. 15 della direttiva 2002/58/CE).

Si segnala anche un primo documento di lavoro adottato dal Gruppo (WP 86 del 23 gennaio 2004) sui dispositivi proposti dal consorzio *Trusted Computing Group* per incentivare la sicurezza delle transazioni elettroniche attraverso strumenti non solo *software,* ma anche *hardware* e, soprattutto, il documento di lavoro adottato il 17 marzo 2004 (WP 91) sul trattamento dei dati genetici.

Nel documento di lavoro, come già rappresentato nella *Relazione 2003*, il

Gruppo ha preferito affrontare il progresso tecnologico nel campo della genetica e le sue ripercussioni nella sfera della riservatezza scegliendo un approccio analitico volto ad individuare i settori in cui maggiori sono le preoccupazioni in relazione al trattamento dei dati genetici.

22.6. *Il trasferimento dei dati* Pnr *dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea*

Uno dei temi più delicati e controversi a livello europeo ed internazionale resta il trasferimento dei dati *Pnr* dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea (v. già la *Relazione 2003*). Infatti, come sottolineato anche da un recente intervento del commissario europeo Frattini, la richiesta da parte delle autorità pubbliche di Paesi terzi di ottenere dalle compagnie aeree europee i dati dei passeggeri ai fini di prevenzione del crimine non solo deve essere valutata alla luce del rispetto del diritto fondamentale alla protezione dei dati personali, ma è collegata anche alla delicata questione della protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia nell'Unione europea (cd. Terzo Pilastro), che risulta tuttora frammentaria e non armonizzata.

Il Gruppo ha dedicato grande attenzione al tema, occupandosi non solo del sistema proposto dalle autorità statunitensi, su cui si era già espresso nel corso del 2002 e del 2003, ma anche dalle analoghe richieste provenienti dall'Australia e dal Canada, nella convinzione che i comuni obiettivi di lotta al terrorismo debbano essere perseguiti nel rispetto dei diritti fondamentali ed in particolare del diritto alla protezione dei dati personali.

Per quanto riguarda gli Stati Uniti, il Gruppo è tornato ad evidenziare, nel parere 2/2004, le lacune del sistema statunitense, proponendo una serie di miglioramenti atti a garantire che il trasferimento dei dati dei passeggeri avvenga nel rispetto dei principi stabiliti dalla normativa europea in materia di protezione dati. Fra questi, il Gruppo ha segnalato, in particolare, il principio di finalità, in base al quale i dati del *Pnr* dovrebbero essere utilizzati soltanto per contrastare il terrorismo ed altri specifici reati ad esso connessi; il principio di proporzionalità nei dati richiesti, evitando il trasferimento di dati superflui; la conservazione dei dati per un periodo limitato; il divieto di trattare dati sensibili; il diritto dei passeggeri ad essere adeguatamente informati e ad essere messi in condizione di esercitare agevolmente i propri diritti (accesso, rettifica). Inoltre, il Gruppo ha chiesto che le garanzie per i passeggeri non si basino meramente su impegni unilaterali privi di vincolatività giuridica per la controparte americana e tali da non creare diritti che i terzi (in questo caso i cittadini europei) possano far valere negli Usa in caso di controversie.

Anche il Parlamento europeo, condividendo molte delle critiche espresse dal Gruppo, nel marzo 2004 ha approvato due risoluzioni con cui, sottolineando gli insoddisfacenti risultati del negoziato tra autorità statunitensi e Commissione europea, invitava quest'ultima ad ottenere garanzie reali affinché fosse rispettato il diritto alla protezione dei dati personali dei cittadini europei, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Ue.

La Commissione ha però deciso di procedere con la propria iniziativa contenuta nel "pacchetto *Pnr*", adottando una decisione relativa all'adeguatezza della protezione accordata dagli Stati Uniti ai dati personali dei passeggeri aerei, fondata su impegni unilaterali (cd. "*undertakings*") delle autorità statunitensi. A tale iniziativa ha fatto seguito l'approvazione di un accordo internazionale da parte del Consiglio dei ministri dell'Ue,

22

con cui si impone alle compagnie aeree europee di consentire alle autorità doganali statunitensi l'accesso diretto ai dati contenuti nei propri sistemi di prenotazione (cfr. al riguardo i documenti riprodotti nei par. 43-45 in *Documentazione*).

Entrambi gli atti sono stati approvati a maggio 2004, nonostante le preoccupazioni espresse dal Gruppo art. 29 e la richiesta del Parlamento europeo, presentata ad aprile alla Corte di giustizia delle Comunità europee, di un parere preliminare sulla compatibilità con l'ordinamento comunitario del proposto accordo internazionale.

Ai sensi del "pacchetto *Pnr*", le autorità doganali statunitensi sono autorizzate ad accedere direttamente ad un novero molto ampio di dati (34 elementi, fra cui indirizzi, numeri di telefono, indirizzi di posta elettronica, numeri di carte di credito, informazioni contenute nei programmi "*frequent flyer*") e a conservare per almeno tre anni e mezzo le informazioni relative ai dati di tutti i passeggeri (al contrario del sistema australiano, approvato dai Garanti europei, in cui i dati vengono conservati solo in presenza di un reato o di una indagine per un presunto reato). I dati possono essere trattati per finalità che esorbitano dalla lotta al terrorismo ed essere ulteriormente trasmessi ad altre autorità, anche di Paesi terzi.

Allo stato, sono accessibili dati "neutri" e sensibili; con riguardo a questi ultimi, gli *undertakings* prevedono specifici impegni da parte delle autorità statunitensi a non farne uso. In futuro, i dati sensibili (riguardanti la salute, le convinzioni religiose o politiche, ecc.) non saranno più accessibili grazie ad un apposito sistema di filtraggio.

Infine, i diritti dei passeggeri europei ad essere informati, ad accedere ai propri dati ed eventualmente a rettificarli non sono sembrati adeguatamente garantiti: fra l'altro, sia per l'assenza di un organo di ricorso veramente indipendente, sia per la dubbia vincolatività giuridica degli impegni assunti dalle autorità statunitensi.

Pertanto, il Parlamento europeo ha deciso di presentare un ricorso alla Corte di giustizia delle Comunità europee (che si aggiunge a quello, decaduto a seguito della firma dell'accordo, presentato in sede pregiudiziale e del quale si è fatto cenno nella *Relazione 2003*) per far annullare la decisione della Commissione e l'accordo internazionale. Secondo il Parlamento europeo, non soltanto la soluzione raggiunta non tutelerebbe adeguatamente i diritti dei passeggeri, ma la stessa Commissione avrebbe oltrepassato le proprie competenze e non avrebbe assicurato la dovuta partecipazione del Parlamento al processo decisionale.

Tale ricorso è stato condiviso nel merito anche dal Garante europeo della protezione dati (la cui attività è iniziata di recente), il quale ha presentato nel novembre scorso alla Corte di giustizia una richiesta di intervento a sostegno delle posizioni del Parlamento europeo.

Nelle more della pronuncia della Corte, il Gruppo art. 29 si è adoperato per tutelare il più possibile i diritti dei passeggeri. Nel giugno 2004 è stato approvato il parere 6/2004 in cui, in relazione all'attuazione da parte delle compagnie aeree del "pacchetto *Pnr*", si è auspicato un rapido passaggio dal meccanismo che consente alle autorità statunitensi di accedere direttamente ai sistemi di prenotazione (cd. sistema *"pull"*) ad un meccanismo in cui siano le stesse compagnie aeree a filtrare i dati ed inviarli (sistema *"push"*), nonché a fornire l'informazione completa e chiara ai passeggeri.

Per approfondire tali temi, il Garante ha ospitato a Roma un incontro fra le autorità di protezione dati europee e i rappresentanti delle compagnie aeree. In seguito a questo incontro, il Gruppo art. 29 ha approvato il parere 8/2004, in cui si propongono modelli di informativa da fornirsi ai passeggeri dei voli transatlantici da parte delle compagnie aeree, degli agenti di viaggio e dei sistemi di prenotazione via *computer* facenti parte del circuito di prenotazione dei voli.

Come già detto, il sistema statunitense è solo il primo di una serie di analoghe e

sempre più numerose iniziative che hanno finora interessato Canada, Australia, Sudafrica e Corea del Sud.

Il Gruppo, pur nella convinzione che una soluzione multilaterale sia preferibile e più aderente al principio di non discriminazione, ha esaminato nel corso del 2004 le richieste dell'Australia e del Canada.

Il sistema australiano prevede il trasferimento di un numero più limitato di dati personali che sono raccolti per finalità di lotta al terrorismo e reati connessi e sono conservati solo in casi specifici. Inoltre, i diritti dei passeggeri sono garantiti a livello sia normativo, sia istituzionale. Per queste ragioni, il Gruppo ha espresso un parere sostanzialmente favorevole (parere 1/2004 del 16 gennaio 2004) ad una dichiarazione di adeguatezza da parte della Commissione dopo che saranno chiariti e risolti alcuni aspetti controversi.

Per quanto riguarda il Canada, il parere 3/2004 dell'11 febbraio 2004 ha evidenziato una serie di problemi che dovranno essere risolti prima che si possa dare avvio al trasferimento di dati.

Bisogna, infine, sottolineare come la dimensione internazionale della questione del trasferimento dei dati dei passeggeri abbia spinto diverse organizzazioni internazionali, quali l'Ocse e l'Icao, ad occuparsi del tema al fine di trovare adeguate soluzioni multilaterali (v. *infra*).

22.7. *Cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Nel 2004 si è evidenziata la tendenza ad un ulteriore incremento delle iniziative legislative adottate a livello comunitario per rafforzare la cooperazione tra le autorità nazionali di polizia e giudiziarie. Tali iniziative, come si è visto, spesso implicano lo scambio di informazioni personali e, talvolta, la creazione di nuove basi di dati europee ovvero l'ampliamento della possibilità di accesso ai dati dei sistemi di informazione esistenti a soggetti nuovi rispetto a quelli previsti nelle convenzioni istitutive.

È necessario che queste attività rispettino al contempo le esigenze richieste da un'effettiva cooperazione tra forze di polizia e autorità giudiziarie e il diritto fondamentale alla tutela dei dati personali (solennemente introdotto dalla Carta dei diritti fondamentali e dal Trattato per una Costituzione europea) e si svolgano quindi nei limiti consentiti dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Attualmente, le iniziative dell'Ue che comportano la raccolta, la conservazione o lo scambio di dati personali ai fini dell'applicazione della legge sono numerose: tra gli esempi più significativi vi sono misure per consentire lo scambio di informazioni e la cooperazione rispetto ai reati terroristici, la semplificazione dello scambio di informazioni e di "*intelligence*" tra i servizi repressivi degli Stati, l'accesso ai dati ed agli archivi da parte degli organi giudiziari e le forze di polizia, lo scambio di dati sui passeggeri di voli aerei, nonché proposte per richiedere la conservazione dei dati delle comunicazioni. Vi sono poi, come ricordato, le diverse proposte volte ad introdurre elementi biometrici nei documenti rilasciati dagli Stati Ue a cittadini e stranieri, con la previsione di larghe basi di dati a livello europeo che si aggiungerebbero a quelle già esistenti, moltiplicando i rischi e gli effetti di un erroneo inserimento di dati o di accessi non autorizzati.

Questi ed altri sviluppi, quali il suggerimento di trasformare in futuro l'Europol in un'agenzia investigativa, possono avere rilevanti implicazioni anche per i diritti degli individui.

22

Per il modo della loro elaborazione e per la frammentarietà delle competenze in materia in seno all'Unione, molte delle nuove iniziative dell'Unione europea che riguardano dati personali sono al momento sottratte al controllo delle autorità di protezione dei dati poiché non rientrano in modo netto in uno dei tradizionali pilastri dell'Ue. Nonostante i ripetuti inviti del Parlamento europeo, queste attività hanno continuato ad essere svolte solo in gruppi di lavoro a composizione specializzata, senza il coinvolgimento adeguato delle istituzioni e degli organismi che a livello nazionale e comunitario hanno responsabilità in materia –con la conseguenza che spesso possono sfuggire sia alla tempestiva valutazione del Gruppo articolo 29, sia all'esame delle autorità di controllo esistenti nel cd. Terzo Pilastro (Schengen, Europol, Dogane)– senza, peraltro, un'adeguata base giuridica fondata sull'elaborazione di principi di protezione dei dati validi per i trattamenti proposti.

Già da tempo le autorità di protezione dei dati avevano segnalato il progressivo venir meno di "momenti istituzionalizzati" che favorissero la necessaria valutazione dell'impatto che tali misure erano destinate a produrre sui diritti fondamentali della persona e, più specificamente, sulla tutela dei dati personali. Infatti, i gruppi di lavoro il cui mandato specifico nel Consiglio dell'Ue era la protezione dati, rispettivamente nel Primo e Terzo Pilastro, sono stati soppressi fin dal 2002 e solo nei primi mesi del 2004 il Garante europeo per la protezione dei dati ha iniziato la sua attività, peraltro limitata ai trattamenti effettuati dalle istituzioni comunitarie "nei settori di competenza del diritto comunitario".

Considerato che i pilastri dell'Ue con l'adozione del Trattato firmato a Roma il 29 ottobre 2004 sono destinati a convergere e la protezione dei dati personali ha assunto il rango di diritto fondamentale, in occasione della Conferenza delle autorità incaricate della protezione dei dati svoltasi a Rotterdam nel 2004, è stato deciso che i rappresentanti delle autorità che operano a livello comunitario si riuniscano per coordinare la loro attività e cercare di svolgere un ruolo adeguato ai bisogni rappresentati.

Alla prima riunione di questo gruppo "di pianificazione", che ha avuto luogo nel giugno 2004, hanno partecipato il Garante europeo della protezione dei dati, i presidenti delle autorità di controllo comune e la presidenza del Gruppo art. 29.

La situazione si è evoluta nel settembre 2004 in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati a Wroclaw, quando una sessione a porte chiuse delle autorità europee ha approvato una risoluzione in cui si chiede che le istituzioni dell'Ue promuovano un *forum* nel quale le autorità europee incaricate della protezione dei dati possano discutere le implicazioni a livello di protezione dei dati degli sviluppi del Terzo Pilastro. Fino alla creazione di tale *forum*, le iniziative del Terzo Pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune, saranno esaminate da un gruppo di lavoro delle autorità europee incaricate della protezione dei dati.

Le autorità di controllo hanno pertanto deciso, avvalendosi della struttura di segreteria comune prevista per assistere i lavori delle autorità Schengen, Europol e Dogane, di prevedere alcune riunioni congiunte, invitando anche il Garante europeo per la protezione dei dati e l'autorità di controllo istituita per Eurojust, ove informarsi e discutere, al momento informalmente, delle iniziative esistenti ed eventualmente definire proposte unitarie da presentare agli organismi competenti, avvalendosi anche delle aperture che sembrano presenti nel nuovo programma per il rafforzamento dell'area di libertà, sicurezza e giustizia per il periodo 2005-2009.

Un canale particolare di dialogo si è aperto con la *House of Lords*, il cui sottocomitato specializzato ha richiesto un parere sulla protezione dei dati nel Terzo Pilastro, ed è stato rafforzato il legame esistente con il Parlamento europeo, Commissione libertà e diritti dei cittadini, che ha voluto incontrare più volte i rap-

presentanti delle autorità in previsione della discussione di alcune delle iniziative menzionate. Va ricordato in proposito che a partire dal 1° gennaio 2005 il Parlamento ha acquisito il diritto alla codecisione in materie quali le politiche di visti, asilo, immigrazione e le altre politiche connesse alla realizzazione del principio della libera circolazione delle persone e sarà quindi necessario il suo accordo per la loro adozione.

Ma certamente la novità più positiva in materia è legata alla nomina del nuovo Commissario italiano come vice presidente e responsabile del settore Libertà, sicurezza e giustizia. Fin dalla presentazione del suo programma davanti al Parlamento europeo il Commissario Frattini ha infatti chiarito che intende far garantire il pieno rispetto del diritto alla protezione dei dati personali e favorire il dialogo con le autorità di protezione dei dati per le materie affidate alla sua competenza.

A rafforzamento di questo impegno il Commissario ha incontrato le autorità di controllo comuni nella loro riunione congiunta del 21 dicembre pronunciando un apprezzabile discorso disponibile in rete che contiene precise linee di azione ed impegni in materia e che dovrebbe servire da guida anche per i successivi interventi dei rappresentanti della Commissione.

22.8. *L'attività del Garante nell'Autorità di controllo comune Schengen*

Il Garante è autorità nazionale di controllo per l'Italia con il compito di esercitare un controllo indipendente dell'archivio della sezione nazionale del Sistema d'informazione Schengen (Sis) e verificare che l'elaborazione e l'utilizzazione dei dati inseriti non leda i diritti della persona interessata, ai sensi dell'art. 114 della Convenzione; in tale veste entra a comporre l'Autorità di controllo comune (Acc).

Fra le attività di maggior rilievo dell'Acc, alle cui riunioni il Garante ha partecipato attivamente fin dall'inizio nella persona del segretario generale, prima vice presidente poi nel biennio 2002-2003 presidente dell'Autorità, va ricordata quella di verifica e controllo del funzionamento della parte centrale del Sis e di vigilanza sulla corretta applicazione delle disposizioni della Convenzione, attività che viene svolta anche attraverso l'indicazione, ove necessario, degli aggiustamenti e delle prassi corrette da adottare. Considerato che ad una persona può essere rifiutato l'accesso al territorio Schengen (e non più solo al territorio nazionale) sulla base di informazioni contenute nel sistema, resta di immediata ed ovvia importanza assicurare che le informazioni siano ad esempio accurate ed aggiornate.

L'attività dell'Acc continua ad essere di particolare rilievo e, al riguardo, va notata la crescente attenzione prestata dal Consiglio dell'Unione europea ai pareri dalla stessa espressi, come ad esempio mostra la recente Decisione relativa alla "lotta contro la criminalità connessa con veicoli". Il testo approvato ha recepito largamente le osservazioni critiche formulate dall'Acc rispetto alla proposta iniziale e non prevede più di allargare l'accesso diretto al Sis a soggetti diversi da quelli già autorizzati, limitandosi a richiedere da parte delle autorità competenti il tempestivo inserimento nel sistema di una segnalazione ogniqualvolta vengano denunciati furti di veicoli o di carte di circolazione e l'informazione degli uffici nazionali della motorizzazione.

Nel corso del 2004 gran parte dell'attività dell'Acc ha continuato ad essere concentrata sui problemi legati allo sviluppo del Sistema informativo Schengen, il cd. Sis II.

In estrema sintesi, vi sono due aspetti che preoccupano fortemente l'Acc, il primo concernente le informazioni che il Sis deve contenere (anche a fronte delle diverse proposte per introdurre nuove categorie di informazioni e nuovi tipi di dati); l'altro,

22

in merito all'accesso al Sis e all'uso dei dati nel sistema. Con queste proposte, peraltro frutto e sintomo di un approccio normativo frammentario, si tende ad trasformare il Sis in un sistema di indagine e non più solo di informazione, mutandone quindi radicalmente le finalità rispetto a quelle definite dalla Convenzione del 1990.

L'Autorità ha ricordato nel parere adottato il 19 maggio che l'ampliamento delle categorie di informazioni registrabili nel sistema, il possibile inserimento di dati biometrici, la modifica di alcuni meccanismi di accesso e utilizzazione dei dati proposti a livello tecnico, possono essere praticati, ma devono essere fondati su un'appropriata base giuridica. L'Acc ha rimarcato l'assenza di tale base ed ha ricordato il necessario rispetto del testo attuale della Convenzione, la quale individua esattamente le categorie di dati inseribili e le autorità che possono accedere ai dati, fissandone i limiti. Anche i compiti delle autorità di supervisione e controllo sono disegnati in relazione alle attuali funzionalità del sistema.

Qualunque cambiamento, inclusi quelli definiti con il recente regolamento del Consiglio del 29 aprile 2004 (v. *Documentazione* par. 49), deve essere considerato ed "equilibrato" rispetto al disegno dell'intero sistema. L'Acc ha chiesto pertanto che le proposte siano previamente e adeguatamente discusse considerando anche quale sarebbe il loro impatto sui diritti fondamentali della persona e sul rispetto dei principi in materia di protezione dei dati, in particolare il principio di proporzionalità delle modifiche richieste. In questa valutazione, deve essere anche considerato il rischio che il Sis, incorporando nuove funzioni e nuove categorie di dati, possa duplicare inutilmente sistemi di informazioni già esistenti in seno all'Unione. L'Acc si è dichiarata disponibile ad assistere con la sua competenza le istituzioni comunitarie ed ha comunque richiesto una puntuale informazione sui lavori in corso, per poter essere in grado di formulare indicazioni in tempo utile rispetto all'adozione degli atti.

I timori dell'Acc si fondano sull'osservazione del modo in cui i lavori per il Sis II vengono portati avanti. Sarebbe infatti logico far precedere lo sviluppo tecnico del sistema sia da decisioni politiche che ne fissino le finalità e le relative modalità di funzionamento, sia dalla definizione di un idoneo quadro giuridico che modifichi le disposizioni attualmente vigenti specificando le finalità del sistema e stabilendo le norme necessarie per definire le modalità di accesso e gli altri elementi essenziali. Invece, in mancanza di decisioni appropriate, le proposte formulate dalla Commissione cercano di costruire un sistema basato sulla massima flessibilità tecnica, prevedendo il maggior numero di funzioni e di accessi. *"Pertanto"*, si legge nel parere dell'Acc, *"la messa a punto del sistema avviene sotto l'impulso delle mutevoli istanze provenienti dal settore giustizia e affari interni dell'Ue, anziché sulla base di obiettivi espressi e definiti all'interno di un quadro giuridico preciso"*.

Preoccupazioni analoghe sono state rappresentate anche dal Parlamento europeo che si è dimostrato molto sensibile alle sollecitazioni provenienti dalle autorità di protezione dei dati personali.

L'Acc ha inoltre proseguito l'attività di verifica sulle modalità dell'inserimento nel Sis delle segnalazioni di stranieri al fine di non ammetterli sul territorio Schengen, per valutare se vi siano discrepanze fra gli Stati Parte nell'applicazione e/o nell'interpretazione dell'art. 96 della Convenzione. Nel corso dell'anno, le autorità nazionali di controllo hanno richiesto, sulla base di un modulo appositamente predisposto, specifiche informazioni sulle procedure seguite dagli uffici che sono abilitati ad inserire i dati nel sistema (per l'Italia: oltre ad alcuni uffici centrali del Ministero dell'interno, le questure) e hanno svolto colloqui che hanno interessato anche il Sis nazionale (N-Sis) ed il Sirene.

Di queste attività, che sono state svolte in maniera coordinata in tutti gli Stati

Schengen, è stata data ampia informazione all'Acc la quale predisporrà un documento riassuntivo e, ove necessario, linee-guida. Una seconda parte dell'indagine, consistente in una ispezione agli archivi per verificare in concreto la correttezza degli inserimenti ed il rispetto delle regole in materia di trattamento e conservazione dei dati, sarà svolta, sempre con modalità coordinate, nei primi mesi del 2005.

A completamento di quanto detto, si può segnalare, anche se non direttamente legata all'attività dell'Acc, la visita di valutazione che gli esperti del Consiglio dell'Unione europea hanno svolto in Italia nel mese di settembre 2004 per gli aspetti relativi alla protezione dei dati. Di essa si è già reso conto nel par. 6.3; è opportuno evidenziare qui le preoccupazioni manifestate dagli esperti per l'alto numero di segnalazioni inserite ai sensi dell'art. 96 con il conseguente invito a verificarne la qualità.

22.9. *Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso*

L'Autorità comune di controllo ha presentato il 23 novembre scorso la seconda relazione di attività che copre il biennio da novembre 2002 ad ottobre 2004 (v. *Documentazione* par. 54).

Nella relazione, l'Acc ha ricordato come, in un periodo fortemente caratterizzato dalle misure adottate per combattere il terrorismo dopo i tragici eventi dell'11 settembre 2001 negli Stati Uniti e, recentemente, dagli attentati di Madrid nel marzo 2004, l'Autorità stessa nei suoi pareri e nelle iniziative attuate abbia dimostrato che è possibile, e per nulla incompatibile, sostenere l'obiettivo comune della lotta al terrorismo internazionale e alla criminalità organizzata, salvaguardando nel contempo i diritti dei singoli.

L'Acc ha anche evidenziato che risulta sempre più evidente che il campo della cooperazione di polizia e giudiziaria necessita di norme chiare e specifiche sulla protezione dei dati, con la formulazione di un parere indipendente e di un'attività di controllo armonica.

Relativamente all'attività svolta nel corso del 2004, si segnala in particolare la vigilanza sulle modalità di applicazione dell'accordo Europol-Stati Uniti per la trasmissione di dati personali.

Secondo i dati acquisiti dall'Acc lo scambio della maggior parte delle informazioni tra l'Ue e le autorità di polizia statunitensi sembrerebbe essere avvenuto in base ad accordi bilaterali esistenti tra gli Stati Uniti e singoli Stati membri. L'Autorità, tuttavia, ritenendo che il volume di informazioni scambiate tra Europol e Stati Uniti aumenterà, ha deliberato di concentrare le ispezioni future dell'Europol sull'esame dei dati di natura personale trasmessi nell'ambito dell'accordo, per assicurare che vi sia conformità alle disposizioni pertinenti. Inoltre, l'Acc cercherà di coordinare l'attività di vigilanza, collaborando con le autorità nazionali incaricate della protezione dei dati personali negli Stati membri e con il *Chief Privacy Officer* presso il Dipartimento della sicurezza interna negli Stati Uniti.

La conduzione d'ispezioni *in loco* delle attività dell'Europol costituisce peraltro uno dei modi adottati dall'autorità di controllo comune per ottemperare al suo mandato. L'Acc ha al riguardo definito gli obiettivi ed i criteri che guideranno le ispezioni future (di regola annuali), anche alla luce della considerazione che il ruolo dell'Europol si sta sviluppando rapidamente, con un numero sempre maggiore di dati trattati.

Nel marzo 2004 è stata effettuata una nuova ispezione, incentrata sulla qualità dei dati trattati negli archivi per fini di analisi. Come risultato, il *team* d'ispezione ha riscontrato che, nel complesso, la qualità dei dati è soddisfacente, almeno per

quanto riguarda la rispondenza dei dati negli archivi con quelli forniti dagli Stati membri. Tuttavia, è stata confermata la percezione di un'incapacità generale da parte degli Stati membri di valutare correttamente i dati trasmessi ad Europol (verificando la fonte, l'affidabilità e così via). L'Acc ha sottolineato che, per risolvere questo problema, occorre migliorare la cooperazione tra Stati Membri ed Europol.

Altro tema rilevante riguarda le squadre investigative comuni: l'Acc sta attualmente valutando la portata del sostegno in materia di analisi fornito dall'Europol.

Una decisione del Consiglio ha introdotto regole comuni per queste squadre ed ha previsto la possibilità che le stesse includano "funzionari di organismi costituiti ai sensi del Trattato sull'Unione europea": una definizione che interessa dunque anche il personale dell'Europol. I particolari riguardanti la partecipazione di questo organismo a squadre investigative comuni sono stati definiti in un successivo Protocollo ai sensi del quale il suo personale parteciperebbe solamente con "funzioni di supporto". Tuttavia, sempre in base al Protocollo, gli agenti dell'Europol verrebbero comunque inseriti nella catena di comando e le informazioni detenute negli archivi sarebbero condivise con i componenti della squadra; inoltre, le informazioni da questa raccolte sarebbero a loro volta inserite nelle banche dati dell'Europol.

L'Acc ha chiesto all'Europol di essere informata in merito alle decisioni riguardanti il tipo di sostegno che sarebbe offerto alle squadre investigative comuni. Ed in particolare sul modo in cui l'organismo intende utilizzare i suoi servizi di analisi ed ha intenzione di vigilare per assicurare il rispetto della Convenzione.

L'attività del comitato ricorsi

Nel 2004 l'Europol (in base a dati dallo stesso forniti) ha ricevuto circa dieci richieste di accesso (un dato relativamente stabile negli ultimi due anni) mentre risultano in aumento i casi di contenzioso.

Nell'ultimo anno il comitato ha deciso in merito a due ricorsi e attualmente vi sono parecchi casi su cui deve ancora esprimersi.

I casi affrontati hanno portato a decisioni relative a importanti questioni di principio. In particolare, è stato affermato che l'Europol deve considerare nel merito ogni richiesta di accesso, anziché applicare un approccio generale e che deve rispondere ad ogni richiesta nella lingua in cui la stessa è formulata, purché sia una delle lingue ufficiali dell'Unione europea.

22.10. *Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune*

Come si è ricordato nelle precedenti Relazioni, a seguito della ratifica ed entrata in vigore della Convenzione sull'uso dell'informatica nel settore doganale, è stato creato un sistema informativo automatizzato comune ai paesi membri dell'Ue (Sistema informativo doganale-Sid) per facilitare la prevenzione, ricerca e repressione delle infrazioni sia delle norme comunitarie, sia delle leggi nazionali, attraverso lo scambio di dati ed informazioni fornite dai servizi doganali di ciascuno Stato membro.

Il sistema consiste in una base di dati centrale cui si può accedere tramite terminali in ogni Stato membro. La Commissione europea provvede alla gestione tecnica dell'infrastruttura del Sid.

La vigilanza sul corretto funziamento del Sid è affidata ad una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

Nel corso del 2004 l'Autorità si è riunita due volte ed in particolare nella seconda riunione, svoltasi nel mese di dicembre, sono stati affrontati aspetti cruciali per la sua configurazione ed attività.

In primo luogo è emerso un delicato problema di funzionalità dell'Acc: infatti, pur essendo state approvate le linee guida per svolgere la prima ispezione al Sid e costituito il *team* di esperti per effettuarla, la stessa non ha potuto svolgersi per mancanza di disponibilità finanziaria. Le attuali disposizioni di *budget* del Consiglio consentono il rimborso –tra l'altro non all'Autorità nazionale che sostiene le spese, ma al Governo– delle sole spese di viaggio di un componente in occasione delle riunioni dell'Acc e non ci sono stanziamenti per consentire le altre attività, pur previste dalla Convenzione. L'attività di ispezione dovrebbe quindi svolgersi ad intero carico delle autorità che compongono il *team* di esperti.

Ne è scaturita una riflessione tra i componenti i quali hanno lamentato che la situazione creatasi incide gravemente sulla funzionalità dell'Autorità e lede il presupposto stesso della sua esistenza, quello, cioè, di sorvegliare sul funzionamento del Sid anche attraverso l'accesso allo stesso (v. art. 18 della Convenzione). È stato chiesto al Presidente di rappresentare nei modi più appropriati tale doglianza.

Altro punto importante riguarda l'ancora scarsa utilizzazione del sistema da parte delle autorità doganali. Per approfondire gli aspetti che rendono problematico l'utilizzo del sistema, nella riunione di dicembre sono stati invitati rappresentanti dell'Olaf e del Gruppo di cooperazione doganale del Consiglio.

Ne è emerso un quadro complesso, legato anche alla presenza contestuale di numerose basi di dati nel settore: i rappresentanti delle istituzioni comunitarie hanno però confermato la volontà di far sì che il Sid sia posto al centro della cooperazione doganale e di prevederne addirittura il potenziamento, al fine di metterlo in grado di svolgere attività di analisi dei rischi. L'Autorità, su questo punto, ha ricordato la necessità del pieno rispetto della Convenzione ed ha auspicato un analogo potenziamento del suo ruolo, dichiarandosi disponibile a fornire ogni contributo ai futuri lavori.

22.11. *La partecipazione ad altri comitati e gruppi di lavoro*

IWGDPT

Il Garante ha partecipato ai due incontri dell'*International Working Group on Data Protection in Telecommunications* (IWGDPT) che si sono svolti in Argentina (Buenos Aires, 14-15 aprile 2004) e in Germania (Berlino, 18-19 novembre 2004).

Il primo incontro ha preso in esame in particolare i problemi connessi alla libertà di espressione nel mondo *on-line*, ai nuovi servizi di comunicazione (*wireless*, *Mms*) e agli effetti che essi producono sulla *privacy*, nonché alle problematiche concernenti le tecnologie *Rfid*. Su questi temi i delegati hanno adottato tre documenti che richiamano l'esigenza di garantire il rispetto dei principi di protezione dati, anche attraverso un'adeguata informativa del pubblico, la disponibilità di strumenti che consentano agli interessati l'esercizio dei diritti loro riconosciuti e l'adozione di idonee misure di sicurezza.

Durante il secondo incontro sono stati adottati due documenti rispettivamente dedicati agli strumenti e alle procedure per combattere le frodi informatiche nel rispetto della *privacy* e alle modalità concrete attraverso le quali i soggetti deputati alla sicurezza delle reti possano acquisire le necessarie conoscenze dal punto di vista della protezione dei dati. Sono stati inoltre affrontati i problemi legati alle tecnologie di localizzazione e di videosorveglianza (con particolare riferimento alla registrazione delle immagini, all'utilizzo di sistemi di riconoscimento dello *stress* attraverso l'analisi della voce e i pericoli connessi al *Voice over IP* nel caso in cui il terminale usato per la ricezione delle comunicazioni sia un *computer*).

La delegazione italiana ha chiesto, in conclusione, di inserire il tema dell'*e-health*, ed in particolare della cartella clinica *on-line*, nell'ordine del giorno dei prossimi incontri.

CIRCA Complaints

Gli incontri, a cadenza semestrale, dedicati alla trattazione di ricorsi e segnalazioni transnazionali ed allo scambio di buone prassi e informazioni su questioni applicative concrete, si sono svolti a Stoccolma (11-12 marzo 2004) e a Praga (4-5 novembre 2004).

Tutti i 25 Paesi dell'Unione hanno inviato propri rappresentanti. Conformemente allo spirito che da sempre ha ispirato questi incontri, molto spazio è stato dedicato all'esame di singoli casi e al confronto sugli approcci seguiti. Sono state sollevate e proposte questioni di interesse comune, quali il trattamento dei dati biometrici; le attività di sensibilizzazione svolte a livello nazionale e i possibili suggerimenti da esse ricavabili in termini di buone prassi; le attività ispettive, le tematiche inerenti al trattamento e alla conservazione dei dati di traffico da parte dei gestori di servizi di telefonia mobile, casi di bilanciamento di interessi con particolare riguardo ai rapporti di lavoro. Una particolare riflessione è stata svolta in relazione alle decisioni assunte dal Gruppo art. 29 in materia di *enforcement,* in vista del possibile sviluppo di iniziative comuni e "sincronizzate" nei settori che risultano più problematici.

In particolare, l'incontro di Praga ha offerto la possibilità di un aggiornamento sullo *status* delle autorità di protezione dati nei dieci Stati membri recentemente entrati a far parte dell'Ue e sui principali problemi che esse incontrano: da più parti è stato lamentato un *deficit* di trasparenza rispetto ai trattamenti di dati effettuati per scopi di sicurezza e giustizia da soggetti pubblici (in particolare le forze di polizia), anche se su queste tematiche le autorità mantengono grande attenzione e ricevono un forte sostegno da parte dell'opinione pubblica. Lo stesso, inoltre, ha consentito di individuare alcune priorità per le attività future con l'approvazione della proposta di una ridefinizione del mandato del *Workshop* sulla scorta di quanto indicato dalla *Spring Conference of European Data Protection Commissioners* tenutasi a Rotterdam nel mese di aprile 2004. Senza modificare l'approccio pragmatico finora seguito dai *Workshop*, è stato costituito un *drafting group* (comprendente l'Italia) per redigere una sorta di "statuto" dei *Complaints Handling Workshop* che ne fissi le caratteristiche fondamentali (trattazione di ricorsi o segnalazioni, soprattutto attraverso *case studies*, sui quali confrontare i diversi punti di vista; particolare attenzione rispetto ai casi più difficili ed alle questioni che richiedono una valutazione armonizzata a livello Ue; mantenimento della struttura flessibile del programma dei *Workshop*).

22.12. *Consiglio d'Europa*

Nel mese di maggio del 2004 sono stati definitivamente approvati dal Comitato dei Ministri del Consiglio d'Europa i principi guida elaborati dal CJ-PD rispetto al trattamento di dati personali attraverso "carte intelligenti", ossia carte contenenti un *microchip* in grado di effettuare particolari operazioni (accesso ai servizi in rete, pagamenti *on-line* ecc.) e nel quale è possibile inserire un notevole numero di informazioni personali, dai dati identificativi a quelli biometrici, come le impronte digitali (v. *Documentazione* par. 73).

I principi-guida ribadiscono che i dati personali raccolti e trattati attraverso *smart card* devono essere limitati al minimo indispensabile ed essere utilizzati solo per scopi legittimi e specifici. I dati sulla salute, in particolare, possono essere trattati solo se vi è una previsione di legge, oppure con il consenso dell'interessato, e dovranno essere adottate misure di garanzie come la cifratura. I cittadini devono essere informati sull'uso che viene fatto delle loro informazioni personali ed occorre procedere con cautela nell'utilizzazione di *smart card* come mezzo di pagamento se in esse sono registrati dati sensibili.

I principi-guida sono rivolti in via primaria ai soggetti che rilasciano le *smart card* in quanto titolari delle relative operazioni di trattamento, ma riguardano anche tutte le altri parti in causa (progettisti di sistemi, gestori, operatori, interessati); nel caso di una carta multiuso, si avrà una situazione di contitolarità da parte dei soggetti che raccolgono ed utilizzano i dati.

Il Comitato T-PD ha proseguito i lavori sulle implicazioni per la protezione dati delle applicazioni biometriche, continuando una riflessione già avviata dal CJ-PD (comitato soppresso, come ricordato nella *Relazione 2003*) e cercando di acquisire le esperienze maturate in questo settore dal Gruppo art. 29 e dall'Ocse. Nel corso della prossima riunione potrebbe essere approvato un documento che descrive lo stato dell'arte e le questioni tuttora aperte relativamente alle tecnologie biometriche, alla luce dei principi fissati nella Convenzione n. 108.

Il Comitato ha anche iniziato una attività rivolta alla valutazione dell'applicazione dei principi di protezione dati a Internet. Sulla scorta dell'analisi contenuta in un rapporto sul principio dell'autodeterminazione informativa nell'era di Internet, si stimolerà la riflessione sull'applicabilità della Convenzione n. 108 alle reti di comunicazione elettronica.

Come ben evidenziato nel rapporto, si è assistito alla crescita esponenziale dei supporti di comunicazione che ha creato la possibilità di "registrare" la vita di tutti, mentre il costo di tali operazioni è sempre più accessibile. Lo sviluppo tecnologico è, però, avvenuto su scala mondiale senza soggetti o attori in grado di stabilire i relativi limiti, e soprattutto senza che i problemi relativi alla vita privata, fortemente minacciata dalle reti, siano stati tecnicamente affrontati. Vi è oggi, quindi, la necessità di definire un modello efficace di protezione dati, attraverso l'imposizione di norme operative per i terminali, i protocolli e gli operatori di telecomunicazioni.

Per quanto concerne poi la possibilità di applicare le disposizioni della Convenzione n. 108 alle reti di telecomunicazione, è stata rilevata come preminente l'esigenza che l'utente sia adeguatamente informato sui trattamenti di dati effettuati dagli operatori e possa partecipare al "negoziato" che riguarda il trattamento dei dati personali a lui riferiti; l'obbligo di informativa dovrebbe ricadere sui produttori.

22.13. *Ocse*

Spam

Il Garante ha partecipato ai lavori del *Working Party on Information Security and Privacy* che, in relazione ai temi di protezione dati, si è occupato dell'applicazione delle linee-guida sulla sicurezza, dello *spam*, della sicurezza dei trasporti e dei modelli di informativa.

Per quanto riguarda lo *spam*, l'Ocse ha organizzato nel 2004 un seminario pubblico sullo *spam* ospitato dalla Commissione europea con l'obiettivo di studiare la dimensione internazionale del fenomeno e le possibili strategie di contrasto.

Analizzato il fenomeno dello *spam* (anche in termini di impatto economico e sociale), ha formato oggetto di discussione l'individuazione delle varie strategie di contrasto (in particolare attraverso legislazione e autoregolamentazione, in un quadro di cooperazione internazionale fra le Autorità di protezione dei dati e le altre autorità competenti, incluse le forze dell'ordine e giudiziarie).

I partecipanti comprendono rappresentanti delle istituzioni, del mondo delle imprese, della società civile e studiosi di livello universitario. Per l'Italia era presente il segretario generale dell'Autorità con una relazione sulle difficoltà e le sfide della cooperazione internazionale contro lo *spam* ed una illustrazione delle attività svolte dall'Autorità per contrastarne gli effetti. Nella analisi conclusiva delle prospettive

22

sulla lotta allo *spam*, tenuto conto dell'ampiezza e complessità del fenomeno, si è proposta l'adozione di strategie "multilivello".

Il nodo problematico più difficile da affrontare rimane comunque quello del *law enforcement*, anche perché le competenze in materia di *spam* sono attribuite all'interno dei singoli paesi ad istituzioni differenti e non sempre si riesce ad avere un referente unitario. Per ovviare a tale difficoltà è stata costituita una specifica *Task Force* che avrà il compito di svolgere una ricognizione delle istituzioni competenti in questa materia nei singoli paesi e dei poteri loro attribuiti. La *Task Force* si occuperà di studiare le tecniche utilizzate dagli *spammer*, di analizzare lo *spam* telefonico, di coinvolgere il settore pubblico e quello privato e di costituire una *contact list*.

Biometria

L'Ocse si è inoltre occupato del problema della sicurezza e riservatezza delle informazioni raccolte nel campo della sicurezza internazionale dei viaggiatori. È stato costituito a tal fine un gruppo di lavoro congiunto Ocse/Icao (di cui fa parte anche il Garante) che ha iniziato ad occuparsi del tema dell'inserimento dei dati biometrici nei documenti di viaggio. Sono in fase di elaborazione delle linee-guida che saranno messe a punto nei prossimi mesi. Gli aspetti più delicati sotto il profilo della protezione dati sono legati all'individuazione dei dati da inserire, all'architettura del sistema (centralizzato/decentralizzato) e alle funzionalità dello stesso (autenticazione/identificazione).

Con riferimento al tema dell'informativa, in seguito alla risoluzione approvata alla Conferenza mondiale dei Garanti della *privacy* che si è svolta a Sidney nel 2003, è stato presentato un documento volto a promuovere l'elaborazione di un modello di informativa semplice, efficace e comprensibile, nella convinzione che la trasparenza nella comunicazione delle informazioni relative ai dati personali sia il necessario presupposto di un reale sviluppo della protezione dei dati. Il valore aggiunto di un lavoro su questo tema portato avanti in sede Ocse dovrebbe essere quello di mettere insieme le esperienze maturate nel settore privato e nel settore pubblico. Uno studio condotto su modelli di informativa predisposti da numerose società multinazionali ha fatto emergere con immediatezza che i modelli predisposti sono generalmente poco leggibili e non chiari nei contenuti. Su questo tema lavorerà nei prossimi mesi un gruppo ristretto di delegati, fra i quali è presente anche il Garante.

23 Attività di ricerca, comunicazione e formazione

23.1. *La comunicazione del Garante: profili generali*

Nel 2004, l'attività di comunicazione curata dal Garante si è concentrata in maniera particolare sull'illustrazione delle maggiori novità introdotte dal Codice e sull'individuazione di criteri per bilanciare gli interessi in gioco riguardo ad alcuni temi problematici quali la sanità, la sicurezza, le grandi banche dati.

L'attività di informazione e comunicazione ha seguito, pertanto, l'impegno dell'Autorità nei confronti di particolari aspetti applicativi della normativa, incentrandosi su una serie di importanti settori, oggetto specifico di intervento da parte del Garante, che vanno dalla tutela dei dati sanitari dei lavoratori, allo *"spamming"* (telematico e telefonico), ad Internet, alle tecnologie biometriche, alle intercettazioni, alla necessaria trasparenza nelle operazioni finanziarie, al giornalismo, con speciale riguardo alla dignità della persona, alla tutela dei minori e ai rischi dell'accanimento informativo. In questi ambiti, il Garante è spesso intervenuto in favore di una nuova nozione di protezione dati come "valore aggiunto" per imprese e pubbliche amministrazioni al fine di instaurare un rapporto nuovo con utenti e consumatori nell'economia del mercato globale.

Oltre che su tali questioni, l'attività di comunicazione si è intensificata nella promozione della protezione dei dati personali come diritto fondamentale e autonomo, sancito anche dal Trattato che adotta una Costituzione per l'Europa.

L'Autorità ha mantenuto la scelta di affidare la sua informazione ad un linguaggio rigoroso, ma attento ad una funzione divulgativa, per corrispondere alle esigenze dei cittadini. Nel dar conto della propria attività e delle tematiche all'ordine del giorno, l'Autorità ha richiamato l'attenzione di istituzioni, pubbliche amministrazioni, imprese e, in generale, degli utilizzatori di dati, sugli obblighi da attuare, sui rischi di violazione e sul valore sociale e culturale del diritto alla *privacy*.

La tipologia dei prodotti informativi ed editoriali è stata ampia, differenziata e connotata da una forte caratterizzazione, favorita peraltro dall'adozione di una *corporate identity* nella documentazione e comunicazione dell'Autorità e da una strategia integrata di comunicazione, nella quale spicca anche un aumentato utilizzo di *mass media* tradizionali, come radio e tv, nonché di media *on-line* e prodotti multimediali.

In particolare, la presenza sulle pagine dei maggiori quotidiani e periodici nazionali ed internazionali e dei media *on-line* delle tematiche riguardanti la protezione dei dati personali e l'attività del Garante si è mantenuta costantemente alta in questi anni. Nel periodo che va dal 1° gennaio 2004 al 31 dicembre 2004 le pagine dedicate alle questioni legate generalmente alla *privacy* sono risultati oltre 8400, delle quali circa 1700 dedicate specificamente all'attività del Garante. Le "prime pagine" dedicate ai temi della protezione dei dati personali sono state circa 1200 (di cui oltre 640 riguardanti la sola Autorità). Numerose sono state le interviste pubblicate sulla carta stampata (91), su tv e radio nazionali e locali (138) e diverse anche su pubblicazioni *on-line*.

23

23.2. *Prodotti informativi*

La *Newsletter* settimanale, che si appresta ad entrare nel suo sesto anno di pubblicazione (per un totale complessivo di 250 numeri), è diventata uno strumento di centrale riferimento dell'attività di comunicazione del Garante, fornendo una illustrazione in chiave giornalistica dei provvedimenti e dell'attività dell'Autorità, nonché un articolato panorama di temi e problematiche. Maggiore attenzione è stata sempre più dedicata a quanto avviene in campo comunitario ed internazionale, non solo riguardo ai temi della protezione dei dati, ma anche al più largo ambito della tutela dei diritti fondamentali.

La *Newsletter* può essere consultata *on-line* sul sito *web* del Garante ed è inviata in via telematica ad un numero sempre maggiore di abbonati (istituzioni, privati cittadini, imprese, liberi professionisti).

Nel 2004, è giunto alla sua XII edizione il *Cd Rom* "*Cittadini e Società dell'informazione"* che contiene, in forma integrale e nell'originale veste editoriale, i provvedimenti del Garante, la documentazione relativa alla normativa nazionale ed internazionale di riferimento, le pubblicazioni realizzate. L'archivio digitale ipertestuale, che consente una consultazione con funzioni di ricerca "*full-text*", rappresenta uno strumento conosciuto e costantemente richiesto da parte di amministrazioni pubbliche, imprese, liberi professionisti e cittadini. Nella recente edizione il Cd contiene anche una presentazione multimediale del Garante e dei temi di particolare interesse affrontati nel corso della sua attività.

Tra le pubblicazioni va annoverato il *Bollettino* che raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa ed altra documentazione. Per questa pubblicazione è prevista una revisione complessiva.

La necessità di promuovere una sempre maggiore conoscenza delle norme sulla protezione dei dati e dei diritti della persona oggi riconosciuti ai cittadini, ha spinto l'Autorità a sviluppare nuove modalità di informazione: oltre agli strumenti di comunicazione già utilizzati –da quelli tradizionali (comunicati stampa, *Newsletter*, conferenze stampa, *press briefing*) a quelli multimediali ed interattivi– l'Autorità ha realizzato nuovi prodotti.

L'impegno per una comunicazione agile e diretta al cittadino ha trovato attuazione nella realizzazione di *depliant* illustrativi dei diversi aspetti connessi alla protezione dei dati. I primi tre pieghevoli sono stati dedicati, rispettivamente, all'esercizio dei diritti riconosciuti dalla normativa; all'attività e al ruolo del Garante; alla difesa della *privacy* su Internet. Un quarto, di recente pubblicazione, riguarda le caratteristiche che avranno i nuovi elenchi telefonici.

Il progetto di comunicazione istituzionale proseguirà con la realizzazione di una ulteriore serie di *depliant* relativi a diverse tematiche (videosorveglianza, credito al consumo, rapporti di lavoro ecc.).

23.3. *Prodotti editoriali*

È giunto al suo dodicesimo numero il notiziario bimestrale, *"Garanteprivacy.it"*, una pubblicazione destinata a personalità del mondo imprenditoriale ed istituzionale, caratterizzata da una comunicazione mirata ed essenziale; la pubblicazione è volta a sottolineare l'attività dell'Autorità nei diversi settori di intervento, con particolare attenzione anche al panorama internazionale.

Prosegue la pubblicazione di volumi nell'ambito della collana *"Contributi"*, che ospita testi attinenti specifiche problematiche sulla protezione dei dati personali e la

tutela della dignità della persona. Ai primi due volumi della collana, il *"Massimario 1997-2001"*, a cura di Luigi Pecora e Giuseppe Staglianò, e *"Privacy e giornalismo"*, a cura di Mauro Paissan, si è aggiunto *"Da costo a risorsa. La tutela dei dati personali nelle attività produttive"*, curato da Gaetano Rasi.

Nel primo libro, l'attività di massimazione dei provvedimenti assunti nel corso degli anni è stata 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 –a breve disponibile anche in formato elettronico– si indirizza in particolar modo a giuristi, operatori del diritto, ordini professionali, imprese, istituzioni pubbliche e private.

Il secondo volume, preceduto da un saggio introduttivo del curatore, raccoglie, invece, diverse decisioni adottate dall'Autorità in materia di tutela della persona e libertà di manifestazione del pensiero. Come in una sorta di manuale pratico per i giornalisti, ma anche per i cittadini, si possono agilmente rintracciare le decisioni riguardanti la tutela dei minori, i rapporti tra cronaca e giustizia, l'uso dei dati di personaggi pubblici, la trasparenza delle fonti pubbliche, i divieti e i rischi derivanti dalla diffusione dei dati sulla salute e sulla vita sessuale, l'uso di fotografie e foto segnaletiche.

L'ultima opera, invece, affronta i temi della funzione della protezione dei dati in un mercato globale e della necessità che essa debba essere ormai considerata come valore aggiunto e *asset* competitivo per le imprese, fornendo peraltro anche un contributo utile per ridisegnare le relazioni tra aziende e consumatori. Il volume raccoglie i contributi di autorevoli studiosi ed esperti italiani e stranieri che hanno partecipato ad una conferenza internazionale organizzata dal Garante e tenuta a Roma, presso la sede dell'Autorità, nel dicembre 2002. Riproducendo le quattro sessioni della conferenza, il libro si pone l'obiettivo di aprire un ampio confronto tra coloro che operano nelle attività imprenditoriali, professionali e della cultura economica e giuridica.

A queste prime pubblicazioni se ne aggiungerà presto un'altra dedicata ai rapporti tra tutela dei dati personali e nuove tecnologie.

23.4. *Il rapporto con il pubblico*

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. L'informazione e "formazione" del pubblico è svolta anche mettendo a disposizione sul sito una quantità significativa di documenti, con continui aggiornamenti e *dossier* tematici. In questo senso, la piena attività dell'Ufficio relazioni con il pubblico (Urp) ha consentito, in collegamento con un *call center*, di offrire non solo un contributo di chiarificazione e supporto, ma anche di favorire modalità di interazione ancora più funzionali e dirette con tutti i cittadini che hanno bisogno di informazioni, strumenti illustrativi e divulgativi, sviluppando così un flusso costante di informazioni verso l'esterno e consentendo, nello stesso tempo, di conoscere le esigenze provenienti dalla società civile, dal mondo delle imprese, dal settore della ricerca e dalle pubbliche amministrazioni.

Il grande interesse suscitato dalla *privacy* è quotidianamente dimostrato dal numero consistente di contatti diretti del cittadino con l'Urp, in costante aumento. Tali significativi incrementi registrati nel corso dell'anno rispetto al 2003 hanno stimolato la ricerca di nuove e più mirate risposte per favorire il dialogo con i cittadini, che avviene attraverso una attività di *back office* –con la ricezione di quesiti e

richieste di documentazione per *e-mail* (13.000)– nonché in maniera diretta mediante un'impegnativa, quanto essenziale, attività di *front office*, attraverso il *call-center* (10.000 telefonate pervenute) e il ricevimento diretto del pubblico presso l'Ufficio (2.400 visitatori).

Le tematiche che nel periodo in esame hanno formato maggiormente oggetto di quesiti rivolti all'Ufficio o per le quali è stato più frequentemente richiesto materiale informativo, sono state: il trattamento dei dati da parte di sistemi di informazione creditizia; la videosorveglianza con gli approfondimenti dettati dalle nuove regole in materia; l'esercizio dei diritti previsti dall'art. 7 del Codice; lo *spamming;* l'applicazione delle misure minime di sicurezza ed il trattamento dei dati nell'ambito del rapporto di lavoro.

23.5. *Le attività di formazione*

Al fine di promuovere la cultura della protezione dei dati personali, nella convinzione che la conoscenza e la comprensione dei principi e delle norme del Codice siano il presupposto per una corretta attuazione degli adempimenti nell'attività quotidiana, nel primo semestre del 2004 sono state realizzate presso la sala conferenze del Garante tre giornate di formazione, denominate *"Incontri con il Garante"*: due dirette alle imprese, uno alle pubbliche amministrazioni (con particolare riferimento alle problematiche degli enti locali). La conduzione di questi corsi è stata affidata ai responsabili dei dipartimenti giuridici interni dell'Autorità, coordinati dal segretario generale.

L'iniziativa, nuova per l'Autorità, ha suscitato vivo interesse, rivelando una domanda di formazione/informazione qualificata molto forte (in particolare, nell'ambito della consulenza professionale).

In parallelo a queste iniziative sono stati elaborati due CD-Rom multimediali, rivolti rispettivamente al mondo imprenditoriale e professionale e a quello delle pubbliche amministrazioni, che hanno come punto di riferimento l'esperienza maturata nell'ambito dei predetti incontri; è prevista a breve la distribuzione di tali prodotti, al fine di renderne possibile un'agevole fruizione ad un numero molto elevato di utenti interessati ad approfondire norme ed adempimenti previsti dal Codice.

Altre iniziative, di natura analoga, verranno intraprese nel corso del 2005. In particolare, il Garante ha organizzato un incontro di approfondimento sull'applicazione del Codice presso organismi sanitari pubblici e privati (2 febbraio 2005).

Principale obiettivo dell'iniziativa, destinata prevalentemente agli operatori degli organismi sanitari, è quello di illustrare le concrete modalità di realizzazione delle misure adottate per garantire nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati. Sulla base delle più significative esperienze maturate da taluni organismi sanitari, avvalendosi anche di un confronto dialettico con il Garante, sarà possibile offrire una gamma di modelli operativi, utili alle varie realtà sanitarie chiamate ad applicare le disposizioni del Codice.

23.6. *Manifestazioni e conferenze*

Anche nel corso del 2004 si è confermato un grande interesse da parte del pubblico per l'attività dell'Autorità in occasione di seminari, convegni ed altre iniziative. 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 suoi rappresentanti a dibattiti e convegni.

Nell'ambito del *Forum P.A.* edizione 2004, svoltosi a Roma dal 10 al 14 maggio, il Garante è stato invitato ad illustrare i temi dei rapporti tra comunicazione al cittadino e *privacy*, del rispetto delle norme sulla riservatezza da parte delle pubbliche amministrazioni, delle misure organizzative e tecnologiche da adottare per garantire la sicurezza dei dati personali.

Il presidente Stefano Rodotà è intervenuto al convegno dal titolo: *"Tra norme e prassi: per una organizzazione della funzione di comunicazione nelle pubbliche amministrazioni"* con un intervento dedicato al tema: *"La funzione di comunicazione nell'interpretazione delle Autorità garanti"*. Il vice presidente Giuseppe Santaniello ha invece partecipato al convegno *"Semplificazione e qualità delle regole"*. Gaetano Rasi, componente dell'Autorità, ha partecipato al convegno dal titolo: *"La sicurezza partecipata: coordinamento e cooperazione interistituzionale"*. Il segretario generale Giovanni Buttarelli, oltre che nel convegno *"L'identità digitale e gli strumenti di autenticazione in rete tra necessità di semplicità e tutela della* privacy*"*, è intervenuto anche a quello sul tema: *"Funzionamento e organizzazione delle* authorities*: esperienze a confronto"*. Lo stesso segretario generale è stato poi relatore al Master P.a. sul tema: *"Il Codice per la protezione dei dati personali: le novità riguardanti la Pubblica Amministrazione"*.

L'Autorità Garante è stata presente anche al Com-P.a. 2004, Salone della comunicazione pubblica, dedicato quest'anno al tema *"La comunicazione pubblica guarda all'Europa"*, svoltosi a Bologna dal 3 al 5 novembre. In particolare, il Com-P.a. ha offerto l'occasione per affrontare i temi legati alla protezione dei dati nelle telecomunicazioni, nell'*e-government* e per approfondire le novità più significative introdotte dal Codice.

Il vice presidente dell'Autorità ha partecipato al convegno dedicato a *"Democrazia e partecipazione, accesso e comunicazione"*. Nell'ambito di una tavola rotonda, organizzata dalle Asl della regione Emilia-Romagna, dedicata al diritto di cronaca e alla *privacy* nella sanità è stato presentato un video con un contributo di Mauro Paissan, componente dell'Autorità. Rappresentanti dell'Ufficio del Garante hanno partecipato a diversi convegni e incontri dedicati rispettivamente a: *"Comunicazione pubblica, tutela dei dati e sicurezza"*; *"La nuova frontiera della comunicazione nelle autorità di garanzia e promozione"*; *"Sicurezza dei dati nelle scuole"*.

L'Autorità è stata presente alle due manifestazioni con un proprio *stand* presso il quale è stato programmato un video esplicativo sull'attività del Garante e sulle tematiche della *privacy* e sono state distribuite le pubblicazioni curate dall'Ufficio, i *depliant* divulgativi e la nuova edizione del CD-Rom *"Cittadini e Società dell'informazione"*, aggiornata con il Codice in materia di protezione dei dati personali.

Incontri internazionali

L'Autorità ha ricevuto il 26 maggio 2004 Peter Schaar, Incaricato federale tedesco per la protezione dei dati ed attuale presidente del Gruppo che riunisce le Autorità di protezione dei dati europee. L'incontro è stato l'occasione per uno scambio di opinioni sulla situazione della tutela della protezione dei dati nei rispettivi Paesi, sulle iniziative del Gruppo dei Garanti europei e sulle questioni strategiche oggi al centro dell'attenzione, quali ad esempio, i dati genetici, Internet e l'uso delle nuove tecnologie, in particolare delle *Rfid*, le cosiddette *"etichette intelligenti"*. Riguardo a questo aspetto in particolare, Schaar ha annunciato la costituzione di un sottogruppo *ad hoc* nell'ambito dell'attività del Gruppo dei Garanti Ue.

Sul problema del trasferimento dei dati da parte delle compagnie aeree alle auto-

rità americane, le due Autorità hanno convenuto di intraprendere un'azione comune al fine di sensibilizzare ulteriormente il Parlamento Europeo e di individuare modalità rispettose della *privacy* dei cittadini europei, dichiarandosi pronte ad una collaborazione bilaterale sui temi affrontati nell'incontro.

Nel maggio del 2004 il segretario generale dell'Autorità, Giovanni Buttarelli, ha partecipato alla Conferenza organizzata a Washington dall'*Electronic Privacy Information Center (Epic)* per celebrare il decennale della propria attività. Epic è una delle principali organizzazioni *no-profit* attive negli Usa nel settore dei diritti civili e della tutela della riservatezza. La conferenza, cui hanno preso parte i proff. Santaniello e Rasi, ha dato l'opportunità a molti dei più autorevoli studiosi in materia di fare il punto della situazione rispetto ai rischi per libertà e diritti civili negli USA ed in altri Paesi.

Nel settembre 2004 presso l'Istituto italiano di cultura di Lisbona si è svolta una Conferenza su *"Il sistema delle garanzie della privacy nell'ordinamento italiano, alla luce del nuovo Codice per la protezione dei dati personali"*. La conferenza ha offerto l'occasione per trattare i temi legati alle novità introdotte dal Codice, che segna il passaggio dalla concezione della *privacy* come inviolabilità della sfera privata alla proiezione della persona nella società, e per sottolineare l'importanza che la tutela dei dati personali dei consumatori riveste in quanto requisito essenziale per la competitività delle imprese.

23.7. *L'attività di ricerca e documentazione*

Il carattere trasversale della normativa sulla protezione dei dati personali rende necessario procedere ad un costante aggiornamento sulle novità normative e giurisprudenziali di interesse dell'Autorità, nonché rivolgere una particolare attenzione alle innovazioni che, specie nel settore delle nuove tecnologie, possono avere ripercussioni sull'applicazione delle norme del Codice.

L'attività di ricerca dell'Ufficio è proseguita nella consapevolezza che essa ha un ruolo determinante al fine dell'acquisizione di un adeguato bagaglio conoscitivo indispensabile all'Autorità per rispondere alle costanti sollecitazioni provenienti dall'esterno. Ciò, tanto nell'ipotesi in cui il Garante sia chiamato ad intervenire in base a ricorsi, reclami o segnalazioni provenienti dai cittadini, quanto nei casi in cui l'Autorità ritenga opportuno agire di proprio impulso anche in vista dei molteplici eventi che a livello normativo, scientifico e tecnologico, si ripercuotono sulla materia della protezione dei dati.

È in questa prospettiva che sono state affrontate, ad esempio, le problematiche emerse nel cd. *Digital Rights Management*, o, ancora, le tematiche legate al controllo del lavoratore attraverso strumenti elettronici. Sempre in tale ottica, è inoltre proseguita l'attività di approfondimento su televisione interattiva, sistemi di geolocalizzazione e *Rfid*, attraverso la quale si è cercato di fornire un quadro di insieme sulle tecnologie in questione, nonché di prospettare soluzioni e proposte sui profili applicativi del Codice anche in vista dell'elaborazione di provvedimenti da parte dell'Autorità.

Per ciò che concerne l'attività di aggiornamento e documentazione, essa si è concretata nella predisposizione di notiziari periodici nei quali si sono raccolte le novità normative e giurisprudenziali di rilevanza per il lavoro dell'Ufficio, nonché le elaborazioni della dottrina in merito alle tematiche legate alla protezione dei dati e, più in generale, dei diritti della persona.

La documentazione e l'aggiornamento del personale sono stati svolti attraverso

la diffusione di un Notiziario, la predisposizione di un apposito sito Intranet e l'invio di una *Newsletter* interna nella quale sono raccolti, proposti e commentati articoli apparsi su riviste e siti di informazione giuridica. In tal quadro, hanno formato oggetto di studio, ad esempio, le problematiche legate all'*e-government* e alla documentazione informatica nella pubblica amministrazione; la firma elettronica; la carta sanitaria elettronica; i codici deontologici nel settore delle telecomunicazioni; il diritto alla conoscenza delle proprie origini biologiche; il diritto alla riservatezza nelle tecniche di riproduzione assistita.

Sempre attraverso la *Newsletter*, sono stati diffusi diversi approfondimenti tematici, talvolta resi in occasione della pubblicazione di sentenze provenienti anche da giurisdizioni straniere e da istituzioni europee e comunitarie.

Particolare attenzione è stata data, ad esempio, alla recente decisione della Corte di giustizia delle Comunità europee in materia di fatturazione dettagliata (14 settembre 2004, Causa C-411/02), agli ultimi orientamenti della Corte europea dei diritti dell'uomo sulla pubblicazione di foto di personaggi noti (59320/00, 24 giugno 2004, v. par. 6.4) e di persone coinvolte in procedimenti penali (50774/99, 11 gennaio 2005, v. par. 6.4), alla giurisprudenza statunitense in merito alle liste negative per il *direct marketing* e ai messaggi di posta elettronica, nonché al recente orientamento della Corte di cassazione sul reato di illecito trattamento di dati personali (Cass. n. 30134/2004; Cass. n. 28680/2004).

L'Ufficio del Garante

III - L'Ufficio del Garante

24 La gestione amministrativa dell'Ufficio

24.1. *Il bilancio e gli impegni di spesa*

Il bilancio di previsione del 2004, riferito all'ottavo anno di attività del Garante, è stato elaborato secondo le direttive del regolamento del Garante n. 3/2000.

Le risorse finanziarie sono state indirizzate prevalentemente verso i settori individuati nel documento programmatico di accompagnamento al bilancio di previsione che ha fissato gli obiettivi dell'Ufficio per l'esercizio 2004.

Nell'anno di riferimento sono stati raggiunti numerosi obiettivi: il più significativo, dal punto di vista contabile, è stato quello concernente la notificazione per via telematica (*on-line*). Con l'entrata in vigore del Codice, avvalendosi dei poteri accordati dall'art. 156, comma 3, lett. *e*), l'Autorità ha aggiornato per il 2004 i diritti di segreteria per le notificazioni fissati ad euro 150,00. Il conseguente incremento delle entrate legate a questa voce ha rappresentato circa il 14 per cento del totale delle entrate dell'anno 2004.

Le risorse a disposizione del Garante per il 2004, previste nell'esercizio in euro 12.356.000,00, al 31 dicembre 2004 sono state riscosse per euro 12.186.638,40 di cui euro 9.618.000,00 provenienti dal contributo dello Stato. Le restanti risorse finanziarie sulle quali ha potuto contare l'Autorità per entrate proprie si riferiscono invece ai circoscritti 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 partecipazione di rappresentanti del Garante a riunioni a Bruxelles e nelle altre sedi comunitarie, agli interessi maturati sui fondi relativi agli avanzi pregressi, alle entrate derivanti dalla sublocazione dei locali del IV piano della scala A dell'edificio di piazza di Monte Citorio 115, ad entrate accertate per sanzioni pecuniarie, ai rimborsi spese per la concessione in uso della sala delle conferenze.

Il contributo dello Stato per il 2004 è stato ridotto rispetto all'anno precedente di euro 634.000,00; si tratta di una sensibile riduzione di risorse ormai costante, con continui decrementi a partire dal 2001.

L'anno appena concluso finanziariamente è stato comunque solo in parte condizionato dalla forte riduzione del contributo dello Stato, poiché le minori entrate sono state compensate da alcuni maggiori introiti provenienti dai diritti dovuti per le notificazioni: si tratta, tuttavia, di entrate (sostanzialmente *una tantum*) che non si ripeteranno in analoga misura nei successivi esercizi finanziari.

Mentre la forte riduzione del contributo dello Stato all'Autorità ha condizionato solo in parte l'anno finanziario relativo al 2004, i primi inconvenienti legati alla progressiva riduzione delle risorse prevista dalla tabella C della legge finanziaria (euro 9.177.000,00 per il 2005; euro 8.906.000,00 per il 2006) inizieranno a farsi avvertire a partire dal 2005. Ciò, per due motivi:

- le spese rispetto al 2004 aumenteranno sia perché nell'anno trascorso si sono compressi tutti gli oneri, sia perché con la deliberazione n. 10 del 10 dicembre 2004 si è proceduto a ratificare gli accordi negoziali per i dovuti incrementi retributivi al personale che erano fermi al 1° gennaio 2002;
- le entrate del Garante diminuiranno drasticamente: quelle provenienti dallo Stato si ridurranno di euro 634.000,00; quelle proprie si prevede che subiscano una riduzione di circa euro 1.000.000,00.

D'altro canto, le entrate per notificazioni si stabilizzeranno approssimativamente su euro 10.000,00-12.000,00 mensili, cosicché si dovrà far ricorso massicciamente all'avanzo di amministrazione pregresso per coprire anche le spese correnti. Sarebbe stata intenzione del Garante, invece, ricorrere all'utilizzo dell'avanzo soltanto per le spese d'investimento, soprattutto per quelle tecnologiche e informatiche.

La tabella allegata riassume sinteticamente per gli anni di attività del Garante, dal 1997 al 2004, le risorse finanziarie che lo Stato ha previsto e trasferito all'Autorità per la sua attività, nonché le somme riscosse e le somme pagate ogni anno. Da essa si rileva che il Garante ha condotto un'accorta amministrazione delle sue risorse e che soltanto l'esercizio 2003 si è necessariamente chiuso con un piccolo disavanzo coperto dall'avanzo di amministrazione.

Anno di riferimento	Traferimenti da parte dello Stato		Somme riscosse compreso il contributo dello Stato		Somme pagate	
	lire	*euro*	*lire*	*euro*	*lire*	*euro*
1997	8.029.000.000	4.146.632,44	8.029.000.000	4.146.632,44	1.372.350.430	708.759,85
1998	12.045.000.000	6.220.723,35	12.045.000.000	6.220.723,35	5.491.467.960	2.836.106,51
1999	22.045.000.000	11.385.292,34	27.045.000.000	13.967.576,84	8.725.548.850	4.506.369,90
2000	22.045.000.000	11.385.292,34	22.293.735.850	11.513.753,69	14.235.888.830	7.352.223,00
2001	22.000.000.000	11.362.051,78	24.285.004.432	12.542.158,08	20.019.011.761	10.338.956,74
2002		10.849.996,00		12.186.883,99		11.510.285,48
2003		10.252.000,00		11.244.455,31		13.102.960,92
2004		9.618.000,00		12.694.621,09		12.680.672,89
*2005		9.177.000,00		10.955.000,00		16.376.846,00

Obiettivo dell'esercizio 2004 è stato il massimo contenimento delle spese dirette di gestione e delle spese per gli investimenti. Ciò ha comportato, come si rileva dai dati riportati in tabella, che anche nell'anno chiuso al 31 dicembre 2004 –e nel quale, come detto, vi è stata la forte riduzione delle risorse finanziarie trasferite dallo Stato– l'esercizio si chiuderà con un leggero prevalere delle entrate sulle uscite.

24.2. *L'attività contrattuale*

Tra le novità normative si segnala sul piano comunitario la direttiva 2004/18/CE del Parlamento europeo e del Consiglio del 31 marzo 2004 relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi, che unifica e razionalizza la disciplina in materia e dovrà essere attuata entro il 31 gennaio 2006.

Nell'ordinamento interno appare di particolare rilievo la legge 30 luglio 2004, n. 191, di conversione, con modificazioni, del decreto-legge 12 luglio 2004, n. 168, recante interventi urgenti per il contenimento della spesa pubblica, il cui art. 1, in particolare –per quanto riguarda le convenzioni stipulate dalla Consip per l'acquisizione di beni e servizi per le pubbliche amministrazioni– consente di utilizzare i rela-

(*) dati previsionali del 2005 per le somme da riscuotere le somme da pagare

tivi parametri di prezzo-qualità come limiti massimi, prevedendo la responsabilità amministrativa per la stipulazione di un contratto in violazione della disposizione.

I contratti stipulati non rendono compiutamente conto dell'attività svolta, da un lato, nel determinare in maniera apprezzabile le prestazioni necessarie, per eventualmente verificare previamente la disponibilità di risorse proprie, ovvero per individuare le procedure più adeguate di acquisizione, ed accorpare per quanto possibile richieste diverse in modo da ottenere condizioni complessivamente più vantaggiose, nonché, dall'altro lato, nei rapporti con i fornitori, anche nella fase esecutiva dei contratti. Si è in particolare registrata l'esigenza di verificare attentamente la regolarità delle fatture trasmesse che, in più di un caso, non tengono conto delle riduzioni del prezzo convenute ai sensi dell'art. 54 del regolamento per l'amministrazione del patrimonio e per la contabilità generale dello Stato (r.d. n. 827/1924).

L'attività si è svolta principalmente sulla base di trattative private con ricerche di mercato, in considerazione della norma regolamentare che prevede tale modalità (art. 25 del regolamento di contabilità del 2000), del limitato importo delle acquisizioni, relative ad una struttura ormai per vari aspetti consolidata ed a prestazioni al momento non oggetto di convenzioni Consip, mentre sulla base di convenzione con la Consip è stato stipulato il contratto per l'allestimento della sala conferenze dell'Autorità.

Nel rispetto dell'art. 26 del citato regolamento di contabilità del 2000 si è proceduto con comparazione di offerte per gli acquisti oltre i cinque milioni di vecchie lire: data la relativa macchinosità per acquisizioni di importo contenuto, sono allo studio ipotesi di modifica del regolamento che consentano un ulteriore snellimento delle procedure riservate agli acquisti di modesto valore.

Tra i contratti conclusi si segnala quello sulla connettività IP, affidato al precedente fornitore congiuntamente al servizio di *housing* per i relativi apparati, dopo averne sia pur sinteticamente verificato la convenienza rispetto ad ipotesi alternative.

Tra le forniture *in itinere* va segnalata quella per la telefonia mobile, per la quale, essendo in fase di studio la relativa convenzione Consip, si è prevista in termini relativamente ampi la possibilità di recedere (anche da parte dell'impresa), nonché l'obbligo per l'impresa selezionata, nel caso in cui risulti aggiudicataria anche la convenzione Consip, di informarne il Garante per consentirgli l'adesione alla convenzione medesima con adeguato preavviso.

Degna di menzione, per quanto riguarda la difficoltà di accrescere il grado di concorrenza tra i fornitori senza incidere sul livello di affidabilità, la vicenda della predisposizione dei supporti tecnologici nell'ambito dei concorsi pubblici per la selezione di personale; in questo caso, tramite una ricerca di mercato sull'allestimento tecnologico si è riusciti ad ottenere un apprezzabile risparmio rispetto all'esborso che si sarebbe sostenuto rivolgendosi anche per questo alla struttura ospitante il concorso.

24.3. *Le novità legislative e regolamentari e l'organizzazione dell'Ufficio*

Il 2004 ha segnato un'altra importante tappa nel processo di consolidamento e potenziamento dell'Ufficio del Garante.

In attuazione dell'art. 182 del Codice sono state completate le procedure propedeutiche all'inquadramento nel ruolo organico del personale in posizione di fuori ruolo o equiparato presso l'Ufficio del Garante in servizio alla data di pubblicazione del Codice nella *Gazzetta Ufficiale*, sulla base dei presupposti individuati dall'Autorità.

24

Nel dicembre 2004, a conclusione di una lunga trattativa, sono stati sottoscritti quattro accordi negoziali con organizzazioni sindacali del personale.

Gli accordi sono finalizzati ad attuare alcuni istituti retributivi già previsti e rimasti in parte inattuati, ad un riequilibrio del trattamento economico di segmenti di personale di cui si compone l'Ufficio, nonché all'adeguamento di taluni profili della disciplina dei contratti a tempo determinato e dell'orario di lavoro alle novità legislative di recente intervenute.

Ciò ha comportato circoscritte modifiche al regolamento del Garante n. 2/2000, concernente il trattamento giuridico ed economico del personale, pubblicate sulla *Gazzetta Ufficiale* 23 dicembre 2004, n. 300.

In particolare, con tali modifiche sono state ridefinite nuove modalità applicative dell'istituto della progressione economica (già previsto dalle disposizioni regolamentari) e sono stati introdotti criteri per valutare e valorizzare l'esperienza e la professionalità del personale di nuova immissione.

Con deliberazione del Garante sono stati rimodellati alcuni profili della disciplina dei contratti a tempo determinato adeguandoli alla normativa comunitaria e interna, riducendo ad un anno la durata dei contratti di specializzazione (destinati a giovani laureati) e allungando quella dei contratti a tempo determinato sino a tre anni (rinnovabili per non più di due volte), ferma restando la previsione che a tale tipologia contrattuale è possibile ricorrere solo in presenza di particolari esigenze organizzative e funzionali.

24.4. *Il personale e i collaboratori esterni*

Il processo di consolidamento dell'Autorità è proseguito nel periodo considerato con l'immissione in servizio, il 21 gennaio 2005, dei vincitori di due concorsi pubblici banditi nel febbraio del 2004 (*G.U.* 9 febbraio 2004, n. 3, quarta serie speciale); tali concorsi prevedevano una riserva del trenta per cento dei posti per il personale non di ruolo, in conformità all'art. 182 del Codice.

Le commissioni esaminatrici, composte da tre docenti universitari e dal segretario generale e presiedute da due magistrati amministrativi nominati, su richiesta del Garante, dal Consiglio di presidenza della giustizia amministrativa, hanno concluso i lavori nel mese di ottobre. Dei tredici posti complessivamente banditi (di cui nove per la qualifica di funzionario e quattro per quella impiegato operativo), ne sono stati coperti solo dieci (n. 7 posti di funzionario e n. 3 di impiegato operativo); la riserva di posti, altresì, è rimasta inutilizzata in quanto i candidati riservatari risultati idonei si sono classificati in posizione utile nella graduatoria di merito di ciascun concorso.

Con il completamento di tali procedure l'organico dell'Autorità risulta attualmente coperto all'ottantacinque per cento. E ciò malgrado le crescenti difficoltà finanziarie, segnalate in altra parte della presente *Relazione*, le quali hanno imposto valutazioni e scelte di ordine organizzativo e di politica del personale volte prevalentemente al rafforzamento delle qualificazioni medio-alte da destinare all'area giuridica, in considerazione dei nuovi compiti che il Codice assegna al Garante.

La definizione delle procedure per l'inquadramento nel ruolo organico del personale in posizione di fuori ruolo o equiparato, ai sensi dell'art. 182, comma 1, lett. *a*), del Codice, e la contestuale immissione in servizio dei vincitori dei predetti concorsi pubblici, contribuiscono a rendere più stabile l'organico dell'Ufficio, sinora caratterizzato da una relativa precarietà dovuta alla notevole incidenza sul totale di personale in prestito da altre amministrazioni o a contratto.

L'inversione di tale tendenza è sottolineata da una contrazione, sia pur limitata, del contingente di contratti a tempo determinato, che per espressa previsione normativa non può essere superiore a venti unità.

La selezione per il reclutamento di (sino a) 3 giovani laureati con contratto di specializzazione a tempo determinato, bandita nel febbraio del 2004 ed in via di imminente ultimazione, è destinata ad incrementare tale contingente.

Nel periodo considerato si sono svolti alcuni *stage* (vedi *Relazione 2003*), taluni dei quali in collaborazione con università (nell'ambito di *master*) e con la Scuola superiore della pubblica amministrazione nell'ambito di corsi di formazione dirigenziale. Attualmente è in corso un solo *stage*.

Allo stato l'Ufficio può contare su 94 unità (di ruolo, in posizione di fuori ruolo o a contratto), di cui 87 effettivamente in servizio (cfr. prospetto in par. 25.1).

L'Autorità al momento non si avvale della collaborazione di consulenti. Nel periodo considerato si è reso necessario ricorrere solo a esigui incarichi professionali occasionali per acquisire competenze qualificate in materia informatica per le problematiche concernenti il sistema informativo interno e il sito *web* del Garante, per la sistemazione della biblioteca e dell'ampio materiale documentale acquisito e prodotto dall'Autorità nel corso della sua attività, nonché per la verifica, la manutenzione e il necessario aggiornamento del registro informatico dei trattamenti.

Avvalendosi delle convenzioni Consip, sono state conferite in *outsourcing* e *insourcing* alcune attività di natura esecutiva che non richiedono un apporto lavorativo di elevato contenuto professionale (ad esempio, con riguardo al *call center*).

Il Garante si avvale, altresì, di un servizio di controllo interno presieduto da un dirigente della Ragioneria generale dello Stato e composto, altresì, da un magistrato della Corte dei Conti e da un dirigente generale in quiescenza della medesima Ragioneria generale.

24.5. *Lo sviluppo del sistema informativo e l'attività in ambito tecnologico*

L'attività del Dipartimento risorse tecnologiche nel 2004 è stata volta principalmente a consolidare il sistema informativo, arricchendolo di nuove funzionalità e perfezionando quelle esistenti, e ad incrementare l'efficienza della sua gestione, per pervenire ad un'efficacia ancora maggiore delle risorse tecnologiche offerte come strumento di produttività individuale e collettiva o come soluzioni sistemiche nell'ambito dell'Ufficio del Garante.

Perdurando una situazione di carenza di risorse umane specialistiche, massima priorità hanno assunto le attività di manutenzione e di assistenza agli utenti interni, con relativa riduzione dell'attività di sviluppo e progettazione di nuovi interventi. È utile porre in evidenza che, a prescindere dalle sue formali attribuzioni, il Dipartimento ha svolto un'intensa attività di consulenza e supporto nei confronti dei dipartimenti giuridici e dell'Unità ricorsi, contribuendo ad esempio a definire le procedure di trattamento tecnico dei ricorsi in materia di *spam* e di abusi relativi alla rete Internet; ha collaborato con il collegio e con il segretario generale nella trattazione di casi che hanno richiesto una competenza tecnica informatica.

Nel gennaio 2004 è stato attivato un nuovo sistema di gestione del protocollo basato su una moderna tecnologia *web oriented*, che ha reso interscambiabili le postazioni di lavoro ed ha consentito l'accesso diversificato al registro e ai documenti in esso memorizzati tramite la rete interna. Con il nuovo sistema ciascun assegnatario di documenti protocollati riceve una notifica di assegnazione a mezzo *e-mail* e può accedere, tramite interfaccia *web*, ai documenti per i quali ha ricevuto apposita

autorizzazione. Il sistema si presta all'implementazione di un vero e proprio sistema di *workflow* documentale, e in tal senso se ne prevede l'espansione già nel corso del 2005, unitamente alla realizzazione di meccanismi di accesso selettivo tramite cui implementare procedure per l'accesso ai documenti amministrativi improntate alla massima trasparenza ma con garanzie di sicurezza.

Contestualmente al sistema di protocollo è stato attivato un nuovo sistema di posta elettronica, totalmente basato su *software open source*, progettato, organizzato e gestito dal personale tecnico dell'Ufficio. Questo sistema ha consentito di interrompere il ricorso a fornitori esterni di servizi *e-mail* e, nello stesso tempo, di raggiungere un elevato livello di prestazioni grazie alla rete locale ad alta velocità su cui si basano tutti i servizi informatici interni e alla disponibilità di adeguate risorse di memoria secondaria. Tra i servizi offerti nell'ambito del sistema vi è l'accesso tramite interfaccia *webmail* dalle reti esterne, con il ricorso a protocolli sicuri (Ssl), la certificazione digitale dell'identità dei *server* utilizzati, l'accettazione da parte degli stessi *server* di flussi di trasporto crittografati, l'autenticazione del mittente per l'accettazione della posta da instradare e non destinata alla consegna locale, che consente anche al personale in missione e collegato a reti esterne di usufruire dei servizi *Smtp* dell'Ufficio.

La disponibilità del nuovo protocollo informatico, che consente anche la protocollazione automatica di documenti e posta elettronica, con la verifica delle firme digitali, ha reso possibile l'avvio della procedura *web* per la notificazione telematica, che ha permesso a più di diecimila titolari di trattamento di dati personali di adempiere agli obblighi di legge tramite la rete Internet, realizzando così il primo esperimento di interazione in rete di una pubblica amministrazione con i cittadini, con una procedura avente un rilevante significato giuridico, andando quindi oltre il livello meramente informativo che ha finora caratterizzato la presenza in rete delle pubbliche amministrazioni. Si è trattato inoltre del primo utilizzo su larga scala in ambito pubblico della firma digitale, da cui sono state ricavate interessanti indicazioni in favore di una maggiore apertura delle procedure amministrative nei confronti dell'interazione in rete.

La procedura *web* è stata realizzata interamente all'interno dell'Ufficio, integrandosi con il protocollo informatico e la posta elettronica e con un sistema di *database* sviluppato con la collaborazione di una ditta specializzata.

Il sistema amministrativo contabile è stato perfezionato e arricchito di nuove funzionalità ed ha permesso, per la prima volta, di gestire un intero esercizio in modo totalmente automatizzato. L'esperienza di questo primo anno ha consentito di ricavare indicazioni e parametri su cui basare l'affinamento del sistema per andare incontro ancora di più alle esigenze dell'Ufficio.

La disponibilità di dati di bilancio e amministrativi da una parte, insieme ai dati relativi alle pratiche inserite nel protocollo informatico, a quelli relativi al lavoro nei vari servizi e dipartimenti desunti dal sistema automatizzato di rilevamento delle presenze, ha consentito di avviare alcune procedure di analisi statistica dei carichi di lavoro, nell'ottica della graduale implementazione di un sistema informativo direzionale per il controllo di gestione.

Sono state sviluppate e programmate estese funzionalità di *reporting*, corrispondendo adeguatamente alle esigenze informative dei vertici amministrativi e istituzionali dell'Autorità. Terminata una dettagliata fase di analisi, le funzioni di *reporting* confluiranno nel futuro sistema informativo direzionale.

Per consentire una migliore efficienza nell'attività di assistenza è stato realizzato il portale *web* dei servizi informatici dell'Ufficio, tramite cui l'utenza interna può contattare il personale tecnico per ogni esigenza e, in particolare, per le richieste di

assistenza. Queste ultime vengono gestite tramite un sistema di *helpdesk* integrato, sviluppato con *software opensource*, che consente di tracciare le richieste, gestire il processo di assegnazione e di monitoraggio della prestazione richiesta, elaborare statistiche.

Accanto alle attività prettamente strumentali alle necessità funzionali dell'Ufficio, è stato dato un contributo cospicuo allo svolgimento di altre attività di rilevante interesse istituzionale: in particolare, con riguardo allo svolgimento delle attività ispettive e dell'attività formativa e divulgativa (con un contributo in materia di sicurezza informatica nel corso dei segnalati *"Incontri con il Garante"*) ; inoltre, organizzando presso la sede dell'Autorità una giornata di studio sugli *standard* di sicurezza informatica, in collaborazione con esperti dell'Università di Pisa e, in collaborazione con *"Società Internet"* (sezione italiana di *Internet Society*), un seminario sullo *spam* che ha visto la presenza dei maggiori specialisti italiani del settore (i cui lavori sono stati successivamente pubblicati da Società Internet nella collana *"Quaderni"*) .

Avvalendosi del contributo specifico del Dipartimento risorse tecnologiche, l'Ufficio ha preso parte a convegni e seminari sulla sicurezza informatica organizzati dall'Università di Udine (nel marzo 2004), dalla società Inet di Milano (*Internet Security Day*, nell'aprile 2004), dall'Università di Genova (nel maggio 2004) e dall'Ordine dei dottori commercialisti di Palermo (nel giugno 2004).

Per quanto riguarda la collaborazione istituzionale, l'Ufficio ha preso parte ai lavori del Comitato per la biometria nella p.a. istituito presso il Cnipa (Centro nazionale per l'informatica nella pubblica amministrazione), che ha prodotto le linee-guida per l'utilizzo delle tecnologie biometriche in un quadro di piena compatibilità con il dettato normativo. In ambito internazionale, ha partecipato ai lavori della *Internet Task Force* che svolge attività di supporto nei confronti del *Working Party Art. 29* in sede europea, contribuendo all'elaborazione dei *dossier* sugli importanti casi affrontati in quella sede, tra cui si segnalano i sistemi di autenticazione in rete (*Passport, Liberty Alliance*), i nuovi servizi di posta elettronica (tra questi, il discusso servizio *Gmail* di *Google*) e le tecnologie *Rfid*.

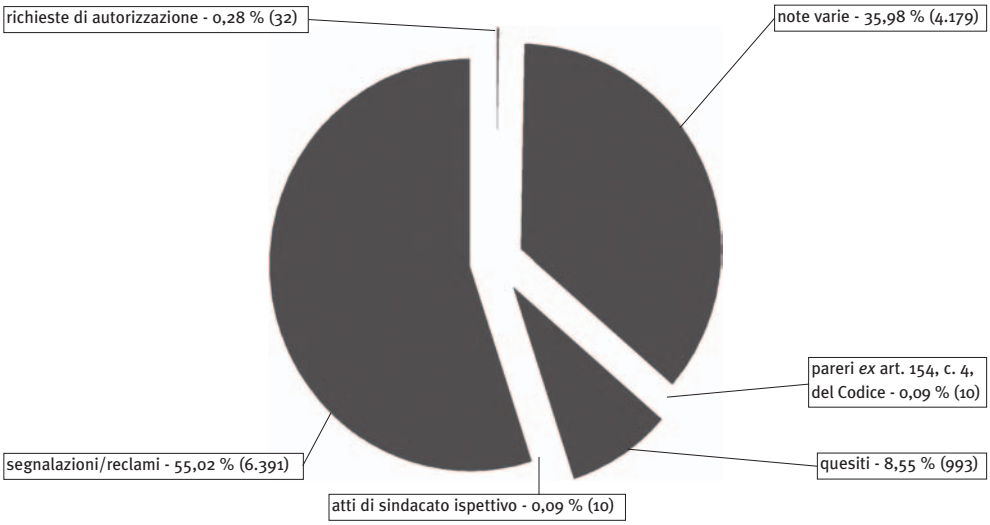
In particolare nel corso del 2004, l'Autorità ha proseguito il monitoraggio del rispetto da parte di Microsoft degli impegni assunti sulla base delle Raccomandazioni del Gruppo art. 29, attraverso la *road map* concordata con la Commissione europea nel 2003. Va segnalato, inoltre, che a fine 2004 Microsoft ha annunciato la cessazione del progetto "*Passport*" come sistema di autenticazione unica su Internet, limitandone l'uso futuro ai soli servizi offerti da Microsoft.

Il Garante ha, inoltre, preso parte al coordinamento tra i servizi di supporto e consulenza informatica delle autorità di garanzia europee sulla *privacy*, avviato per impulso dell'autorità francese Cnil con il convegno di Parigi del giugno 2004.

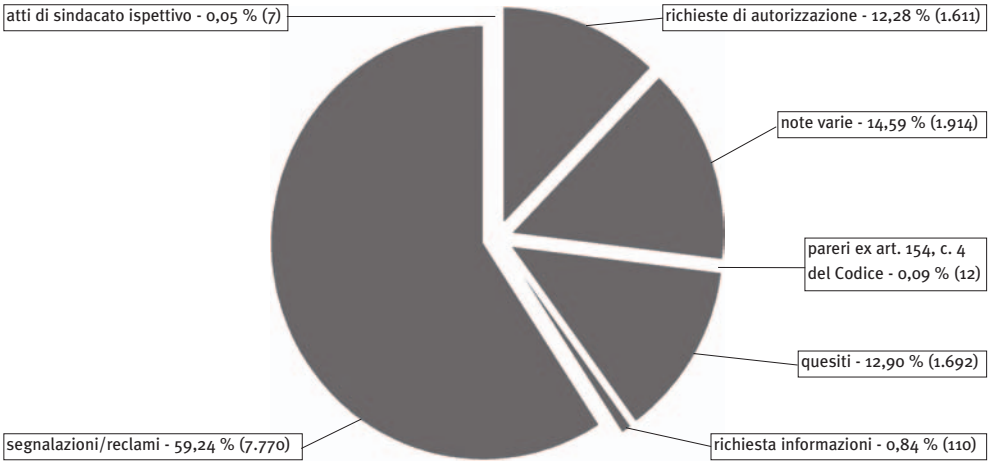
25 Dati statistici

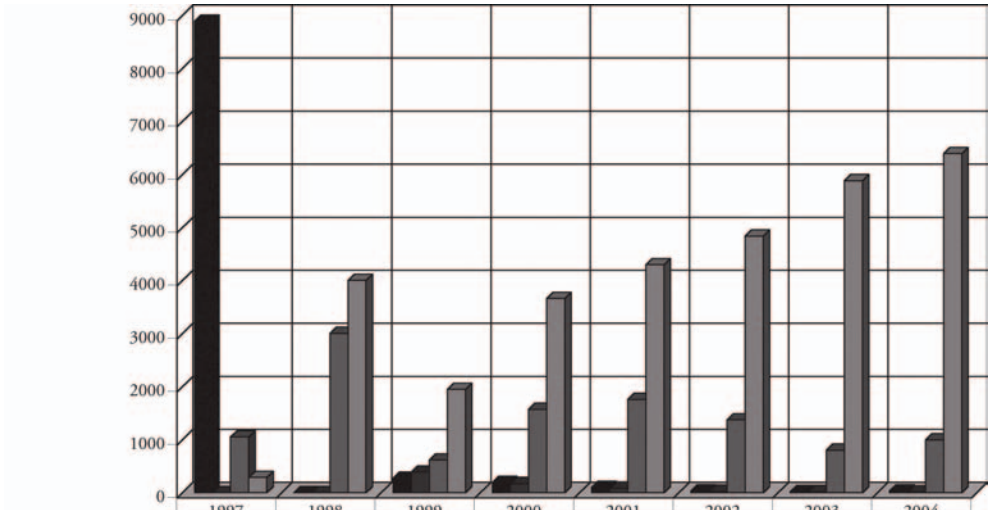
25.1. *Grafici e tabelle*

1. Principali tipologie di richieste pervenute nel 2004



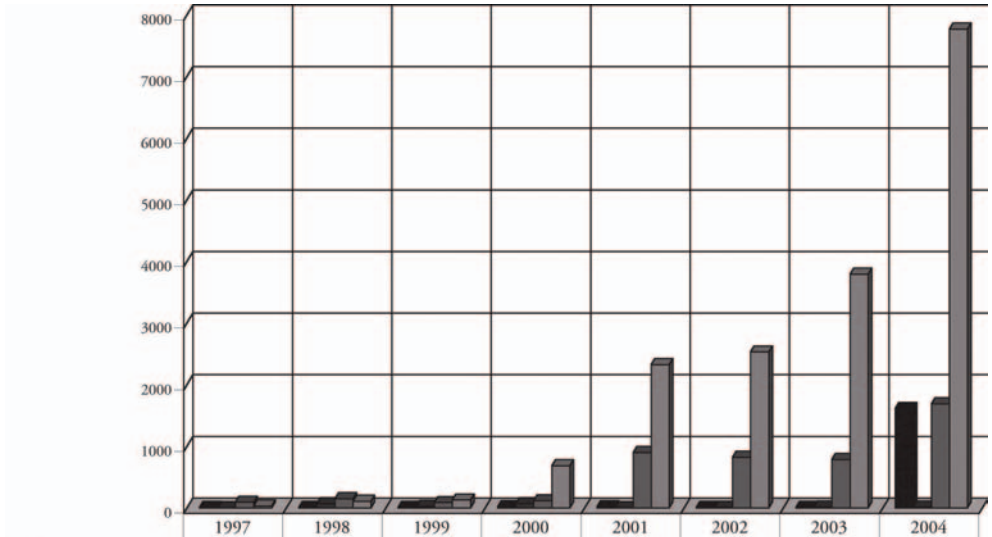
2. Principali tipologie di risposte rese nel 2004





	1997	1998	1999	2000	2001	2002	2003	2004
Autorizzazioni	8889	0	272	191	98	28	17	32
Pareri	0	0	386	170	81	22	16	10
Quesiti	1050	3000	615	1569	1755	1371	799	993
Segnalazioni/Reclami	285	4000	1946	3661	4295	4836	5880	6391

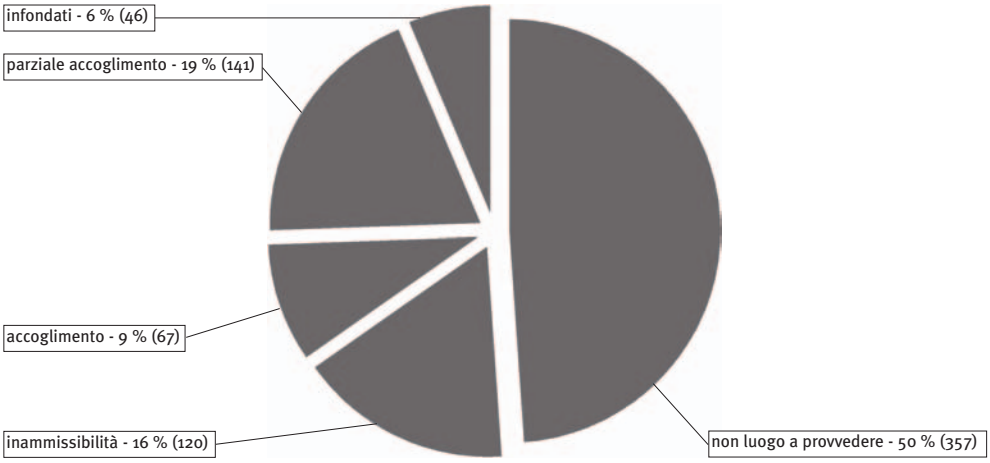
3. Principali tipologie di richieste pervenute negli anni 1997 - 2004



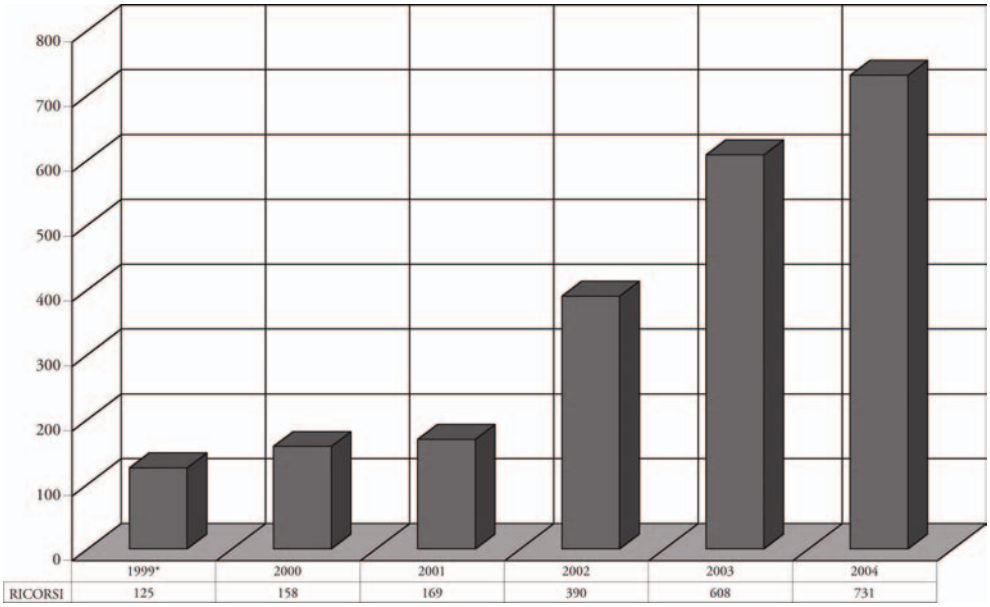
	1997	1998	1999	2000	2001	2002	2003	2004
Autorizzazioni	6	6	11	20	19	7	7	1611
Pareri	0	70	27	70	3	7	14	12
Quesiti	95	150	89	118	898	824	786	1692
Segnalazioni/Reclami	31	112	130	687	2327	2532	3796	7770

4. Principali tipologie di risposte rese negli anni 1997 - 2004

5. Tipologie delle decisioni adottate su ricorso nel 2004



6. Ricorsi decisi negli anni 1997 - 2004



(*) A partire dal 16 febbraio 1999

7. Richieste di autorizzazione

Richieste di autorizzazione	
pubbliche amministrazioni	2
assicurazioni	1
associazioni di volontariato	1
aziende di ricerca medica ed epidemiologica	3
aziende editoriali	1
aziende private in generale	10
comuni	2
liberi professionisti	7
regioni	1
strutture del servizio sanitario nazionale	1
strutture sanitarie private	2
altri settori	1
Totale richieste presentate nel 2004	**32**
Totale risposte inviate nel 2004	**22**
Totale risposte relative a richieste presentate negli anni precedenti	**1.589**

8. Segnalazioni/Reclami

Segnalazioni/Reclami	
agenzie fiscali	22
pubbliche amministrazioni	79
altri enti locali diversi da regioni provincie e comuni	4
assicurazioni	134
associazioni	38
associazioni di volontariato	7
aziende di consulenza e revisione contabile	2
aziende di fornitura acqua gas elettricità	22
aziende di investigazione privata	9
aziende di *marketing*	11
aziende di ricerca e selezione del personale	4
aziende di ricerca medica ed epidemiologica	2
aziende di ricerca sociologica e di opinione	4
aziende di sorveglianza privata	4
aziende di trasporto	23
aziende editoriali	157
aziende per il lavoro interinale	1
aziende postali e di recapito	47
aziende private in generale	628
aziende radiofoniche e televisive	145
aziende telefoniche	580
Banca d'Italia	18
banche e finanziarie	2.515
biblioteche	3
camere di commercio	55
centrali rischi private	778
centri di assistenza fiscale	1
comuni	218

(segue)

Avvertenza:
le tabelle illustrano l'attività del Garante per tipologia di intervento e, limitatamente al 2004, per settore di riferimento.
I dati sono riferiti al 2004. Viene altresì rappresentato il dato aggregato delle risposte fornite dall'Autorità nel 2004, in relazione a richieste pervenute al Garante negli anni precedenti.

25

(segue)

concessionari per la riscossione dei tributi	23
condomini e multiproprietà	32
enti pubblici non economici nazionali	3
forze armate	7
forze di polizia	45
informazioni commerciali	2
Internet service provider	49
Istat	1
istituti pubblici di previdenza e assistenza	46
istituti scolastici	34
liberi professionisti	72
ministeri	46
ordini professionali	13
partiti e movimenti politici	52
prefetture uffici territoriali del governo	3
privati	48
province	15
questure	1
regioni	13
sindacati	22
strutture del servizio sanitario nazionale	161
strutture sanitarie private	28
uffici di collocamento	4
uffici giudiziari	41
Ufficio italiano dei cambi	1
università pubbliche	8
altri settori	110
Totale richieste presentate 2004	**6.391**
Totale risposte inviate 2004	**3.595**
Totale risposte relative a richieste presentate negli anni precedenti	**4.175**

9. Pareri *ex* art. 154, comma 4, del Codice

Pareri ex art. 154, comma 4, del Codice	
Totale richieste 2004	**10**
Totale risposte 2004	**10**
Totale risposte anni 1997-2003	**2**

10. Atti di sindacato ispettivo e di controllo

Atti di sindacato ispettivo e di controllo	
pubbliche amministrazioni	2
trattamento dati passeggeri vs. USA	3
Internet	2
altri settori	3
Totale richieste 2004	10
Totale risposte 2004	7
Totale risposte relative a richieste degli anni precedenti	–

Note varie	
agenzie fiscali	8
pubbliche amministrazioni	34
assicurazioni	2
associazioni	54
associazioni di volontariato	3
aziende di consulenza e revisione contabile	1
aziende di investigazione privata	1
aziende di *marketing*	1
aziende di ricerca e selezione del personale	2
aziende di ricerca medica ed epidemiologica	3
aziende di trasporto	4
aziende editoriali	5
aziende private in generale	226
aziende radiofoniche e televisive	4
aziende telefoniche	23
Banca d'Italia	1
banche e finanziarie	55
camere di commercio	2
centrali rischi private	27
chiese e organizzazioni religiose	1
comuni	185
condomini e multiproprietà	2
enti pubblici non economici nazionali	2
forze armate	1
forze di polizia	8
Internet service provider	3
Istat	6
istituti pubblici di previdenza e assistenza	16
istituti scolastici	11
liberi professionisti	45
ministeri	42
ordini professionali	8
organismi di sicurezza	1
privati	37
province	10
regioni	21
sindacati	11
strutture del servizio sanitario nazionale	92
strutture sanitarie private	60
uffici giudiziari	4
università private	1
università pubbliche	11
altri settori	3.145
Totale richieste 2004	**4.179**
Totale risposte 2004	**1.098**
Totale risposte relative a richieste degli anni precedenti	**816**

12. Richieste di informazioni da parte del Garante

Richieste di informazioni da parte del Garante (*)	
altre pubbliche amministrazioni	1
associazioni	4
aziende di ricerca medica ed epidemiologica	2
aziende di trasporto	1
aziende editoriali	3
aziende postali e di recapito	3
aziende private in generale	21
aziende radiofoniche e televisive	1
aziende telefoniche	6
banche e finanziarie	21
camere di commercio	5
centrali rischi private	14
comuni	9
Internet service provider	1
istituti pubblici di previdenza e assistenza	2
istituti scolastici	3
liberi professionisti	1
ministeri	1
partiti e movimenti politici	1
privati	2
regioni	1
strutture del servizio sanitario nazionale	5
strutture sanitarie private	1
università pubbliche	1
Totale anno 2004	**110**

13. Quesiti

Quesiti (*)	
agenzie fiscali	8
altre pubbliche amministrazioni	23
altri enti locali diversi da regioni province e comuni	5
assicurazioni	9
associazioni	32
associazioni di volontariato	1
aziende di consulenza e revisione contabile	5
aziende di fornitura acqua gas elettricità	10
aziende di investigazione privata	9
aziende di *marketing*	3
aziende di previdenza e assistenza	2
aziende di ricerca e selezione del personale	1
aziende di ricerca medica ed epidemiologica	3
aziende di ricerca storica	1
aziende di sorveglianza privata	1
aziende di trasporto	6
aziende editoriali	4
aziende postali e di recapito	3
aziende private in generale	122
aziende radiofoniche e televisive	2
aziende telefoniche	9

(*) Avvertenza:
oltre alle risposte singole, ai numerosi quesiti aventi caratteristiche analoghe, l'Autorità fornisce riscontro con atti di carattere generale

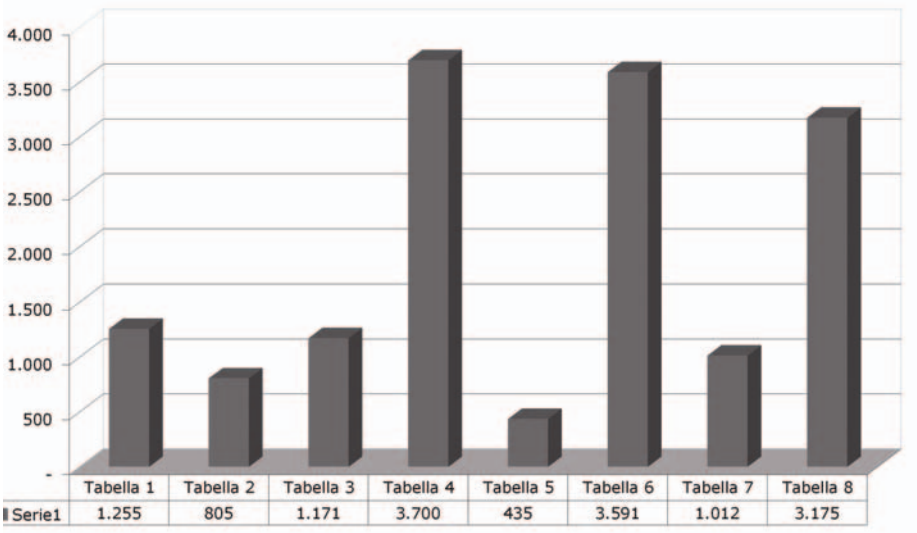
(segue)

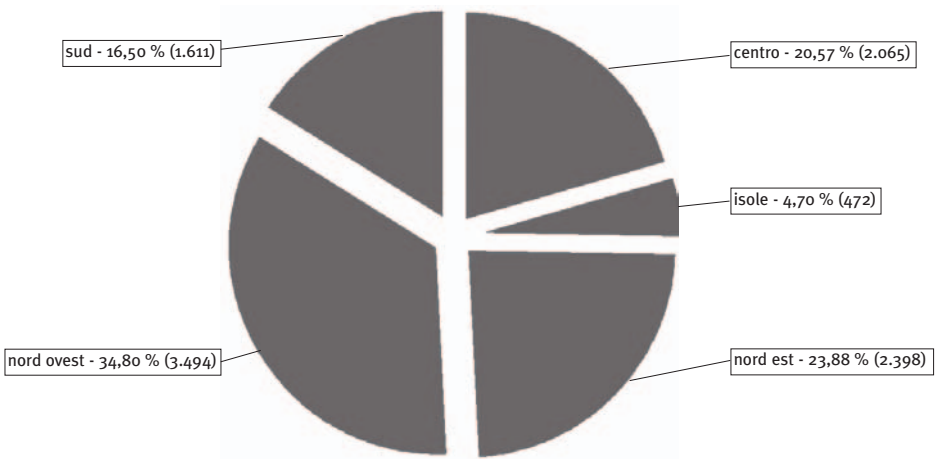
segue

Banca d'Italia	1
banche e finanziarie	37
biblioteche	1
camere di commercio	8
centrali rischi private	10
comuni	272
concessionari per la riscossione dei tributi	1
condomini e multiproprietà	8
enti pubblici non economici di regioni ed enti locali	2
enti pubblici non economici nazionali	1
forze armate	2
forze di polizia	5
informazioni commerciali	1
Internet service provider	1
Istat	3
istituti pubblici di previdenza e assistenza	9
istituti scolastici	21
liberi professionisti	51
ministeri	17
ordini professionali	15
partiti e movimenti politici	6
prefetture uffici territoriali del governo	5
privati	30
province	24
questure	1
regioni	22
sindacati	10
strutture del servizio sanitario nazionale	85
strutture sanitarie private	40
uffici giudiziari	12
università private	1
università pubbliche	10
altri settori	22
Totale richieste 2004	**993**
Totale risposte 2004	**319**
Totale risposte relative a richieste degli anni precedenti	**1.373**

14. Tabella e grafico riferiti alla tipologia dei trattamenti notificati

Tabella 1 - Trattamento di dati genetici	1.255
Tabella 2 - Trattamento di dati biometrici	805
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	1.171
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	3.700
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	435
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	3.591
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	1.012
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	3.175

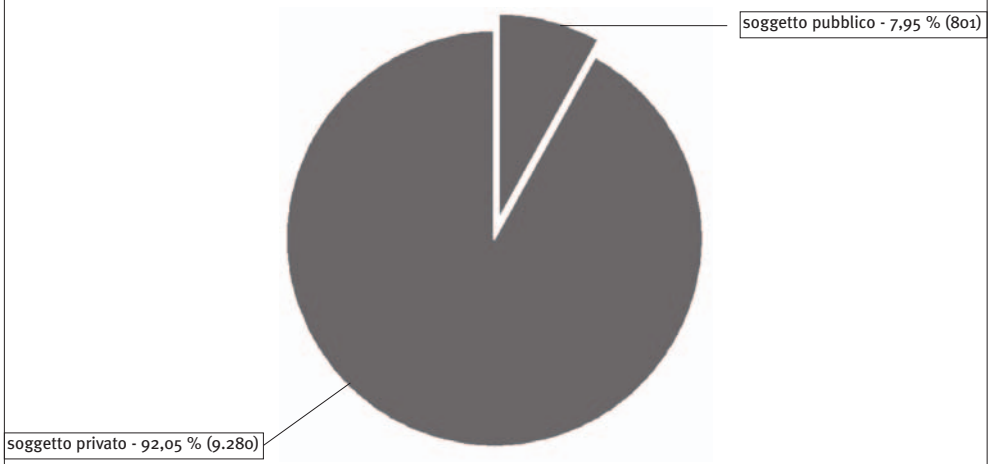




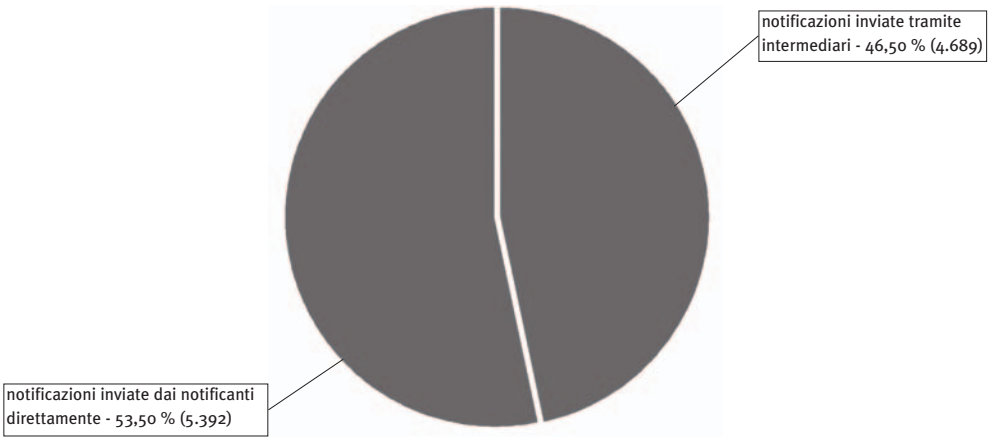
15. Distibuzione notificazioni per aree (esclusi paesi esteri)

Tipologia	Numero pervenute	di cui soggetto pubblico	di cui soggetto privato
Cessazione	36	0	36
Modifica	168	11	157
Prima notificazione	9.877	790	9.087
Totale	**10.081**	**801**	**9.280**

16. Tabella e grafico riferiti ai soggetti notificanti, pubblici e privati



17. Modalità di invio della notificazione



18. Attività Urp dal 1° gennaio 2004 al 31 dicembre 2004

e-mail in entrata *urp@garanteprivacy.it*	13.000
e-mail in entrata *garante@garanteprivacy.it*	9.900
Telefonate	10.000
Visitatori	2.400

19. Personale in servizio

Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	Personale a contratto	TOTALE
Dirigenti	26	15	5		20
Funzionari	45	35	5		40
Operativi	26	17	5		22
Esecutivi	3				0
Personale a contratto	20			12	12
TOTALE	120	67	15	12	94