Relazione 2003

Il diritto alla protezione dei dati personali e le nuove garanzie nel Codice

www.garanteprivacy.it

Indice

Indice

V - La privacy e le sfide del futuro

VII - La gestione amministrativa dell'Ufficio

Dati statistici

PARTE III – DOCUMENTAZIONE

VIII - Provvedimenti del Garante

IX - Unione europea

Indice

Elenco delle abbreviazioni

La presente Relazione è riferita al 2003 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 31 marzo 2004, relative a sviluppi significativi che si è ritenuto opportuno menzionare.

art.	articolo
Bollettino	Bollettino del Garante per la protezione dei dati personali *"Cittadini e Società dell'Informazione"*
c.c.	codice civile
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cd.	cosiddetto/a
cfr.	confronta
Cost.	Costituzione
d.l.	decreto legge
d.lg.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
Pa	Pubblica amministrazione
parag.	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

Premessa

La Relazione per il 2003 presenta una struttura in parte innovativa rispetto alle precedenti edizioni, allo scopo di dare un quadro ancora più adeguato dei principali problemi concreti che, nel presente e nell'immediato futuro, contraddistinguono la protezione dei dati personali.

La Relazione è quindi, in primo luogo, incentrata sul ruolo fondamentale che nel settore in esame hanno avuto nel 2003 le innovazioni normative.

Quello appena trascorso può infatti ben definirsi un anno "storico" per la privacy, in quanto ha visto ultimare il processo di armonizzazione delle molteplici fonti normative regolanti tale materia in un testo unico di rango legislativo, emanato con il d.lg. 30 giugno 2003, n. 196 (cd. Codice, citato nella Relazione con la maiuscola anche per distinguerlo dai codici deontologici di settore).

Tale fondamentale sviluppo normativo, la cui attuazione a livello amministrativo ha assorbito e sta assorbendo una consistente parte dell'attività dell'Autorità, è analizzato nel capitolo iniziale della Relazione in cui si dà conto anche del complessivo stato di recepimento delle direttive comunitarie in materia di dati personali negli Stati membri.

Il secondo capitolo, invece, riassume i diritti attribuiti agli interessati dalla normativa, come delineati da provvedimenti del Garante intervenuti nel 2003, nonché i principali doveri dei soggetti che trattano i dati personali, con particolare riferimento alle misure di sicurezza ed alla notificazione, anche alla luce dei recenti interventi dell'Autorità in proposito.

Nel terzo capitolo, poi, viene analizzata la ricca casistica relativa ai rapporti tra la privacy ed i diritti tutelati a livello costituzionale che con essa vengono continuamente a confrontarsi: in particolare, vengono prese in considerazione la libertà associativa (in cui si è fatto rientrare pure il fenomeno religioso e quello politico), la libertà di informazione e quella di iniziativa economica (art. 41, secondo comma, Cost.).

Nel quarto capitolo viene affrontato il delicato tema dell'applicazione della normativa sulla protezione dei dati personali nelle pubbliche amministrazioni centrali e locali: i provvedimenti del Garante mettono qui in luce il carattere solo parziale ed ancora insoddisfacente di tale applicazione e il perdurare, anche per il 2003, della necessità di interventi chiarificatori dell'Autorità sui rapporti tra la normativa in materia di privacy e le specifiche discipline di settore che regolano l'agire delle pubbliche amministrazioni.

Il quinto capitolo, che chiude la prima parte della Relazione, guarda a quei settori nei quali, in un prossimo futuro, la privacy dovrà fronteggiare le sfide più importanti che l'evoluzione tecnologica porta al necessario rispetto dei diritti della persona, secondo la prospettiva –costantemente seguita dal Garante nei suoi interventi– di una giusta sinergia tra la diffusione delle nuove tecnologie e l'elevato livello della tutela dei dati personali ora assicurato dal Codice.

La seconda parte della Relazione, infine, è dedicata all'Ufficio del Garante, visto sotto i due profili dell'attività e della gestione amministrativa.

Il diritto alla protezione dei dati personali

I - Il quadro normativo
Normativa nazionale

1 Il Codice in materia di protezione dei dati personali

1.1. Il percorso per arrivare al Codice

Nel 2003 è stato completato l'*iter* normativo di integrazione e razionalizzazione della disciplina in materia di protezione dei dati personali: con il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), per la prima volta nel panorama internazionale, viene riunita in un unico corpo normativo una materia, quella della protezione dei dati, la cui disciplina si era formata nel tempo con vari interventi integrativi e modificativi della l. 31 dicembre 1996, n. 675, apportati in attuazione della delega originariamente contenuta nella legge n. 676/1996 e, successivamente, nella l. 24 marzo 2001, n. 127 (v. art. 1, comma 4).

Il delicato lavoro preparatorio di ricognizione e di studio delle norme da riunire nel testo unico, svolto da un'apposita commissione istituita presso il Dipartimento per la funzione pubblica della Presidenza del Consiglio dei ministri e presieduta dal prof. Cesare Massimo Bianca, si è concluso nei primi mesi del 2003 con una scelta orientata per l'adozione di un testo unico di rango legislativo, anziché misto, in linea con i nuovi orientamenti della legge di semplificazione per il 2001 (l. 29 luglio 2003, n. 229), all'epoca in fase di approvazione. Il doppio vaglio da parte del Consiglio dei ministri, i pareri delle competenti commissioni parlamentari e di questa stessa Autorità hanno evidenziato una positiva convergenza di intenti e un'obiettiva sinergia di apporti diretti a mantenere ed innalzare il livello di garanzia dei diritti delle persone (in alcuni casi anche sviluppato in nuovi settori di disciplina) ed al tempo stesso a semplificare adempimenti e modalità di esercizio dei diritti.

1.2. La sistematica del Codice

Il Codice, che ha anche recepito la direttiva n. 2002/58/CE in tema di tutela della vita privata nel settore delle comunicazioni, e del quale è possibile indicare in questa sede solo alcuni tratti essenziali, si compone di tre parti: la prima, recante le disposizioni generali applicabili a tutti i trattamenti ed alcune ulteriori regole specifiche per i trattamenti effettuati da soggetti pubblici o privati; la seconda, nella quale sono riunite disposizioni particolari esclusive per alcuni trattamenti, che integrano o in qualche caso derogano alle disposizioni generali della parte prima; la terza, concernente la tutela amministrativa e giurisdizionale dell'interessato, i controlli ed il sistema delle sanzioni.

1.3. I principi: il diritto alla protezione dei dati personali e il rafforzamento delle garanzie

Sul piano generale delle garanzie, il Codice reca il solenne riconoscimento, nel nostro ordinamento, dell'autonomo diritto alla protezione dei dati personali (art. 1, d.lg. n. 196/2003), in armonia con quanto già previsto nella Carta dei diritti fondamentali dell'Unione europea e nel progetto di Costituzione europea.

1

Pur essendo informato ai canoni di semplificazione, armonizzazione ed efficacia, il Codice prescrive che il trattamento dei dati personali si svolga in un quadro di elevata tutela (art. 2, comma 2, d.lg. n. 196/2003) per i diritti delle persone e nel rispetto del "principio di necessità" nel trattamento stesso (art. 3, d.lg. n. 196/2003), principio esteso ai sistemi informativi ed ai *software*, anche per ciò che riguarda la loro configurazione, affinché i dati personali o identificativi siano utilizzati solo se indispensabili per raggiungere le finalità consentite nei singoli casi.

1.4. Le novità normative in tema di accesso ai dati

In materia di accesso ai dati personali, il Codice contiene alcune novità di rilievo sul piano pratico-applicativo.

Accesso ai dati valutativi

In particolare, si conferma espressamente che la richiesta di accesso ai dati personali e l'esercizio degli altri diritti connessi possa riguardare anche i dati di tipo valutativo, salvo per quanto attiene alla loro rettifica o integrazione (art. 8, comma 5, d.lg. n. 196/2003). In relazione ai limiti all'esercizio dei diritti dell'interessato, resta poi significativa la qualificazione di quel pregiudizio per lo svolgimento di investigazioni difensive o per l'esercizio di un diritto, che legittima il "differimento" dell'accesso e, sotto altro profilo, rende possibile accedere ai dati relativi a chiamate telefoniche in entrata, altrimenti non accessibili, in termini di pregiudizio "effettivo e concreto".

Altra novità importante in materia di accesso è contenuta nell'art. 7, comma 2, lett. *e)*, del Codice, secondo cui l'interessato ha il diritto di ottenere dal titolare anche l'indicazione dei soggetti che, in qualità di responsabili o di incaricati, possono venire a conoscenza dei dati che lo riguardano.

Conoscibilità delle informazioni relative a terzi

Infine, sono previste particolari modalità di riscontro alla richiesta di accesso, allo scopo di facilitarne la comprensione sotto il profilo espositivo, come pure la possibilità, per l'interessato, di conoscere informazioni relative a terzi quando la scomposizione dei dati personali renderebbe incomprensibili i dati richiesti (art. 10, commi 4, 5 e 6, d.lg. n. 196/2003).

1.5. Tutela dei diritti

Ampliamento dei termini del riscontro

In chiave di maggiore tutela per l'interessato, nonché di semplificazione anche per il titolare del trattamento, devono essere lette alcune disposizioni del Codice che snelliscono l'esercizio dei diritti e favoriscono la soluzione preventiva delle potenziali controversie direttamente fra l'interessato e il titolare o responsabile del trattamento. Viene perciò previsto un termine più ampio rispetto al passato per completare il riscontro all'esercizio dei diritti stessi (quindici giorni dal ricevimento della richiesta) e si pone a disposizione del titolare un possibile ampliamento di tale termine sino a trenta giorni quando le operazioni necessarie per un integrale riscontro sono di particolare complessità, ovvero ricorre altro giustificato motivo (art. 146 d.lg. n. 196/2003).

Per quanto riguarda poi la tutela in sede giudiziaria dei diritti, il Codice armonizza i vari riti innanzi al giudice ordinario, ora ricondotti opportunamente ad un'unica procedura intentata mediante ricorso al solo tribunale (art. 152 d.lg. n. 196/2003).

1.6. Semplificazioni: notificazione, informativa, consenso

Non mancano, nel Codice, altri interventi di snellimento delle modalità di esercizio dei diritti e degli adempimenti cui sono tenuti i titolari del trattamento, pubbliche amministrazioni e imprese. Nel solco del processo di semplificazione (senza intaccare le garanzie) già intrapreso con il d.lg. n. 467/2001, vengono individuati in modo espresso i casi, più ridotti rispetto al passato, in cui è previsto l'obbligo di notificazione del trattamento al Garante (che può ora essere effettuata solo in via telematica) in relazione ai soli trattamenti che possono presentare rischi per l'interessato (artt. 37 e 38 d.lg. n. 196/2003). Con le modifiche apportate, si è così individuato un insieme più circoscritto di trattamenti oggetto di notificazione, capovolgendo il precedente impianto della normativa nei limiti consentiti dalla specifica disciplina comunitaria. Ulteriori trattamenti possono peraltro essere sottratti all'obbligo di notificazione con provvedimento del Garante (come quello, di cui si dirà oltre, adottato il 31 marzo 2004), provvedimento che, del pari, può individuare eventuali altri trattamenti da notificare, benchè non inclusi nella lista normativa di cui all'art. 37 del Codice.

Semplificazioni sono state previste anche in materia di informativa all'interessato: si prevede, infatti, che il Garante possa individuare modalità semplificate per fornire l'informativa, in particolare in assenza di una relazione diretta con l'interessato (si pensi ad un *call-center*: art. 13, comma 3, d.lg. n. 196/2003). Il Codice, inoltre, introduce modalità semplificate per l'informativa e per la manifestazione del consenso dell'interessato in relazione al trattamento di dati in ambito sanitario.

Infine, notevole valenza semplificativa, sempre nel mantenimento di un elevato livello di tutela, ha l'estensione dei casi in cui il trattamento può essere effettuato da soggetti privati ed enti pubblici economici in assenza del consenso dell'interessato. Così è per il trattamento di dati "comuni" effettuato da organismi *no-profit*, a condizione che il trattamento riguardi dati degli associati e non preveda la comunicazione ad altri soggetti e la diffusione, analogamente a quanto disposto per i dati sensibili (art. 24, comma 1, lett. *h)*, d.lg. n. 196/2003). La norma, tuttavia, a garanzia degli interessati, condiziona questo presupposto equipollente al consenso all'individuazione, da parte dei titolari del trattamento, delle specifiche modalità di utilizzo dei dati, da rendere note agli associati con l'informativa (analoga condizione è stata inserita per i trattamenti di dati sensibili nell'art. 26, comma 4, lett. *a)*, del d.lg. n. 196/2003).

Dal consenso si può parimenti prescindere quando il trattamento di dati sensibili è necessario per adempiere a specifici obblighi previsti dalla normativa in materia di gestione del rapporto di lavoro, sempre che siano rispettati i limiti previsti dall'autorizzazione del Garante (art. 26, comma 4, lett. *d)*, d.lg. n. 196/2003).

1.7. Diritto nazionale applicabile e flussi transfrontalieri

Principio di "stabilimento"

Con il Codice viene completato il recepimento del principio comunitario di "stabilimento" del titolare del trattamento (art. 4, direttiva n. 95/46/CE) quale criterio principale per individuare la disciplina nazionale applicabile. In linea con il principio di semplificazione nelle operazioni di esportazione dei dati, si esclude poi l'obbligo di notificare specificatamente al Garante il trasferimento dei dati personali verso Paesi non appartenenti all'Ue (con la conseguente soppressione dell'obbligo di attendere il decorso del termine previsto dall'art. 28, comma 2, della legge n. 675/1996 prima di poter procedere al trasferimento), consentendo

di indicare tale operazione nell'unica notificazione cui eventualmente il titolare del trattamento sia tenuto (art. 37 d.lg. n. 196/2003).

1.8. Misure di sicurezza

Misure idonee e minime

In tema di misure di sicurezza il Codice conferma il "doppio binario" per gli obblighi cui sono tenuti i titolari già in base alla legge n. 675/1996, prevedendo, sul piano della liceità del trattamento e della stessa responsabilità civile, l'obbligo di adottare tutte le misure "idonee" a ridurre al minimo i rischi di danni per l'interessato (artt. 15 e 31 d.lg. n. 196/2003), e, per quanto concerne quella penale, l'obbligo di adottare quanto meno quelle cd. "misure minime" (artt. 33-36 e 169 d.lg. n. 196/2003).

Disciplinare tecnico

Le "misure minime" di sicurezza, già contenute nel d.P.R. 28 luglio 1999, n. 318, sono state peraltro aggiornate anche sulla base del progresso tecnologico degli ultimi anni e sono indicate in un apposito disciplinare tecnico allegato al Codice (all. B), modificabile con decreto ministeriale onde consentirne agevolmente il costante adeguamento.

1.9. I trattamenti in ambito pubblico

L'impianto della parte generale di disciplina relativa ai trattamenti effettuati da soggetti pubblici non ha subito rilevanti mutamenti, salvo alcuni interventi comunque significativi, anche di chiarimento, riguardanti in specie le comunicazioni al Garante ed il trattamento di dati sensibili.

I soggetti pubblici possono continuare a trattare dati sensibili solo se la legge o, in via transitoria il Garante, abbiano previamente individuato le rilevanti finalità di interesse pubblico perseguite con un determinato trattamento, e i soggetti pubblici stessi abbiano, parimenti, individuato e previamente reso conoscibili i tipi di dati e di operazioni eseguibili (art. 20 d.lg. n. 196/2003, già art. 22, comma 3-*bis*, legge n. 675/1996).

Ora, il Codice consente alle pubbliche amministrazioni, che non abbiano ancora provveduto in proposito, di adempiere al più tardi entro il 30 settembre 2004 (art. 181, comma 1, lett. *a)*, d.lg. n. 196/2003). In ragione della natura sensibile dei dati trattati, che richiede in ogni caso elevate garanzie, l'atto con il quale i soggetti individuano i tipi di dati e di operazioni eseguibili deve avere natura regolamentare, in linea con quanto ritenuto dal Garante già sotto la previgente normativa; al fine di assicurarne la più ampia omogeneità si prevede, inoltre, che i regolamenti possano essere redatti anche sulla base di schemi-tipo (art. 20, comma 2, d.lg. n. 196/2003).

1.10. I codici di deontologia e di buona condotta

Al fine di rendere il dato normativo sempre più aderente alla realtà, con il d.lg. n. 196/2003 si è rafforzata l'importanza dei codici di deontologia e di buona condotta in materia di protezione dei dati personali, prevedendone la sottoscrizione in molteplici e significativi settori: si pensi ai trattamenti di dati effettuati tramite Internet, ovvero per la gestione del rapporto di lavoro, per fini di *direct marketing* come pure da parte delle "centrali rischi" private o, ancora, con riguardo alla videosorveglianza. A tutti i codici deontologici viene ora esteso il principio secondo cui il rispetto delle norme in essi contenute è condizione essenziale per la liceità dei trattamenti (previsione originariamente riferita solo ai codici indicati nell'art. 20 del

d.lg. n. 467/2001, nonché a quelli in materia di ricerca statistica e storica).

Codici di deontologia di imminente sottoscrizione

Per taluni di essi, in particolare quelli riferiti ai trattamenti effettuati nell'ambito di sistemi informativi gestiti da "centrali rischi" private, come pure per quelli concernenti l'attività di investigazione privata o relativi agli scopi statistici e di ricerca scientifica perseguiti in ambito privato, i lavori sono sostanzialmente terminati o in fase di avanzata elaborazione.

1.11. La conservazione dei dati di traffico

D.l. 24 dicembre 2003, n. 354

Nonostante la sua recente approvazione, il Codice ha subito un intervento modificativo in un settore di rilievo, quello dei trattamenti effettuati per ragioni di giustizia. Con il d.l. 24 dicembre 2003, n. 354, convertito, con modificazioni, dalla l. 26 febbraio 2004, n. 45, è stata, tra l'altro, introdotta una modificazione all'art. 132 del Codice, che disciplina la conservazione dei dati di traffico per finalità di accertamento e repressione di reati.

Nella sua formulazione originaria, l'art. 132 del Codice prevedeva che i fornitori di servizi di comunicazione elettronica dovessero conservare i "dati relativi al traffico telefonico" per trenta mesi, per finalità di accertamento e repressione di reati.

Sulla base di alcuni successi investigativi in delicate inchieste riguardanti atti di terrorismo, si è avviato uno specifico dialogo tra il Garante e alcuni uffici giudiziari, in particolare la Direzione nazionale antimafia, che ha portato ad approfondire alcune possibili nuove soluzioni di disciplina, le quali sono state doverosamente segnalate alle autorità di governo.

Modifiche all'art. 132 del Codice

Intendendo garantire l'efficacia di tali investigazioni su delitti di particolare gravità che possono richiedere indagini lunghe ed articolate, il decreto legge in esame aveva però drasticamente soppresso il riferimento al traffico telefonico (riferendosi in modo più ampio ai "dati di traffico"), introducendo anche un'ulteriore fase di conservazione dei dati per altri trenta mesi per il perseguimento dei delitti di cui all'art. 407, comma 2, lett. *a)*, c.p.p., nonché di quelli in danno di sistemi informatici o telematici. Inoltre, modificando l'originaria versione dell'art. 132, il decreto legge aveva previsto una disciplina più dettagliata delle modalità di acquisizione dei dati da parte dell'autorità giudiziaria; si era altresì demandata ad un successivo decreto interministeriale, da adottarsi su conforme parere del Garante, l'individuazione delle modalità di conservazione e di trattamento dei dati, in base a taluni criteri-guida normativamente prefissati (individuazione di talune misure di sicurezza; conservazione separata dei dati per i successivi trenta mesi; garanzia del diritto di accesso e degli altri diritti previsti dall'articolo 7 del d.lg. n. 196/2003; distruzione periodica dei dati decorsi i periodi di conservazione).

Le soluzioni prefigurate dal decreto legge hanno suscitato un ampio dibattito.

Rischi segnalati dal Garante

Al fine di assicurare il pieno rispetto dei diritti fondamentali della persona, subito dopo l'emanazione del decreto legge e durante i lavori per la sua conversione (AC 4594), anche nel corso dell'audizione del presidente dell'Autorità innanzi alla Commissione giustizia della Camera (tenutasi il 20 gennaio scorso), il Garante ha segnalato al Parlamento che le formule ipotizzate per prolungare i tempi di conservazione dei dati (tornati, dagli originari trenta mesi del Codice, ad un periodo mas-

simo di cinque anni) e, soprattutto, l'estensione delle nuove regole al traffico su Internet, avrebbero determinato una forte compressione delle garanzie della persona, anche in relazione ai principi costituzionali in materia di libertà delle comunicazioni e segretezza della corrispondenza.

L'approvazione delle mozioni

Anche alla luce del dibattito svoltosi il 14 gennaio 2004 nell'aula della Camera, dove, con orientamenti unanimi, sono state approvate due convergenti mozioni della maggioranza e dell'opposizione (le quali hanno impegnato il Governo a *"rimuovere tutte le norme potenzialmente lesive dei diritti di riservatezza"* previsti, fra l'altro, *"dall'articolo 15 della Costituzione"* e a *"regolamentare in modo più efficace il trattamento dei dati di traffico della telefonia mobile, al fine di tutelare il diritto degli individui")*, la Commissione ha approvato alcune prime modifiche al decreto legge fra le quali, in particolare:

Modifiche al decreto legge:
• in commissione

a) il riferimento non già, genericamente, ai dati inerenti al traffico, ma ai *"dati relativi al traffico telefonico o alla corrispondenza in via telematica"*;

b) la riduzione dei tempi di conservazione dei dati, dai cinque anni complessivi (trenta mesi più altri trenta mesi), a quattro anni (ventiquattro mesi più altri ventiquattro mesi);

c) l'attribuzione al Garante, con proprio provvedimento da adottare ai sensi dell'articolo 17 del Codice (cd. *prior checking*) del compito di disporre particolari misure a garanzia dell'interessato.

• in assemblea

Nel corso della discussione in Assemblea è poi emersa la più ampia scelta di sopprimere ogni riferimento ai dati di traffico diversi da quello telefonico, stante la particolare delicatezza di una *data retention* sistematica dei dati di traffico in Internet. Si è ritenuto infatti necessario procedere ad una valutazione più approfondita, e sulla base di un dibattito pubblico, delle implicazioni che ciò avrebbe sullo sviluppo delle reti. Si sono altresì considerate le importanti implicazioni che il trattamento di quei dati può avere sulla riservatezza e sugli altri diritti e libertà fondamentali degli interessati, come pure l'oggettiva complessità e difficoltà della loro conservazione e gestione.

L'Assemblea ha, invece, confermato la scelta della Commissione circa la riduzione dei tempi di conservazione a quattro anni complessivi ed ha eliminato il rinvio ad un apposito decreto interministeriale per la determinazione delle modalità di trattamento e di conservazione dei dati.

Il Senato ha, infine, approvato definitivamente il testo licenziato dalla Camera.

2 Altre attività normative

Nel corso dell'anno sono stati approvati numerosi altri provvedimenti riguardanti aspetti d'interesse per la materia del trattamento dei dati personali rispetto ai

quali, schematicamente, si segnalano i profili più rilevanti:

a) l'art. 50 del d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, dalla l. 24 novembre 2003, n. 326, "collegato" alla legge finanziaria 2004, con cui sono state introdotte disposizioni per il controllo della spesa sanitaria.

L'art. 50 del d.l. n. 269/2003)

Il Garante, nel corso dei lavori di conversione del decreto legge, ha richiamato l'attenzione delle Camere sui delicati problemi sollevati da tale disposizione, che prevede, fra l'altro, la costituzione di banche dati a fini di controllo della spesa sanitaria. Tale finalità, pur essendo ispirata dall'esigenza di incentivare il monitoraggio della spesa pubblica è però, allo stato, perseguita attraverso strumenti che (senza fermi accorgimenti che potrebbero essere introdotti, almeno in parte, nei vari decreti attuativi previsti) rischiano di compromettere il diritto dei cittadini alla protezione dei dati e in particolare di quelli riguardanti lo stato di salute, protetti da particolari garanzie. Attraverso i farmaci prescritti e le prestazioni specialistiche ottenute può essere infatti ricostruita analiticamente la storia sanitaria di ciascun soggetto.

Le preoccupazioni manifestate dal Garante

L'Autorità ha ricordato che la legislazione vigente prevede già procedure per il monitoraggio della spesa sanitaria che non presuppongono la costituzione di banche dati centralizzate sulla salute. Tali procedure possono essere rese più efficienti, ma non possono tradursi in una compressione del diritto alla protezione dei dati personali. Le finalità di contenimento della spesa possono essere egualmente perseguite con altre modalità basate su una verifica della genuinità di dichiarazioni e attestazioni relative al reddito, sull'uniformità dei *software* utilizzati e con un accesso particolarmente selettivo ad altri dati, effettuato solo localmente e laddove vi sia un'effettiva e concreta necessità, escludendo un accumulo sistematico di milioni e milioni di posizioni.

L'Autorità ha sottolineato, peraltro, che il sistema disegnato dal decreto legge potrebbe anche discriminare i cittadini in base al reddito, in quanto chi può permettersi di pagare direttamente i farmaci e le prestazioni specialistiche non verrebbe inserito nelle banche dati. Infine, il Garante ha sottolineato che la previsione di una tessera sanitaria rischierebbe di favorire la confusione nel settore della carte elettroniche identificative, dove un'ulteriore tessera andrebbe ad aggiungersi a quelle già in fase di sperimentazione.

Le preoccupazioni manifestate dal Garante non sono state fugate dall'ulteriore testo dell'art. 50 convertito in legge, anche tenendo conto della previsione del progressivo assorbimento della tessera sanitaria nella carta d'identità elettronica o nella Carta nazionale dei servizi (art. 50, comma 13, d.l. n. 269/2003). Sul piano applicativo, poi, si è determinata una sovrapposizione fra il decreto legge e il Codice per la messa a punto del modello di ricetta medica, in quanto anche il decreto legislativo n. 196 del 2003 reca disposizioni in proposito (art. 87). Il dibattito parlamentare sviluppatosi sul punto è sfociato in un ordine del giorno della Camera, con cui si impegna il Governo *"ad adottare le adeguate iniziative normative al fine di escludere il trattamento dei dati sensibili degli assistiti"*. Il Garante, in ogni caso, continuerà a seguire attivamente queste tematiche anche in sede di formulazione dei necessari pareri sugli schemi dei decreti di attuazione dell'art. 50 (art. 154, comma 4, d.lg. n. 196/2003), come pure nell'esprimere il necessario parere ai fini del trattamento dei dati sensibili (art. 20);

L'ordine del giorno della Camera

b) la l. 19 febbraio 2004, n. 40, recante disposizioni in materia di procreazione assistita: nel corso dell'esame del disegno di legge si è tenuta alla Camera un'audizione del presidente dell'Autorità, prof. Stefano Rodotà, nella quale sono stati segnalati alcuni aspetti d'interesse in materia di protezione dei dati personali. Successivamente, in sede di prima applicazione della legge, si è ottenuto, in accordo con il Ministro della salute, che le comunicazioni (che i centri autorizzati ad applicare le tecniche di procreazione assistita dovevano trasmettere ai sensi del relativo art. 17) fossero effettuate utilizzando codici numerici in luogo dell'indicazione nominativa delle persone che si erano rivolte ai medesimi centri;

Le nuove norme in materia di occupazione e mercato del lavoro

c) il d.lg. 10 settembre 2003, n. 276, recante "Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui alla legge 14 febbraio 2003, n. 30": contiene alcune disposizioni in materia di trattamento di dati personali effettuati nell'ambito del rapporto di lavoro (artt. 8-10, 15, 16 e 73 d.l. n. 276/2003) che sarebbe stato più opportuno inserire nel Codice. In relazione a queste disposizioni, il Garante fornirà comunque alcune indicazioni in occasione dell'espressione del parere sugli schemi di decreto ministeriale cui spetta individuare alcune modalità di trattamento dei dati e definire flussi informativi volti ad agevolare l'incontro tra domanda ed offerta di lavoro (artt. 8, comma 2, e 16, comma 2, d.lg. n. 276/2003). Il decreto prevede anche alcune garanzie a fini di informazione agli interessati in caso di annunci di lavoro pubblicati su giornali o effettuati mediante reti di comunicazione elettronica (art. 9 d.lg. n. 276/2003). Sono poi vietate le discriminazioni che possono derivare dal trattamento di dati sensibili o di dati non pertinenti ed eccedenti rispetto alle finalità tipiche del rapporto di lavoro, divieto esteso alle agenzie per il lavoro e agli altri soggetti abilitati alla selezione del personale o all'effettuazione di indagini (art. 10 d.lg. n. 276/2003);

La legge di semplificazione per il 2001 e le norme del Codice sulla diffusione *on line* delle sentenze (artt. 51 e 52)

d) la l. 29 luglio 2003, n. 229, cd. legge di semplificazione per il 2001: ha riflessi sulla materia della protezione dei dati, da un lato per la delega di riordino della normativa concernente il documento informatico, la firma elettronica e digitale, la sicurezza dei dati e dei sistemi e l'accesso informatico (in relazione alla quale l'Autorità ha già fornito una prima collaborazione nell'ambito della commissione istituita su iniziativa del Dipartimento per la funzione pubblica); dall'altro, in ragione di una disposizione in tema di riproduzione e diffusione mediante strumenti telematici delle sentenze e delle altre decisioni del giudice amministrativo e contabile (art. 19 legge n. 229/2003) che dovrà essere applicata, come peraltro segnalato dall'Autorità, nel rispetto dei principi di protezione dei dati. Il Codice contiene, infatti, alcune disposizioni per favorire la conoscenza sia dei dati identificativi dei giudizi pendenti, sia delle decisioni giudiziarie adottate, attraverso la loro disponibilità *on line* nei siti Internet delle autorità giudiziarie interessate (art. 51). Al tempo stesso, però, il Codice prevede in favore delle parti alcune situazioni di anonimato nel caso in cui la sentenza sia riprodotta su riviste giuridiche, mediante *compact disk*, o tramite Internet, senza intaccare le vigenti disposizioni processuali sulla pubblicazione delle sentenze e sulla conoscibilità di atti giudiziari secondo le regole dei codici di rito (art. 52). Si prevede infatti che ciascun interessato possa richiedere "per motivi legittimi" alla cancelleria o alla segreteria competenti l'apposizione, sull'originale della decisione, di un'annotazione per precludere, in caso di riproduzione della sentenza, l'indicazione

delle proprie generalità o di altri dati identificativi. L'annotazione può essere altresì apposta d'ufficio dal giudice, a garanzia della dignità dell'interessato. Anche a prescindere da tale annotazione, chiunque diffonda provvedimenti giudiziari deve omettere i dati personali dai quali possa desumersi anche indirettamente l'identità di minori (art. 52, comma 5, d.lg. n. 196/2003): è qui evidente l'intento di assicurare più ampie garanzie di riservatezza a soggetti particolarmente meritevoli di protezione, in linea con altri strumenti già presenti nell'ordinamento (cfr. art. 734-*bis* c.p.). Una disposizione transitoria limita l'obbligo di omettere i dati identificativi dell'interessato per le sentenze adottate prima dell'entrata in vigore del Codice, prevedendolo solo nel caso in cui l'interessato medesimo ne faccia espressa richiesta e, comunque, per i documenti pubblicati mediante Internet o diffusi su nuovi supporti, informatici o cartacei (art. 181, comma 5, d.lg. n. 196/2003).

Come già ricordato, poi, la legge n. 229/2003 sostituisce il ricorso ai testi unici, anche misti, con la distinta codificazione della normativa primaria e secondaria: a questa modifica si è tempestivamente ispirato il Governo includendo, nel Codice in materia di protezione dei dati personali, norme aventi tutte rango primario;

e) la l. 20 giugno 2003, n. 140, che reca disposizioni in materia di intercettazioni e di acquisizione di tabulati concernenti conversazioni o comunicazioni di parlamentari intercettate nel corso di procedimenti riguardanti terzi, prevedendo la distruzione dei verbali e delle registrazioni relative alle intercettazioni irrilevanti (art. 6). Tale normativa ha effetti in materia di protezione dei dati personali: infatti, la sua eventuale violazione può comportare l'inutilizzabilità dei dati personali trattati (artt. 11, comma 2, 47 e 53 d.lg. n. 196/2003);

f) il d.l. 27 giugno 2003, n. 151, convertito dalla l. 1 agosto 2003, n. 214, recante modifiche al codice della strada, che contiene nuove disposizioni in materia di "accertamenti qualitativi non invasivi" e di ulteriori verifiche sullo stato delle persone da parte degli organi di polizia, in relazione al divieto di guida in stato di ebbrezza o di alterazione psico-fisica per uso di sostanze stupefacenti;

g) il d. l. 9 maggio 2003, n. 105, convertito dalla l. 11 luglio 2003, n. 170, il cui art. 1-*bis* istituisce l'anagrafe nazionale degli studenti e dei laureati delle università: sul tema, l'Autorità sta collaborando con il Ministero dell'istruzione, dell'università e della ricerca per la messa a punto del decreto di attuazione dell'anagrafe, con il quale vengono individuati i dati personali che possono esservi inseriti;

h) la l. 16 gennaio 2003, n. 3, recante "Disposizioni ordinamentali in materia di pubblica amministrazione" (c.d."collegato" alla finanziaria 2002): ha previsto alcuni interventi mediante regolamenti governativi in materia di innovazione tecnologica nella pubblica amministrazione, con riguardo, in particolare, alla diffusione della Carta nazionale dei servizi (Cns) e all'accesso telematico agli atti della pubblica amministrazione (art. 27); rispetto ad essa il Garante ha espresso il parere di competenza sullo schema di regolamento recante disposizioni per la diffusione e l'uso della Carta nazionale dei servizi (v. *infra*, parag. 45.2.).

3 Lavori parlamentari

Oltre ai provvedimenti normativi sin qui descritti, vanno segnalati i lavori parlamentari relativi ad altre iniziative legislative ugualmente d'interesse per la tematica della protezione dei dati personali. In proposito si ricordano:

a) alcune proposte di legge in materia di vigilanza privata (AC 4209 del Governo e proposte abbinate, all'esame della Commissione affari costituzionali della Camera) e di investigazione privata (AS 490, presso la Commissione giustizia del Senato) per gli aspetti che riguardano il trattamento dei dati personali, anche ai fini della sottoscrizione da parte delle categorie interessate del codice di deontologia e di buona condotta in materia di investigazione privata e indagini difensive, in fase di avanzato approfondimento (art. 135 d.lg. n. 196/2003);

Protesti bancari

b) due disegni di legge in materia di cancellazione dei dati personali dagli elenchi dei protesti bancari e di omonimia nei protesti bancari (AS 1368 ed AS 839, esaminati congiuntamente dalla Commissione giustizia del Senato). Tali proposte di legge assumono rilievo anche in vista dell'adozione del codice deontologico in materia di informazioni commerciali, nell'ambito del quale devono essere individuati termini armonizzati di conservazione dei dati personali contenuti in banche di dati pubbliche e private riferite al comportamento debitorio dell'interessato, diverse dalle "centrali rischi" private (artt. 117, 118 e 119 d.lg. n. 196/2003);

c) alcuni disegni di legge che recano modifiche al codice di procedura civile (AS 2430 ed abb. presso la Commissione giustizia del Senato), per i quali appare opportuno un coordinamento con le disposizioni introdotte dal Codice in materia di notificazioni di atti giudiziari (art. 174 d.lg. n. 196/2003);

d) il disegno di legge del Governo recante disposizioni per l'attuazione della decisione del Consiglio dell'Unione europea che istituisce Eurojust (AC 4293, all'esame della Commissione giustizia della Camera);

e) tre proposte di legge di iniziativa parlamentare, sostanzialmente identiche, che prevedono l'istituzione del Difensore dei diritti delle persone private della libertà personale (AC 411, Pisapia ed altri, AC 3229, Mazzoni e AC 3344, Finocchiaro ed altri, all'esame della Commissione affari costituzionali della Camera).

Il Garante o Difensore civico nelle carceri è già conosciuto ed operante in molti Paesi europei, ma non è allo stato previsto dalla legislazione nazionale: recentemente, invece, è stata sottoposta all'attenzione dell'Autorità una legge regionale che ha istituito tale autorità in ambito locale. In base a quanto previsto dal testo unificato delle tre proposte di legge, recentemente elaborato, al Difensore civico è riconosciuto il compito di tutelare i diritti fondamentali delle persone detenute o comunque private della libertà personale, in conformità ai principi ed alle disposizioni contenuti nella

Costituzione, nelle leggi e nelle convenzioni internazionali sui diritti umani; gli è inoltre riconosciuto il diritto di accesso presso tutte le pubbliche istituzioni nelle quali la legge prevede sia limitata la libertà personale, nonché il diritto di incontrare chiunque senza restrizioni;

Il progetto sull'accesso della polizia ai dati detenuti dai vettori

f) una proposta di legge in materia di accesso delle forze di polizia ai dati detenuti da vettori aerei e navali (AC 2630), della quale si è già data notizia nella precedente *Relazione* annuale. Nell'ambito dei lavori presso la Commissione affari costituzionali della Camera si è tenuta, il 14 gennaio 2003, un'audizione del presidente del Garante, il quale ha espresso l'esigenza che il progetto normativo rispetti i principi in materia di protezione dei dati personali applicabili ai trattamenti effettuati per finalità di polizia, prevedendosi, in ogni caso, richieste di informazioni circostanziate, selettive e finalizzate unicamente al perseguimento di gravi reati di terrorismo o di criminalità organizzata.

Il recepimento delle direttive comunitarie

4 Stato di recepimento delle direttive comunitarie negli Stati membri

4.1. Il recepimento della direttiva n. 95/46/CE

Gli attuali quindici Paesi dell'Ue hanno provveduto in tutto o in parte all'attuazione della direttiva n. 95/46/CE. La Francia, pur non avendo ancora completato l'*iter* parlamentare per l'adozione della legge nazionale di recepimento, ha comunicato alla Commissione europea l'approvazione della legge "Informatica e libertà", la quale, nonostante risalga al gennaio del 1978, contiene principi analoghi a quelli introdotti dalla direttiva.

Presentiamo di seguito la tabella riassuntiva delle normative nazionali adottate dai Paesi dell'Unione.

Tabella di recepimento della direttiva 95/46/CE – aprile 2004

Stato	Normativa nazionale di recepimento	Entrata in vigore
AUSTRIA	Datenschutzgesetz 2000 (legge sulla tutela dei dati 2000) del 17 agosto 1999	1° gennaio 2000
BELGIO	Legge dell'8 dicembre 1992 sulla tutela della *privacy* nel trattamento di dati personali, come modificata dalla legge 11 dicembre 1998 di trasposizione della direttiva n. 95/46/CE	1° settembre 2001
DANIMARCA	Legge n. 429 del 31 maggio 2000	1° luglio 2000
FINLANDIA	Legge n. 523/99	1° giugno 1999
GERMANIA	Bundesdatenschutzgesetz (legge federale sulla protezione dei dati) del 23 maggio 2001 e successive modificazioni	23 maggio 2001
FRANCIA	Legge su informatica e libertà del 6 gennaio 1978 e successive modificazioni (sono previsti emendamenti per recepire integralmente la direttiva)	Progetto di legge (Petite Loi) di recepimento approvato dalla Assemblea Nazionale il 30 gennaio 2002, modificato dal Senato il 1° aprile 2003
GRECIA	Legge n. 2472 del 10 aprile 1997 (Protezione delle persone rispetto al trattamento di dati personali)	10 novembre 1997
IRLANDA	Data Protection (Amendment) Act 2003 del 10 aprile 2003, che modifica il Data Protection Act (legge sulla protezione dei dati) del 13 luglio 1988. (Gli artt. 4, 17, 25 e 26 della direttiva erano stati attuati con regolamento approvato il 19 dicembre 2001)	1° luglio 2003 (alcune norme sono entrate in vigore successivamente) 1° aprile 2002

•/• segue

Stato	Normativa nazionale di recepimento	Entrata in vigore
ITALIA	Legge 31 dicembre 1996, n. 675, e successive modificazioni (abrogata dal 1° gennaio 2004); decreto legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali")	8 maggio 1997 1° gennaio 2004
LUSSEMBURGO	Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel	1° dicembre 2002
PAESI BASSI	Wet bescherming persoonsgegevens (legge per la tutela dei dati personali) del 6 luglio 2000	1° marzo 2001
PORTOGALLO	Legge sulla protezione dei dati n. 67/98, del 26 ottobre 1998	27 ottobre 1998
REGNO UNITO	Data Protection Act 1998 (legge sulla protezione dei dati 1998) e legislazione secondaria (regolamenti di attuazione)	1° marzo 2000
SPAGNA	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (legge organica 15/1999, del 13 dicembre, sulla protezione dei dati personali)	14 gennaio 2000
SVEZIA	Personuppgiftslagen (1998:204) (legge sui dati personali del 29 aprile 1998) integrata dall'ordinanza sui dati personali (1998:1191) del 3 settembre 1998	24 ottobre 1998

4.2. Il recepimento delle direttive n. 97/66/CE e n. 2002/58/CE

La direttiva n. 2002/58/CE relativa alla vita privata ed alle comunicazioni elettroniche (i cui tratti salienti sono già stati rappresentati nella *Relazione* per il 2002, p. 106 s.), con la quale si è sostituita la direttiva n. 97/66/CE sulla protezione dei dati nel settore delle telecomunicazioni, è stata tempestivamente recepita con il d.lg. n. 196/2003 (Titolo X, artt. 121-132. Delle modifiche all'art. 132 apportate con il d.l. n. 354 del 24 dicembre 2003, convertito in l. 26 febbraio 2004, n. 45, si è già ampiamente fatto cenno *supra*, a parag. 1.11.).

Altri cinque Paesi dell'Ue hanno emanato norme nazionali di recepimento entro il termine del 31 ottobre 2003 (Austria, Danimarca, Irlanda, Regno Unito e Spagna).

L'art. 13 della direttiva n. 2002/58/CE

Il 5 dicembre 2003 la Commissione europea ha attivato le iniziative preliminari all'avvio della procedura di infrazione nei confronti di alcuni Stati (Belgio, Finlandia, Francia, Germania, Grecia, Lussemburgo, Paesi Bassi, Portogallo, Svezia), per la mancata comunicazione delle norme nazionali adottate nel settore delle comunicazioni elettroniche. Il Portogallo ha successivamente emanato un decreto legge (n. 7/2004 del 7 gennaio 2004) con cui ha recepito la disposizione (art. 13) della predetta direttiva che fissa il principio del consenso preventivo per le comunicazioni indesiderate; inoltre, l'iniziativa avviata nei confronti della Svezia si riferisce esclusivamente al mancato recepimento del medesimo art. 13, dal momento che le altre disposizioni erano già state attuate nell'ordinamento interno e la relativa comunicazione era pervenuta alla Commissione nei termini stabiliti.

Il 1° aprile 2004 la Commissione ha emesso un parere motivato (seconda fase del procedimento di infrazione) nei confronti dei suddetti Paesi, ad eccezione della Svezia, che ha nel frattempo provveduto a recepire l'art. 13. Il parere prevede un termine di due mesi per l'adeguamento, scaduto il quale la Commissione procede alla presentazione del ricorso alla Corte di giustizia.

Tabella di recepimento della direttiva n. 2002/58/CE - aprile 2004

Stato	Normativa nazionale di recepimento
AUSTRIA	Art. 107 Telekommunikationsgesetz 2003 (legge sulle telecomunicazioni: introduce, in particolare, l'obbligo del consenso preventivo) Artt. 6-8 E-Commerce-Gesetz 2001 (legge sul commercio elettronico: prevede la possibilità per l'abbonato di farsi inserire in un elenco di soggetti che rifiutano la ricezione di messaggi commerciali) Art. 12 Wertpapieraufsichtsgesetz 1996 (legge per il controllo sui titoli monetari)
DANIMARCA	Marketing Practices Act (n. 699 del 17 luglio 2000, modificato dalla legge 428 del 6 giugno 2002 e, per quanto riguarda parte della direttiva n. 2002/58/CE, dalla legge 450 del 10 giugno 2003)
IRLANDA	European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003 (entrato in vigore il 6 novembre 2003)
ITALIA	Decreto legislativo n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali")
REGNO UNITO	Privacy and Electronic Communications (EC Directive) Regulations 2003 (entrato in vigore l'11 dicembre 2003)
SPAGNA	Ley 32/2003 del 3 novembre 2003 (Legge generale sulle telecomunicazioni)

5 Il primo rapporto sull'attuazione della direttiva europea in materia di protezione dei dati

Il 15 maggio 2003 la Commissione europea ha pubblicato il primo rapporto sullo stato di attuazione della direttiva n. 95/46/CE. Il documento, sulla base della consultazione pubblica tenutasi nel 2002 (nella quale oltre diecimila soggetti hanno fatto pervenire le proprie osservazioni), nonché delle osservazioni giunte dagli Stati membri e dalle autorità nazionali di controllo, traccia un bilancio positivo dell'applicazione della direttiva escludendo, allo stato attuale, l'opportunità di una sua revisione; posizione, questa, che la Commissione sottolinea essere condivisa dalla maggioranza degli Stati e delle predette autorità.

Difficoltà segnalate

Nel rapporto sono anche evidenziate alcune difficoltà di applicazione omogenea dei principi della direttiva che sarebbero riconducibili a talune divergenze nelle legislazioni di recepimento, ad una ridotta sensibilizzazione dell'opinione pubblica (come risulta da una recente indagine condotta da Eurobarometro), ad un'imperfetta osservanza delle disposizioni nazionali da parte dei titolari del trattamento e all'asserita onerosità di talune disposizioni nazionali sulla notificazione e sul trasferimento dei dati verso Paesi terzi.

Trattamento dei dati in forma di immagini e suoni

Infine, si mettono in luce alcuni profili problematici rispetto al trattamento dei dati in forma di suoni ed immagini. Per ciascun aspetto, il rapporto propone alcune strategie di intervento nell'ambito di un vero e proprio "Piano di lavoro" la cui attuazione è prevista per la fine del 2004. Nel 2005 la Commissione intende esaminare nuovamente lo stato di applicazione della direttiva valutando anche, alla luce della maggiore esperienza acquisita, l'eventuale necessità di introdurre misure ulteriori.

6 La protezione dei dati nell'Ue secondo l'Eurobarometro

Come appena accennato, nel febbraio del 2004 sono stati resi noti i risultati dell'indagine condotta da Eurobarometro per conto della Commissione, riguardante l'applicazione delle norme sulla *privacy* previste dalla direttiva n. 95/46/CE.

Il documento comprende due sezioni dedicate l'una ad aziende e imprese quali titolari di trattamento e, l'altra, ai cittadini interessati dal trattamento di dati personali.

Aziende e imprese

I risultati dell'indagine (tra i quali si evidenzia la posizione positiva dell'Italia) offrono un panorama vario della protezione dei dati personali in Europa. Oltre il 60% dei cittadini dell'Ue afferma di nutrire preoccupazioni forti o molto forti sulla tutela della *privacy*. Tutte le imprese che raccolgono, utilizzano e conservano dati personali giudicano positivamente l'esistenza di norme comunitarie e nazionali in materia, ma quasi la metà ritiene insufficiente l'armonizzazione a livello comunitario. Diversa è anche la valutazione riferita al livello di tutela offerto dalla rispettiva legge nazionale ed agli obblighi che quest'ultima impone. Dal lato degli utenti, invece, si lamenta un rispetto insufficiente delle disposizioni sull'informativa da parte delle imprese e la scarsa conoscenza delle norme fra piccole imprese.

Cittadini

Per quanto riguarda i cittadini interpellati, un terzo degli intervistati è a conoscenza dei diritti loro riconosciuti dalle discipline di protezione dei dati e degli obblighi di trasparenza in capo ai titolari del trattamento. Nonostante ciò, la stragrande maggioranza degli interpellati ritiene che sia giusto ottenere queste informazioni e, soprattutto, conoscere se i dati che li riguardano siano diffusi o comunicati a terzi e per quali finalità.

La situazione italiana

In relazione al livello di conoscenza e di applicazione delle norme sulla protezione dei dati, i cittadini italiani risultano essere i più informati sui propri diritti e sull'esistenza di un'autorità indipendente; le imprese italiane ritengono più delle altre (61%) che sia stata raggiunta un'effettiva armonizzazione a livello comunitario e risultano più rispettose delle prescrizioni legate al dovere di informativa degli interessati. Ancorché oltre il 75% di esse si identifichi chiaramente come titolare del trattamento e rappresenti agli interessati le finalità del trattamento posto in essere, molte imprese manifestano ancora la necessità di maggiori chiarimenti sull'applicazione delle norme. Altro elemento importante è che la percentuale dei cittadini particolarmente preoccupati per la propria *privacy* è scesa in Italia dal 47% del 1991, quando mancava una legislazione specifica nazionale, al 14% del 2003.

II - I diritti dell'interessato I doveri del titolare

I diritti

7 Diritto di accesso

7.1. Rapporto di lavoro

Con due decisioni del 28 marzo 2003, il Garante ha esaminato i ricorsi di due lavoratori che si erano rivolti all'Autorità lamentando l'incompletezza del riscontro fornito dal loro ex datore di lavoro ad istanze di accesso ai dati personali riguardanti, tra l'altro, le ragioni del loro trasferimento ad altro reparto. Il titolare del trattamento ha risposto in entrambi i casi di aver comunicato ai richiedenti tutti i dati personali detenuti nei propri archivi e di non considerarsi obbligato a creare appositamente altri dati, per soddisfare ulteriori e diverse esigenze informative dei richiedenti stessi.

L'Autorità ha ritenuto la risposta della società conforme alla disciplina vigente in tema di tutela dei dati personali, che attribuisce al lavoratore il diritto di accedere ai propri dati personali detenuti dal datore di lavoro e di ottenerne la comunicazione in forma intelligibile e completa, ma non di ottenere la creazione di dati inesistenti o la loro approfondita rielaborazione secondo criteri indicati dal lavoratore medesimo.

Un'altra pronuncia del Garante (*Provv.* 2 luglio 2003) ha avuto origine dal ricorso di un ex dipendente che ha lamentato il mancato riscontro da parte del datore di lavoro ad un'istanza di accesso ai dati personali che lo riguardavano contenuti in documenti riferiti ad un intervallo temporale di circa trenta anni. Rilevato che il riscontro da fornire all'interessato era particolarmente complesso (i dati richiesti riguardavano sia un periodo risalente nel tempo, sia un rapporto di lavoro cessato da diversi anni, sia, infine, un datore di lavoro che aveva subito numerose trasformazioni nel proprio assetto societario), il titolare del trattamento si era limitato a manifestare solo una generica disponibilità a fornire i dati richiesti. L'Autorità ha ritenuto che la società resistente avrebbe dovuto adoperarsi per un riscontro più idoneo e tempestivo e le ha quindi assegnato un termine breve per provvedere a quanto non correttamente omesso.

Dati riferibili a persone identificate o identificabili

Sempre con riferimento al diritto di accesso del lavoratore ai dati che lo riguardano, il Garante ha stabilito (*Provv.* 29 ottobre 2003) che non rientra nell'ambito di applicazione della normativa sulla protezione dei dati personali la richiesta di conoscere unicamente mere notizie di carattere contrattuale o professionale (ad es. gli accordi collettivi nazionali o aziendali), che non sono in nessun modo riferibili a persone identificate o identificabili.

Il diritto di accesso consente, infatti, al lavoratore di conoscere tutti i dati che lo riguardano detenuti dal proprio datore di lavoro, ma non può essere esercitato per

apprendere notizie impersonali che non siano riferibili ad un interessato identificato o identificabile.

7.2. Accesso ai dati per ragioni di giustizia

Il Garante ha nuovamente rilevato, in occasione di una decisione su un ricorso presentato nei confronti di un ufficio giudiziario (procura della Repubblica), che ai trattamenti effettuati per "ragioni di giustizia" (v., ora, art. 47 d.lg. n. 196/2003) alcune disposizioni in materia di protezione dei dati personali non sono applicabili o sono applicate con alcuni adattamenti.

Modalità di esercizio dei diritti

In particolare, non è previsto l'esercizio in forma diretta del diritto di accesso e degli altri diritti degli interessati, né la presentazione di un ricorso all'Autorità. È invece possibile esercitare tali diritti in forma diversa dalla richiesta rivolta al titolare o al responsabile del trattamento, presentando un'istanza al Garante per sollecitare la verifica della conformità del trattamento ai requisiti stabiliti (*Provv.* 5 novembre 2003).

Il Codice ha poi confermato l'inesperibilità del ricorso al Garante, prevedendo che il diritto di accesso e gli altri diritti degli interessati possano essere esercitati anche nei confronti dei trattamenti effettuati per "ragioni di giustizia" attraverso una segnalazione a questa Autorità. Le diverse modalità di esercizio dei diritti non incidono, quindi, sul sostanziale livello di tutela garantito agli interessati, poiché il Garante mantiene il potere di verificare la liceità e la correttezza dei trattamenti, con modalità peraltro adeguate alla specificità del contesto in cui questi sono effettuati, ovvero nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo giudiziario procedente (artt. 8, 47 e 160 d.lg. n. 196/2003).

7.3. Associazioni

Nel 2003 sono pervenute numerose segnalazioni relative all'accesso, da parte di soci o iscritti, a dati personali di altri aderenti ad un ente o associazione.

Dati non sensibili degli associati

Come in passato, l'Ufficio del Garante ha evidenziato che il trattamento dei dati personali non sensibili degli associati è consentito senza il loro consenso quando persegue finalità lecite sulla base di quanto previsto dall'atto costitutivo o dallo statuto dell'associazione o ente, oppure se ricorre uno degli ulteriori presupposti del trattamento equipollenti al consenso, previsti dalla normativa vigente (ad esempio, per adempiere ad un obbligo di legge o per esigenze di difesa di un diritto in sede giudiziaria).

Tale impostazione è stata ribadita dal Codice con riferimento al trattamento dei dati effettuato da associazioni od organismi senza scopo di lucro, anche non riconosciuti, in riferimento agli aderenti ed ai soggetti che con essi hanno contatti regolari (artt. 24, comma 1, lett. *h)* e 26, comma 4, lett. *a),* d.lg. n. 196/2003).

7.4. Dati di traffico: fatturazione dettagliata

Il Garante ha ribadito la piena applicabilità dell'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) alle informazioni incluse nella fatturazione, trattandosi di dati di carattere personale. In particolare, con una decisione del 30 aprile 2003

l'Autorità, nell'accogliere un ricorso, ha ordinato ad un fornitore di servizi di telecomunicazione di comunicare gratuitamente al ricorrente i dati di traffico "in uscita" con l'indicazione integrale delle cifre dei numeri chiamati, che nel caso di specie erano relativi ad una carta prepagata intestata all'interessato.

Chiamate "in uscita"

Non possono, invece, trovare accoglimento le richieste, rivolte ai gestori telefonici, di conoscere gli estremi identificativi e gli indirizzi dei soggetti cui corrispondono i numeri telefonici riportati nel tabulato delle chiamate "in uscita" (*Provv.* 22 settembre 2003). Esercitando il diritto di accesso, l'interessato può infatti conoscere i dati personali che lo riguardano, ma non può chiedere di acquisire dati e informazioni relativi a terzi, come ora precisa espressamente il Codice (art. 10, comma 5, d.lg. n. 196/2003).

Sempre con riferimento alle chiamate "in uscita", l'Autorità ha precisato che il titolare deve fornire idoneo riscontro soltanto alle istanze di accesso formulate dalla persona cui si riferiscono i dati personali oggetto della richiesta. In un caso è stato, pertanto, ritenuto illecito il riscontro fornito dal titolare ad un'istanza di accesso presentata da una persona che non risultava essere il reale utilizzatore dell'utenza telefonica (*Provv.* 30 dicembre 2003).

Con decisione del 13 novembre 2003, il Garante ha altresì chiarito che l'accesso dell'interessato deve essere garantito anche nei confronti dei dati relativi a chiamate verso numeri a tariffazione speciale (ad es., quelli che iniziano con il prefisso "709").

7.5. Dati di traffico: chiamate in entrata e chiamate di disturbo

La problematica dei giusti limiti da porre all'esercizio del diritto d'accesso ai dati identificativi delle cd. chiamate in entrata ha trovato una soluzione di conferma nel Codice, il quale precisa che l'accesso a tali dati non è previsto per esercitare un diritto in sede civile ed è lecito soltanto quando, omettendo di darne comunicazione, si determinerebbe un pregiudizio "effettivo e concreto" per lo svolgimento delle investigazioni difensive in ambito penale (art. 8, comma 2, lett. *f)*, d.lg. n. 196/2003; l. 7 dicembre 2000, n. 397).

Questa previsione del Codice, come ha nuovamente constatato l'Autorità con una decisione del 18 febbraio 2004, traccia un bilanciamento tra il diritto dell'interessato ad accedere ai dati che lo riguardano e il diritto alla riservatezza di terzi (gli utenti-persone fisiche chiamanti e i soggetti chiamati), circoscrivendo il diritto di accesso alle sole comunicazioni "in entrata" di cui sia realmente necessaria la conoscenza, negando le quali si arrecherebbe un pregiudizio reale per lo svolgimento delle investigazioni difensive, che deve risultare comprovato, in concreto, caso per caso.

Anche con riferimento alle chiamate in entrata, è stato ribadito che il diritto d'accesso può essere esercitato dall'interessato soltanto nei confronti dei dati che lo riguardano. Nel decidere su un ricorso, il Garante ha pertanto dichiarato inammissibile la richiesta volta ad identificare utenze diverse da quella dell'interessato (e le relative coordinate delle chiamate), da cui erano originate alcune chiamate effettuate a nome di quest'ultimo verso il *call-center* di una società di telefonia mobile (*Provv.* 5 novembre 2003).

Riguardo, invece, all'accesso alle chiamate di disturbo, specie quando non sia possibile identificare sull'apparecchio la linea chiamante, il Codice conferma il diritto dell'abbonato di richiedere al fornitore del servizio di rendere temporaneamente inefficace la soppressione dell'identificazione della linea chiamante (e di conservare i dati relativi alla provenienza della chiamata ricevuta) e riconosce espressamente il diritto di venirne a conoscenza (art. 127 d.lg. n. 196/2003).

7.6. Messaggi di posta elettronica indesiderati

Anche al destinatario di messaggi di posta elettronica non sollecitati sono riconosciuti i diritti di cui all'art. 7 del Codice, fra i quali il diritto di conoscere da quale fonte siano stati ricavati i propri dati, di far interrompere in qualsiasi momento la loro ulteriore utilizzazione a fini commerciali o pubblicitari e, ancora, di far cancellare quelli trattati in violazione di legge.

Ferma restando la tutela che su un altro piano, quello penalistico, è data dalla natura di reato dello *spamming* (art. 167 del Codice), l'interessato può, gratuitamente e senza particolari formalità, rivolgere comunque un'esplicita richiesta al mittente del messaggio indesiderato e, ove non riceva un soddisfacente riscontro nel termine di quindici giorni (o di trenta giorni, se sono necessarie operazioni di particolare complessità), può rivolgersi all'autorità giudiziaria ordinaria oppure proporre ricorso al Garante (che resta incompetente riguardo ad eventuali pretese risarcitorie del danno subito).

Accesso ai dati relativi ai terzi

Negli innumerevoli ricorsi esaminati in materia di *spamming* l'Autorità ha peraltro precisato che l'esercizio del diritto di accesso e la successiva proposizione di un ricorso al Garante non sono consentiti con riferimento a dati personali relativi a terzi. Sono stati pertanto dichiarati inammissibili alcuni ricorsi, una volta accertata la loro proposizione da parte di soggetti privi della relativa legittimazione, in quanto si trattava di persone diverse da quelle cui erano riferiti i dati concernenti gli indirizzi di posta elettronica dei quali era stato lamentato l'illecito trattamento (*Provv.* 25 luglio, 5 e 16 dicembre 2003).

7.7. Credito

Con riferimento al trattamento dei dati personali in ambito bancario, un profilo delicato ha riguardato l'esercizio del diritto di accesso ai dati personali di persone decedute, il quale è qui approfondito in un apposito paragrafo (cfr. subito parag. 7.10.).

Gratuità del riscontro all'interessato

Per quanto concerne la disciplina del diritto di accesso dell'interessato ai dati personali che lo riguardano detenuti da istituti di credito, va ricordato che il titolare è tenuto ad assicurare un riscontro gratuito alle richieste di accesso rivoltegli dagli interessati.

In alcune occasioni, taluni istituti di credito hanno invece subordinato tale riscontro al versamento, da parte del cliente, di somme occorrenti per ricercare e mettere a disposizione i documenti richiesti: ciò per far fronte alle spese che gli istituti sostenevano di dover affrontare per il reperimento dei dati e la loro comunicazione all'interessato.

Tale comportamento è stato giudicato illegittimo dal Garante in alcune decisioni su ricorsi (*Newsletter* n. 199, 3-9 novembre 2003; v. anche *Provv.* 10 dicembre 2003) poiché, nel vigore della legge n. 675/1996, il contributo spese poteva essere richiesto all'interessato solo nel caso in cui presso il titolare non fosse risultata confermata l'esistenza di suoi dati personali. Pertanto, si è affermato che l'esercizio del diritto di accesso vantato dal ricorrente doveva essere garantito gratuitamente e non poteva essere condizionato, nelle sue modalità di esercizio, a quanto stabilito, a ben altri fini, dal testo unico in materia bancaria e creditizia (d.lg. n. 385/1993). È stato quindi ordinato alle banche resistenti di estrarre dagli atti e dai documenti da essa detenuti tutte le informazioni personali richieste, concernenti le movimentazioni effettuate, e di comunicarle in breve termine agli interessati in modo intelligibile.

7.8. "Centrali rischi" private

Al Garante sono pervenute ancora numerose richieste da parte di cittadini per il tramite di associazioni e studi legali, indirizzate direttamente o per semplice conoscenza all'Autorità ed aventi ad oggetto l'esercizio dei diritti di cui all'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) in merito al trattamento dei dati da parte delle "centrali rischi" private. Sul punto si è ribadito che gli interessati possono rivolgersi direttamente al titolare o al responsabile del trattamento dei dati al fine di esercitare i diritti in esame, non risultando indispensabile, nella prima fase di questo interpello, rivolgersi subito al Garante, anche solo per conoscenza.

"Messa in chiaro" dei dati

In numerosi casi, i riscontri forniti alle richieste di accesso rivolte a banche e società finanziarie sono risultati lacunosi, in quanto limitati alla comunicazione dei dati solo per categorie od a un semplice rinvio agli estratti conto forniti mensilmente, senza nessun riferimento alle "centrali rischi". Al riguardo l'Autorità ha ripetutamente invitato le società ad integrare i riscontri già forniti in modo generico, provvedendo alla "messa in chiaro" di tutte le notizie di carattere personale oggetto di trattamento relative anche ai rapporti finanziari con i clienti, pur se provenienti da "centrali rischi". Di queste ultime, infatti, nella modulistica relativa ai contratti di finanziamento anteriori al provvedimento generale del Garante del 31 luglio 2002, spesso non sono indicati i puntuali estremi identificativi e i recapiti.

Credit scoring

Anche il riscontro fornito dalle "centrali rischi" in caso di accesso esercitato direttamente nei loro confronti è risultato in più casi parziale e insoddisfacente. Ad esempio, una società non aveva comunicato, come invece specificamente richiesto dall'interessato, i dati personali detenuti in forma di punteggi sul grado di affidabilità/solvibilità, qualificati genericamente come "indicatori numerici o punteggi diretti a fornire una rappresentazione sintetica, in termini predittivi o probabilistici, del complessivo profilo di rischio di un determinato interessato, della sua affidabilità o solvibilità". Pertanto, la società è stata invitata ad integrare la risposta fornita con riferimento all'integralità dei propri archivi, comunicando tutti gli ulteriori dati personali relativi all'interessato, anche se appunto espressi in forma di punteggio (cd. *credit scoring*, v. *Provv.* 29 dicembre 2003).

7.9. Assicurazioni

In ambito assicurativo, l'Autorità ha ribadito il principio che le informazioni personali comprese nelle valutazioni e negli altri elementi di giudizio riportati nelle perizie medico-legali delle compagnie di assicurazione rientrano nella sfera dei dati

personali e vanno pertanto comunicate all'interessato quando questi ne faccia richiesta: così nel caso del cittadino che, a seguito di un sinistro di cui era rimasto vittima, si era rivolto all'impresa assicuratrice della controparte per avere conferma dell'esistenza di dati personali che lo riguardavano.

L'art. 8, comma 4, del Codice ha, poi, individuato opportune soluzioni in riferimento all'accesso a dati di tipo valutativo, relativi a giudizi, opinioni o altri apprezzamenti di tipo soggettivo, confermando però il diritto di accesso, che trova riconoscimento anche nel successivo regolamento sull'accesso agli atti delle imprese di assicurazione (art. 5 comma 2, d.m. 20 febbraio 2004, n.74).

Comunicazione all'interessato di dati sulla salute

Il Garante aveva inoltre riaffermato in passato che in caso di comunicazione all'interessato di dati che riguardano la sua salute acquisiti nell'ambito di una visita medica dal consulente sanitario della compagnia, tale comunicazione doveva avvenire per il tramite di un medico designato dall'interessato o dalla compagnia assicuratrice titolare del trattamento (*Provv.* 7 maggio 2003; *Newsletter* n. 195, 8-21 dicembre 2003); la questione è ora diversamente disciplinata dall'art. 84 del Codice.

Differimento temporaneo dell'accesso

Per altro verso, la normativa consente ancora al titolare del trattamento di differire temporaneamente l'esercizio del diritto di accesso, per il periodo durante il quale potrebbe derivargli un pregiudizio per lo svolgimento delle cd. indagini difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria (*Provv.* 21 marzo 2003; *Provv.* 29 dicembre 2003). Come già osservato, la valutazione dell'esistenza di un effettivo pregiudizio, tale da giustificare il temporaneo differimento dell'accesso, deve essere effettuata caso per caso sulla base di elementi concreti allegati dal titolare del trattamento o comunque presenti in atti (v. ora art. 8, comma 2, lett. *e)*, del Codice).

7.10. Accesso ai dati di persone decedute

Uno degli aspetti più delicati affrontati nella materia dell'accesso ai dati personali è stato quello dell'accesso ai dati del defunto.

Settore bancario

La questione si è posta in primo luogo, come accennato, nel settore bancario. L'art. 13, comma 3, della legge n. 675/1996, riconosceva tale diritto a chiunque vi avesse interesse: in base a tale disposizione, si è ammesso il diritto degli eredi di accedere ai dati personali del defunto, inclusi eventuali dati riferiti a terzi (ad es., cointestatari del conto corrente o soggetti delegati ad operare sul conto medesimo), nel caso in cui quelli relativi all'interessato e le notizie relative a terzi fossero intrecciati al punto da rendere i primi, se presi isolatamente, incomprensibili, oppure snaturati nel loro contenuto (v. *Provv.* 8 ottobre 2003 e *Provv.* 10 dicembre 2003, che richiamano sul punto il *Provv.* 23 giugno 1998). Al contrario, non poteva essere accolta la richiesta di accesso a dati personali trattati da una banca e riferiti ad una persona deceduta, se volta a conoscere specificamente e direttamente l'identità della persona delegata dal defunto ad effettuare determinate operazioni bancarie (*Provv.* 13 novembre 2003).

La disposizione, come modificata dal Codice (v. l'art. 9, comma 3), specifica ora l'ambito dei soggetti legittimati ad accedere ai dati personali di persone decedute in favore di chi ha un interesse proprio, o agisce a tutela dell'interessato, o per ragioni familiari meritevoli di protezione.

Settore assicurativo

Nel 2003, il Garante è stato chiamato a pronunciarsi sulla questione dell'accesso ai dati relativi al defunto anche in ambito assicurativo: in proposito si è affermato che il diritto di accesso ai dati personali di un defunto non riguarda le informazioni relative a terzi, come ad es. i terzi beneficiari di polizze assicurative (*Provv.* 31 marzo 2003; *Provv.* 22 settembre 2003; *Provv.* 13 novembre 2003): pertanto, sebbene all'erede legittimo spetti il diritto ad accedere a tutte le informazioni personali che riguardano il defunto, non è tuttavia consentito alla società assicuratrice di comunicargli il nome del beneficiario della polizza.

Nei casi a suo tempo esaminati, l'Autorità ha riconosciuto legittima la richiesta di alcuni eredi di accedere ai dati personali riconducibili ai familiari deceduti, benché impropriamente formulata (sul piano della protezione dei dati personali), nella parte in cui si chiedeva l'accesso ad interi documenti detenuti dalle imprese di assicurazioni. La messa a disposizione dell'intera documentazione da parte del titolare del trattamento, in copia o in visione, può essere infatti disposta dal Garante, in applicazione del Codice, qualora sussistano reali, oggettive difficoltà di estrapolazione dei dati richiesti all'interno di documenti, ed avendo comunque cura di oscurare i dati personali eventualmente riferiti a terzi. È stato quindi intimato alle società di estrarre dagli atti e dai documenti detenuti, comprese le eventuali polizze sottoscritte, tutte le informazioni personali relative al defunto, comunicandole in modo intelligibile all'erede legittimo, con esclusione di tutte le informazioni non direttamente riferite al medesimo defunto (e, quindi, nello specifico, non comunicando i dati personali relativi al beneficiario della polizza).

La tematica va ora considerata anche da un diverso angolo visuale, alla luce dell'ulteriore diritto di accesso agli atti delle imprese di assicurazione, disciplinato innovativamente dal già citato d.m. 20 febbraio 2004, n.74.

Un'altra questione ha riguardato la legittimità del rifiuto, opposto da un ufficio delle imposte, di rilasciare copia della dichiarazione dei redditi presentata, a suo tempo, da un parente deceduto del richiedente. In questo caso, il Garante ha riconosciuto al richiedente stesso il diritto di accedere ai dati personali relativi al congiunto deceduto contenuti nella dichiarazione dei redditi di quest'ultimo, ribadendo che tale diritto può essere esercitato da chiunque vi abbia interesse (*Nota* 12 febbraio 2004).

7.11. Giornalismo

Il Garante ha riaffermato il principio in base al quale i diritti di accesso e gli altri diritti ora previsti dall'art. 7 del Codice –esercitabili pure nei confronti degli editori e dei direttori responsabili delle testate giornalistiche (cfr. *Provv.* 26 marzo e 23 aprile 2003)– possono essere fatti valere anche in riferimento a fotografie e ad altri dati personali diffusi attraverso pubblicazioni consultabili via Internet (*Provv.* 8 ottobre 2003 e 8 gennaio 2004).

7.12. Rai

Con la decisione del 19 novembre 2003 è stata dichiarata inammissibile la richiesta dell'interessato volta a conoscere il nominativo della persona incaricata dalla Rai –Radiotelevisione Italiana S.p.A.– di effettuare una visita presso il domicilio dell'interessato stesso nell'ambito delle attività relative alla gestione e riscossione del canone di abbonamento. In proposito, va ricordato che l'art. 7, comma 2, lett. *e)*,

del Codice consente ora, all'interessato, di ottenere dal titolare anche l'indicazione dei soggetti che in qualità di responsabili o incaricati possono venire a conoscenza dei dati che lo riguardano.

8 Cancellazione dei dati

8.1. Cancellazione dei dati trattati dalla pubblica amministrazione

Il diritto ad ottenere la cancellazione dei dati personali trattati da una pubblica amministrazione ha formato oggetto di numerosi ricorsi.

Delibera di giunta comunale

Va ricordata in particolare la decisione su un ricorso con il quale era stata domandata la cancellazione di dati personali contenuti in una deliberazione di giunta comunale, affissa all'albo pretorio, che faceva riferimento ad una controversia in cui era coinvolto il ricorrente (*Provv.* 12 gennaio 2004).

L'Autorità non ha accolto la richiesta dell'interessato, ritenendo la diffusione dei dati che lo riguardavano necessaria allo svolgimento delle funzioni istituzionali dell'ente e conforme alle vigenti disposizioni sullo svolgimento dei procedimenti amministrativi e sulla pubblicazione degli atti (cfr. art. 124 d.lg. n. 267/2000). Nella deliberazione, peraltro, non venivano riportati dati di carattere giudiziario e le informazioni contenute risultavano esatte e non eccedenti rispetto all'esigenza di trasparenza delle deliberazioni comunali. Il Garante ha però riaffermato la necessità di rispettare i principi di pertinenza e non eccedenza, nel bilanciare le esigenze di riservatezza e di trasparenza dell'attività amministrativa.

Quesito referendario

Analogamente, è stata ritenuta infondata la richiesta volta ad eliminare dal testo di un quesito referendario (concernente il progetto di ristrutturazione di una scuola elementare), le generalità del ricorrente, lì indicate in quanto si trattava dell'autore di un progetto che era contestato nella vicenda referendaria. I dati in questione non sono stati ritenuti eccedenti rispetto alla finalità di illustrare l'iniziativa alla popolazione, considerata pure l'esattezza e l'obiettività con cui essi erano stati riportati, come anche l'ampia conoscibilità che queste informazioni avevano già avuto nella comunità locale (*Provv.* 25 settembre 2003).

8.2. Cancellazione dei dati concernenti i comportamenti debitori

La problematica dei limiti entro cui si può ottenere la cancellazione dei dati relativi ai comportamenti debitori si è posta più volte nel periodo considerato, con riferimento sia ai dati personali contenuti in banche dati pubbliche, sia a quelli registrati in banche dati private, "alimentate" peraltro con dati tratti da registri o elenchi accessibili a tutti.

Trascrizione di pignoramenti

Con riferimento all'esercizio dei diritti riconosciuti dalla normativa sulla protezione dei dati nei confronti dei pubblici registri immobiliari, l'Autorità, in una decisione del 30 dicembre 2003, ha affermato che la tutela della riservatezza non può essere invocata per ottenere la cancellazione di una trascrizione di pignoramento

immobiliare in difformità dalle specifiche ipotesi e particolari procedure previste dalla normativa di settore.

Su questa base il Garante ha giudicato infondato il ricorso presentato da un cittadino che lamentava di non aver ricevuto riscontro ad una sua istanza presentata all'Agenzia del territorio, nella quale aveva chiesto l'immediata cancellazione dei dati personali relativi una procedura esecutiva immobiliare promossa nei suoi confronti.

L'art. 2668 c.c. consente all'interessato di presentare domanda per la cancellazione delle trascrizioni quando ritiene che sussistano le condizioni per esercitare questo suo diritto. I competenti uffici possono apporre l'annotazione di cancellazione della trascrizione nel pubblico registro immobiliare solo dopo aver verificato la completezza della documentazione richiesta ed accertato la regolarità formale e sostanziale della domanda stessa.

Nel caso in esame, la richiesta di immediata cancellazione è stata quindi giudicata infondata, poiché non era emerso, da parte dell'Agenzia, un uso dei dati personali difforme dalla disciplina in materia, sia rispetto alle modalità di annotazione e tenuta dei registri immobiliari, sia rispetto alle formalità richieste dalla normativa per la cancellazione delle trascrizioni.

Banche dati private contenenti dati raccolti da elenchi pubblici

Sempre in materia di registri immobiliari, l'Autorità ha esaminato la richiesta di cancellazione di dati personali contenuti non in registri pubblici, bensì in banche di dati create e gestite da società private ed alimentate da informazioni estratte da fonti pubbliche accessibili da chiunque. La vicenda, sollevata in un ricorso, riguarda la problematica della pertinenza e completezza delle informazioni a contenuto economico in rapporto al diritto dell'interessato alla conservazione limitata nel tempo dei dati che lo riguardano, ossia per il tempo necessario al perseguimento delle finalità per le quali i dati stessi sono raccolti e successivamente trattati (art. 9 legge n. 675/1996; ora, art. 11 d.lg. n. 196/2003).

Nella decisione (*Provv.* 22 settembre 2003), il Garante ha ricordato che il trattamento di dati provenienti da pubblici registri può essere effettuato anche in assenza del consenso dell'interessato ed ha richiamato la disciplina introdotta in materia dal Codice, il quale, nel confermare la prossima adozione di un codice deontologico in materia, demanda a quest'ultimo il compito di individuare nuovi limiti temporali di conservazione dei dati relativi al comportamento debitorio (art. 119 d.lg. n. 196/2003).

Nelle more dell'adozione di tali fonti, il trattamento dei dati consistente nell'estrazione e comunicazione di informazioni accessibili a chiunque può ritenersi lecito; di qui l'infondatezza del ricorso, fermo restando il riconoscimento del diritto dell'interessato di ottenere, nei modi di legge, l'integrazione e/o l'aggiornamento delle informazioni che lo riguardano (per es., in ordine ad eventuali sentenze di riabilitazione pronunciate in suo favore).

Omonimie

Con un altro ricorso l'Autorità è stata chiamata a pronunciarsi su una richiesta di cancellazione di dati personali da un pubblico registro, motivata da una pretesa omonimia tra il ricorrente e il soggetto cui si riferivano i dati relativi ad un assegno protestato. Nel caso di specie non è stato possibile accertare inequivocabilmente nel procedimento se i dati riportati nell'elenco dei protestati corrispondessero a quelli

del ricorrente: tuttavia, nel disporre l'apertura di un autonomo procedimento, il Garante ha affermato che la situazione soggettiva dell'interessato doveva ritenersi comunque meritevole di tutela. Pertanto, l'Autorità ha disposto il blocco del trattamento effettuato dalla camera di commercio con riferimento alle informazioni che si contestava essere riconducibili al ricorrente, riservandosi ulteriori accertamenti sul punto (*Provv.* 12 gennaio 2004).

9 Opposizione al trattamento

9.1. Attività tributarie

Con importante decisione del 12 gennaio 2004, e in senso analogo a quanto disposto in passato, l'Autorità ha accolto l'opposizione di un contribuente alla comunicazione, da parte di una concessionaria provinciale del servizio riscossione tributi, di informazioni concernenti la posizione debitoria dell'interessato a terzi con i quali l'interessato stesso aveva intrattenuto rapporti professionali. La comunicazione veniva effettuata tramite l'invio a questi ultimi di una "richiesta di dichiarazione stragiudiziale" circa l'esistenza di eventuali crediti vantati dall'interessato nei loro confronti. Poiché tale particolare procedura è risultata non legittimata da alcuna specifica previsione normativa e non rispondente ai principi di pertinenza e non eccedenza dei dati rispetto alle finalità perseguite, nelle more degli ulteriori accertamenti (in corso) sulla questione è stato disposto, quale misura cautelare, il blocco dei dati oggetto di trattamento (cfr. *infra*, parag. 26.).

Diffusione degli elenchi dei contribuenti

In merito al regime di pubblicità dell'elenco dei contribuenti l'Autorità ha ribadito che non vi è incompatibilità tra la protezione dei dati personali e determinate forme di pubblicità di dati previste per finalità di interesse pubblico o della collettività. In particolare, con decisione del 2 luglio 2003, il Garante ha rilevato che la disciplina contenuta nel d.P.R. n. 600/1973 (art. 69), in base alla quale gli elenchi nominativi dei contribuenti che hanno presentato la dichiarazione dei redditi sono consultabili da chiunque presso alcuni uffici finanziari e i comuni interessati, non è stata abrogata, né modificata dalla disciplina sulle modalità di presentazione e trasmissione delle dichiarazioni per via telematica (d.P.R. 22 luglio 1998, n. 322). Pertanto, l'istanza di opposizione per motivi legittimi alla diffusione dei dati personali contenuti nelle dichiarazioni dei redditi attraverso la pubblicazione degli elenchi in questione non poteva essere accolta, poiché il regime di pubblicità previsto risponde ad una scelta normativa di carattere generale operata per favorire la trasparenza in materia di dati raccolti dalla pubblica amministrazione attraverso le dichiarazioni fiscali

9.2. Attività investigative

In una decisione dell'8 gennaio 2004 l'Autorità ha affrontato la questione della liceità del trattamento di dati personali contenuti nel materiale raccolto nell'ambito di indagini investigative e successivamente prodotto in un procedimento giudiziario.

In proposito, il Garante ha ribadito il principio in base al quale il trattamento dei dati a fini di esercizio di un diritto in sede giudiziaria è ammesso, anche in man-

canza del consenso dell'interessato, soltanto quando risulti strettamente "necessario" per la tutela del diritto esercitato. Una volta conclusa l'attività investigativa, il trattamento deve cessare in ogni sua forma, fatta salva l'immediata comunicazione dei dati al difensore o al soggetto che ha conferito l'incarico.

In particolare, nell'ambito di un procedimento di modifica delle condizioni economiche della separazione consensuale tra coniugi è stata ritenuta illecita la produzione di relazioni investigative e di fotografie, precedentemente commissionate ad un'agenzia d'investigazione, riguardanti una pretesa relazione extraconiugale mai stata oggetto di accertamento giudiziario.

9.3. Condominio

Nel 2003 sono stati esaminati dall'Autorità diversi ricorsi aventi ad oggetto il diritto di opposizione al trattamento di dati personali riguardanti situazioni di morosità di singoli condomini. Al riguardo, è stato ribadito che la normativa sulla protezione dei dati personali non ha modificato la disciplina sul condominio degli edifici prevista dal codice civile (art. 1117 s. c.c.), precisando che il condominio può tuttavia trattare solo i dati pertinenti e non eccedenti rispetto alle finalità di gestione. In particolare, i singoli condomini, che sono contitolari di un unico trattamento di cui l'amministratore ha la concreta gestione, hanno diritto di conoscere le informazioni utili riguardanti l'amministrazione ed il funzionamento del condominio, comprese quelle concernenti posizioni debitorie e creditorie dei condomini nei confronti del condominio stesso.

Comunicazione e diffusione dei dati sulle morosità dei condomini

Così, la comunicazione di informazioni relative alla morosità di un condomino nel corso dell'assemblea di condominio e la successiva trascrizione di queste informazioni in un verbale inviato ai soli condomini è stata giudicata dal Garante conforme ai principi di pertinenza e non eccedenza dei dati raccolti o successivamente trattati (*Provv.* 16 luglio 2003).

L'opposizione alla diffusione (tramite affissione nella bacheca condominiale) di dati personali concernenti presunte posizioni di morosità relative ad alcuni condomini è stata oggetto di un'ulteriore decisione dell'Autorità. In tale occasione, il Garante ha, però, ritenuto infondato il ricorso, in quanto l'istanza di opposizione era stata avanzata al titolare in un momento successivo alla rimozione dell'elenco dei morosi dalla bacheca condominiale (*Provv.* 19 novembre 2003).

I doveri

10 Rapporto di lavoro

Il Codice sulla protezione dei dati personali ha introdotto nel contesto lavorativo importanti novità ispirate, in particolar modo, alla semplificazione di alcuni adempimenti da parte del datore di lavoro. Ad esempio, per i dati sensibili, quando il trattamento è necessario per eseguire specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, non è più necessario acquisire il consenso scritto del lavoratore interessato, fermo restando il rispetto dell'autorizzazione del Garante e delle regole che saranno individuate mediante il codice di deontologia in materia di lavoro e previdenza (art. 26, comma 4, lett. *d)*, d.lg. n. 196/2003).

Raccordo con il d.lg. n. 276/2003

A prescindere dagli sviluppi a breve termine di tale codice deontologico, questo nuovo quadro normativo va peraltro raccordato con i recenti mutamenti introdotti dal d.lg. n. 276/2003 in attuazione delle deleghe in materia di occupazione e mercato del lavoro di cui alla legge n. 30/2003 (cd. riforma Biagi).

Sotto questo profilo, assume rilievo, in primo luogo, la previsione di un ulteriore divieto di indagini sulle opinioni e trattamenti discriminatori (art. 10 d.lg. n. 276/2003), sul quale sono già state avanzate all'Autorità richieste di chiarimenti da parte di talune organizzazioni sindacali. Rilevano inoltre la disposizione sull'ambito di diffusione dei dati relativi all'incontro tra domanda ed offerta di lavoro (art. 8 d.lg. n. 276 cit.) e quella sulle comunicazioni a mezzo stampa, Internet, televisione o altri mezzi di informazione (art. 9 d.lg. n. 276 cit.).

In particolare, con quest'ultima disposizione è stato recepito, a livello normativo, il consolidato orientamento dell'Autorità in materia di modalità dell'informativa ai candidati interessati ad una selezione o ricerca di personale, che deve essere in sostanza resa, sin dal momento della pubblicazione degli annunci di lavoro (cfr. *Provv.* 10 gennaio 2002).

Settori di intervento

Tra i diversi settori in cui l'Autorità è dovuta intervenire, vanno ricordati poi: il controllo a distanza dei lavoratori a mezzo di apparecchiature di videosorveglianza; le modalità di custodia e conservazione dei dati dei dipendenti a cura dei datori di lavoro; l'accesso dei lavoratori ai dati che li riguardano.

In relazione al divieto di controllo a distanza dei lavoratori, l'Autorità ha curato vari approfondimenti e si pronuncerà a breve con un provvedimento di carattere generale concernente le verifiche effettuate dai datori di lavoro sull'uso, da parte dei lavoratori, degli strumenti informatici e telematici loro assegnati per ragioni di servizio e, in particolare, sulle navigazioni in Internet e sulla gestione della posta elettronica.

Sul piano del contenzioso al riguardo merita di essere ricordata la delicata questione, portata all'attenzione del Garante, dell'impugnativa (da parte del dipendente

10

di una banca) di un licenziamento disciplinare motivato dall'uso irregolare delle infrastrutture informatiche fornitegli quali strumenti di lavoro.

In particolare, a fronte della domanda del lavoratore di tutela d'urgenza avverso il licenziamento, la banca ha sostenuto l'assenza di *periculum in mora* per l'avvenuta corresponsione del trattamento di fine rapporto. Tra il materiale probatorio prodotto in proposito, la banca ha tuttavia inserito anche la documentazione di cui aveva la disponibilità in qualità di parte non del rapporto di lavoro, bensì del rapporto di conto corrente che era stato instaurato con il medesimo dipendente.

L'Ufficio ha pertanto deciso di verificare in tempi brevi il rispetto, nel caso di specie, sia dei principi pertinenza e non eccedenza dei dati utilizzati e di liceità e correttezza del trattamento, sia delle norme in tema di informativa, consenso e relativi casi di esclusione (artt. 11, 13, 23 e 24 d.lg. n. 196/2003).

Eguale urgente approfondimento istruttorio è stato disposto sull'avvenuta conoscenza, da parte di alcuni dipendenti della medesima banca, dei dati personali dell'interessato emersi nell'ambito delle attività ispettive svolte nei suoi confronti, nonché sulle misure di sicurezza adottate con riferimento alle informazioni contenute nei documenti ed altri supporti presi in custodia in esito a tali attività.

Vari sono stati, poi, i reclami inviati al Garante da parte di organizzazioni sindacali (in particolare a livello aziendale), in merito all'installazione di impianti di videosorveglianza sul luogo di lavoro. In molti casi (riguardanti, soprattutto, apparecchiature installate a protezione del patrimonio aziendale, ma che riprendono anche postazioni di lavoro dei dipendenti), sono state impartite indicazioni ai datori di lavoro ai fini del pieno rispetto delle vigenti disposizioni in materia e del primo "decalogo" del Garante (v. la parte di *Relazione* inerente alla sorveglianza e ai sistemi biometrici: parag. 37.-38.).

È poi da segnalare, tra gli altri, un caso relativo alla modalità di recapito, da parte di un'azienda, di una comunicazione di contestazione disciplinare al domicilio privato di un dipendente, contenuta in un foglio ripiegato per errore in modo da rendere possibile la conoscenza dell'oggetto della lettera.

Il datore di lavoro è stato richiamato ad impartire precise istruzioni a tutti gli uffici e dipendenti incaricati di analoghi trattamenti di dati, al fine di assicurare una corretta applicazione della disciplina sulla protezione dei dati personali e garantire la riservatezza di comunicazioni contenenti dati relativi ai lavoratori interessati, in particolare per evitare la conoscenza, anche casuale, alle informazioni riportate al loro interno da parte di terzi estranei.

Cedolini delle buste paga

Il Garante è tornato ad occuparsi anche della questione relativa alla modalità di redazione e consegna dei cedolini delle buste paga ai dipendenti. Con decisione del 16 luglio 2003, l'elaborazione e la consegna dei cedolini in busta chiusa sigillata da parte di appositi incaricati del trattamento è stata ritenuta conforme ai principi della disciplina sulla protezione dei dati personali.

Indirizzo *e-mail* aziendale dell'ex dipendente

Infine, il Garante si è pronunciato sull'istanza volta a ottenere la chiusura dell'indirizzo di posta elettronica aziendale attivato a nome di un ex dipendente durante il rapporto di prestazione d'opera con una società. L'Autorità, ritenendo la

richiesta rilevante anche quale sostanziale opposizione per motivi legittimi, ha giudicato soddisfacente il riscontro fornito all'interessato da parte dell'ex datore di lavoro: quest'ultimo aveva infatti creato un nuovo indirizzo *e-mail* ed aveva inserito all'indirizzo dell'interessato un messaggio di risposta automatica che dava comunicazione dell'avvenuta disattivazione della casella di posta oggetto di contestazione (*Provv.* 22 dicembre 2003).

11 Sicurezza dei dati e dei sistemi

E-banking

Nel periodo di riferimento l'Autorità si è occupata di un caso assai significativo per la materia in esame, relativo alla sicurezza dei dati personali concernenti i rapporti bancari con i clienti, trattati da un istituto di credito nell'ambito di servizi di *e-banking*.

Il caso ha suscitato viva attenzione nel settore bancario e spiega effetti rilevanti, come caso pilota, per il livello di futuro sviluppo e di affidabilità dei servizi bancari prestati per via telematica.

È infatti accaduto che un cliente, il quale usufruiva di questi servizi via Internet, dopo un primo accesso ai dati che lo riguardavano, ricollegandosi a distanza di poco tempo al sito per controllare nuovamente la propria posizione contabile, si è trovato accidentalmente a consultare anche *file* relativi a conti correnti di altri clienti. I dati in tal modo visualizzati e memorizzati in appositi prospetti riguardavano operazioni bancarie, inclusi i numeri di conto corrente o delle carte di pagamento utilizzate per effettuare le singole transazioni (nonché, a volte, i dati dei relativi titolari), e recavano l'indicazione del pagamento di utenze domiciliate, tasse, imposte e persino emolumenti erogati da datori di lavoro. In molti casi le informazioni riguardavano anche familiari dei titolari dei conti correnti oggetto dell'accidentale consultazione, nonché terzi con i quali i correntisti avevano effettuato singole transazioni bancarie.

La banca ha fornito alcune giustificazioni sostenendo, tra l'altro, che l'unico caso di accesso indebito era stato quello oggetto di segnalazione, e che esso si era verificato solo per un breve arco temporale.

Il Garante, a conclusione di complesse verifiche, ha invece rilevato che l'erronea configurazione del sistema e dei programmi per l'accesso al servizio di *e-banking* aveva violato l'obbligo di garantire la riservatezza dei dati personali relativi a numerosi clienti e la loro protezione da accessi non autorizzati, con un abbassamento della sicurezza del sistema al di sotto della soglia minima di tutela prescritta dalla legge, rilevante non solo sul piano dell'eventuale responsabilità civile, ma anche a livello penale.

Nel caso di specie, inoltre, l'indebita comunicazione a terzi dei dati dei correntisti, realizzata mediante la messa a disposizione di informazioni caratterizzate da un'elevata confidenzialità (soprattutto in considerazione del rischio di utilizzo abusivo o illecito degli stessi dati da parte di terzi), ha configurato una violazione del cd. segreto bancario, inteso come obbligo per la banca di mantenere il riserbo su operazioni, conti e posizioni degli utenti dei servizi bancari.

11

Per prevenire il ripetersi delle violazioni contestate, il Garante ha segnalato alla banca l'esigenza di aggiornare l'analisi dei rischi connessi alla prestazione dei servizi di *e-banking*, in modo da adottare preventivamente misure di sicurezza idonee a garantire un livello di protezione elevato dei dati accessibili attraverso tali servizi. L'Autorità ha inoltre prescritto alla banca di verificare e di confermare l'utilizzo di codici identificativi personali e parole chiave da parte sia dei dipendenti incaricati, sia degli utenti del servizio di *e-banking*; ha poi disposto contestualmente la comunicazione all'autorità giudiziaria penale di copia degli atti. Da ultimo, a seguito dell'adempimento alle prescrizioni impartite, la banca è stata ammessa dall'Ufficio del Garante al pagamento di una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione, con conseguente dichiarazione di estinzione del reato, in conformità alla normativa vigente (cfr. ora l'art. 169 del Codice).

L'attivazione di analoghi accertamenti si è poi resa necessaria in altri due casi riguardanti la sicurezza dei dati degli utenti trattati da società concessionarie del servizio di erogazione dell'energia elettrica e del gas, mediante l'installazione di contatori per il monitoraggio dei consumi della clientela, il cui procedimento è in procinto di essere concluso.

Alla fine del 2003 sono stati inoltre instaurati alcuni procedimenti relativi alle misure adottate da datori di lavoro per la custodia di comunicazioni contenenti dati personali di lavoratori, al fine di renderne il contenuto inaccessibile ad eventuali terzi estranei alle vicende oggetto di comunicazione o di contestazione.

Da ultimo, va ricordato che, a chiarimento del nuovo quadro normativo in materia di misure di sicurezza introdotto dal Codice, e alla luce dei numerosi quesiti e richieste di proroga inviate da molte imprese, il Garante ha predisposto apposite istruzioni.

Codice e misure di sicurezza: le istruzioni del Garante (Nota 22 marzo 2004)

In particolare, il 22 marzo scorso il Garante ha fornito diverse indicazioni sui tempi e sulle modalità per una corretta applicazione delle novità normative introdotte dal Codice in materia di "misure minime" per la sicurezza dei dati e dei sistemi informatici.

L'Autorità ha sottolineato come il Codice abbia confermato la disciplina in materia di sicurezza dei dati personali introdotta nel 1996, ribadendo il principio in base al quale le "misure minime", la cui mancata adozione costituisce reato, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza. Vi è, infatti, il dovere più generale, rilevante anche sul piano della responsabilità civile, di custodire i dati personali per contenere il più possibile il rischio che essi siano distrutti, dispersi, trattati in modo illecito, ovvero che diventino conoscibili fuori dei casi consentiti, come pure il dovere di introdurre ogni utile dispositivo di protezione legato alle nuove conoscenze tecniche.

L'elenco delle "misure minime" di sicurezza è stato aggiornato dal Codice, il quale ha specificato alcune modalità di applicazione in un apposito disciplinare tecnico. Analogamente a quanto avveniva in passato, le "misure minime" sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici, nonché a seconda che riguardi o meno dati sensibili o giudiziari.

Premesso che le "misure minime" obbligatorie anche in passato, devono essere ulteriormente mantenute senza attendere il decorso di termini transitori, in considerazione delle novità introdotte il Codice ha invece stabilito che, in sede di prima applicazione

del mutato quadro normativo, le nuove misure possono essere adottate entro il 30 giugno 2004. Un periodo più ampio per l'adeguamento (1° gennaio 2005) è previsto solo nel caso particolare in cui ricorrano obiettive e documentate ragioni di natura tecnica, che non consentano di installare immediatamente le nuove misure rispetto agli elaboratori e ai programmi utilizzati.

Il documento programmatico sulla sicurezza (Dps)

Con la recente comunicazione, l'Autorità ha ricordato che tra le "misure minime" di sicurezza rientra anche la redazione del documento programmatico sulla sicurezza (Dps) da parte dei soggetti che effettuano un trattamento di dati sensibili o giudiziari con l'ausilio di strumenti elettronici.

Si tratta di una misura non nuova; tuttavia, è cambiato parzialmente il contenuto del documento ed è aumentato il numero dei casi e dei soggetti destinatari dell'obbligo.

Proprio per questi motivi il Garante ha ritenuto che, solo in sede di prima applicazione della nuova disciplina, il Dps possa essere predisposto al più tardi entro il 30 giugno 2004: ciò permetterà di utilizzare il modello base semplificato predisposto dall'Autorità per effettuare, soprattutto presso realtà medio-piccole, l'analisi dei rischi che incombono sui dati personali, per individuare gli accorgimenti da adottare al fine di prevenire la loro distruzione o eventuali accessi abusivi e per pianificare gli interventi formativi nei riguardi del personale.

Dal 2005, decorso il periodo transitorio connesso all'entrata in vigore del Codice, il termine per redigere annualmente il Dps aggiornato rimarrà fissato ad un'unica scadenza, quella del 31 marzo di ogni anno, come dispone la regola tecnica n. 19 che disciplina tale misura.

Obbligo di riferire della redazione o aggiornamento del Dps

Il Garante ha inoltre precisato le modalità da seguire per l'attuazione di un'altra rilevante "misura minima" introdotta dal Codice, quella relativa all'obbligo di riferire, nella relazione di accompagnamento al bilancio di esercizio, dell'avvenuta redazione o aggiornamento del Dps. Questa misura, diretta a sensibilizzare e responsabilizzare gli organi di vertice aziendali o amministrativi sulla programmazione annuale degli adempimenti in tema di sicurezza, deve essere rispettata già nel 2004. Per questo primo anno, si è considerato il menzionato regime transitorio e la circostanza che alcuni soggetti non erano tenuti a redigere o aggiornare il Dps in base alla legge n. 675/1996. Sono state fornite varie indicazioni relative ai singoli casi, che si possono sintetizzare nel seguente specchietto riassuntivo che è stato accluso alla risposta data a Confindustria, Confcommercio e a diversi altri operatori pubblici e privati:

Disposizioni transitorie

Termini	Adempimenti
30 giugno 2004	Adozione per il 2004 di tutte le "misure minime" non previste dalla precedente disciplina. Termine ultimo di predisposizione del documento a data certa per descrivere le obiettive ragioni tecniche che non consentono di applicare immediatamente alcune nuove "misure minime" *(documento utilizzabile unicamente nel caso del tutto particolare previsto dall'art. 180, comma 2, del Codice per i soli strumenti elettronici)*.
1° gennaio 2005	Adozione nuove "misure minime" su strumenti elettronici non previste in base alla precedente disciplina (solo per i soggetti legittimati a predisporre il predetto documento a data certa).

Relazione accompagnatoria del bilancio esercizio 2003

Misure	Soggetti già tenuti a redigere o aggiornare il Dps [1]	Soggetti non obbligati a redigere o aggiornare il Dps in base alla previgente disciplina
Dps 2004	Aggiornamento Dps entro il 30 giugno 2004	Redazione Dps entro il 30 giugno 2004
Relazione accompagnatoria del bilancio esercizio 2003	Riferimento al Dps redatto o aggiornato nel 2003 (con facoltà di indicazione aggiuntiva dell'aggiornamento 2004 *in itinere*), oppure menzione dell'aggiornamento eventualmente già effettuato nel 2004	Nessun riferimento se il Dps 2003 o il Dps 2004 non sono stati adottati, oppure riferimento al Dps eventualmente già adottato nel 2004. Facoltà di indicazione del Dps eventualmente predisposto nel 2003 e facoltà di indicazione dell'aggiornamento 2004 *in itinere*

Ulteriori indicazioni pratiche sono state fornite nel corso della prima edizione del ciclo di seminari di formazione curati dal Garante presso la propria sede (2 aprile 2004) e nel *Cd-Rom* multimediale in fase di predisposizione con i materiali del seminario.

12 Notificazione

Casi sottratti alla notificazione: il provvedimento del 31 marzo 2004

Con il provvedimento del 31 marzo 2004 (pubblicato in *G.U.*, Serie generale, 6 aprile 2004, n. 81 e che è riportato tra gli allegati di questa *Relazione*), il Garante ha individuato i trattamenti di dati personali che non sono oggetto di notificazione all'Autorità, in conformità a quanto stabilito dall'art. 37, comma 2, del Codice.

Come è stato già evidenziato, quest'ultimo ha introdotto una robusta semplificazione in argomento, individuando alcune specifiche categorie di trattamento per le quali vige l'obbligo di notificare preventivamente all'Autorità l'avvio di un trattamento di dati.

Fin dalle prime settimane di applicazione del Codice, e in vista del termine transitorio del 30 aprile 2004 per la presentazione delle notificazioni, il Garante ha ritenuto necessario individuare nuove semplificazioni che interessano, a date condizioni, imprese, enti locali, operatori sanitari (in particolare medici di medicina generale e pediatri), liberi professionisti, datori di lavoro e gestori di impianti di videosorveglianza.

Con tale provvedimento il Garante ha recepito diversi suggerimenti formulati, in questi primi mesi di vigenza del Codice, da alcuni operatori e associazioni di categoria, ravvisando che i trattamenti effettuati nelle predette ipotesi, specialmente in ragione delle relative modalità, potessero essere sottratti all'obbligo di notificazione, ferma restando, ovviamente, l'osservanza degli ulteriori principi ed obblighi previsti dal Codice.

(1) Titolari di un trattamento di dati sensibili o relativi a provvedimenti giudiziari di cui agli artt. 22 e 24 della legge n. 675/1996, effettuato per mezzo di elaboratori accessibili mediante una rete di telecomunicazione disponibili al pubblico

Il Garante ha invece ritenuto, allo stato, di non individuare ulteriori trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato oltre a quelli indicati all'art. 37, comma 1, e da sottoporre pertanto all'obbligo di notificazione. Non è comunque da escludere 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 notifica.

III - La privacy e gli altri diritti
La salute

13 Trattamento di dati idonei a rivelare lo stato di salute

Nel 2003 l'Autorità è stata nuovamente chiamata ad intervenire sul tema dei trattamenti di dati personali effettuati nell'ambito del Servizio sanitario nazionale.

Tra le questioni di maggiore rilievo affrontate si pone, in primo luogo, quella dei limiti alla comunicazione di dati sulla salute e sulla vita sessuale a soggetti diversi dall'interessato. La comunicazione di queste informazioni può, infatti, ritenersi giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti fondamentali e inviolabili. Tale principio è ora confermato dal Codice (artt. 26, comma 4, lett. *c)*, 60, 71 e 92 comma 2, d.lg. n. 196/2003).

Con un provvedimento del 9 luglio 2003, del quale ci si occupa in dettaglio nel capitolo dedicato alla pubblica amministrazione, l'Autorità ha fornito ulteriori indicazioni in ordine a tale problema (cfr. parag. 19.2.).

Recupero coattivo dei crediti affidato a società esterne

Sempre in materia di comunicazione di dati idonei a rivelare lo stato di salute, il Garante ha indicato particolari cautele che le aziende sanitarie locali devono rispettare nell'affidare a società esterne l'attività di recupero coattivo dei crediti derivanti dal mancato pagamento dei *ticket* e dal mancato ritiro dei referti medici.

In tali casi, le aziende debbono designare i soggetti che hanno accesso ai dati dei pazienti in qualità di responsabili o incaricati del trattamento ed informare preventivamente gli interessati sulla possibilità che le informazioni che li riguardano siano utilizzate per finalità di recupero dei crediti. Dovranno poi essere forniti alla società che collabora all'esterno i soli dati personali strettamente necessari al recupero della somma dovuta (dati anagrafici, indirizzo, importo, ecc.) e non anche ulteriori informazioni quali, ad esempio, quelle riguardanti il tipo di analisi effettuata o il relativo referto, in ossequio ai principi di pertinenza e non eccedenza nel trattamento dei dati (*Nota* 22 aprile 2003).

Comunicazione dei dati sulle situazioni di abbandono dei minori

Si è invece ritenuto legittimo che gli operatori di un servizio per le tossicodipendenze segnalino alla procura della Repubblica presso il tribunale dei minorenni situazioni di abbandono o di pregiudizio. La normativa di settore riconosce infatti a chiunque la facoltà di segnalare alle autorità competenti situazioni di abbandono di minori. Sui pubblici ufficiali, gli incaricati di un pubblico servizio e gli esercenti un servizio di pubblica necessità grava, poi, l'obbligo di riferire al più presto al procuratore competente per territorio sulle condizioni dei minori in situazione di abbandono di cui vengano a conoscenza in ragione del proprio ufficio (art. 9, comma 1, legge n. 184/1983).

In quanto espressamente prevista dalla legge, la comunicazione all'autorità giudiziaria di situazioni di abbandono o di pregiudizio ad opera dei servizi per le tossicodipendenze, pubblici o privati, non contrasta, perciò, con la disciplina sulla protezione dei dati. L'operatore deve tuttavia comunicare al tribunale i soli dati pertinenti e necessari ad illustrare la situazione di abbandono in cui versa il minore (*Nota* 1° luglio 2003).

Non può ritenersi invece ammessa la comunicazione, da parte della prefettura ad una amministrazione comunale che ha in assegnazione obiettori di coscienza, di provvedimenti sanzionatori relativi all'uso di sostanze stupefacenti adottati nei confronti di questi ultimi, in assenza di una specifica norma di legge che lo consenta (*Nota* 25 agosto 2003).

Sono poi all'attenzione dell'Autorità le procedure seguite da diversi comuni per controllare la legittimità degli accessi alle zone a traffico limitato (Ztl) ad opera dei medici che hanno necessità di visitare a domicilio i pazienti residenti in tale aree.

In argomento, l'indicazione del nominativo dell'assistito può risultare idonea a rivelare lo stato di salute del paziente, e come tale da trattare con l'adozione delle cautele previste per questo tipo di informazioni e nel rispetto dei principi di pertinenza e di non eccedenza. Si deve, pertanto, valutare con estrema attenzione se, per perseguire la finalità di accertamento delle infrazioni alla disciplina delle zone a traffico limitato, non sia sufficiente conoscere il recapito (via e numero civico) presso cui l'intervento medico è stato prestato.

Allo stesso modo è, poi, sotto esame la prassi seguita da alcune amministrazioni comunali di richiedere ai medici un'attestazione del consiglio dell'ordine con la quale si dichiari che il professionista si è recato nella zona a traffico limitato per ragioni legate all'esercizio della professione medica.

In base all'art. 74 del d.lg. n. 196/2003, i contrassegni rilasciati per il transito in zone a traffico limitato o per la circolazione e la sosta di veicoli a servizio di persone invalide devono contenere i soli dati indispensabili ad individuare il tipo di autorizzazione, ed essere privi di simboli o diciture da cui possa desumersi la speciale natura dell'autorizzazione, per effetto della sola visione del contrassegno.

Le generalità e l'indirizzo della persona fisica interessata, inoltre, devono essere riportati sui contrassegni con modalità tali da non permettere la loro diretta visibilità, se non in caso di richiesta di esibizione o necessità di accertamento.

Elenco dei beneficiari di assegni di cura

In applicazione del divieto di diffusione dei dati idonei a rivelare lo stato di salute, ribadito ora dal Codice (art. 22, comma 8, d.lg. n. 196/2003), il Garante ha prescritto di non affiggere, nei locali di un'azienda sanitaria locale, un elenco contenente alcuni dati personali dei beneficiari di assegni di cura. Anche l'indicazione negli elenchi delle sole iniziali dei beneficiari di tali assegni può infatti consentirne l'identificazione: quindi, le esigenze di pubblicità dell'amministrazione potevano essere ugualmente soddisfatte attraverso l'apposizione di diciture generiche o codici numerici (*Nota* 29 agosto 2003).

Si deve pure ricordare che, nell'ottobre del 2003, il Garante ha siglato un protocollo di intesa con l'Azienda ospedaliera universitaria "Policlinico Tor Vergata",

volto a sperimentare sul campo, in una struttura di recente creazione, l'applicazione della normativa a tutela della riservatezza nel settore sanitario.

A seguito dell'entrata in vigore del Codice, l'Autorità sta poi esaminando alcune questioni relative al trattamento dei dati effettuato per la tenuta e la gestione dei registri tumori: si deve, infatti, verificare in quale misura le operazioni connesse alla tenuta ed alla gestione di questi registri possano considerarsi comprese tra le attività di rilevante interesse pubblico individuate dal Codice (in particolare, dall'art. 98).

Ricerca scientifica

In materia di ricerca scientifica (oltre al codice deontologico su statistica e ricerca i cui lavori sono in fase di imminente conclusione), occorre ricordare che la disciplina di favore prevista per la ricerca in campo medico, biomedico ed epidemiologico è stata confermata dal Codice (art. 110 d.lg. n. 196/2003). Per il perseguimento di queste finalità è possibile utilizzare dati personali idonei a rivelare lo stato di salute degli interessati anche a prescindere dal consenso di questi ultimi, qualora la ricerca sia prevista da un'espressa previsione di legge che contempli specificamente il trattamento, o sia compresa in un programma di ricerca biomedica o sanitaria, e ne sia data previa comunicazione al Garante (art. 39 d.lg. n. 196/2003). A queste ipotesi il Codice aggiunge il caso in cui, per particolari ragioni, non sia possibile informare l'interessato e il programma di ricerca sia oggetto di parere favorevole da parte del competente comitato etico (nonché autorizzato dal Garante, anche con provvedimenti di carattere generale: art. 40 d.lg. n. 196/2003).

Per quanto concerne il trattamento dei dati personali dei soggetti sieropositivi, si è esaminata la questione dell'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 dell'Autorità.

Sul tema è stato costituito un gruppo di lavoro, in cui, oltre all'Autorità ed alla Commissione ora indicata, 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, in particolare, i presupposti che rendono lecito il trattamento dei dati personali dei sieropositivi, i dati utilizzati, i loro flussi e le modalità con le quali rendere l'informativa agli interessati nonché le misure di sicurezza da adottare.

Le novità introdotte dal d.l. 30 settembre 2003, n. 269 in tema di monitoraggio della spesa sanitaria hanno determinato l'attivazione dell'Autorità, con riferimento al complesso meccanismo che verrebbe basato su un modello di ricetta medica a lettura ottica e sulla costituzione di una o più banche dati.

Come già accennato, il Garante ha rilevato che la finalità di razionalizzazione del controllo della spesa sanitaria va perseguita nel pieno rispetto del diritto dei cittadini alla protezione dei dati personali, soprattutto in relazione alle informazioni riguardanti la salute. La banca (o le banche) dati di cui è prevista la realizzazione permetterebbe infatti di risalire, anche tramite il codice fiscale, all'identità dell'assistito ed all'intera sua storia sanitaria.

Ricordando che la legislazione vigente prevede già procedure di monitoraggio della spesa sanitaria che non richiedono banche dati nominative centralizzate,

l'Autorità ha precisato che l'unico sistema di controllo conforme alla normativa sulla protezione dei dati comporta l'esclusione del trattamento sistematico di qualsiasi informazione identificativa sullo stato di salute degli assistiti. Altrimenti, si correrebbe il rischio di introdurre nel sistema forme di discriminazione dei cittadini a vantaggio di chi sia in grado di pagare direttamente i farmaci e le prestazioni specialistiche (*Comunicato stampa* 28 ottobre 2003).

Anche a seguito delle indicazioni fornite dall'Autorità, il sistema di monitoraggio previsto dal decreto è stato però solo in parte modificato in sede di conversione (l. 24 novembre 2003 n. 236; cfr. *supra*, parag. 2., lett. *a)*).

L'attenzione si sposta ora, anche a seguito dei primi contatti intercorsi con il Ministero dell'economia e delle finanze, sulle modalità che verranno prescritte per la concreta applicazione del d.l. n. 269/2003.

Sono infatti previsti diversi decreti per l'attuazione delle relative disposizioni e l'Autorità svolgerà al riguardo i propri compiti istituzionali con ogni dovuta attenzione all'elevato livello di garanzia assicurato dal Codice e reso indispensabile anche dagli obblighi derivanti dal quadro comunitario e dalla giurisprudenza della Corte europea dei diritti dell'uomo a proposito dell'art. 8 della Convenzione sui diritti dell'uomo.

Tra le questioni all'avanzato studio dell'Autorità in materia di dati sulla salute, meritano di essere indicate le seguenti:

- utilizzo delle principali applicazioni telematiche (collegamenti ad Internet, *e-mail*, ecc.) e reti satellitari per i dati sulla salute, in particolare per l'offerta di servizi informativi sulle attività svolte da diverse strutture sanitarie, per la prenotazione di esami clinici e visite diagnostiche ed il rilascio dei relativi risultati, per le schede cliniche informatizzate, nonché per sistemi di teleconsulto, telediagnosi e telemedicina;

- trasmissione per via telematica all'Inps dei certificati di malattia predisposti da medici di medicina generale;

- valutazione delle procedure adottate dalle aziende sanitarie locali per il rilascio della tessera di esenzione dal pagamento del *ticket*.

Ispezioni svolte dal Garante in materia sanitaria

Tra le attività ispettive svolte dal Garante, di rilievo è anche quella effettuata in una struttura sanitaria presso cui erano state abbandonate numerose cartelle cliniche, immediatamente dopo le prime notizie di stampa e in collaborazione con la Guardia di finanza. L'Ufficio del Garante ha svolto un sostanziale ruolo di coordinamento degli interventi delle autorità locali, già avviati su indicazione della Procura della Repubblica di Lecce, allo scopo di verificare che il recupero e la conservazione delle cartelle cliniche avvenissero in modo idoneo ad evitare accessi non autorizzati ai dati personali in esse contenuti (ispezione presso un'ex colonia di Santa Maria di Leuca del 12 febbraio 2004).

Un'analoga vicenda si è verificata in Roma nel cortile di una biblioteca comunale, liberamente accessibile al pubblico, dove sono stati rinvenuti numerosi documenti sanitari (ricette e cartelle cliniche). Anche in questo caso il Garante ha otte-

nuto, subito dopo le segnalazioni di stampa, la rapida rimozione dei documenti, al fine di impedire la conoscibilità dei dati personali in essi contenuti da parte di terzi non autorizzati (ispezioni del 10 e 12 gennaio 2004).

È stato poi compiuto un terzo accertamento ispettivo nei confronti di un policlinico universitario, dove erano stati segnalati alcuni furti di *computer*. In questo caso, è stato tuttavia accertato *in loco* il rispetto della normativa sulla protezione dei dati personali e, in particolare, l'adozione delle "misure minime" di sicurezza (ispezione presso l'Azienda ospedaliera universitaria Policlinico Federico II).

Sempre con riferimento al trattamento dei dati in ambito sanitario, il Codice prevede modalità semplificate per l'informativa e l'acquisizione del consenso utilizzabili dai medici di medicina generale, dai pediatri di libera scelta e dagli organismi sanitari pubblici e privati. Al fine di agevolare l'applicazione di questa disciplina da parte degli operatori sanitari, il Garante completerà entro breve termine, in collaborazione con competenti organi rappresentativi, un modello semplificato di informativa utilizzabile anche dai medici e suggerirà formule sintetiche e colloquiali per raccogliere il consenso (lettera al Ministro della salute del 6 febbraio u.s.).

In materia di "misure minime" di sicurezza, l'Autorità presterà inoltre la propria collaborazione, all'interno di un gruppo di lavoro istituito con i rappresentanti degli operatori sanitari, per la redazione di un modello adattato di documento programmatico sulla sicurezza. Ulteriori chiarimenti e delucidazioni saranno, poi, fornite ai medici di medicina generale e ai pediatri a seguito del provvedimento del 31 marzo 2004 (su cui *supra*, parag. 12.) con cui il Garante ha introdotto alcune semplificazioni in materia di notificazione, che interessano, tra gli altri, gli operatori sanitari (*Nota* 1° aprile 2004).

Misure di carattere organizzativo

Oltre alle norme di semplificazione, il Codice detta alcune misure di carattere organizzativo intese a garantire il rispetto della dignità e degli altri diritti dell'interessato nella fornitura delle prestazioni e dei servizi sanitari, quali ad es. la cd. distanza di cortesia, la riservatezza nei colloqui e regole di condotta analoghe al segreto professionale per gli incaricati che non vi sono già sottoposti. Specifiche cautele sono poi previste per le informazioni identificative dell'assistito riportate sulle ricette mediche (art. 87 d.lg. n. 196/2003).

La necessità di rispettare tali garanzie è stata tenuta presente negli accertamenti avviati nei riguardi della prassi temporaneamente instaurata nella Regione Sicilia che, in attuazione di una legge regionale sull'introduzione di un sistema di esenzione del *ticket* basato sul reddito, ha adottato una procedura che rendeva conoscibili alcune informazioni personali relative a quanti intendessero usufruire dell'esenzione. In particolare, al momento dell'acquisto dei medicinali in farmacia, si richiedeva agli assistiti di autocertificare la propria situazione economica sul retro della ricetta.

Il Garante ha già completato le prime verifiche anche alla luce dell'analoga esperienza verificatasi in Abruzzo, che ha portato la relativa amministrazione regionale a modificare precedenti orientamenti.

Le libertà associative

14 Associazioni, movimenti politici e partiti

14.1. Associazioni

L'entrata in vigore del nuovo Codice ha interessato il settore delle associazioni con riferimento al trattamento sia dei dati comuni, sia dei dati sensibili.

Il consenso

Il trattamento di informazioni riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria non è più assoggettato alla specifica disciplina in materia di dati sensibili, fondata sul consenso scritto dell'interessato e sull'autorizzazione del Garante (art. 26, comma 3, lett. *b)*, d.lg. n. 196/2003).

Inoltre, le associazioni e gli organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale (inclusi i partiti o movimenti politici) non sono più tenuti ad acquisire il consenso degli aderenti o dei soggetti che, in relazione alle finalità statutarie perseguite, hanno contatti regolari con l'ente stesso, per poter trattare i loro dati sensibili. Tutto ciò, a patto che i dati non siano divulgati a terzi e l'associazione adotti idonee misure per la loro tutela, prevedendo modalità di utilizzo dei dati con una determinazione che deve essere resa nota agli interessati all'atto dell'informativa (art. 26, comma 4, lett. *a)*, d.lg. n. 196/2003).

Anche nel periodo considerato il Garante è stato chiamato ad occuparsi, sotto più profili, di questioni connesse al trattamento di dati personali da parte delle realtà associative.

Casistica

Tra i numerosi interventi dell'Autorità è da ricordare, in primo luogo, il caso della convenzione stipulata tra una confederazione sindacale ed un'associazione di consumatori, avente ad oggetto l'iscrizione promozionale all'associazione stessa, come soci aggregati, di persone appartenenti alle rappresentanze delle varie organizzazioni aderenti alla confederazione sindacale. Si è rilevato in proposito che la convenzione non aveva comportato una comunicazione diretta e automatica dei dati personali dei potenziali soci aggregati dalla confederazione sindacale all'associazione dei consumatori, e che la raccolta di tali dati sarebbe potuta avvenire solo su iniziativa di ciascun interessato, al momento dell'eventuale richiesta di adesione all'associazione dei consumatori. Inoltre, si è richiamata l'attenzione sulla necessità di integrare l'informativa resa agli interessati, in modo da rendere più chiari gli elementi caratterizzanti il trattamento.

Un altro caso significativo ha riguardato la richiesta, avanzata da un'associazione di categoria, di autorizzazione al trattamento dei dati sensibili relativi alla salute della clientela degli associati; in tale occasione –come già in vicende analoghe– la richiedente è stata invitata a verificare se i trattamenti effettuati non rientrassero tra quelli già autorizzati dal Garante in via generale e, in caso contrario, ad indicare le circostanze del tutto particolari o le situazioni eccezionali in base alle quali si sarebbe resa eventualmente necessaria un'autorizzazione specifica.

14

Infine, l'Ufficio si è occupato della richiesta di utilizzo dei dati degli associati ad una federazione sportiva per finalità di propaganda elettorale, in vista delle elezioni degli organi di vertice della federazione.

Al riguardo, premesso che l'attuale natura privatistica delle federazioni sportive (come stabilita dal d.lg. n. 242/1999) non consentiva di applicare alla vicenda le norme sul trattamento dei dati personali da parte degli enti pubblici, si è chiarito che occorreva individuare uno dei presupposti di liceità che la legge prevede per il trattamento dei dati da parte di soggetti privati: quindi, il consenso informato e specifico per tale operazione di trattamento (in relazione allo statuto o all'atto costitutivo), oppure uno degli altri presupposti di legge.

14.2. Movimenti politici e propaganda elettorale

Nel periodo considerato sono state analizzate problematiche assai rilevanti per il settore in esame, in connessione anche con alcuni appuntamenti elettorali.

In particolare, durante la campagna elettorale svoltasi per le elezioni amministrative tenute in alcune regioni italiane nell'estate del 2003, sono pervenute varie segnalazioni aventi ad oggetto l'invio di comunicazioni elettorali a clienti di società, da parte di dipendenti, collaboratori o agenti delle società stesse, candidati alle elezioni o comunque sostenitori di candidati.

In tali casi, in accordo con l'orientamento già espresso in precedenti occasioni dal Garante (cfr. *Provv.* 7 marzo 2001; *Provv.* 9 ottobre 2000), va rilevato che per l'uso a fini di propaganda elettorale dei dati anagrafici raccolti presso banche dati pubbliche, registri o elenchi conoscibili da chiunque, deve essere fornita una chiara informativa agli interessati.

Il provvedimento del Garante del 12 febbraio 2004

Di recente il tema è stato già affrontato in termini generali nel provvedimento del Garante del 12 febbraio 2004 (pubblicato in *Gazzetta Ufficiale* 24 febbraio 2004, n. 45, e riportato negli allegati alla presente *Relazione*), che ha individuato i presupposti, le garanzie e i limiti per l'utilizzo di liste e indirizzari formati anche nell'ambito della prestazione di attività e servizi, al fine di inviare note di propaganda a favore di candidati interni o sostenuti da società, enti o associazioni.

In particolare, in vista delle consultazioni elettorali europee ed amministrative indette per il 12 e 13 giugno prossimi, il Garante, nel provvedimento del 12 febbraio 2004, ha indicato i casi in cui partiti, movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare dati personali a fini di propaganda elettorale a prescindere dal consenso degli interessati, fornendo loro un'adeguata informativa. Tale ipotesi può ricorrere quando si utilizzano dati 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. Si tratta, ad esempio, delle liste elettorali comunali, degli elenchi di iscritti ad albi e collegi professionali, dell'elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo, delle cd. liste aggiunte dei cittadini elettori di uno Stato membro dell'Ue, dell'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle relative liste elettorali e di quello degli aventi diritto al voto per l'elezione dei Comites (su cui cfr. *infra*, parag. 21.).

I dati estratti dagli elenchi della telefonia fissa possono essere invece trattati a fini di propaganda elettorale sotto forma di invio di posta ordinaria o di chiamate telefoniche effettuate da un operatore, a meno che gli interessati non si siano opposti. Fuori da ipotesi di questo tipo, non è possibile svolgere attività di propaganda politica senza un consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente gli scopi per i quali i dati sono utilizzati. Ciò, in particolare, quando si ricorra all'invio di fax, di messaggi *Sms* e *Mms*, o di *e-mail*, nonché a chiamate telefoniche senza l'intervento di un operatore oppure a chiamate a terminali di telefonia mobile.

Quando si utilizzano dati di iscritti ad associazioni politiche o a partiti, il consenso specifico deve essere manifestato per iscritto, versandosi in un caso di trattamento di dati di tipo sensibile (v., per altro, quanto previsto dagli artt. 26, comma 4, lett. *a)* e 181, comma 1, lett. *b)* del Codice). L'utilizzazione di dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politica è possibile invece solo quando sia disposta legittimamente in base all'ordinamento interno, le modalità di utilizzo dei dati a fini di propaganda siano compatibili con gli scopi principali perseguiti dall'associazione e ne venga fatta menzione nell'informativa resa agli iscritti al momento dell'adesione o del suo rinnovo.

Il Garante ha anche precisato che i titolari di alcune cariche elettive non sono legittimati ad ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per la propaganda anche dopo la scadenza dal mandato; gli stessi possono però utilizzare i dati personali raccolti direttamente, nel quadro delle relazioni interpersonali con cittadini ed elettori.

In ogni caso, l'informativa che chi svolge attività di propaganda elettorale è tenuto a rendere agli interessati deve essere inserita nel materiale di propaganda e può essere resa anche in forma sintetica. Limitatamente alle imminenti consultazioni elettorali, il Garante ha tuttavia esonerato a date condizioni dall'obbligo di fornire l'informativa i soggetti che utilizzano dati personali per esclusivi fini di propaganda, ritenendo tale adempimento sproporzionato nel caso in cui i dati siano estratti da elenchi pubblici e gli interessati non vengano poi contattati, nonché quando il materiale propagandistico sia di dimensioni talmente ridotte da non permettere di inserire agevolmente l'informativa (art. 13, comma 5, d.lg. n. 196/2003).

Uso dei dati a fini promozionali e commerciali

Particolare attenzione è stata prestata al requisito della specificità del consenso richiesto per l'uso dei dati a fini promozionali e commerciali e alla necessità che eventuali utilizzi ulteriori per fini di propaganda politica siano indicati in tali consensi in modo univoco. Il problema è stato affrontato anche successivamente su richiesta della Federazione delle concessionarie di pubblicità e di un operatore del settore ai quali, con note del 25 marzo e del 6 aprile 2004, sono state rappresentate le necessarie garanzie che consentono o precludono l'invio di *e-mail* di propaganda o l'inserzione di pubblicità elettorale all'interno di *newsletter* richieste dagli interessati per altri fini.

14.3. Confessioni religiose

Per quanto riguarda il trattamento di dati sensibili in ambito religioso, occorre sottolineare l'importante novità normativa introdotta sul punto dal Codice.

Nel sistema previgente, in parziale applicazione dei principi comunitari in materia di associazioni e di altri organismi senza scopo di lucro, era infatti prevista una disciplina particolare per la Chiesa cattolica e per le altre confessioni religiose che avessero stipulato accordi o intese con lo Stato italiano.

Questa disciplina si basava sulla possibilità di prescindere dal consenso degli interessati e dal rispetto dell'autorizzazione del Garante per trattare i dati sensibili degli aderenti e degli altri soggetti che avessero contatti regolari con le confessioni, purché fossero rispettate certe condizioni, tra le quali l'osservanza di idonee garanzie che le confessioni stesse avrebbero dovuto introdurre nei propri ordinamenti.

La modifica introdotta dal Codice

Il Codice estende ora questa specifica disciplina alle altre confessioni religiose, purché i dati non siano diffusi o comunicati al di fuori delle confessioni e vengano osservate idonee garanzie di cui le stesse devono dotarsi, nel rispetto dei principi contenuti in un'autorizzazione del Garante (art. 26, comma 3, lett. *a)*, d.lg. n. 196/2003).

L'art. 181, comma 6, del d.lg. n. 196/2003 consente poi alle confessioni religiose che, prima dell'entrata in vigore del Codice, abbiano già adottato le garanzie richieste nell'ambito dei propri ordinamenti, di proseguire il trattamento nel rispetto delle medesime.

Nella materia in esame, il Garante ha tra l'altro affrontato la questione del trattamento di dati idonei a rivelare convinzioni religiose, effettuato da un'associazione per avviare le pratiche di annullamento di matrimoni religiosi. In proposito, l'Autorità ha ribadito che i dati raccolti dovevano essere trattati soltanto per le procedure rivolte all'accertamento della nullità del matrimonio davanti al tribunale ecclesiastico e non anche per scopi ulteriori (*Nota* 10 aprile 2003).

I registri dei battezzati

Nel corso del 2003 sono anche pervenuti ricorsi e segnalazioni tesi ad ottenere l'aggiornamento e l'integrazione di dati personali contenuti nei registri dei battezzati presenti negli archivi parrocchiali, con specifico riferimento al dato sull'appartenenza religiosa degli interessati che non risulti più rispondente alla realtà.

Al riguardo, il Garante ha confermato la legittimità delle richieste intese a far annotare, a margine del dato da aggiornare, la volontà degli interessati di non appartenere più alla Chiesa cattolica, reputando l'annotazione compatibile con la necessaria documentazione del fatto storico dell'avvenuto battesimo.

L'Autorità ha poi chiarito che la conservazione dell'istanza presentata dall'interessato in allegato al registro dei battesimi non è sufficiente a far risultare in modo inequivoco e permanente la volontà del medesimo interessato di non appartenere più alla Chiesa cattolica. In presenza di una richiesta di integrazione e aggiornamento del dato relativo all'appartenenza religiosa, occorre quindi effettuare un'apposita annotazione a margine sul registro dei battesimi (*Provv.* 19 marzo 2003).

In una decisione su un ricorso, l'Autorità ha infine precisato che, per presentare la richiesta finalizzata ad aggiornare ed integrare i dati personali del richiedente con spe-

cifico riferimento al dato relativo all'appartenenza religiosa, non è necessario recarsi personalmente presso determinati uffici (ad esempio, quelli del Vicariato) al fine di dimostrare e controfirmare la dichiarazione di non voler essere più considerato appartenente alla Chiesa cattolica. La normativa sulla protezione dei dati personali non prevede, infatti, che il richiedente debba presentarsi di persona presso la sede del titolare per esercitare i propri diritti e, nel caso esaminato, confermare la menzionata volontà. È stata invece ritenuta legittima ogni eventuale attività della Curia volta a richiamare l'attenzione dell'interessato sugli effetti che l'istanza produce (*Newsletter* 10-16 novembre 2003).

In tema di questioni concernenti il trattamento dei dati religiosi, l'Autorità si sta occupando anche del regime di pubblicità delle anagrafi parrocchiali e della raccolta di dati idonei a rivelare convinzioni religiose in occasione di visite specialistiche o ricoveri ospedalieri.

La libertà di informazione

15 Attività giornalistiche e mezzi di informazione

Continuano a pervenire numerosi quesiti, segnalazioni e reclami in ordine alle problematiche relative al trattamento di dati personali effettuato nell'esercizio dell'attività giornalistica. Parallelamente è cresciuta, nei confronti di tali temi, l'attenzione degli operatori dell'informazione, che hanno interpellato il Garante chiedendo chiarimenti sul corretto utilizzo delle informazioni, nel quadro delle vigenti norme in materia di protezione dei dati personali e del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*Provv.* 29 luglio 1998, in *Gazzetta Ufficiale* 3 agosto 1998, n. 179).

Nel corso dell'anno è stato avviato un nuovo confronto tra il Garante ed il Consiglio nazionale dell'ordine dei giornalisti. In tale contesto, si è costituito un gruppo di lavoro comune incaricato, tra l'altro, di elaborare documenti utili a fornire un concreto contributo al lavoro di chi opera nel mondo dell'informazione e ad esaminare alcuni aspetti applicativi del d.lg. n. 196/2003. Sulla base dei primi spunti di riflessione pervenuti dall'ordine, il Garante ha fornito da ultimo un quadro di approfondite indicazioni circa la liceità e la correttezza della raccolta e diffusione di specifiche fonti di informazione.

Allo scopo di dare un utile riscontro a tale accresciuta attenzione, il Garante ha poi pubblicato una raccolta dei più significativi provvedimenti adottati dall'Autorità in materia di giornalismo e tutela dei dati personali. Il volume, curato da Mauro Paissan, componente del collegio, è stato presentato a Roma il 6 novembre 2003 alla presenza del Presidente della Camera e di diversi esponenti del mondo politico e dell'informazione. La raccolta –organizzata per macroargomenti (tutela dei minori, rapporti tra cronaca e giustizia, uso dei dati relativi a personaggi pubblici, trasparenza delle fonti pubbliche, tutela dei dati relativi alla salute ed alla sfera sessuale, uso di fotografie)– è preceduta da un quadro di sintesi delle disposizioni del codice di deontologia dei giornalisti e da una generale riflessione del curatore dell'opera sulle principali problematiche che emergono nella delicata opera di bilanciamento tra tutela della persona e libertà di manifestazione del pensiero (cfr. pure *infra*).

15.1. Tutela dei minori

Il Garante è nuovamente intervenuto a tutela dei diritti dei minori coinvolti in fatti di cronaca, vietando, tra l'altro, con un provvedimento d'urgenza diretto a diversi editori e direttori di quotidiani, nazionali e locali, l'ulteriore diffusione di informazioni relative a due bambini vittime di atti di violenza. Nel caso di specie, pur non essendo stata resa apertamente nota l'identità dei minori e dei genitori, sono state diffuse varie informazioni (tra cui anche la foto segnaletica dell'adulto ritenuto responsabile di dette violenze) giudicate, oltre che eccedenti e non indispensabili a rappresentare la vicenda, tali da rendere comunque immediatamente riconoscibili i minori all'interno della cerchia familiare, degli amici e dei conoscenti. In questo modo risultavano violate le garanzie normative, nazionali e internazionali (art. 13

della Convenzione sui diritti del fanciullo; art. 734-*bis* c.p.; art. 13 d.P.R. 22 settembre 1988 n. 448; art. 7 codice deontologico; Carta di Treviso) poste a tutela della sfera privata dei minori, riaffermate ed ampliate anche dal Codice (artt. 50 e 52).

La vicenda presenta sviluppi ancora in fase di svolgimento, come dimostrano, ad esempio, le note con le quali il direttore di una delle testate oggetto di divieto, si è poi attivato per prevenire analoghe infrazioni, mentre un consiglio dell'ordine locale ha chiesto al Garante di fornire i nomi dei giornalisti autori degli articoli pubblicati ai fini della loro convocazione.

15.2. Foto segnaletiche e cronache giudiziarie

L'Autorità è intervenuta in maniera incisiva nei confronti della prassi diffusa presso organi di informazione di pubblicare fotografie di persone arrestate o indagate.

Il provvedimento del Garante del 19 marzo 2003

È stata più volte riscontrata la violazione degli specifici divieti, riaffermati anche dal codice deontologico per l'attività giornalistica, a tutela delle persone coinvolte nei fatti oggetto della notizia. Il Garante ha osservato che, fermo restando il divieto di pubblicare immagini di persone con ferri o manette ai polsi, ovvero sottoposte ad altri mezzi di coercizione fisica, senza il consenso dell'interessato, la diffusione di fotografie di individui in stato di detenzione è ammessa solo per comprovati fini di giustizia e di polizia e in ogni caso nel rispetto della dignità personale (*Provv.* 19 marzo 2003). Limitatamente ad una delle testate interessate dal divieto, il provvedimento è stato caducato con decreto del 26 giugno 2003 del Tribunale di Milano, dinanzi al quale era stata proposta la relativa impugnazione. Il tribunale, pur ritenendo in punto di fatto non interamente comprovata la constatazione dell'Autorità (provenienza delle immagini da foto "segnaletiche" oppure da documenti di identità) e quindi accogliendo il ricorso, ha comunque confermato il principio di diritto affermato dal Garante, in base al quale, come si è detto, la diffusione di fotografie riguardanti persone sottoposte a misure restrittive della libertà personale è ammessa, in mancanza del consenso delle persone ritratte, per il perseguimento di esclusive finalità di giustizia e di polizia e nel rispetto della disposizione del codice deontologico sull'attività giornalistica (art. 8) che vieta le riprese in stato di detenzione.

Tale principio è stato ribadito di recente con riguardo alla diffusione di foto "segnaletiche" di alcune persone coinvolte in un'indagine su stupefacenti e prostituzione avviata dalla magistratura romana (*Provv.* 26 novembre 2003). In questo caso l'Autorità, rilevando l'assenza dei presupposti di legge, ha vietato l'utilizzazione delle foto "segnaletiche" ed ha segnalato al Capo della polizia le illiceità rilevate. Ha inoltre provveduto a richiedere informazioni agli uffici di polizia interessati dalle operazioni di trattamento oggetto del divieto, anche con riferimento alla diffusione di altri dati (dettagli relativi al contenuto di conversazioni telefoniche, estremi identificativi di utenze telefoniche) inerenti all'indagine in corso.

In relazione alle problematiche generali riguardanti le cronache giudiziarie, l'Autorità ha più volte ricordato agli organi di informazione che l'esigenza di informare l'opinione pubblica su vicende giudiziarie non deve recare pregiudizio alla vita privata delle persone. Ha quindi ribadito che la diffusione di tale tipo di informazioni, anche in mancanza del consenso dell'interessato, non è preclusa; deve tuttavia essere assicurato il rispetto dei limiti previsti per l'esercizio del diritto di cronaca, in particolare quello dell'essenzialità dell'informazione riguardo a fatti di interesse

pubblico, oltre che l'osservanza degli specifici divieti posti dagli ordinamenti penale e processualpenale.

15.3. Privacy dei personaggi pubblici

Il Garante, con una decisione adottata su ricorso, ha rilevato i limiti entro cui può considerarsi legittima l'informazione su fatti di cronaca coinvolgenti persone che godono di una certa notorietà in ragione del ruolo o della funzione ricoperti. Un caso ha riguardato, ad esempio, il trattamento di dati relativi ad un ingegnere, noto in ambito locale per la sua attività di progettista e direttore dei lavori di un piano di riassetto territoriale. L'Autorità ha ritenuto lecita la pubblicazione dei dati relativi alla posizione del professionista, ai suoi impegni e agli onorari percepiti, in ragione della rilevanza pubblica della notizia (giustificata anche da esigenze di trasparenza sull'utilizzo del denaro pubblico), nonché della notorietà del ricorrente, impegnato a vario titolo e con ruoli di responsabilità in un'operazione urbanistica ed economica di primario rilievo locale. Si è ritenuto invece che fosse fonte di illiceità sia la diffusione, nell'ambito dello stesso servizio giornalistico, di dati attinenti alla sfera privata ed allo stato salute del ricorrente (disagi psicologici per i quali era ricorso ad una specifica terapia psicoanalitica), sia il collegamento effettuato con le vicende personali del fratello, in gravi condizioni di salute psicofisica. In tale caso il Garante ha pure prescritto all'editore di unire copia della propria decisione inibitoria agli esemplari del servizio giornalistico oggetto della decisione, conservati presso lo stesso editore, e di dare conferma all'Autorità dell'avvenuto adempimento (*Provv.* 29 dicembre 2003).

La Dichiarazione del Consiglio d'Europa del 12 febbraio 2004

I principi richiamati dal Garante trovano conferma nella Dichiarazione del Consiglio d'Europa del 12 febbraio 2004, nella quale viene precisato, fra l'altro, come l'esigenza di bilanciare libertà di espressione e diritto al rispetto per la vita privata imponga di non rivelare particolari della vita privata delle figure pubbliche, a meno che tali informazioni non siano di diretto interesse pubblico per le modalità con cui tali soggetti svolgono o hanno svolto le funzioni alle quali sono state chiamati, e venga tenuta in debita considerazione la necesssità di non danneggiare terze persone.

La Decisione della Corte europea dei diritti dell'uomo sul "caso Craxi"

Da ultimo merita di essere ricordato che, nella nota vicenda relativa all'On. Bettino Craxi, l'Italia è stata condannata dalla Corte europea dei diritti dell'uomo di Strasburgo per violazione del diritto al rispetto della vita privata sancita dall'art. 8 della Convenzione europea dei diritti dell'uomo (Decisione 17 luglio 2003). La vicenda concerneva la diffusione di contenuti di intercettazioni telefoniche a carattere personale relative a conversazioni intrattenute dal *leader* del Partito socialista italiano nell'ambito di un procedimento penale a suo carico presso il Tribunale di Milano. I contenuti delle intercettazioni e i nomi degli interlocutori, infatti, erano stati letti in udienza dal pubblico ministero e successivamente diffusi dai giornali.

La Corte europea ha osservato che, nel caso in esame, le autorità italiane non hanno tutelato la riservatezza delle intercettazioni, né hanno svolto indagini efficaci sulle modalità con cui le conversazioni telefoniche private sono divenute di pubblico dominio. Secondo la Corte, inoltre, nell'ambito del processo, si sarebbe dovuto provvedere, in sede di udienza preliminare, ad escludere i passaggi delle conversazioni non necessari ai fini del procedimento. La pubblicazione degli stralci di inter-

cettazioni a contenuto strettamente personale, infine, è apparsa non necessaria rispetto alla legittima finalità di informare il pubblico.

15.4. Essenzialità dell'informazione

Anche nel periodo considerato, il Garante ha riscontrato violazioni delle norme deontologiche in relazione alla diffusione, nel contesto di una notizia di possibile rilevanza generale, di dati personali non essenziali, eccedenti e non pertinenti rispetto alla finalità del trattamento. In particolare, nel caso di un giornale che, riferendo di un delitto commesso in un appartamento, aveva pubblicato le generalità di colui che risultava essere proprietario dell'immobile, il Garante ha ritenuto insussistenti i presupposti –originalità del fatto, descrizione dei modi particolari in cui è avvenuto e qualificazione dei protagonisti (art. 6, comma 1, codice deontologico)– che consentono la divulgazione di informazioni anche dettagliate (*Provv.* 23 gennaio 2003).

Pure nella vicenda di un'emittente radiofonica che, commentando l'operato di un'agente della polizia municipale, ha diffuso, oltre alle generalità dell'agente, altri dettagli (e cioè l'età, il comune di residenza, l'indirizzo, nonché i nomi dei suoi genitori) si è constatata l'inosservanza del principio di non eccedenza rispetto al legittimo esercizio del diritto di critica e di cronaca sulla vicenda (*Nota* 23 febbraio 2004).

15.5. Dati idonei a rivelare lo stato di salute ovvero le opinioni politiche o filosofiche

Ripetuti sono stati i richiami del Garante al rispetto delle specifiche garanzie a tutela della riservatezza e della dignità delle persone malate, dettate dal codice deontologico per l'attività giornalistica (artt. 5 e 10). Ne è esempio emblematico la vicenda, di ampio clamore nei *media*, che ha avuto come protagonista una donna rifiutatasi di sottoporsi ad un intervento chirurgico ad una gamba ritenuto dai medici necessario per salvarle la vita. In tale occasione il Garante ha richiamato gli organi di informazione alla salvaguardia della dignità della persona malata, nonché al rispetto delle esigenze di riservatezza espresse dalla sua famiglia. L'Autorità ha inoltre evidenziato come la diffusione di indirizzi e dati personali dell'interessata, e l'insistenza nella ricerca di particolari sulla vicenda, finisse per lederne non solo la riservatezza, ma la stessa libertà di autodeterminazione nel maturare in silenzio e tranquillità una difficile scelta personale (cfr. *Comunicato stampa* 3 febbraio 2004).

Il Garante è stato chiamato ad occuparsi anche della pubblicazione –su taluni quotidiani e riviste– di elenchi di iscritti ad associazioni massoniche, nonché di altre informazioni ad essi relative (luogo di residenza e professione). Al riguardo, sono state chieste informazioni ai responsabili dei giornali, al fine di valutare la liceità e correttezza del trattamento, in special maniera sotto il profilo dell'essenzialità dei dati personali diffusi rispetto alla finalità di informare su fatti di interesse pubblico (*Note* 13 agosto 2003).

15.6. Esercizio dei diritti e giornalismo on line

Come già accennato più sopra (cfr. parag. 7.11.), il Garante ha chiarito che i diritti spettanti agli interessati in base all'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) possono essere esercitati anche laddove il trattamento consista nella diffusione di fotografie e di altri dati personali attraverso pubblicazioni consultabili tramite Internet.

15

In particolare, nell'esaminare due ricorsi concernenti la stessa pubblicazione disponibile anche via *web*, nei quali le ricorrenti contestavano l'autenticità delle dichiarazioni di consenso acquisite dalla società che aveva originariamente raccolto i dati, il Garante ha posto l'accento sulla necessità che l'editore si accerti della genuina identità degli inserzionisti e dell'affidabilità del materiale informativo che intende utilizzare. L'Autorità ha ritenuto pertanto necessario approfondire in altra sede i presupposti di liceità del trattamento effettuato dall'editore e dalle altre società coinvolte nella vicenda.

Pubblicazione occasionale di articoli o saggi

La diffusione di dati personali tramite siti Internet può essere effettuata anche nell'ambito di attività di manifestazione del pensiero diverse dal giornalismo, compiute da soggetti che non esercitano professionalmente l'attività giornalistica, ma finalizzate anch'esse alla pubblicazione o diffusione occasionale di articoli, saggi ed altre manifestazioni del pensiero. Ai trattamenti di dati svolti nell'ambito di queste attività, secondo la disciplina della legge n. 675/1996 confermata dal Codice, si applicano le disposizioni previste per l'attività giornalistica. Si tratta di regole semplificate in materia di informativa e consenso, nonché di altre prescrizioni, contenute anche nel codice deontologico, volte a contemperare i diritti della persona con il diritto all'informazione ed alla libertà di espressione. Il principio è stato ribadito dall'Autorità nell'esaminare un ricorso relativo ad una vicenda in cui la pubblicazione di dati personali via *web* era stata effettuata tramite la riproduzione di una pagina originariamente creata dal ricorrente (*Provv.* 16 gennaio 2004). Il Garante ha inoltre precisato che la medesima disciplina è applicabile anche alla diffusione di dati derivanti da attività che si caratterizzano come modalità di esercizio del diritto di critica, con riferimento a personaggi conosciuti nell'ambito della "rete" (*Provv.* 10 dicembre 2003).

La libertà di iniziativa economica

16 Settore del credito finanziario e assicurativo

16.1. Credito

Nel 2003 il settore del credito è stato oggetto di particolare attenzione da parte del Garante, in special modo a seguito dei numerosi ricorsi, segnalazioni e reclami da parte di clienti di istituti di credito e di associazioni di consumatori, concernenti specialmente l'impropria divulgazione di dati personali da parte di uffici o dipendenti di banche.

Diversi cittadini si sono ad esempio lamentati delle particolari modalità con cui sono stati contattati telefonicamente da impiegati di istituti bancari per esigenze connesse allo svolgimento del rapporto bancario. In varie occasioni, infatti, addetti di istituto di credito, per mezzo del telefono, hanno comunicato a persone diverse dal diretto interessato informazioni relative al rapporto in essere o hanno addirittura sollecitato la regolarizzazione di situazioni di sofferenza, anche di lieve entità.

In altri casi, alcuni clienti hanno lamentato l'invio di comunicazioni bancarie in busta aperta (che ne ha reso conoscibile il contenuto da parte di terzi), oppure l'erroneo invio ad estranei di comunicazioni bancarie relative invece ai segnalanti e ad altri clienti.

In merito alle predette vicende, l'Autorità ha sottolineato in varie occasioni la necessità, per gli istituti di credito, di impartire precise istruzioni ai propri dipendenti ed incaricati e di predisporre apposite procedure per limitare al minimo indispensabile la divulgazione anche accidentale a terzi di dati personali dei clienti, non necessari per espletare le comunicazioni bancarie.

Per ciò che concerne, invece, l'esercizio dei diritti previsti dall'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice), le questioni più rilevanti affrontate dall'Autorità nel settore del credito, anche in relazione alle novità normative, hanno riguardato il diritto di accesso ai dati personali del defunto e la gratuità dell'accesso, come già illustrato nella parte di questa *Relazione* specificamente dedicata al diritto di accesso ai dati personali (v. *supra*, parag. 7.7.).

16.2. Intermediazione finanziaria

Anche il settore dell'intermediazione finanziaria ha visto presentare, nel 2003, vicende di rilevante interesse per l'Autorità.

Trattamento di dati da parte di promotore finanziario

In particolare, merita di essere ricordato un caso che ha riguardato il trattamento di alcuni dati personali (compresi quelli relativi a rapporti bancari e finanziari) da parte di un promotore finanziario, pure incaricato in termini generali del trattamento da parte della banca titolare. Il promotore ha trattato i dati in discorso prima

16

che gli fosse formalmente richiesto di curare clienti già seguiti da altri promotori. Questo trattamento era finalizzato alla presa di contatto con i clienti per conto della banca, così da consentire la continuità del rapporto contrattuale.

In tale occasione il Garante ha segnalato alla banca la necessità e l'urgenza di specificare meglio ai promotori finanziari della propria rete di distribuzione l'ambito e le modalità del trattamento nella fase antecedente alla formale assegnazione dei clienti già seguiti da altri promotori, assicurando la puntuale osservanza delle istruzioni e dei compiti impartiti in proposito e rispettando i principi di necessità e pertinenza. L'Autorità ha inoltre prescritto alla banca di fornire ai clienti maggiori chiarimenti in ordine all'ambito ed alle modalità del trattamento in questione, con particolare riferimento alla possibile comunicazione dei loro dati personali ad un promotore finanziario, anche prima della sua formale investitura, nonché al ruolo rivestito dal promotore medesimo in tale fase.

16.3. "Centrali rischi" e società finanziarie

Nel 2003 si è registrato un ulteriore e significativo incremento delle istanze riguardanti il trattamento di dati personali relativi a richieste o a rapporti di finanziamento da parte di banche, società finanziarie e "centrali rischi" private. I numerosi ricorsi, segnalazioni e reclami hanno messo in luce soprattutto il mancato rispetto dei principi e degli obblighi richiamati nel provvedimento generale adottato in materia dal Garante il 31 luglio 2002.

La delicata materia del trattamento dei dati relativi ai sistemi di informazione gestiti da soggetti privati, ed utilizzati per il rilascio di crediti al consumo e la valutazione dell'affidabilità e puntualità nei pagamenti, è destinata a trovare nel più breve periodo una compiuta regolamentazione con il codice deontologico di cui è imminente la sottoscrizione.

Il codice deontologico

I lavori di tale codice hanno richiesto un notevole impegno soprattutto per la definizione dello schema delle nuove regole di comportamento che, dopo un ampio confronto con gli operatori interessati, è stato sottoposto alle valutazioni di soggetti e organismi controinteressati, in particolare delle associazioni dei consumatori e degli altri soggetti partecipanti ai lavori del codice. Lo schema, dopo la temporanea diffusione del suo contenuto anche tramite il sito *web* del Garante, verrà presto formalmente sottoscritto.

Le linee essenziali del codice deontologico riguarderanno in particolare:

- l'ambito soggettivo, con la precisazione delle categorie degli enti partecipanti e delle modalità con le quali gli stessi potranno accedere caso per caso alle singole tipologie di informazioni;

- le modalità con cui viene resa l'informativa agli interessati e le procedure adottate per consentire loro l'esercizio dei diritti di accesso e degli altri diritti ora previsti dall'art. 7 del Codice (d.lg. n. 196/2003);

- le modalità di trattamento relative all'utilizzo di tecniche o sistemi cd. di *credit scoring*, nonché le misure di sicurezza adottate per la protezione dei dati e dei sistemi informativi;

- i tempi di conservazione dei dati nei sistemi di rilevazione del rischio creditizio, con particolare attenzione alla distinzione tra le informazioni di tipo positivo e i cd. dati negativi (relativi, ad esempio, a morosità o sofferenze), nel rispetto dei principi in tema di consenso degli interessati e relativi casi di esclusione (tra cui, il bilanciamento degli interessi: v. art. 24, lett. *g)*, d.lg. n. 196/2003).

I cd. dati negativi

Proprio con riferimento a quest'ultimo aspetto, l'Autorità, a seguito dei ricorsi presentati da alcuni consumatori, ha ribadito la necessità di cancellare entro un anno dall'avvenuta regolarizzazione le segnalazioni relative a "sofferenze" successivamente sanate senza alcuna perdita per l'ente finanziatore, confermando l'illiceità di ogni ulteriore conservazione dei dati relativi a finanziamenti così estinti da un termine più lungo.

Cancellazione delle "sofferenze"

Non è stata poi ritenuta conforme ai principi espressi nel citato provvedimento generale del luglio 2002 l'annotazione da parte di una società, in via temporanea, della dicitura "regolarizzato", accanto al nominativo della ricorrente, per documentare l'integrale estinzione del debito: anche in tal caso si deve comunque procedere alla cancellazione integrale dei dati relativi a ritardi di pagamento regolarizzati senza debiti residui, che non possono essere ulteriormente conservati rispetto ai tempi indicati dal Garante (*Provv.* 12 marzo 2003 e 5 novembre 2003).

Il "diritto all'oblio" per i dati positivi

È stata quindi affrontata la questione della conservazione ed ulteriore comunicazione dei dati cd. positivi, che evidenziano un andamento regolare dei pagamenti degli interessati. Anche per questo tipo di dati è stato rivendicato il "diritto all'oblio": nelle decisioni adottate a seguito dei numerosi ricorsi presentati in proposito, si è confermato che, a prescindere dalla mancanza di specifiche annotazioni "negative" per l'interessato, i dati riferiti a tali posizioni estinte da tempo non possono essere ulteriormente trattati in assenza di un idoneo presupposto del trattamento, e in particolare del consenso dell'interessato (*Provv.* 5 novembre 2003 e 22 dicembre 2003).

Nonostante quanto puntualmente indicato nel citato provvedimento del 2002, la condotta di alcune finanziarie o "centrali rischi" private non è risultata in vari casi conforme alle relative prescrizioni e ciò ha determinato l'accoglimento anche parziale di innumerevoli ricorsi che continuano a caratterizzare buona parte del contenzioso pendente presso il Garante. L'Autorità si è anche costituita in giudizio in tutti i procedimenti instaurati dai predetti operatori allorché questi hanno impugnato decisioni del Garante, e seguirà con estrema attenzione l'affermazione dei principi di diritto già evidenziati, confidando comunque che il nuovo codice deontologico possa porre rapidamente fine in modo condiviso ad un quadro che non è ancora tranquillizzante per i cittadini interessati.

Comunicazione dei dati alla centrale rischi gestita dalla Banca d'Italia

Numerose sono state le istanze relative alle segnalazioni obbligatorie effettuate da banche e società finanziarie, anche a quelle riguardanti il sistema di centralizzazione dei rischi gestito dalla Banca d'Italia. In particolare, è stata lamentata la comunicazione di dati effettuata da parte di alcuni istituti di credito a tale centrale, erroneamente inseriti nella categoria di censimento "sofferenze". L'Autorità ha osservato che la comunicazione, da parte delle banche, alla centrale rischi gestita dalla Banca d'Italia dei dati di clienti relativi all'indicazione di un particolare stato contabile del rapporto, come quello ascrivibile alla categoria di "sofferenza", deve essere effettuata attenendosi scrupolosamente a quanto prescritto dalla stessa Banca d'Italia nelle

proprie istruzioni rivolte agli intermediari creditizi. In particolare, le istruzioni prevedono che la segnalazione di una sofferenza sia preceduta da un'attenta valutazione, da parte dell'intermediario, della complessiva situazione finanziaria del cliente e non possa invece scaturire automaticamente da un mero ritardo nei pagamenti.

In base a tali considerazioni, l'Autorità ha pertanto sollecitato gli istituti di credito ad adottare misure ed accorgimenti, anche organizzativi, idonei ad assicurare il pieno rispetto dei principi di correttezza, pertinenza e non eccedenza dei dati, nonché delle istruzioni per gli intermediari creditizi impartite dalla Banca d'Italia, in relazione alla comunicazione dei dati alla centrale rischi gestita da quest'ultima.

16.4. Anagrafe degli assegni bancari e postali

Anche l'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento istituito ai sensi della legge n. 205/1999 e del d.lg. n. 507/1999 presso la Banca d'Italia, e in funzione dal giugno 2002, è interessato dalle novità introdotte dal d.lg. n. 196/2003, in materia, ad esempio, di trattamento dei dati giudiziari, dei diritti degli interessati e di misure di sicurezza.

Centrale d'allarme interbancaria

L'archivio, denominato Centrale d'allarme interbancaria (Cai), è composto, in primo luogo, da una sezione centrale presso la Banca d'Italia, che, oltre ai dati anagrafici degli interessati, contiene ulteriori segmenti relativi agli strumenti di pagamento presi in considerazione, assegni o carte di pagamento, ad informazioni rilevate riguardanti, ad esempio, smarrimenti o revoche, nonché ad eventuali sanzioni amministrative e penali. La Cai è inoltre composta da sezioni remote che riproducono, in tutto o in parte, l'intero archivio presso le banche, gli uffici postali e gli intermediari finanziari vigilati emittenti carte di pagamento, abilitati alla loro consultazione ed interessati all'individuazione di situazioni anomale od irregolari, anche rispetto alla propria clientela.

La Banca d'Italia e tali soggetti dovranno adeguarsi alle nuove disposizioni del Codice, con particolare riferimento alle attività di trasmissione e ricezione dei dati, nel rispetto del livello minimo di sicurezza previsto per i trattamenti di dati effettuati con l'ausilio di strumenti elettronici e per la gestione dei dati giudiziari (ciò per la parte dell'archivio relativa a sanzioni anche di natura penale).

Come ricordato nelle precedenti relazioni annuali, l'archivio risponde alla finalità di interesse generale di assicurare il regolare funzionamento del sistema dei pagamenti e viene alimentato da soggetti pubblici (autorità giudiziaria e Ministero dell'interno) e privati (banche, uffici postali, società emittenti carte di credito), tenuti a trasmettere i provvedimenti o le segnalazioni riguardanti sia persone che hanno emesso assegni senza autorizzazione o provvista, sia titolari di carte di pagamento revocate (per mancato pagamento o costituzione di fondi), sia, ancora, carte di pagamento o assegni sottratti, smarriti, o bloccati.

Nei confronti delle persone i cui nominativi risultano iscritti nella Cai, vi è un obbligo, per la banca, di revoca dell'autorizzazione ad emettere assegni, con un divieto che si estende anche agli altri istituti di credito per non meno di sei mesi.

Nel 2003 sono pervenute all'Autorità diverse segnalazioni relative al trattamento dei dati personali effettuato da alcune banche, uffici postali e società di carte di

pagamento nell'ambito della Cai. È aumentato anche il numero delle istanze presentate dagli interessati al fine di ottenere l'accesso, la rettificazione o la cancellazione dei dati iscritti nell'archivio. In particolare, è stato lamentato che la segnalazione nell'archivio avviene spesso senza rispettare i termini previsti per il dovuto preavviso, oppure a fronte di meri errori o disguidi nei pagamenti.

Segnalazione di scoperti di lieve importo

In relazione all'utilizzo di carte di pagamento, si rileva che taluni automatismi segnalati, relativi all'iscrizione in Cai anche per scoperti di conto corrente di lieve importo, rischiano di penalizzare i clienti che non riuscirebbero a tutelare in maniera tempestiva i propri diritti anche a causa dell'assenza (diversamente da quanto accade per gli assegni) di precise indicazioni circa le modalità di preavviso dell'eventuale revoca della carta di pagamento. Tali profili saranno oggetto d'esame nei prossimi mesi, anche nell'ambito della collaborazione avviata con la Banca d'Italia in questa materia sin dalla fase di istituzione dell'archivio.

16.5. Assicurazioni

Il settore assicurativo continua ad essere interessato da novità normative che si riflettono sulla materia della protezione dei dati personali. A tal proposito si può fare accenno, in primo luogo, al d.m. n. 74/2004 sull'accesso agli atti delle imprese di assicurazione (v. *infra*, parag. 45.2.). Merita pure di essere ricordato l'art. 120 del Codice, il quale riproduce le disposizioni dell'art. 2, commi 5-*quater* e 5-*quinquies*, della legge n. 137/2000, recanti l'istituzione, presso l'Isvap, di una banca dati dei sinistri relativi all'assicurazione obbligatoria per i veicoli a motore immatricolati in Italia, al fine di rendere più efficace la prevenzione ed il contrasto di comportamenti fraudolenti in tale settore (per le procedure e le modalità di funzionamento della banca dati, nonché di accesso alle informazioni in essa contenute, cfr. il provvedimento Isvap n. 2179 del 10 marzo 2003, già menzionato nella *Relazione* 2002).

Anche l'annunciata emanazione di un "Codice delle assicurazioni private", allo studio del Ministero per le attività produttive, potrebbe offrire l'occasione per approfondire alcuni aspetti dell'attività assicurativa che hanno delle implicazioni sulla protezione dei dati personali.

L'Autorità ha avviato una nuova riflessione con l'associazione di categoria, per esaminare alcune problematiche del settore connesse all'entrata in vigore del Codice, nonché per risolvere questioni da tempo evidenziate dagli operatori.

Il problema della "catena assicurativa"

In particolare, questi ultimi hanno sostenuto che la formulazione dell'informativa agli interessati dovrebbe tenere in considerazione le peculiari caratteristiche dei trattamenti effettuati in questo settore e la complessa struttura della "catena assicurativa". In proposito si deve peraltro osservare che, anche nel 2003, l'Autorità ha avviato l'esame di numerosi reclami e segnalazioni riguardanti carenze nelle informative fornite dalle società di assicurazioni a clienti o a soggetti cui liquidare i sinistri, carenze che –si ricorda– si riflettono sulla validità del consenso manifestato dagli interessati. La necessità di rivedere i modelli di informativa si pone anche nei casi, frequenti, in cui l'impresa di assicurazioni intenda acquisire, con uno stesso modulo, il consenso ai diversi trattamenti effettuati da altri autonomi titolari dei trattamenti.

L'Autorità ha comunque confermato la propria disponibilità a fornire un ausilio per la predisposizione di un idoneo modulo *standard* di informativa delle imprese

alla clientela (in analogia con quanto avvenuto per le banche), nonché ad affrontare alcuni delicati problemi interpretativi concernenti i presupposti di liceità del trattamento di dati sensibili, in particolare quelli sanitari.

Sempre nel merito dell'attività svolta dall'Autorità nel settore, va inoltre ricordata la segnalazione di un assicurato che aveva chiesto il rimborso della penale prevista per l'annullamento di un viaggio prenotato anche per conto di altre persone e poi annullato per la malattia di un congiunto di un compagno di viaggio. L'impresa di assicurazioni ha negato il rimborso a causa della mancata acquisizione della cartella clinica del malato, il cui esame, sarebbe stato a suo avviso necessario per verificare se la patologia che aveva determinato l'annullamento del viaggio rientrava o meno tra i rischi assicurati.

Al riguardo l'Ufficio del Garante ha in primo luogo richiamato la disposizione (art. 3 legge n. 675/1996, ora, art. 5, comma 3, d.lg. n. 196/2003), in base alla quale il trattamento di dati effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione della normativa sulla protezione dei dati solo se i dati sono destinati alla comunicazione sistematica o alla diffusione. Nel caso esaminato, si è pertanto constatata l'inapplicabilità di tale normativa alla raccolta ed al trattamento di dati personali anche sensibili relativi a compagni di viaggio –e relativi familiari– del segnalante, effettuati da quest'ultimo, pure per conto di altri, per prenotare il viaggio. Ad identica conclusione si è giunti per quanto riguarda la comunicazione all'impresa di assicurazione della documentazione necessaria al rimborso della penale conseguente all'annullamento del viaggio, visto il carattere non sistematico della comunicazione.

Inoltre, l'Autorità ha ritenuto indebita la peculiare forma di acquisizione dei dati consistente nell'esercizio, da parte del segnalante o di altri soggetti, del diritto di accesso alla cartella clinica detenuta dalla struttura ospedaliera presso cui la persona interessata è stata ricoverata. Infatti, alla luce dell'art. 60 del Codice e dei principi richiamati dal Garante nel provvedimento del 9 luglio 2003 (su cui v. *infra* lo specifico paragrafo 19.2.), l'accesso alle cartelle cliniche detenute presso strutture sanitarie deve ritenersi consentito solo se la situazione giuridica 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. Ciò non si era invece verificato nel caso segnalato, in cui il diritto fatto valere aveva ad oggetto unicamente la pretesa al rimborso della penale pagata al *tour operator* in seguito all'annullamento del viaggio. A breve, l'Autorità valuterà nuovamente la questione all'esito del riscontro chiesto all'impresa assicurativa.

Trattamento di dati idonei a rivelare lo stato di salute

Infine, l'Autorità è tornata ad esaminare il problema dei limiti di ammissibilità del trattamento di dati idonei a rivelare lo stato di salute da parte delle imprese di assicurazione, in relazione alla gestione del contratto assicurativo ed all'acquisizione dei dati di assicurati o di terzi.

Sul punto, si è ribadita la liceità della raccolta di dati sanitari contenuti in cartelle cliniche degli assicurati qualora tali dati siano strettamente necessari per fornire le specifiche prestazioni richieste dagli interessati. Si è tuttavia osservato che, in ossequio a quanto stabilito dalla legge (art. 26, comma 1, del Codice) e dalle autorizzazioni generali nn. 2/2002 e 5/2002 (efficaci sino al 30 giugno 2004), la previsione contrattuale dell'onere di fornire, ai fini del rimborso, copia della cartella clinica in

caso di ricovero, è comunque subordinata anche all'acquisizione del consenso scritto dell'interessato al quale si riferiscono i dati contenuti nella cartella. Il consenso deve essere preceduto da idonea informativa e deve avere specifico riguardo al trattamento dei dati sanitari. Rispetto alla vicenda analizzata, sono state pertanto ritenute inoperanti le ipotesi equipollenti al consenso individuate dalla normativa (v. l'art. 26, comma 4, del Codice).

In ogni caso, come si è detto, la raccolta ed il successivo trattamento dei dati sanitari devono essere effettuati in conformità ai principi di indispensabilità, pertinenza e non eccedenza dei dati rispetto alle finalità perseguite (art. 11 del Codice) e ciò proprio con riguardo alla stretta necessità per l'impresa di assicurazione di acquisire copia integrale di una cartella clinica ai fini della liquidazione di un sinistro. La stessa acquisizione dell'intera cartella clinica può non essere rispettosa di tali principi poiché tale documento, insieme ad elementi che potrebbero essere necessari ai fini delle verifiche effettuate dalla società di assicurazione per procedere al rimborso richiesto dall'assicurato (riguardo, ad esempio, ad informazioni che permettono di stabilire la natura della malattia, documentabile in modo idoneo con modalità alternative), contiene ulteriori dati di carattere sanitario che possono non avere alcun rilievo ai fini delle verifiche e che devono essere quindi stralciati.

Comunicazione dei dati contenuti nelle perizie medico-legali

Va ricordato anche in questo paragrafo che il Garante ha riaffermato più volte il principio (ora confermato anche nel citato d.m. del 2004) secondo cui le informazioni personali comprese nelle valutazioni e negli altri elementi di giudizio riportati nelle perizie medico-legali delle compagnie di assicurazione rientrano nella sfera dei dati personali e vanno pertanto comunicate all'interessato quando questi ne faccia richiesta. La questione è stata affrontata in dettaglio nella parte della *Relazione* specificamente dedicata al diritto di accesso ai dati personali, cui si fa rinvio (parag. 7.9.; cfr. pure parag. 50.1.)

17 *Marketing*

Numerosi reclami e quesiti hanno confermato la forte sensibilità di consumatori rispetto alle intrusioni nella propria vita privata derivanti dall'adozione di nuovi strumenti e strategie di commercializzazione di prodotti o servizi.

In particolare, nel corso dell'anno sono stati sottoposti al Garante diversi episodi di ricezione di lettere, telefonate ed altre comunicazioni indesiderate da parte di operatori di *direct marketing*, soprattutto nell'ambito di attività di promozione di carte di credito.

Utilizzo delle liste elettorali a fini di *marketing*

Per quanto riguarda, poi, la prassi, diffusa tra gli operatori commerciali, di attingere dati personali da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per intraprendere operazioni di *marketing*, il Garante ha evidenziato alcune importanti novità introdotte nel settore in esame dal Codice. L'art. 177, comma 5, del d.lg. n. 196/2003 ha, infatti, modificato le norme relative all'utilizzabilità delle liste elettorali, prevedendo che tali liste possano essere accessibili e rila-

17

sciate in copia solo "in applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca scientifica o storica, o a carattere socio-assistenziale" o, ancora, per la tutela di un interesse collettivo o diffuso. Perciò, le liste elettorali, sebbene di formazione "pubblica", non possono più essere sfruttate per scopi commerciali o pubblicitari, a differenza di quanto era consentito alla luce della disciplina in vigore fino al 31 dicembre scorso, che dava invece la possibilità a chiunque di copiarle, stamparle o metterle in vendita.

In ambito diverso, oggetto anch'esso di approfondita analisi, il Garante ha poi autorizzato una casa editrice, previa fissazione di limiti e garanzie, a trattare eventuali dati sensibili forniti spontaneamente all'atto della formulazione di quesiti rivolti ad esperti di vari settori, da parte delle persone che richiedono servizi di consulenza *on line* offerti a pagamento attraverso siti e pagine *web* di testate giornalistiche.

Consulenze *on line* e dati sensibili

L'Autorità, nel richiamare la casa editrice al rispetto dell'autorizzazione generale n. 2/2002 riguardante i dati idonei a rivelare lo stato di salute e la vita sessuale, ha autorizzato il trattamento di altri dati sensibili, eventualmente rilasciati, soltanto se realmente pertinenti all'argomento trattato o al quesito posto, oltre che indispensabili per fornire il servizio di consulenza *on line*. Alla società istante è stato, quindi, prescritto di inserire in modo visibile, nell'informativa fornita agli utenti, l'invito a non indicare nei quesiti dati di carattere sensibile non strettamente necessari per la risposta.

Nell'eventualità, poi, che la domanda e la risposta siano inserite, previo consenso dell'utente, negli spazi consultabili liberamente dal pubblico (ad esempio in una rubrica delle domande più frequenti, cd. *faq*), l'Autorità ha imposto alla società di verificare prima della loro pubblicazione che, oltre al nome ed all'indirizzo *e-mail* dell'interessato, non vi compaiano altri dati, anche diversi da quelli sensibili, che possano rendere identificabile l'utente. Gli esperti *on line* –designati responsabili del trattamento– devono perciò controllare che nelle risposte pubblicate non vi sia alcun elemento che permetta di risalire all'identità della persona che ha richiesto la consulenza. Essi devono ricevere poi adeguate istruzioni in merito alla necessità di verificare la pertinenza dei dati sensibili riportati nei quesiti, in vista della loro eliminazione ove non necessari per la prestazione del servizio.

Nel periodo di riferimento, sono stati anche completati gli accertamenti (v. *Relazione* 2002, p. 104) riguardanti la raccolta e il trattamento dei dati personali nell'ambito della distribuzione nei supermercati di carte di fidelizzazione della clientela per promuovere operazioni a premi o sconti. È quindi imminente l'adozione di un provvedimento di carattere generale su tale tematica, per richiamare l'attenzione di quanti ricorrono a tali iniziative sulla necessità di riformulare alcuni modelli di informativa agli interessati e di richiesta del consenso, e di adottare altre misure necessarie per conformare alle leggi i trattamenti di dati.

Profilazione della clientela

Dall'istruttoria svolta è già emersa la necessità di far assicurare il rispetto della normativa sulla *privacy* nei casi di trattamento dei dati con finalità di profilazione della clientela, quando, cioè, sulla base dei volumi di spesa e delle tipologie di prodotti acquistati dai singoli clienti, vengono predefinite determinate categorie o gruppi di consumatori abituali o meno, per procedere poi alla realizzazione di promozioni ed offerte ad essi mirate (volte a premiare la frequenza di visita, a promuovere l'acquisto di determinati prodotti, ecc.).

È stata peraltro già rilevata la tendenza di alcune società ad effettuare in tutto o in parte il trattamento dei dati dei clienti in forma prevalentemente anonima.

Particolare rilevanza riveste poi, per il settore in esame, la prossima 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. Tale codice dovrà, infatti, prevedere a breve forme semplificate per la manifestazione del consenso da parte dell'interessato, ovvero per rendere meglio conoscibile la sua eventuale opposizione all'invio di determinate comunicazioni commerciali.

Codice di condotta proposto dalla Fedma

A livello europeo si segnala infine l'approvazione, a seguito della consultazione delle parti interessate, del codice di condotta proposto dalla Federazione europea del *marketing* diretto. Nel Parere 3/2003 del 13 giugno 2003, il Gruppo istituito dall'art. 29 della direttiva n. 95/46/CE ha ritenuto il codice di condotta conforme alla direttiva sulla protezione dei dati ed alle disposizioni nazionali di attuazione. Il codice in questione affronta i problemi specifici della protezione dei dati nel settore del *marketing* diretto e propone alcune soluzioni.

IV - La privacy nelle pubbliche amministrazioni

18 Profili generali Dati sensibili e giudiziari

Al trattamento dei dati personali effettuato dai soggetti pubblici continua ad applicarsi una disciplina in parte differenziata rispetto a quella cui sono sottoposti i soggetti privati e gli enti pubblici economici.

Sulla base di alcuni principi generali fissati dal Codice per tutti i trattamenti effettuati da soggetti pubblici e privati, le amministrazioni pubbliche sono legittimate a trattare dati personali comuni, sensibili o giudiziari soltanto per svolgere funzioni istituzionali, rispettando gli eventuali altri presupposti e limiti stabiliti da disposizioni normative estranee al Codice ed astenendosi dall'acquisire il consenso degli interessati, specie per rendere lecito un trattamento altrimenti non ammesso.

Malgrado questi principi non siano di nuovo conio, si registrano ancora nel settore pubblico vari ritardi applicativi nell'adempiere agli obblighi previsti in materia di protezione dei dati. Per contribuire a risolvere queste difficoltà anche sul piano della comunicazione e formazione, l'Autorità sta completando un *vademecum* sui principali adempimenti a carico delle amministrazioni e sui diritti dei cittadini, modelli di informativa e di designazione dei responsabili e degli incaricati del trattamento, nonché il testo di alcune *Faq (Frequently asked questions)* funzionali alla risoluzione di questioni di carattere generale che si presentano nel settore pubblico anche sanitario.

Problemi peculiari continua a porre il trattamento dei dati sensibili (attinenti a profili particolarmente delicati della sfera privata delle persone: la salute, le abitudini sessuali, le convinzioni religiose, politiche, sindacali e filosofiche, l'origine razziale ed etnica) o giudiziari.

La legislazione previgente aveva introdotto già particolari garanzie per entrambe le categorie di informazioni, garanzie che sono rimaste sostanzialmente inattuate o eluse in numerosi uffici pubblici a causa della perdurante inerzia delle amministrazioni nell'adeguare i propri ordinamenti alla normativa in materia di riservatezza, malgrado le reiterate proroghe di termini e alcune disposizioni di favore rispetto al settore privato.

Il Codice rafforza ulteriormente le garanzie per i cittadini; inoltre, ridefinisce la categoria dei dati giudiziari, anche alla luce della nuova disciplina in materia di casellario giudiziario (d.P.R. 14 novembre 2002, n. 313), includendovi le informazioni relative alla qualità di indagato o di imputato, secondo le nozioni che ne danno, rispettivamente, gli artt. 60 e 61 c.p.p.

In particolare, viene rafforzato e sviluppato il principio di proporzionalità nel trattamento di queste informazioni, ritenendosi legittimo il trattamento dei soli dati

sensibili e giudiziari "indispensabili" allo svolgimento di attività che non potrebbero essere adempiute mediante il ricorso a dati anonimi o a dati personali di diversa natura (art. 22 d.lg. n. 196/2003).

Con questo limite, resta ferma la possibilità per i soggetti pubblici di trattare i dati sensibili o giudiziari quando ciò sia previsto da una norma di legge (oppure, se si tratta di dati giudiziari, da un provvedimento del Garante) che specifichi espressamente le rilevanti finalità di interesse pubblico perseguite, i dati personali che possono essere utilizzati e le operazioni di trattamento eseguibili (v. anche art. 27 d.lg. n. 196/2003).

Per quanto riguarda i dati sensibili, nel caso in cui la legge (o, in via transitoria, il Garante) specifichi soltanto le finalità di rilevante interesse pubblico, il Codice conferma l'adeguata soluzione secondo cui l'atto con il quale le amministrazioni devono individuare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili deve avere natura regolamentare e non già meramente amministrativa (artt. 20 s. d.lg. n. 196/2003).

Secondo la nuova disciplina, i regolamenti devono essere inoltre adottati in conformità al parere reso dal Garante, che può essere formulato anche su schemi-tipo al fine di rendere più agevole e rapida l'adozione di tali atti. Qualora gli schemi regolamentari predisposti dalle amministrazioni corrispondano ai modelli su cui il Garante ha reso un parere conforme, non sarà quindi necessario sottoporli caso per caso allo specifico esame da parte dell'Autorità.

Termine per l'adozione del regolamento

Al fine di consentire un efficace adeguamento al sistema di garanzie delineato dal Codice, per i trattamenti iniziati prima della sua entrata in vigore è stato anche fissato un termine improrogabile (30 settembre 2004) entro il quale i soggetti pubblici formalmente o sostanzialmente inadempienti (alcuni atti già adottati, a volte anche senza il parere del Garante, non recano alcuna effettiva disciplina o ricognizione della materia) dovranno emanare il regolamento. In vista di tale scadenza, è in corso di prossima adozione un provvedimento con il quale il Garante fornirà chiarimenti ed indicazioni di carattere generale allo scopo di agevolare l'adempimento da parte dei soggetti pubblici.

Al riguardo, va anche ricordato che l'Autorità, nel parere del 4 settembre 2003 sullo schema di regolamento predisposto dal Ministero degli affari esteri, ha sottolineato come varie finalità di rilevante interesse pubblico che possono giustificare il trattamento di dati sensibili e giudiziari, sono espressamente individuate dalla legge (ora, dal Codice). È peraltro insufficiente l'indicazione solo di alcune macro-tipologie di dati, corredata da descrizioni del loro impiego, dovendosi piuttosto specificare i tipi di dati concretamente utilizzati e le operazioni su di essi effettuate.

19 Trasparenza dell'attività amministrativa

La necessità di bilanciare il principio di trasparenza dell'attività amministrativa, sancito dalla legge n. 241/1990 e da altre disposizioni di settore (per gli enti locali, cfr. l'art. 10, comma 1, del d.lg. n. 267/2000) con quello di tutela della riservatezza continua a rappresentare una delle problematiche che più di frequente vengono sottoposte all'attenzione del Garante.

Di tale tematica si è già dato parzialmente conto più sopra (cfr. parag. 8.2.), in riferimento all'esercizio, ad opera degli interessati, del diritto alla cancellazione dei dati trattati in violazione di legge. In quella sede si è detto che un criterio guida del bilanciamento tra riservatezza e trasparenza dell'attività amministrativa è stato individuato dall'Autorità anche nel rispetto dei principi di pertinenza e non eccedenza.

Pubblicità delle deliberazioni comunali e divieto di diffusione dei dati sulla salute

Con particolare riferimento agli enti locali, l'Autorità ha ribadito poi in varie occasioni che, sebbene la normativa preveda la pubblicità per le deliberazioni comunali attraverso la loro affissione all'albo pretorio, nel caso in cui esse contengano dati sulla salute occorre tenere presente il divieto di diffusione di tali informazioni (art. 23, comma 4, legge n. 675/1996; ora, art. 22, comma 8, d.lg. n. 196/2003). L'ente può quindi utilizzare unicamente diciture generiche, codici numerici o lettere puntate che impediscano di giungere all'identificazione dell'interessato, attraverso una nuova tecnica di redazione dei provvedimenti soggetti ad obbligatoria pubblicazione, che lascia comunque impregiudicato il diritto dei controinteressati ad accedere in conformità ai presupposti di legge, presso gli uffici dell'ente, ai dati sensibili (da omettere, invece, nella delibera diffusa ad un pubblico indeterminato).

Anche in riferimento ad altri momenti della vita amministrativa, le amministrazioni sono tenute in termini più generali a selezionare con particolare attenzione i dati personali, specie se di tipo sensibile o attinenti a vicende giudiziarie, la cui menzione sia effettivamente necessaria per perseguire, nei singoli casi, le finalità di trasparenza delle attività dei propri organi, nel rispetto dei principi di pertinenza e non eccedenza (art. 9 legge n. 675/1996; ora, art. 11 d.lg. n. 196/2003).

La necessità del rispetto di tali principi, quale criterio che deve concorrere al bilanciamento tra le esigenze di riservatezza e quelle di trasparenza dell'attività amministrativa, è stata ribadita anche in altre circostanze.

Così, nel caso di un ente locale (che aveva riportato su un manifesto affisso per le vie del comune l'ordine del giorno di una seduta del consiglio comunale, contenente vari dati personali riferiti ad un dipendente e ad una vicenda giudiziaria che lo vedeva coinvolto), l'Autorità ha ritenuto contraria al principio di non eccedenza l'indicazione dettagliata di informazioni personali, sebbene in forma di pubblicazione effettuata legittimamente dall'amministrazione. L'avviso pubblico destinato all'affissione avrebbe dovuto infatti contenere soltanto la menzione dell'oggetto e degli estremi della pronuncia giudiziaria di interesse, e non anche il nominativo delle parti interessate. La documentazione integrale poteva, invece, essere comunicata ai consiglieri comunali, ai quali va garantita, ai sensi dell'art. 39, comma 4, del d.lg. n. 267/2000, un'informazione adeguata e preventiva sulle questioni sottoposte

al consiglio, per consentire loro l'espletamento dei propri compiti istituzionali (*Provv*. 9 dicembre 2003).

Analogamente, non è stata giudicata proporzionata l'introduzione, in una deliberazione comunale riguardante una controversia che opponeva l'amministrazione alla ricorrente, del testo integrale di una relazione dell'ufficio legale nella quale era riportata una serie di dati personali concernenti la ricorrente stessa. La relazione, che indicava tra l'altro nel dettaglio le richieste di risarcimento del danno formulate dall'interessata nei confronti del comune, avrebbe potuto essere infatti riportata in sintesi, oppure semplicemente riassunta nella deliberazione, senza con ciò pregiudicare l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, legge n. 241/1990) e rimanendo pur sempre accessibile ai controinteressati, nella sua versione integrale, in base alle norme vigenti in materia (*Provv*. 17 aprile 2003).

È stato per altro verso considerato non contrastante con la normativa sulla riservatezza il rilascio ad organi interni al consiglio comunale, come ad esempio una commissione trasparenza, di determinati verbali di accertamento e di alcuni altri atti stilati dalla locale polizia municipale. In particolare, è stata riconosciuta a tale organo la possibilità di accedere anche a taluni documenti contenenti dati di natura sensibile, tenuto pure conto del fatto che lo svolgimento delle funzioni di controllo, di indirizzo politico e di sindacato ispettivo (nonché di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo), rientra tra le attività di rilevante interesse pubblico per il cui perseguimento è permesso il trattamento di questa categoria di informazioni (*Nota* 13 maggio 2003).

Registrazione di sedute del consiglio comunale

In merito alla pubblicità degli atti e delle sedute del consiglio comunale, l'Autorità ha anche precisato che un consigliere comunale può registrare con l'ausilio di strumenti propri le sedute dell'assemblea consiliare a condizione che, quando la registrazione, in ipotesi particolari, è effettuata per fini esclusivamente personali, i dati non siano destinati alla comunicazione sistematica o alla diffusione, e quando invece è (più spesso) effettuata per scopi diversi, gli interessati siano posti previamente in condizione di essere informati (*Nota* 23 aprile 2003).

Gli obblighi previsti in materia di informativa comportano peraltro che le amministrazioni pubbliche rendano conoscibile agli interessati, con modalità adeguate, anche il trattamento dei dati che li riguardano effettuato a fini istituzionali. In questo senso, può non contrastare con la normativa sulla protezione dei dati la verifica, per motivi di sicurezza, dell'identità delle persone che accedono ad uffici pubblici, purché sia resa l'informativa agli interessati, anche tramite modalità semplificate (ad esempio, mediante l'affissione di avvisi chiari e sintetici), e siano osservati rigorosamente i principi di pertinenza e di non eccedenza dei dati raccolti con particolare riferimento alla mera verifica dell'identità, all'annotazione degli ingressi oppure alla (spesso contestata) prassi di fotocopiare documenti (*Nota* 23 aprile 2003).

Sulla questione della raccolta di dati identificativi degli interessati, è stata infatti completata l'istruttoria sulla prassi adottata da alcuni soggetti pubblici di raccogliere e registrare dati personali mediante l'acquisizione della copia fotostatica di un documento di identità personale, a scopi di sicurezza (come avviene per i dati personali dei visitatori raccolti all'ingresso degli edifici sede di uffici pubblici), o addirittura "statistici", sia nel caso in cui la copia del documento di riconoscimento venga

acquisita per adottare atti o provvedimenti richiesti dal cittadino. La problematica sarà definita entro breve termine con la formulazione di utili prescrizioni al riguardo.

19.1. Accesso ai documenti amministrativi

L'Autorità è stata interpellata innumerevoli volte in merito alle problematiche relative al diritto di accesso agli atti amministrativi che, come ribadito in più occasioni anche alla luce della consolidata giurisprudenza, costituisce ancora una delle più significative applicazioni del principio di trasparenza (cfr., da ultimo, C.d.S. Sez. VI, 9 gennaio 2004, n. 14).

Dati personali contenuti in esposti e denunce

A tal proposito, è stato rilevato (*Nota* 16 maggio 2003) che i principi di pertinenza e non eccedenza non permettono di riportare sugli atti di avvio degli accertamenti in materia di abusi edilizi alcuni dati personali contenuti negli esposti che hanno dato origine all'accertamento. Sebbene le persone interessate possano avere accesso agli atti che li riguardano, compresi, in determinate circostanze, anche eventuali esposti o denunce presentati contro di esse, una pubblicità indifferenziata del contenuto degli esposti non può ritenersi conforme ai principi in materia di protezione dei dati, come peraltro confermato anche dalla giurisprudenza amministrativa (C.d.S. Sez. V, 3 aprile 2000, n. 1916).

Elenchi di intestatari di contratti di fornitura di pubblici servizi

L'Autorità è stata anche chiamata a precisare ulteriormente il rapporto tra il diritto di accesso e quello alla protezione dei dati personali, con particolare riferimento alla possibilità per i comuni di accedere ad elenchi dettagliati detenuti dalle società concessionarie dell'erogazione di pubblici servizi, recanti gli intestatari di contratti di fornitura. Al riguardo è stato evidenziato che i soggetti privati possono comunicare i dati personali con il consenso degli interessati, ovvero in presenza di uno degli altri presupposti di liceità, come ad esempio l'adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. In particolare, si può prescindere dal consenso dell'interessato nel caso in cui sussistano esigenze di istituzione o completamento del catasto degli impianti termici, poiché l'art. 17 del d.P.R. n. 551/1999 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).

Occorre infine segnalare che è allo studio dell'Autorità la predisposizione di un nuovo provvedimento sulla delicata questione del diritto di accesso dei consiglieri comunali e provinciali, già oggetto di varie pronunce in casi specifici.

19.2. Il principio del cd. pari rango

L'esperienza applicativa ha individuato da tempo alcuni opportuni presupposti per bilanciare il diritto alla riservatezza e il diritto di accesso ai documenti amministrativi, specie quando i documenti contengono dati attinenti alla salute o alla vita sessuale.

La questione dei limiti alla comunicazione di dati sulla salute e sulla vita sessuale a persone diverse dall'interessato ha assunto, non di rado, rilevanza nel caso di richieste di accedere 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.).

Con riferimento al caso in cui una pubblica amministrazione riceva una richiesta di accesso a documenti amministrativi contenenti tale tipo di dati, il Codice (art. 60), risolvendo alcuni dubbi interpretativi sorti sulla base delle disposizioni previgenti (art. 16 d.lg. 11 maggio 1999, n. 135), dispone che il trattamento dei dati finalizzato a permettere l'accesso è consentito se la situazione giuridica che si intende tutelare con la richiesta di accesso ai documenti amministrativi è "di rango almeno pari ai diritti dell'interessato", ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile.

Ad identica valutazione sul "rango" della situazione soggettiva fatta valere sono tenuti i soggetti privati nel caso in cui sia loro richiesto di comunicare a terzi singole informazioni sulla salute e sulla vita sessuale dell'interessato, come evidenziato dal Garante in una vicenda riguardante una casa di cura privata (*Nota* 4 settembre 2003).

La valutazione del "rango" della situazione soggettiva

In tutte queste ipotesi il destinatario della richiesta, per decidere se accogliere anche in parte l'istanza di comunicazione di dati o di accesso ai documenti, deve previamente verificare in concreto se il diritto che si intende far valere o difendere sulla base delle informazioni o della documentazione richiesta sia almeno "di pari rango" rispetto al diritto alla riservatezza, alla dignità ed agli altri diritti e libertà fondamentali dell'interessato. La comunicazione di dati che rientrano nella sfera di riservatezza dell'interessato può, in definitiva, ritenersi giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti fondamentali ed inviolabili.

Questa significativa affermazione, ora espressamente confermata dal Codice (artt. 26, comma 4, lett. *c)*, 60, 71 e 92, comma 2, d.lg. n. 196/2003), è contenuta in un provvedimento del 9 luglio 2003 dell'Autorità, con il quale sono stati forniti alcuni criteri guida che devono caratterizzare il bilanciamento delle diverse situazioni coinvolte.

Provvedimento del 9 luglio 2003 (cd. pari rango)

In tale provvedimento si fa riferimento in particolare alla richiesta di accesso, da parte di persone diverse dall'interessato, alla cartella clinica di quest'ultimo (che può presentare delicate informazioni riferite talvolta anche ad individui diversi dall'interessato: si pensi alle anamnesi familiari), accanto ad altre considerazioni utili per altri tipi di documenti detenuti in ambito pubblico o privato.

Si è così precisato che:

- la comunicazione all'interessato di dati personali sulla salute va effettuata solo per il tramite di un medico (art. 23, comma 2, legge n. 675/1996; vedi però, ora, art. 84 d.lg. n. 196/2003, in riferimento agli esercenti le professioni sanitarie e agli organismi sanitari);

- occorre avere presente, quale elemento di raffronto per il bilanciamento degli interessi, non già, in sé considerato, il diritto alla tutela giurisdizionale, che pure è costituzionalmente garantito, bensì il diritto soggettivo sottostante, che si intende far valere sulla base del materiale documentale di cui si vorrebbe avere conoscenza;

- la valutazione sui diritti soggettivi va fatta in concreto, così da evitare "il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica

dei diritti in contesa" (nello stesso senso, C.d.S. Sez. VI, 30 marzo 2001, n. 1882 e 9 maggio 2002, n. 2542; cfr. pure C.d.S. Sez. V, 31 dicembre 2003, n. 9276);

- oltre a verificare, anche nell'ottica di un eventuale accoglimento parziale della richiesta, l'effettiva necessità dei dati ai fini dell'azione o della difesa, occorre osservare comunque i principi di pertinenza e di non eccedenza nel trattamento, al cui rispetto sono tenuti pure i soggetti pubblici (artt. 3-4 d.lg. n. 135/1999; ora, art. 22 d.lg. n. 196/2003);

- se la richiesta è rivolta ad una amministrazione pubblica, nel procedimento instaurato dall'istanza di accesso dovrebbe essere poi informato l'interessato, stimolando un "contraddittorio anticipato" che ponga in condizione quest'ultimo di esercitare i propri diritti ed eventualmente opporsi per motivi legittimi al trattamento delle informazioni che lo riguardano;

- i medesimi criteri devono essere seguiti nel caso in cui la richiesta di accesso o di comunicazione di dati sia formulata da un difensore che abbia ricevuto specifico incarico, anche ai sensi della normativa sulle investigazioni difensive (così la *Nota* 10 dicembre 2003).

Il limite del "pari rango", ad ogni modo, non trova applicazione nel caso di accesso ai dati personali direttamente da parte dell'interessato e per il rilascio di copia della cartella clinica all'interessato medesimo o a persona da lui specificamente delegata (o ancora, in caso di decesso, a chi "ha un interesse proprio o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione": art. 9, comma 3, d.lg. n. 196/2003). Deve trattarsi comunque di un esercizio del diritto di accesso frutto di una libera determinazione da parte dell'interessato e non di una costrizione, come quella che potrebbe venire da una controparte più "forte", nel quadro ad esempio di un rapporto di lavoro o contrattuale.

20 Tessera elettorale

Le problematiche connesse ai dati personali da riportare nella tessera elettorale continuano ad essere seguite con attenzione dall'Autorità. Tale documento, che ha sostituito in via permanente il certificato elettorale, è stato sinora realizzato solo in forma cartacea (d.P.R. 8 settembre 2000, n. 120), sebbene l'art. 13 della l. 30 aprile 1999, n. 120 avesse previsto l'adozione, in via sperimentale, della carta d'identità elettronica con funzioni anche elettorali.

Profili critici

Il Garante ha già espresso in passato il proprio giudizio critico sull'utilizzo del formato cartaceo anziché del supporto informatico, anche alla luce delle caratteristiche del modello cartaceo approvato, nonché della circostanza che la tessera è in ipotesi utilizzabile per diciotto consultazioni elettorali e/o referendarie e presenta vari spazi per apporre timbri che certificano la partecipazione al voto. Tutto ciò

rende conoscibili diversi dati relativi ai comportamenti dell'interessato in occasione delle consultazioni e, in date condizioni, gli stessi suoi orientamenti.

Nel corso del 2003 sono state affrontate anche questioni più di dettaglio, come la richiesta di cancellazione dai documenti elettorali del nome del coniuge separato. In argomento, l'Autorità ha ritenuto conforme alla normativa sulla protezione dei dati personali il diniego opposto dalle autorità locali a tali richieste di cancellazione, poiché la disciplina di settore prevede espressamente che sulla tessera elettorale il cognome delle donne coniugate possa essere seguito da quello del marito (art. 2 d.P.R. n. 299/2000). Inoltre, secondo gli artt. 156-*bis* c.c. e 5, secondo comma, della legge n. 898/1970, la donna, che durante la separazione personale dei coniugi conserva (salvo diverso provvedimento del giudice) il cognome del marito aggiunto al proprio per effetto del matrimonio, lo perde solamente a seguito della sentenza di scioglimento o cessazione degli effetti civili del matrimonio.

21 Documentazione anagrafica e materia elettorale

Anche nel periodo di riferimento sono pervenuti numerosi quesiti sulle modalità di trattamento dei dati contenuti nei registri anagrafici, negli atti dello stato civile e nelle liste elettorali.

Significativa è stata ad esempio l'indicazione fornita dall'Autorità circa la possibilità di affidare la funzione di lettura ottica tramite *scanner* degli atti contenuti nei registri dello stato civile ad un soggetto esterno all'amministrazione comunale, designato quale responsabile del trattamento e sulla base di attente istruzioni, concernenti anche la sicurezza dei dati. Il comune deve poi vigilare sull'osservanza di tali istruzioni e sul più generale rispetto delle norme in materia di protezione dei dati personali, anche tramite verifiche periodiche, e può pure prevedere che sia il responsabile a designare, all'interno della propria struttura, i soggetti aventi legittimo accesso ai dati personali in qualità di incaricati del trattamento (*Nota* 23 aprile 2003).

Conoscibilità dei dati anagrafici

L'Autorità è stata nuovamente interpellata anche sulla possibilità per i comuni di comunicare a privati le informazioni contenute negli archivi anagrafici, e così, ad esempio, di dare una notizia sul comune di emigrazione di una persona già iscritta all'anagrafe. In proposito, si è ribadito ancora una volta che la normativa sulla protezione dei dati non ha modificato espressamente la disciplina vigente in materia di stato civile e anagrafi, secondo cui –a parte la comunicazione dei dati anagrafici, resi anonimi ed aggregati, agli interessati che ne facciano richiesta, per fini statistici e di ricerca– possono essere rilasciati, a chi lo richieda, solo i certificati concernenti la residenza o lo stato di famiglia. Ai sensi dell'art. 33, comma 2, del d.P.R. n. 223/1989, ogni altra posizione desumibile dagli atti anagrafici (quindi, pure l'informazione sul comune di emigrazione) resta attestabile o certificabile, qualora non vi ostino gravi o particolari esigenze di pubblico interesse, dall'ufficiale di anagrafe, d'ordine del sindaco (*Nota* 4 giugno 2003).

Uso degli elenchi anagrafici per finalità di comunicazione istituzionale

In merito al trattamento dei dati contenuti negli elenchi anagrafici, il Codice ha peraltro, integrato la disciplina di settore, che consente l'utilizzo di questi elenchi da parte delle pubbliche amministrazioni esclusivamente per scopi di pubblica utilità (art. 34, comma 1, d.P.R. n. 223/1989). L'art. 177, comma 1, del d.lg. n. 196/2003, sulla scia di due noti casi che avevano interessato in passato i comuni di Roma e Milano, ha ora chiarito, da un lato, che rientrano tra tali scopi di pubblica utilità quelli di applicazione della disciplina in materia di comunicazione istituzionale e, dall'altro, che tra i soggetti pubblici che possono avvalersi di tale opportunità è compreso lo stesso comune presso il quale è istituita l'anagrafe. Ciò comporta, quindi, l'utilizzabilità, da parte del comune, dei dati personali contenuti nei registri anagrafici per le finalità di comunicazione istituzionale ora indicate.

Il Garante è stato di seguito richiesto di verificare l'applicabilità di questo principio con una decisione su un ricorso relativo ad una vicenda in cui un comune aveva inviato a cittadini minorenni un invito a prendere parte alla sagra patronale ed alla festa di *Halloween* organizzate dall'ente. Il Garante non ha riscontrato specifiche violazioni ed ha pronunciato non luogo a provvedere sul ricorso. I dati trattati, ottenuti tramite il locale ufficio anagrafe, non erano conservati presso il comune, la gestione delle comunicazioni effettuate era stata organizzata direttamente dal comune stesso e le finalità e la logica del trattamento consistevano unicamente nell'intenzione di fare conoscere ai bambini il contenuto delle iniziative ricreative organizzate dall'amministrazione (*Provv.* 30 gennaio 2004).

Nel corso dell'anno, il Garante è stato altresì sollecitato in più occasioni a pronunciarsi in materia elettorale.

Liste elettorali ed elenco degli italiani residenti all'estero

Si è in primo luogo nuovamente ribadito a chi ne ha fatto richiesta (*Nota* 7 marzo 2003) che la normativa sulla protezione dei dati personali non aveva a suo tempo modificato la disciplina in materia di ostensibilità delle liste elettorali detenute dai comuni, la quale consentiva a chiunque di copiare, stampare o mettere in vendita le liste elettorali del comune (art. 51 d.P.R. 20 marzo 1967, n. 223).

L'Autorità si è poi pronunciata sulla conoscibilità dell'elenco provvisorio degli aventi diritto al voto detenuto dalle rappresentanze diplomatico-consolari, previsto dal regolamento di attuazione della legge sull'esercizio del diritto di voto dei cittadini italiani residenti all'estero (d.P.R. n. 104/2003, attuativo della legge n. 459/2001).

In alcune note indirizzate al Ministero degli affari esteri, il Garante ha ritenuto applicabili il regime di pubblicità e le modalità ostensive delle liste elettorali detenute dai comuni, anche alla luce della ricordata legge n. 459/2001, che considera equivalenti le funzioni svolte dalle liste elettorali e dall'elenco provvisorio distribuito dagli uffici consolari. Per l'utilizzo dell'elenco dei residenti all'estero l'art. 5 del d.P.R. n. 104/2003 prevede poi una specifica limitazione, vietando la comunicazione e la diffusione dei dati degli elettori per finalità diverse da quelle politico-elettorali stabilite dalla citata legge n. 459 (*Nota* 13 giugno 2003).

Le novità introdotte dal Codice

Rispetto al regime di piena conoscibilità e pubblicità delle liste elettorali degli enti locali, il Codice ha peraltro introdotto una modifica rilevante, prevedendo, in applicazione del principio di finalità (e tenendo conto di quanto prospettato dal Ministero dell'interno in occasione di un quesito sulla *ratio* di questa ipotesi di pub-

blicità), 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 d.lg. n. 196/2003).

Tale modifica, benché posteriore alla normativa sul voto dei cittadini italiani residenti all'estero, non sembra incidere particolarmente sul regime di conoscibilità dell'elenco provvisorio detenuto dagli uffici consolari, in ragione dell'espresso divieto di utilizzare i dati in esso contenuti per finalità diverse da quelle politico-elettorali, come sopra rammentato (*Nota* 4 settembre 2003).

I Comites

Il d.P.R. 29 dicembre 2003, n. 395, recante il regolamento di attuazione della legge n. 286/2003 sull'istituzione dei comitati degli italiani all'estero (Comites), ha peraltro precisato che l'elenco aggiornato degli italiani residenti all'estero può essere utilizzato per finalità riguardanti la determinazione della consistenza delle comunità italiane, in relazione all'istituzione di tali comitati, nonché la predisposizione delle liste e lo svolgimento della campagna elettorale per l'elezione dai componenti dei comitati stessi. Sempre per le finalità politico-elettorali connesse all'elezione dei Comites, l'autorità consolare può consentire a chi ne faccia richiesta di copiare l'elenco degli aventi diritto al voto, ovvero può fornirne copia.

22 Istruzione

Nell'ultimo anno di attività l'Autorità è stata nuovamente sollecitata a chiarire alcuni aspetti relativi alla protezione dei dati nel settore dell'istruzione.

Pubblicità degli esiti scolastici

In questo quadro, è tra l'altro in fase di definizione il procedimento relativo ad un istituto scolastico il quale aveva acquisito dati personali di studenti dagli elenchi affissi all'albo di altri istituti, al termine dell'anno scolastico, ed aveva inviato loro comunicazioni di carattere commerciale. In passato, con riferimento a casi analoghi, il Garante aveva già rilevato che la pubblicità degli esiti scolastici risponde ad essenziali esigenze relative alla vita scolastica dei singoli, nonché al controllo pubblico e dei cointeressati sullo svolgimento delle predette attività. Tale conoscibilità delle valutazioni finali non autorizza, però, i terzi che vi accedano ad utilizzare i dati acquisiti per inviare materiale pubblicitario, dovendosi tener conto delle sole specifiche finalità cui è preordinata la pubblicità del dato.

L'Autorità si è inoltre pronunciata in merito alla liceità dell'affissione, da parte di un'università, dell'elenco nominativo di tutti i soggetti che partecipano agli esami di Stato per l'abilitazione all'esercizio di una professione. Nella specifica vicenda si è ritenuta lecita la pubblicazione dei soli nominativi di coloro che avevano superato le prove d'esame, dal momento che la disciplina di settore (d.m. 9 settembre 1957) prevede un espresso regime di pubblicità solo per questa categoria di soggetti (*Nota* 22 aprile 2003).

La frammentarietà di queste fattispecie ha indotto l'Autorità ad aprire l'istrutto-

ria in vista dell'adozione di un provvedimento di carattere generale volto a riassumere vari aspetti relativi alla diffusione, in singoli casi, degli esiti concorsuali o delle graduatorie da parte di soggetti pubblici, in particolare se effettuata tramite Internet. Proprio in riferimento a quest'ultimo mezzo di diffusione, occorrono infatti soluzioni nuove e specifiche per contemperare l'esigenza di pubblicità di elenchi, liste e graduatorie con il diritto degli interessati a non subire un'ingiustificata divulgazione dei propri dati personali, in particolare quando vi sono dati di carattere sensibile.

È stata pure avviata, come già detto nel parag. 2, lett. *g)*, una collaborazione con il Ministero dell'università, dell'istruzione e della ricerca sul progetto relativo all'istituzione di un'anagrafe degli studenti universitari, con particolare riferimento alle modalità di trattamento di dati di carattere sensibile.

Sono in corso anche alcuni approfondimenti sull'attività di monitoraggio della presenza di allievi stranieri nel territorio provinciale, promossa 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 degli alunni stessi (in particolare, di informazioni relative all'origine razziale o etnica), nonché di altre delicate informazioni di carattere personale, come quelle concernenti adozioni o affidamenti.

23 Enti locali

Al fine di accelerare l'adeguamento da parte dei soggetti pubblici alle disposizioni in materia di trattamento di dati sensibili e giudiziari, proseguono le attività di collaborazione avviate dall'Autorità con organismi rappresentativi delle autonomie locali (Anci, Upi e Uncem).

Ciò anche alla luce delle modifiche introdotte dal Codice, che, come si è già sottolineato, impegna regioni ed enti locali, al pari di altre amministrazioni pubbliche, ad identificare e rendere pubblici non oltre il 30 settembre 2004 (pena l'illiceità del trattamento) i tipi di dati utilizzati e le operazioni effettuate, mediante un atto di natura regolamentare adottato in conformità al parere espresso dal Garante anche attraverso schemi tipo.

Il regolamento sui trattamenti di dati sensibili e giudiziari

Nell'ambito della collaborazione instauratasi, è stata già redatta una prima bozza di regolamento per comuni e comunità montane, da utilizzare per indicare poi 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 anche la sintetica, ma esauriente, descrizione dei trattamenti e dei flussi informativi.

È ormai imminente la pubblicazione del modello predisposto sul sito *web* dell'Anci e dell'Ancitel, al fine di poter raccogliere eventuali suggerimenti, integrazioni ed osservazioni prima che il Garante esprima il parere in proposito e lo ponga formalmente a disposizione dei comuni.

Sono inoltre in corso analoghe forme di collaborazione con l'Upi e con le regioni, per la stesura di analoghi schemi di regolamento utili per amministrazioni provinciali e regionali.

Per quanto riguarda, poi, la collaborazione con le regioni, si è anche tenuto conto dell'esigenza di coinvolgere il Ministero della salute, gli assessorati alla sanità (qualora non già presenti) e le aziende sanitarie locali, considerata la 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 proposito è opportuno aggiungere che il Garante è intervenuto sulla questione dell'individuazione del titolare dei trattamenti effettuati dalle amministrazioni regionali: con la decisione del 30 dicembre 2003 si è infatti chiarito che il titolare deve essere identificato nell'ente regione complessivamente considerato e non anche in suoi specifici uffici od organi, presso i quali possono operare, se designati, responsabili del trattamento.

Il sistema integrato Ina-Saia

Anche nel 2003 l'Autorità si è occupata dei flussi di dati anagrafici previsti dal sistema integrato Ina-Saia (Indice nazionale delle anagrafi-Sistema di accesso e interscambio anagrafico).

Il Garante, nel parere reso al Ministero dell'interno sullo schema di regolamento relativo alla gestione dell'Ina, ha sottolineato la necessità di individuare la fonte normativa legittimata a disciplinare l'utilizzo dei servizi Ina, non essendo adeguato il riferimento alle competenze attribuite dalla legge agli enti interessati. Apposite convenzioni dovrebbero inoltre individuare le specifiche finalità per le quali possono essere utilizzati i dati resi accessibili mediante il sistema. La possibilità di accedere ai servizi per i soggetti diversi dagli enti pubblici dovrebbe poi essere stabilita da una norma di legge o di regolamento e non da mere determinazioni amministrative (*Nota* 13 febbraio 2004).

Flussi documentali tra p.a.

Con riguardo alla gestione dei flussi documentali tra amministrazioni pubbliche, l'Autorità ha ricevuto un quesito dal Ministero dell'interno. La questione concerneva la possibilità di attivare un canale informativo tra l'Ufficio territoriale del Governo di Palermo e la Regione Sicilia, per verificare periodicamente le autocertificazioni presentate dai soggetti che ricoprono incarichi pubblici su nomina regionale, in particolare circa l'inesistenza delle condizioni di cui alla legge n. 55/1990 sulla prevenzione della delinquenza di tipo mafioso (art. 4, comma 1, lett. *h)*, l.r. n. 19/1997). Al riguardo, si è osservato che tale comunicazione dovrebbe essere prevista quantomeno da una norma di rango regolamentare, ancorché sia volta al perseguimento di finalità lecite, per le quali è consentito il trattamento di dati di carattere sensibile (autorizzazione del Garante n. 7/2002; cfr. pure l'art. 11 del d.lg. n. 135/1999).

È stato poi condiviso l'orientamento del Ministero in merito alla necessità che i controlli sulle autocertificazioni siano effettuati dall'amministrazione interessata tramite la consultazione del sistema informativo del casellario giudiziale, ovvero, per quelle informazioni non contenute nei relativi certificati, tramite la competente autorità giudiziaria (*Nota* 8 settembre 2003).

Tra le questioni allo studio dell'Autorità concernenti l'attività degli enti locali, è in corso di definizione quella relativa alle modalità della raccolta differenziata dei rifiuti solidi urbani, per i profili di eventuali violazioni della riservatezza degli interessati che ne possono discendere.

24 Notificazione di atti e comunicazioni

Conformemente alle indicazioni già fornite in passato (cfr. *Provv.* 22 ottobre 1998 e 26 ottobre 1999), il Garante ha ribadito l'esigenza di tutelare la riservatezza delle persone cui sono notificati atti e documenti attraverso l'adozione di prassi più rispettose della loro dignità, in attesa della modifica delle relative norme processuali.

Le novità apportate dall'art. 174 del Codice

La disciplina delle notificazioni degli atti giudiziari e degli altri atti è mutata con l'entrata in vigore del Codice, che ha accolto molte delle indicazioni a suo tempo già fornite dall'Autorità, intervenendo sulle relative disposizioni processuali (art. 174 d.lg. n. 196/2003).

Il principio alla base delle modifiche apportate dal Codice è quello secondo il quale, 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 nell'ambito del processo sia civile, sia 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.

È stata poi modificata anche la disciplina sulla pubblicazione degli avvisi concernenti le vendite giudiziarie. Il Codice ha, infatti, stabilito che negli avvisi relativi all'esecuzione immobiliare deve essere omessa l'indicazione del debitore e che nella vendita senza incanto i dati relativi al debitore possono essere forniti dalla cancelleria del tribunale a chiunque vi abbia interesse.

Visibilità di dati personali sulle buste

Nel merito delle questioni affrontate dall'Autorità nel settore in esame, va ricordato il caso di un istituto previdenziale che aveva inviato tramite posta una comunicazione ad un proprio assistito, utilizzando una busta con finestra trasparente. Ciò consentiva di leggere non solo i dati personali indispensabili all'invio della comunicazione alla persona cui era diretta, ma anche altre informazioni, quali la sua data di nascita e notizie sui rapporti di parentela.

A seguito dell'intervento dell'Autorità, l'istituto previdenziale ha quindi provveduto ad indicare le misure da adottare al riguardo, a cominciare dalla necessità di una modifica dell'applicazione informatica di acquisizione dei dati al fine di rilevare più chiaramente la differenza tra informazioni anagrafiche ed altri tipi di dati. L'istituto ha anche richiamato le sedi periferiche all'osservanza di talune istruzioni volte a tutelare la riservatezza degli interessati, come l'indicazione sulle buste del solo cognome, nome e indirizzo degli aventi diritto alle prestazioni e la menzione del codice fiscale soltanto in casi particolari.

Per quanto concerne, invece, la notifica da parte del comune, attraverso il messo comunale, di un invito a regolarizzare una violazione finanziaria, è stato ricordato che la possibilità per il messo (come pure per gli addetti al protocollo) di accedere al contenuto del documento non integra una violazione delle regole sulla comunicazione dei dati personali, trattandosi di soggetti incaricati del trattamento e per di più tenuti al segreto di ufficio in virtù del loro *status* di dipendenti pubblici (*Nota* 5 agosto 2003).

25 Pubblici registri, elenchi, atti e documenti conoscibili da chiunque

La materia del trattamento dei dati raccolti da pubblici registri, elenchi, atti e documenti conoscibili da chiunque continua a dar luogo a situazioni di insufficiente rispetto della *privacy*, come dimostrano i numerosi ricorsi e segnalazioni tuttora portati all'esame del Garante. Il problema è reso più complicato dalla presenza di normative di settore che solo in minima parte tengono conto dei diritti degli interessati alla protezione dei dati personali. Emblematiche in proposito sono le questioni relative all'accesso ai dati riguardanti procedure concorsuali, dove il rischio è l'azzeramento di fatto dell'efficacia del provvedimento di riabilitazione dal fallimento.

Ancor più significativo è poi il perdurare, pur dopo la legge n. 235/2000, di problemi nel settore dei protesti, dovuti in particolare al differente regime di cancellazione dei protesti cambiari rispetto a quelli levati per il mancato tempestivo pagamento di assegni bancari (sul punto, cfr. Corte cost., 14 marzo 2003, n. 70).

Delle problematiche derivanti dal trattamento dei dati raccolti da pubblici registri, elenchi, atti e documenti conoscibili da chiunque si è già parlato nel paragrafo 8.2., dedicato alle tutele esperibili nei confronti del trattamento dei dati personali concernenti il comportamento debitorio. Si è visto, in quella sede, che su tali aspetti sono stati proposti numerosi ricorsi, volti in particolare ad ottenere la cancellazione dei dati stessi.

Trattamento di dati provenienti da pubblici registri da parte di soggetti privati

Questioni analoghe sono state sottoposte all'attenzione del Garante anche al di fuori dei casi di proposizione di ricorso. Ha così formato oggetto di segnalazione all'Autorità il rifiuto della richiesta di cancellazione di dati personali concernenti la trascrizione di un pignoramento immobiliare da una banca dati gestita da una società e contenente informazioni tratte da pubblici registri. La società, nel rifiutare la cancellazione, ha osservato che i dati corrispondevano a quelli riportati dai pubblici registri (nel caso di specie, la conservatoria dei registri immobiliari) e potevano essere quindi modificati soltanto dopo l'annotazione in tali registri delle relative variazioni.

Nell'attuale assetto normativo, l'attività di consultazione, ad opera di privati, dei dati provenienti dalle conservatorie avviene anche attraverso apposito collegamento telematico; l'abilitazione a tale servizio è rilasciata con convenzione, in base al d.m. 10 ottobre 1992 ed alla circolare del Dipartimento del territorio n. 144T del 17 luglio 2000. Per quanto riguarda invece l'aggiornamento della banca dati catastale

25

ed ipotecaria, il decreto direttoriale del 28 febbraio 2002 stabilisce i termini di un giorno (per l'esecuzione delle formalità di iscrizione nonché di trascrizione di atti) e di novanta giorni (per le annotazioni a margine delle stesse formalità).

Prendendo spunto dalle questioni sottoposte alla sua attenzione, il Garante ha avviato pertanto un approfondimento sulla liceità e correttezza del trattamento di dati provenienti da pubblici registri effettuato in specie da parte di privati, in modo da fornire indicazioni sulla corretta applicazione della normativa in materia di protezione dei dati personali. Ciò specialmente in relazione alla prevista elaborazione sia del codice di deontologia in tema di dati provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (deliberazione del Garante n. 2 del 10 aprile 2002, e art. 61 del Codice), sia di quello in tema di trattamento di dati effettuato a fini di informazione commerciale (cfr. art. 119 del Codice).

In particolare, è stato rilevato che si deve valutare la conformità del termine di novanta giorni previsto per l'annotazione a margine delle formalità al principio della conservazione dei dati per il tempo necessario al perseguimento delle finalità per le quali gli stessi sono raccolti e successivamente trattati, anche con riguardo al più breve termine previsto per l'esecuzione delle formalità di iscrizione e trascrizione di atti.

Per quanto concerne, poi, la banca dati gestita dalla società, è emersa la questione della necessità di assicurare che i privati che gestiscono banche dati di questa categoria aggiornino i dati stessi e forniscano tempestivo riscontro alle richieste di rettificazione o cancellazione avanzate dagli interessati, anche quando negli elenchi pubblici da cui i dati sono tratti non si sia ancora provveduto al relativo aggiornamento.

In relazione a tale profilo, la società ha ipotizzato una soluzione provvisoria in base alla quale il gestore della banca dati cancellerebbe i dati personali relativi ad atti ancora riportati nei registri immobiliari, qualora gli interessati esibiscano copia autentica del titolo su cui si fonda la richiesta di cancellazione dell'atto e la ricevuta della conservatoria, attestante il deposito della domanda di annotazione della cancellazione presso la conservatoria medesima.

La direttiva comunitaria sul riutilizzo dei documenti del settore pubblico

Per quanto concerne gli aspetti di novità della disciplina comunitaria, si segnala anche l'adozione della direttiva n. 2003/98/CE sul riutilizzo dei documenti del settore pubblico, ai cui lavori preparatori ha partecipato attivamente, nell'ambito della delegazione italiana, l'Ufficio del Garante.

L'obiettivo della direttiva è quello di agevolare il riutilizzo delle informazioni del settore pubblico al fine di favorire la creazione di prodotti e servizi a contenuto informativo su scala comunitaria, anche nella prospettiva della diffusione di nuove piattaforme di comunicazione. L'esistenza di norme e prassi diverse negli Stati membri in materia di tariffe, tempi di risposta, accordi di esclusiva e disponibilità generale dei dati ai fini del riutilizzo, rendeva infatti necessaria un'armonizzazione al livello comunitario. Allo scopo di favorire lo sviluppo di prodotti e servizi informativi a valore aggiunto da parte delle imprese, nonché di limitare le distorsioni della concorrenza sul mercato europeo, la direttiva definisce un quadro di garanzie in materia di condizioni di mercato, tariffazione, tempi e modalità di risposta.

I principi dettati non incidono comunque sui regimi nazionali esistenti in materia di accesso ai documenti e sulle garanzie poste a tutela dei dati personali, che sono fatte espressamente salve dalla direttiva.

26 Attività fiscale e tributaria

Nel settore in esame l'Autorità è intervenuta per valutare alcuni aspetti relativi ad attività realizzate dal Ministero dell'economia e delle finanze e da altri soggetti operanti in ambito fiscale (agenzie fiscali e concessionari della riscossione).

In primo luogo il Garante ha approfondito talune problematiche in tema di protezione dei dati personali connesse all'adozione, da parte dell'Agenzia delle entrate, di un *call-center* e di un servizio via *web* volti a snellire il rapporto con i contribuenti, con particolare riguardo alla fase di identificazione di questi ultimi ed a quella di accesso alle informazioni contenute nell'anagrafe tributaria tramite l'uso di un *pin* e di una *password*.

Si è poi verificata la sussistenza dei presupposti di liceità per la comunicazione del codice fiscale, da parte dell'Agenzia delle entrate, ad amministrazioni pubbliche e gestori di pubblici servizi che ne abbiano fatto richiesta, nonché per la comunicazione degli elenchi dei contribuenti da parte dell'amministrazione finanziaria ai comuni e per la pubblicazione delle controversie dei contribuenti stessi da parte delle commissioni tributarie.

Richieste di dichiarazione stragiudiziale sui crediti del contribuente moroso

L'Autorità, a seguito di numerosi quesiti, segnalazioni e ricorsi, ha esaminato anche la prassi delle società concessionarie del servizio per la riscossione dei tributi di chiedere, senza il consenso del contribuente moroso, informazioni personali a terzi per ottenerne una dichiarazione stragiudiziale che attesti la presenza di crediti su cui rivalersi (cfr. *supra*, parag. 9.1.).

Tale attività, che comporta la comunicazione a terzi di informazioni concernenti la situazione debitoria del soggetto ritenuto moroso, è stata giudicata illecita in quanto nessuna previsione legislativa o regolamentare attribuisce alla società concessionaria il potere di effettuare questo tipo di trattamento senza il consenso del contribuente interessato: la procedura è risultata disciplinata, infatti, solo da risoluzioni dell'Agenzia delle entrate e da mere circolari ministeriali.

La procedura è stata inoltre ritenuta in contrasto con il principio di non eccedenza (art. 11 d.lg. n. 196/2003), in quanto sproporzionata rispetto alla finalità di recupero del credito che può essere comunque perseguita con altri strumenti.

In alcuni casi esaminati a seguito di ricorso il Garante ha quindi disposto il blocco del trattamento illecito dei dati di un contribuente da parte delle società concessionarie, che hanno dovuto sospendere l'utilizzo delle informazioni detenute, limitandosi solo a conservarle (*Newsletter* 22 febbraio 2004).

L'Agenzia ha poi emanato un'apposita risoluzione, volta a sollecitare i concessionari della riscossione ad astenersi da questa prassi (Risoluzione 35/E del 12 marzo 2004); a sua volta, l'Inps, con nota del 30 marzo 2004, prendendo atto di quanto stabilito dal Garante, ha deciso di sospendere l'attività di rilascio delle dichiarazioni stragiudiziali ai concessionari, in attesa di ulteriori delucidazioni.

Tra le attività svolte dall'Autorità va sottolineata la collaborazione con l'Ufficio centrale antifrode dei mezzi di pagamento (Ucamp) del Ministero dell'economia e delle finanze, in merito alla realizzazione ed alla gestione di una banca dati informatica relativa alle frodi effettuate attraverso mezzi di pagamento.

L'Autorità ha infine fornito indicazioni all'Ufficio federalismo fiscale del Ministero dell'economia e delle finanze, allo scopo di contribuire alla stesura di uno schema di decreto sullo scambio di informazioni tra l'amministrazione finanziaria e le regioni concernenti l'imposta regionale sulle attività produttive (Irap), rispettoso dei principi di liceità e correttezza del trattamento dei dati personali.

27 Attività giudiziaria ed informatica giuridica

Per quanto riguarda le informazioni contenute nei provvedimenti dell'autorità giudiziaria che dispongono il giudizio penale, il Garante ha ribadito che, fermo restando il rispetto dei principi di pertinenza e di non eccedenza, la normativa in materia di protezione dei dati non pregiudica l'esercizio dell'attività giudiziaria, in particolar modo quando il codice di rito preveda specificamente l'inserimento in tali provvedimenti di precise informazioni per determinate finalità processuali. Specifici suggerimenti sono stati peraltro formulati a proposito dell'eventuale notificazione degli atti per pubblici proclami.

Altra problematica, portata all'attenzione dell'Autorità da alcune segnalazioni, è quella della pubblicazione sui siti Internet dell'autorità giudiziaria di decisioni contenenti informazioni delicate relative alle parti in giudizio.

Pubblicazione *on line* di provvedimenti giurisdizionali

La questione è stata ora risolta dal Codice, il quale agevola sia l'accessibilità *on line* dei dati identificativi delle questioni pendenti presso le autorità giudiziarie di ogni ordine e grado (quindi anche i giudici amministrativi e contabili) da parte di chi vi ha legittimo interesse, sia l'accessibilità al pubblico delle sentenze e delle altre decisioni delle medesime autorità una volta depositate in cancelleria o in segreteria.

Le sentenze devono essere redatte secondo le ordinarie regole che individuano nominativamente tutte le parti interessate. Tuttavia, in caso di riproduzione in qualunque forma di sentenze o altri provvedimenti giurisdizionali effettuata nel quadro delle legittime e doverose attività di informazione a fini giuridici, prima che sia definito il giudizio si può chiedere per motivi legittimi all'autorità giudiziaria (che può disporla anche d'ufficio) l'apposizione sul provvedimento di un'annotazione volta a precludere l'indicazione, nella versione pubblicata, delle generalità e di altri dati identificativi degli interessati.

Una tutela rafforzata è poi garantita dagli artt. 51 e 52 del d.lg. n. 196/2003 per i minori e per i soggetti coinvolti in procedimenti in materia di rapporti di famiglia e di stato delle persone, indipendentemente dall'annotazione apposta sul provvedimento.

Formano oggetto di particolare approfondimento anche alcune iniziative istituzionali intraprese da tribunali e camere di commercio, che si propongono di rendere disponibili sui propri siti istituzionali banche dati contenenti informazioni e documenti relativi a procedure concorsuali.

Per quanto riguarda poi lo sviluppo di metodi alternativi di risoluzione delle controversie, è stato sottoposto all'attenzione dell'Autorità un protocollo di intesa tra una camera di commercio, un tribunale ed un consiglio dell'ordine degli avvocati, che prevede l'avvio di una fase sperimentale di conciliazione delegata fondata sull'individuazione, da parte delle istituzioni coinvolte, di un numero di controversie idonee ad un efficace esperimento del tentativo di composizione stragiudiziale.

Consultazione del casellario giudiziale da parte delle p.a.

In merito alle problematiche connesse all'adozione del decreto dirigenziale del Ministero della giustizia regolante la consultazione del casellario giudiziale da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi, si rimanda alla specifica trattazione che ne verrà fornita nel paragrafo sull'attività consultiva del Garante rispetto agli atti del Governo (cfr. diffusamente, parag. 45.2.)

28 Attività di polizia e Guardia di finanza

Nel settore in esame, l'Autorità si è occupata tra l'altro di verificare talune modalità con le quali la Guardia di finanza accerta le posizioni reddituali e patrimoniali dei nuclei familiari dei soggetti beneficiari di prestazioni sociali agevolate. In particolare, il Garante è intervenuto in una vicenda in cui una struttura periferica del Corpo aveva richiesto ad un comune alcuni elenchi nominativi di beneficiari corredati di tutta la relativa documentazione, a partire dalla tipologia della prestazione sociale e dall'importo del contributo erogato.

A seguito dell'intervento dell'Autorità, il Comando generale ha impartito specifiche direttive alla struttura periferica chiarendo che, in una prima fase del controllo, devono essere acquisiti solo i nominativi dei beneficiari. Ulteriori elementi possono essere eventualmente acquisiti solo in una fase successiva, qualora emerga la reale necessità di svolgere approfondimenti sulla situazione economica dei soggetti sottoposti a controllo.

È in procinto di essere completata la verifica su un protocollo di intesa sottoscritto tra una regione e la Guardia di finanza ai fini del coordinamento dei controlli e dello scambio di informazioni in materia di spesa sanitaria, che presenta profili critici sul piano della proporzionalità e liceità delle modalità di trattamento previste.

Sono stati pure avviati specifici accertamenti sull'attivazione di un sistema infor-

matico realizzato da un comune al fine di garantire alle forze di polizia un accesso preferenziale alle banche dati dell'ente. In particolare, il comune ha consegnato alla Guardia di finanza, all'Arma dei carabinieri ed alla Polizia di Stato una *smart card* con i connessi codici di sicurezza, che consente l'accesso ad una serie di dati personali dei cittadini di carattere anagrafico, patrimoniale, fiscale e giudiziario.

Acquisizione di dati per via telematica da parte delle autorità di p.s.

In argomento va anche ricordato che, dopo le modifiche introdotte dal Codice, l'acquisizione presso terzi di informazioni e documenti da parte delle autorità di pubblica sicurezza e delle forze di polizia, in conformità alla legge ed ai regolamenti, può essere realizzata anche per via telematica attraverso convenzioni, 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 d.lg. n. 196/2003), anche sulla base di convenzioni-tipo adottate dal Ministero dell'interno su conforme parere del Garante.

29 Rapporto di lavoro

L'Autorità si è pronunciata più volte sul tema della protezione dei dati personali nel settore del lavoro e della previdenza sociale, oggetto ora della specifica disciplina dettata dal Titolo VIII del Codice.

Comunicazione o diffusione di dati sulla salute dei dipendenti

Nel settore del pubblico impiego sono stati anzitutto esaminati alcuni casi 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 sia rispettato anche il principio di necessità, in virtù del quale possono essere oggetto di trattamento soltanto i dati indispensabili al raggiungimento di tale finalità. Non è stata ad esempio ritenuta rispondente al principio di necessità l'indicazione, in questo tipo di comunicazione, del luogo del ricovero di un dipendente e della gravità dei motivi di salute su cui era fondata la sua sostituzione, tenuto oltretutto conto dell'invio della comunicazione anche alle rappresentanze sindacali (*Nota* 4 settembre 2003).

Trattamento di dati del personale delle forze armate e di polizia

È in procinto di essere ultimata l'attività del tavolo di lavoro sul trattamento dei dati del personale delle forze armate e di polizia promosso dall'Autorità in collaborazione con le amministrazioni interessate. L'iniziativa mira ad approfondire congiuntamente alcune questioni riguardanti, in particolare, la gestione dei fascicoli personali dei dipendenti, per consentire l'elaborazione di indicazioni e soluzioni a tutela della riservatezza e degli altri diritti degli interessati.

Nell'ambito di tale tavolo di lavoro sono state esaminate varie questioni, tra cui:

- la richiesta di documentare la diagnosi, oltre alla prognosi, indirizzata ai dipendenti che si assentano dal servizio per motivi di salute, e la successiva

conservazione della relativa documentazione nel fascicolo personale;

- il trattamento dei dati sulla salute connesso agli accertamenti dell'idoneità psico-fisica al servizio svolti nei confronti del personale, sia al momento dell'assunzione, sia in costanza del rapporto di lavoro;

- il trattamento dei dati sensibili contenuti in documenti quali il fascicolo personale, il foglio matricolare ed altri atti, con particolare riferimento al principio di necessità dei dati stessi e al periodo della loro conservazione.

L'iniziativa ha consentito anche di sollecitare la cessazione di talune prassi adottate da strutture periferiche delle amministrazioni, già portate all'attenzione dell'Autorità.

Si è posto così rimedio anche al caso verificatosi in un istituto penitenziario, dove era stata affissa in bacheca una lista del personale assente per malattia comprensiva di nominativi, periodi di prognosi e diagnosi. Nel novembre del 2003 l'amministrazione penitenziaria ha emanato una circolare con la quale ha richiamato gli uffici periferici al rispetto delle rigorose cautele apprestate dalla normativa sulla protezione dei dati a tutela delle informazioni di carattere sensibile, con particolare riguardo al divieto di diffondere le notizie sulla salute.

Sempre in materia di trattamento di dati del personale delle forze armate e di polizia, un dipendente di una questura ha presentato un ricorso lamentando che le informazioni relative alle sue condizioni di salute, accertate nel corso di una visita medica cui era stato sottoposto per verificare la sua idoneità al servizio, erano state comunicate ad altri soggetti al fine del ritiro cautelativo dell'arma in dotazione e del tesserino di servizio.

In proposito, l'Autorità ha però constatato che tali comunicazioni erano avvenute lecitamente, in quanto effettuate in conformità alle disposizioni sulle autorizzazioni di polizia per la detenzione ed il porto d'armi e finalizzate all'adozione dei relativi provvedimenti (*Provv.* 15 gennaio 2004).

Questionari di valutazione

In un altro ricorso, il Garante si è invece pronunciato sulla liceità della gestione di questionari di valutazione dell'attività svolta da dipendenti dell'amministrazione.

In particolare, sono stati reputati conformi alla normativa sulla protezione dei dati la raccolta e l'esame di schede anonime di valutazione, quando il trattamento coinvolga soltanto uffici interni all'amministrazione interessata. Si devono peraltro adottare tutte le necessarie misure di sicurezza, anche diverse da quelle minime, al fine di assicurare che i dati contenuti nei questionari siano trattati dal personale specificatamente individuato, per le sole finalità conformi a quelle che rendono lecito il trattamento e con modalità operative rispettose dei principi di pertinenza e di non eccedenza (*Provv.* 22 settembre 2003).

In relazione alla gestione della documentazione matricolare del personale militare, l'Autorità ha inoltre esaminato il ricorso di un dipendente che lamentava l'illiceità della conservazione nel suo stato matricolare di informazioni che lo riguardavano, concernenti l'applicazione di una pena concordata, in quanto erano trascorsi cinque anni dalla data di irrevocabilità della sentenza ed era avvenuta l'estinzione del reato (art. 445, comma 2, c.p.p.).

29

Il Garante ha giudicato infondato il ricorso poiché nel caso di specie non risultavano violate né la normativa di settore (r.d. n. 1236 del 1941), né le disposizioni sulla correttezza e l'aggiornamento dei dati personali; ha poi constatato la liceità del trattamento di informazioni di carattere giudiziario da parte dell'amministrazione per finalità di gestione del rapporto di lavoro (*Provv*. 17 aprile 2003).

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. L'accertamento preliminare ha rilevato che l'elenco era effettivamente accessibile da chiunque attraverso la pagina di apertura di tale sito.

La questione risultava rilevante, visto l'ingente numero di soggetti interessati dalla diffusione indiscriminata di dati idonei a rivelare il loro stato di salute. Il Garante ha pertanto curato ulteriori approfondimenti ai fini del blocco del trattamento, considerando che le disposizioni di settore (art. 8 legge n. 68/1999) non definiscono le modalità per garantire la pubblicità degli elenchi e delle graduatorie degli aventi diritto al collocamento obbligatorio.

Anche a tale proposito occorre comunque 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, dai regolamenti o dalla normativa comunitaria (art. 68, comma 3, d.lg. n. 196/2003).

Comunicazione all'Inail di dati sulla salute dei pazienti

L'Autorità ha altresì verificato la liceità delle segnalazioni trasmesse da medici all'Inail circa le malattie riscontrate nei pazienti, collegabili allo svolgimento di attività lavorative.

Sul punto si è precisato che, secondo il quadro normativo vigente (d.P.R. n. 1124/1965; d.m. 18 aprile 1973 e d.lg. n. 38/2000), il medico può trasmettere all'istituto assicuratore e ad altri organismi preposti le segnalazioni di malattie professionali che potrebbero essere state causate da un'attività lavorativa potenzialmente nociva, indicandone l'anamnesi lavorativa, i rischi e le sostanze cui il lavoratore sia (o sia stato) esposto.

Questa comunicazione deve essere però effettuata nel rispetto delle specifiche disposizioni in tema di assicurazioni contro gli infortuni sul lavoro e le malattie professionali, nonché del principio di pertinenza dei dati rispetto alle finalità per cui sono raccolti e successivamente trattati. (*Nota* alla procura della Repubblica di Torino del 27 ottobre 2003).

È infine nuovamente 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.

30 Ricerca statistica

Codice deontologico

Il 1° ottobre 2002 è entrato in vigore il codice di deontologia e di buona condotta per i trattamenti dei dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Sistan), ora allegato al Codice in materia di protezione dei dati personali.

Il codice deontologico regolamenta l'attività di ricerca statistica effettuata da enti ed uffici statistici che fanno parte, o partecipano, al Sistan per la realizzazione del programma statistico nazionale o per la produzione di informazione statistica in conformità ai rispettivi ambiti istituzionali.

Ai sensi dell'art. 106 del d.lg. n. 196/2003, il Garante deve promuovere la sottoscrizione di uno o più codici di deontologia e buona condotta per soggetti pubblici e privati, comprese le società scientifiche e le associazioni professionali, che trattano dati personali per scopi scientifici e statistici. Dopo l'adozione, a suo tempo, dell'atto di iniziativa, è stato ora portato a compimento il complesso *iter* che dovrebbe consentire di definire, entro un breve termine, un secondo codice deontologico di disciplina della ricerca statistica e scientifica effettuata da società scientifiche, nonché da istituti universitari, enti di ricerca e organismi non appartenenti al Sistan.

Con riferimento al Programma statistico nazionale per gli anni 2004-2006, e tenuto conto dei poteri di indirizzo e di coordinamento spettanti all'Istat nei confronti delle attività statistiche del Sistan, l'Autorità ha sollecitato il pieno rispetto del codice deontologico e della normativa di settore (d.lg. n. 322/1989), chiedendo all'Istituto di verificare l'effettivo adempimento alle relative prescrizioni prima dell'avvio dell'attività prevista dal Programma (*Nota* 1° settembre 2003).

Dati censuari

L'Autorità ha poi ultimato gli accertamenti istruttori già avviati in ordine allo svolgimento del quattordicesimo censimento generale della popolazione, per verificare la conformità delle operazioni censuarie alla normativa sulla protezione dei dati personali, anche in riferimento a trasferimenti di dati in Romania ed in Croazia.

Nel corso del censimento era altresì pervenuta la segnalazione della conservazione di dati censuari in un ufficio comunale anche successivamente al termine delle operazioni di raccolta. A seguito degli accertamenti effettuati dall'Autorità, è emerso che tali dati venivano trattati per svolgere operazioni di confronto con l'anagrafe e di revisione qualitativa dei questionari e sarebbero stati distrutti dopo la conclusione di queste operazioni. Il Garante ha, quindi, provveduto ad accertare l'avvenuta distruzione del materiale (Nota Istat 11 luglio 2003).

È ancora all'attento esame del Garante la questione del censimento linguistico nella Provincia di Bolzano, in merito alla quale già in passato è stata più volte evidenziata alle autorità di governo, a quelle comunitarie e ad organi locali la necessità di un intervento legislativo per conformare le disposizioni attuative dello Statuto provinciale alla normativa sulla protezione dei dati. Tale questione è oggetto, peraltro, di una denuncia di infrazione al diritto comunitario presentata alla Commissione europea. Sul punto l'Autorità tornerà entro breve ad evidenziare punti critici rimasti irrisolti e che anzi, per certi aspetti, sono stati resi più problematici.

31 Ordini e collegi professionali

Nel corso del 2003 sono pervenuti ancora quesiti sul trattamento dei dati personali relativi a soggetti iscritti ad albi e collegi professionali.

In questa materia l'Autorità ha ribadito quanto già affermato in passato e cioè che la legge n. 675/1996 non aveva modificato la disciplina previgente sul regime di pubblicità degli albi e sulla conoscibilità degli atti connessi allo *status* di iscritto.

Rispondendo nuovamente a quesiti e segnalazioni, il Garante ha poi sottolineato le significative innovazioni introdotte in argomento dal Codice, chiarendo anche la portata della nuova disciplina.

Le novità introdotte dal Codice (art. 61)

In primo luogo, è stato ricordato che, ai sensi dell'art. 61 del d.lg. n. 196/2003, 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 anche a privati e diffondere pure per via telematica 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.

L'Ufficio ha poi precisato, in risposta alla segnalazione di un iscritto all'Ordine dei medici chirurghi e degli odontoiatri, che 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 (art. 61, comma 3, cit.). Si é inoltre chiarito che, sempre a richiesta dell'interessato, possono essere fornite a terzi informazioni supplementari, ad es. quelle relative a speciali qualificazioni professionali non menzionate nell'albo o all'eventuale disponibilità a ricevere materiale informativo a carattere scientifico (art. 61, comma 4, d.lg. n. 196/2003).

In merito alle modalità di diffusione dei dati degli iscritti, si è peraltro rilevato che compete a ciascun ordine o collegio professionale valutare quali siano le più appropriate, sottolineando che il Codice autorizza comunque espressamente la pubblicazione dei dati divulgabili su siti Internet istituzionali o mediante altre reti di comunicazioni elettronica (art. 61, cit., comma 2).

Il Garante è anche tornato ad occuparsi della disciplina sulla divulgazione delle informazioni relative a provvedimenti disciplinari. Al riguardo è stato specificato che può essere divulgata pure l'esistenza di provvedimenti atti ad incidere sull'attività dell'iscritto all'albo (come ad es. la sospensione), fermo restando il dovere di porre in circolazione informazioni corrette, complete ed aggiornate, specie con riguardo ad eventuali sviluppi favorevoli per gli interessati (*Nota* 30 dicembre 2003).

Comunicazione di informazioni aggiuntive

Su richiesta dell'Ordine professionale degli assistenti sociali della Regione Sicilia, l'Autorità ha infine precisato che, al di là delle informazioni contenute negli albi professionali in base alla disciplina di settore o alle istanze formulate sul punto dagli stessi interessati nei termini appena precisati, non si possono comunicare a soggetti privati informazioni aggiuntive relative agli iscritti in mancanza di specifiche dispo-

sizioni normative che consentano tale comunicazione (quali ad es. quelle sull'accesso ai documenti amministrativi).

Al contrario, le informazioni aggiuntive possono essere comunicate ad altri soggetti pubblici anche in assenza di un'apposita disposizione che lo consenta, qualora ciò risulti necessario per lo svolgimento delle funzioni istituzionali e ne venga data previa notizia al Garante (art. 19, comma 2, d.lg. n.196/2003).

V - La privacy e le sfide del futuro
Reti di comunicazioni

32 Telefonia e reti di comunicazioni

32.1. Profili generali

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale. Sul punto il Codice ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lg. n. 171/1998, come modificato dal d.lg. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

32.2. Dati relativi al traffico telefonico

Si è già sintetizzata in altra parte della presente Relazione (cfr. parag. 1.11.) la recente vicenda che ha portato a modificare l'art. 132 del Codice e ad individuare garanzie rafforzate in riferimento al più lungo periodo di conservazione dei dati del traffico telefonico. In questa sede giova solo ricordare che il Garante, in conformità a quanto previsto dall'art. 132, comma 5, come modificato dalla legge n. 45/2004, definirà al più presto le misure e gli accorgimenti al cui rispetto è subordinato il trattamento dei dati relativi al traffico telefonico per le finalità di accertamento e repressione dei reati.

32.3. Fatturazione dettagliata ed altre questioni

Anche nel corso del 2003 l'Autorità si è occupata delle questioni connesse al mascheramento delle ultime tre cifre dei numeri telefonici nelle fatture inviate agli abbonati, che rappresenta una delle misure indicate dal Codice per tutelare la riservatezza degli abbonati chiamati, nonché degli utenti diversi dall'abbonato i quali effettuino chiamate dai terminali cui corrisponde l'abbonamento.

Nonostante i numerosi provvedimenti adottati in passato dal Garante, persistono alcuni nodi problematici testimoniati anche dai perduranti reclami e segnalazioni che pervengono all'Autorità.

Delle problematiche legate all'accesso alle informazioni incluse nella fatturazione,

ai limiti all'esercizio del diritto di accesso alle chiamate "in entrata" e alle cd. chiamate di disturbo, si è già parlato (cfr. *supra*, parag. 7.5.). In questa sede occorre, invece, sottolineare che durante il 2003 il Garante ha svolto approfondimenti in materia, destinati a confluire in un imminente provvedimento sulla fatturazione dettagliata, che riguarderà, fra l'altro, gli addebiti sulla linea telefonica dovuti a chiamate verso numeri a tariffazione speciale e a chiamate in entrata che comportano un costo per il ricevente.

Modalità di pagamento alternative alla fatturazione

In tale occasione saranno nuovamente esaminate le problematiche relative alla possibilità che le chiamate effettuate da qualsiasi terminale vengano pagate con modalità alternative alla fatturazione, e alla necessità di garantire in taluni casi la persona fisica del chiamante, ad esempio attraverso l'uso di carte prepagate (cfr. art. 5, comma 1, d.lg. n. 171/1998; ora, art. 124, comma 2, del Codice).

In proposito, secondo quanto confermato dal Codice, va ribadita l'importanza –per la tutela della sfera privata dei chiamanti, diversi dall'abbonato– dell'effettiva e diffusa disponibilità sul mercato di tali modalità alternative, il cui preventivo accertamento da parte del Garante, oltre che per eventuali provvedimenti sfavorevoli nei confronti dei titolari del trattamento inadempienti, costituirà presupposto indispensabile per autorizzare i fornitori ad indicare nella fatturazione i numeri completi relativi alle comunicazioni (art. 124, comma 5, del Codice).

In via preliminare, l'Autorità ha comunque già predisposto una prima nota di carattere generale volta a definire le modalità alternative alla fatturazione, anche anonime, che i fornitori di servizi di telefonia devono rendere disponibili da ogni terminale.

32.4. Banca dati unica dei numeri di telefonia fissa e mobile e nuovi elenchi telefonici

Con la deliberazione dell'Autorità per le garanzie nelle comunicazioni n. 36/02/Cons del 6 febbraio 2002 è stata prevista la costituzione della banca dati dove confluiranno alcuni dati personali di tutti gli abbonati e titolari di carte prepagate e in base alla quale potranno essere realizzati nuovi elenchi telefonici in formato cartaceo ed elettronico. In proposito va segnalato che è in fase avanzata l'analisi di quei profili che, nell'ambito della realizzazione di tale banca dati, riguardano più propriamente l'osservanza della normativa sulla protezione dei dati personali.

In particolare, i principali fornitori di servizi di telefonia fissa e mobile stanno predisponendo, in collaborazione con il Garante, versioni perfezionate dei modelli di informativa e consenso ispirate al rispetto della normativa sulla tutela dei dati personali, da sottoporre (tramite diverse modalità, a seconda che si tratti o meno di clienti con i quali già sussiste un rapporto) all'attenzione degli interessati, al fine dell'inserimento dei loro dati nella banca dati in discorso e, quindi, nei nuovi elenchi telefonici.

La problematica ha richiesto particolari approfondimenti, venendo in considerazione un "serbatoio" di informazioni dal quale innumerevoli soggetti potranno attingere per utilizzare dati relativi ai recapiti ed al numero di utenza degli interessati. La chiarezza, sinteticità e univocità dell'informativa è quindi essenziale per far comprendere a tutti gli abbonati le conseguenze che si determinano nel breve e medio periodo allorché si acconsenta all'utilizzo da parte di terzi dell'indirizzo o del numero di telefono anche mobile per inviare messaggi, missive, *fax*, *Sms* o *Mms*, altre chiamate vocali, ecc.

Con specifico riguardo agli elenchi, il Garante ha infatti segnalato come la relativa disciplina normativa sia stata recentemente oggetto di significative modifiche che ne hanno mutato in radice la natura e le finalità. Non a caso, quindi, il Codice ha attribuito a questa Autorità il compito di individuare, con proprio provvedimento, 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 (art. 129).

Il Garante è pertanto in procinto di adottare tale provvedimento al fine di individuare, in particolare, idonee modalità di manifestazione del consenso degli interessati con riguardo sia alla semplice inclusione dei loro dati negli elenchi, sia all'utilizzo ulteriore dei medesimi dati per finalità riconducibili ad operazioni commerciali, di *marketing*, sondaggi, o simili.

32.5. Altre attività di cooperazione con l'Autorità per le garanzie nelle comunicazioni

In linea con gli obiettivi individuati nel corso della riunione congiunta fra il Garante e l'Autorità per le garanzie nelle comunicazioni del 20 febbraio 2003, si è intensificata l'attività di cooperazione fra le stesse.

Oltre ad incontri su temi di interesse comune, come il nuovo elenco telefonico unico per tutti gli operatori di telefonia fissa e mobile, nonché i servizi non richiesti, il Garante ha partecipato alla consultazione pubblica relativa all'introduzione in Italia del protocollo Enum (*e-number*), ponendo l'attenzione sulle problematiche concernenti la tutela della riservatezza degli interessati.

Protocollo Enum

Il protocollo Enum consente infatti di associare indirizzi Internet e numeri telefonici, al fine di realizzare un numero identificativo universale in grado di instradare il traffico verso i diversi recapiti dell'interessato, rendendo quest'ultimo facilmente rintracciabile.

L'Autorità, nel formulare le considerazioni preliminari sui possibili aspetti critici della materia, ha in particolare evidenziato agli operatori aderenti all'iniziativa alcuni profili relativi alla sicurezza e protezione dei dati personali. I primi risultati della consultazione, discussi anche all'interno di un *workshop* al quale hanno partecipato pure alcuni rappresentanti di questa Autorità, sono stati pubblicati nella *Gazzetta Ufficiale* del 24 aprile 2003, n. 95, e sono disponibili sul sito Internet dell'Autorità per le garanzie nelle comunicazioni *(www.agcom.it)*.

Carrier preselection

Sempre nel corso del 2003 si sono svolti incontri fra alcuni rappresentanti delle due Autorità di garanzia, al fine di verificare diversi punti problematici relativi alla tematica della *carrier preselection (Cps)*, ossia del sistema mediante il quale l'abbonato può instradare il proprio traffico telefonico verso un operatore preselezionato. Ciò, con particolare riferimento agli eventuali limiti ed alle modalità dei trattamenti dei dati connessi alle procedure per la disattivazione della *Cps*. Sull'argomento, l'Autorità ha già predisposto uno schema di provvedimento volto a chiarirne gli aspetti più controversi, ad esempio la necessità o meno per l'operatore di accesso di richiedere il consenso degli interessati.

32.6. Servizi non richiesti e consenso dell'interessato

Anche durante il periodo considerato il Garante ha prestato attenzione alle delicate questioni concernenti l'attivazione di contratti e servizi di telefonia mobile e fissa senza il preventivo consenso degli interessati, in riferimento a casi nei quali si verificano seri danni per gli interessati stessi. Sono stati effettuati anche taluni impegnativi interventi di carattere ispettivo. Uno degli interventi più significativi forma oggetto di trattazione dettagliata nel paragrafo di questa *Relazione* concernente le attività ispettive del capitolo relativo all'attività del Garante (cfr. *infra*, parag. 51.3.).

Sulla base delle informazioni acquisite, è già allo studio l'emanazione di un provvedimento di carattere generale volto ad offrire ulteriori indicazioni e chiarimenti in materia.

32.7. Comunicazioni indesiderate ed utenze telefoniche mobili

Il fenomeno delle comunicazioni di carattere pubblicitario o informativo realizzate su utenze telefoniche mobili ha subito di recente un'enorme espansione, vista la particolare efficacia con cui l'invio di *Sms (Short message service)* permette di comunicare in tempo reale con un numero elevato di interessati, ovunque essi si trovino, con modalità che possono, tra l'altro, risultare particolarmente invasive (si pensi alle ipotesi di ricezione del messaggio in orari notturni).

L'uso pur legittimo degli *Sms* presuppone dunque apposite cautele, specificamente evidenziate da questa Autorità in alcuni provvedimenti.

Sms *istituzionali*

Sms istituzionali

Il Garante ha individuato i principi che i fornitori di servizi di telecomunicazioni e le amministrazioni pubbliche sono tenuti a rispettare per l'invio degli *Sms* cd. istituzionali e cioè di quei messaggi utilizzati da amministrazioni centrali o locali per campagne informative e di sensibilizzazione (ad esempio, in relazione a giornate dedicate a particolari tematiche) o per diffondere notizie ritenute di pubblica utilità (ad esempio, in tema di viabilità, avvenimenti culturali, termini di pagamento di tasse o imposte o validità di documenti).

In un provvedimento del 12 marzo 2003, l'Autorità ha innanzitutto distinto l'ipotesi dell'invio effettuato da gestori di servizi telefonici su incarico delle pubbliche amministrazioni (con utilizzazione dei dati dei propri abbonati senza trasmetterli all'amministrazione che dispone l'invio) da quella dell'inoltro effettuato direttamente dal soggetto pubblico (che ha raccolto in proprio i dati degli abbonati).

Con riguardo al primo caso, è stato osservato che l'utilizzazione dei numeri di telefonia mobile da parte dei gestori per conto della pubblica amministrazione non può prescindere dal consenso espresso degli abbonati, prestato in forma specifica e documentato per iscritto, sia per semplici comunicazioni informative (blocco del traffico, pagamento tributi, ecc.), sia per ulteriori fini di pubblica utilità legati ad eventi culturali, ricorrenze o altro.

Si è inoltre specificato che gli operatori telefonici possono inviare *Sms* istituzionali, prescindendo dal consenso, solo in caso di disastri e calamità naturali o altre reali emergenze di ordine pubblico, e che l'invio dei messaggi in deroga alla disciplina sulla protezione dei dati può essere legalmente disposto solo da un soggetto

32

pubblico che adotti, se consentito dalla legge, un provvedimento d'urgenza per ragioni di ordine pubblico, igiene e sanità pubblica.

L'amministrazione pubblica deve a tal fine valutare preventivamente se la norma di legge che prevede l'adozione di provvedimenti urgenti conferisca effettivamente anche il potere di derogare alla disciplina in materia di trattamento dei dati personali e che, in presenza di accertati presupposti di necessità ed urgenza, la situazione di pericolo per la popolazione non possa essere affrontata con strumenti ordinari.

Gli operatori telefonici devono, in ogni caso, informare preventivamente ed adeguatamente gli utenti della possibilità di ricevere eventuali *Sms* istituzionali, nonché della possibilità di manifestare il consenso a ricevere solo alcune categorie di informazioni e non altre. L'interessato deve avere inoltre la possibilità di esercitare i propri diritti agevolmente e gratuitamente, anche in caso di precedente manifestazione del consenso. Gli operatori devono rispettare in ogni caso l'art. 9 della legge n. 675/1996 (ora, art. 11 del Codice). Di regola devono perciò essere seguite forme di comunicazione che non implichino l'identificazione nominativa degli abbonati. Inoltre l'operatore deve utilizzare i dati nei limiti e per il tempo necessario a trasmettere il messaggio.

Con riguardo, invece, all'invio di *Sms* istituzionali direttamente da parte dei soggetti pubblici ad utenti che abbiano liberamente lasciato i propri recapiti soltanto per essere informati sull'esito di una pratica o per ricevere sistematicamente alcuni tipi di messaggi (anche tramite reti civiche), il Garante ha chiarito che l'acquisizione del consenso è esclusa per l'invio di tali comunicazioni strettamente istituzionali.

È stato comunque richiamato l'obbligo dei soggetti pubblici di informare l'utente sulle modalità e sugli scopi dell'utilizzo dei dati che lo riguardano, nonché il principio secondo cui l'uso dei dati per l'invio degli *Sms* deve essere limitato alle finalità per le quali i dati sono stati rilasciati dagli utenti all'amministrazione.

***Sms* pubblicitari**

Sms *pubblicitari*

Con un provvedimento del 10 giugno 2003 il Garante ha sottolineato l'illiceità dell'invio di *Sms* pubblicitari senza il preventivo consenso libero ed informato degli abbonati, nonché dell'espediente adottato da alcuni fornitori di servizi telefonici, di subordinare la stipula del contratto o l'attivazione della carta prepagata alla prestazione del consenso a ricevere messaggi pubblicitari. Si è pure evidenziato come sia illecito inserire tra gli obblighi contrattuali una dichiarazione *standard* di "impegno" all'invio degli *Sms* commerciali.

Anche i ben distinti messaggi con i quali le società telefoniche pubblicizzano servizi o opportunità che presuppongono un onere aggiuntivo per la clientela –come ha avuto modo di indicare l'Autorità con decisione del 9 aprile 2003– danno luogo ad un trattamento di dati a scopo promozionale ammesso solo con il consenso informato dell'interessato.

L'Autorità ha, inoltre, precisato che il principio del consenso libero ed informato trova applicazione anche nei confronti dei soggetti che trasmettono *Sms* pubblicitari senza estrarre i numeri delle utenze telefoniche da un'apposita banca dati, bensì sulla base di una composizione casuale o automatizzata di numeri, che prescinda da una verifica della loro esistenza o attivazione.

È stato chiarito, ancora, che la necessità di raccogliere una chiara e specifica manifestazione di volontà dei destinatari sussiste anche nel caso in cui gli *Sms* pubblicitari siano inviati da soggetti diversi dai fornitori di servizi di telefonia mobile, quali i fornitori di servizi telematici (ad esempio, gestori di siti *web* che offrano la possibilità di disporre gratuitamente di una casella di posta elettronica).

L'inosservanza dei principi fin qui sintetizzati è stata accertata in diversi ricorsi esaminati dal Garante nel corso dell'anno e concernenti l'invio anche notturno di *Sms* promozionali indesiderati. In questi casi l'Autorità ha avviato procedimenti autonomi rispetto a quelli instaurati con i ricorsi, al fine di verificare i presupposti per applicare sanzioni amministrative, per adottare altri provvedimenti e per l'eventuale denuncia all'autorità giudiziaria penale, in relazione ai reati che si possono configurare anche a seguito della mancata acquisizione del consenso informato degli interessati (*Provv.* 13 e 19 novembre 2003).

Il Codice, nel dettare una disciplina specifica in materia di comunicazioni commerciali non sollecitate, ha peraltro equiparato, quanto alla normativa applicabile, strumenti quali posta elettronica, *Sms*, *Mms* e *fax* (art. 130). Ne discende l'inapplicabilità, ai trattamenti effettuati con tali mezzi, delle fattispecie equipollenti al consenso dell'interessato di cui all'art. 24 del Codice e, quindi, anche l'inoperatività della disposizione riguardante, all'interno di tale articolo, i trattamenti di dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

32.8. Messaggi multimediali (cd. Mms*) e videochiamate*

Completata, con l'adozione del provvedimento del 12 marzo 2003 (in *Relazione* 2002, p. 115) l'analisi delle problematiche legate ai messaggi multimediali (*Mms*), il Garante ha esaminato la questione dei trattamenti di dati personali effettuati in occasione delle cd. videochiamate, ossia delle chiamate (realizzate attualmente tramite la rete *Umts*) nel corso delle quali possono essere trasmesse, oltre a suoni, immagini dei soggetti coinvolti nella conversazione.

La caratteristica peculiare di tali trattamenti consiste nel fatto che, a differenza di quanto accade per l'invio dei *Multimedia messaging service (Mms)*, vengono raccolte immagini contestualmente all'effettuazione della chiamata, le quali riguardano peraltro contemporaneamente il chiamante, il chiamato e persone eventualmente a loro vicine.

In proposito sono in corso di predisposizione chiarimenti ed indicazioni volte ad evitare che in occasione di questo tipo di chiamate si possano violare i diritti dei soggetti a vario titolo coinvolti.

32.9. Localizzazione

Con l'adozione del d.lg. n. 196/2003 è stata introdotta nel nostro ordinamento una disciplina specifica sul tema della localizzazione, che prevede apposite cautele per il trattamento dei dati relativi all'ubicazione diversi dai dati di traffico (art. 126). Ciò, sia per la specifica informativa che il titolare deve rendere preventivamente all'attivazione del servizio, sia in termini di revocabilità del consenso o momentaneo "congelamento" del servizio. La norma dispone infatti che l'interessato possa interrompere gratuitamente e mediante una funzione semplice, anche temporaneamente, il servizio a valore aggiunto.

Proprio in ragione della particolare delicatezza che caratterizza questo tipo di dati, l'Autorità adotterà entro breve termine, sulla base dei risultati di uno studio già ultimato in proposito, un provvedimento per chiarire alcuni termini della questione. Appare comunque utile ricordare che la Commissione europea ha affrontato alcuni aspetti della materia nella Raccomandazione del 25 luglio 2003 (2003/558/CE) sul trattamento delle informazioni relative alla localizzazione del chiamante sulle reti di comunicazione elettronica a fini della fornitura di servizi di chiamata di emergenza con capacità di localizzazione.

33 Trattamento di dati personali in Internet

33.1. Profili generali

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Nel corso del 2003 il Garante ha proseguito l'opera di costante monitoraggio dell'evoluzione tecnica del settore, promuovendo incontri e consultazioni con i diversi operatori, nonché con gli altri organi istituzionali interessati dalle tematiche trattate.

Si deve tenere presente, inoltre, che in ragione delle peculiarità del settore e dell'estrema rapidità con cui la tecnologia va evolvendosi, sono opportunamente destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici e di buona condotta previsti da ultimo dal d.lg. 30 giugno 2003, n. 196.

Le diverse questioni emerse nella materia in esame confermano peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell'Autorità rispetto ai trattamenti di dati personali effettuati da soggetti situati all'estero (sul punto, cfr. il *Provv.* sullo *spamming* adottato dal Garante in data 29 maggio 2003, v. subito *infra*).

L'Autorità ha partecipato attivamente ai lavori svoltisi al riguardo nelle apposite sedi quali Ocse, Commissione europea e Gruppo dei garanti europei istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

In particolare, quest'ultimo ha esaminato le problematiche connesse a Internet ed alle reti di comunicazione nel parere n. 2/2003 del 13 giugno 2003. Sono stati

affrontati i problemi posti, in termini di protezione dei dati, dai cosiddetti *"database Whois"*, consultabili in rete, che contengono informazioni utili per contattare i responsabili dei domini o di siti Internet. In tale occasione, i Garanti hanno segnalato che non dovrebbero essere resi indiscriminatamente pubblici ed accessibili a chiunque i dati contenuti in tali elenchi, come pure l'esigenza di distinguere fra dati assolutamente necessari e dati "opzionali". Inoltre, l'utilizzazione di tali registri o elenchi per finalità di *marketing*, realmente massiccia, non è ammissibile alla luce della direttiva europea sulla protezione dei dati personali in quanto non è conforme agli scopi per i quali i registri stessi sono stati istituiti.

Database Whois

Degli orientamenti emersi a livello europeo il Garante italiano terrà conto anche nell'esame delle diverse segnalazioni e richieste di chiarimenti pervenute in ordine all'attuale regime di conoscibilità dei dati relativi ai soggetti che registrano siti *web* (cd. *registrant*). L'Autorità ha infatti in programma l'emanazione di un provvedimento generale che fornisca alcuni chiarimenti ed indicazioni agli operatori del settore. Specifici approfondimenti sono stati svolti in tal senso in occasione del *summit* mondiale organizzato da Icann a Roma nello scorso mese di marzo, durante il quale il segretario generale dell'Autorità è stato invitato ad illustrare le prospettive esistenti in materia in Italia alla luce del Codice.

33.2. Messaggi di posta elettronica non desiderati e nomi a dominio

L'Autorità ha adottato, in data 29 maggio 2003, un provvedimento generale relativo alla pratica dell'inoltro di messaggi di posta elettronica non sollecitati aventi carattere pubblicitario o commerciale (fenomeno comunemente noto come *spamming*), al fine di precisare il quadro normativo di riferimento ed offrire indicazioni utili agli operatori del settore.

Il Garante ha in primo luogo precisato che il consenso deve essere manifestato liberamente, in modo esplicito e, soprattutto, in forma chiara e differenziata rispetto alle diverse finalità ed alle categorie di servizi e prodotti offerti, prima dell'inoltro del messaggio commerciale. Tale disciplina non può essere peraltro elusa inviando una prima *e-mail* che, pur chiedendo il consenso, presenti un contenuto comunque promozionale o pubblicitario, oppure riconoscendo in concreto al destinatario un mero diritto di opposizione a ricevere in futuro altri messaggi pubblicitari (sistema cd. *opt-out*). Simili precisazioni sono coerenti con la disciplina generale in materia di comunicazioni commerciali non sollecitate dettata dal Codice, che, all'art. 130, ha recepito e rafforzato il principio della necessità del consenso preventivo ed informato (sistema cd. *opt-in*).

Il consenso del destinatario

Tuttavia, come anticipato nel provvedimento ora citato e, poi, confermato dallo stesso Codice (art. 130, comma 4), è stato introdotto nell'ordinamento un parziale temperamento al principio del consenso preventivo. In particolare, le aziende potranno, previa idonea informativa, inviare comunicazioni pubblicitarie o commerciali ai propri clienti con i quali già sussistono rapporti contrattuali, qualora questi ultimi abbiano in precedenza fornito, pur sempre previa idonea informativa, le proprie coordinate di posta elettronica nel contesto della vendita di un prodotto o di un servizio. Ciò, purché si tratti di prodotti o servizi analoghi a quelli per i quali era già stato instaurato un rapporto e purché sia offerta esplicitamente e senza ambiguità, all'inizio del rapporto e in occasione di ogni singolo invio, la possibilità di rifiutare tale pratica commerciale (prime indicazioni utili al

33

riguardo sono rinvenibili nel recente parere del Gruppo art. 29 di cui si tratta in questo stesso paragrafo).

Inoltre è stato chiarito che, nel caso in cui una società acquisisca da altre aziende banche dati contenenti indirizzi di posta elettronica, deve accertarsi che ciascun interessato abbia effettivamente acconsentito validamente alla comunicazione dell'indirizzo anche per fini di promozione pubblicitaria. In ogni caso, la società deve inviare agli interessati un messaggio di informativa, al fine di facilitare a questi ultimi l'esercizio dei diritti di cui all'art. 7 del Codice.

È stato pure ribadito il principio, più volte affermato dall'Autorità, secondo il quale la semplice conoscibilità di fatto di un indirizzo di posta elettronica (ad esempio, in quanto rinvenibile tramite *newsgroup*, *forum* o *chat*) non legittima l'invio di messaggi in assenza del preventivo consenso informato dell'interessato.

Nell'esaminare un ricorso, il Garante ha anche avuto occasione di chiarire che non richiede il preventivo consenso informato dell'interessato l'utilizzo di un indirizzo di posta elettronica rinvenibile in un *newsgroup*, qualora questo sia stato indicato dal medesimo interessato nell'ambito del gruppo di discussione per una specifica finalità e il dato venga utilizzato conformemente alla finalità indicata. In questa ipotesi, è stato ritenuto lecito l'inoltro di una *e-mail* inviata in risposta alla richiesta di informazioni formulata dal ricorrente in un *newsgroup*, poiché l'*e-mail* si riferiva appunto a questioni del tutto pertinenti e correlate con il tema oggetto di discussione (*Provv*. 21 marzo 2003).

Deve però rilevarsi che, in ragione del principio di stabilimento recepito dal Codice, qualora i messaggi provengano da Paesi terzi, il Codice stesso potrebbe risultare inapplicabile. Tuttavia, a parte la possibilità che si applichi comunque la legge penale italiana in virtù di altre circostanze relative ad esempio a reati connessi (es. truffa), vi è non di rado l'ulteriore eventualità di potersi rivolgere alle competenti autorità del Paese nel quale lo *spamming* è considerato illecito in base alla relativa disciplina nazionale.

L'attività di *spamming*, specie se sistematica ed effettuata a fini di profitto o per arrecare ad altri un danno, quando provoca un nocumento costituisce reato e può essere denunciata all'autorità giudiziaria penale (cfr. art. 167 del Codice). È sanzionato penalmente anche l'invio di messaggi indesiderati a scopo promozionale o pubblicitario omettendo l'indicazione del mittente del messaggio e dell'indirizzo fisico presso il quale i destinatari possono rivolgersi per chiedere che i dati personali non vengano più usati.

Il Garante ha intensificato le attività di controllo e verifica presso fornitori di servizi di comunicazione elettronica, individuati grazie anche alle numerosissime segnalazioni pervenute pure nel 2003. In alcuni casi ciò ha portato a sospendere le attività illecite per effetto di provvedimenti di blocco delle banche dati o di divieto di ulteriori trattamenti. Altre volte ne è poi conseguita l'adozione di sanzioni, anche a seguito delle risultanze emerse dalla trattazione dei numerosi ricorsi decisi in materia.

Lo *spamming* nel contesto internazionale

Il tema dello *spamming* è stato oggetto di particolare attenzione altresì a livello internazionale.

A tale questione l'Ocse ha dedicato numerosi documenti e gruppi di lavoro, trattandosi di un argomento rispetto al quale c'è una particolare sensibilità nei Paesi membri. Dopo la creazione di un apposito gruppo di discussione, cui hanno partecipato ventitre delegazioni, si è organizzato un seminario internazionale ospitato dalla Commissione europea, per tracciare un bilancio delle iniziative intraprese ed elaborare una strategia di contrasto comune. Al Garante, rappresentato dal segretario generale, è stato chiesto di svolgere una relazione sui meccanismi di *enforcement* volti ad assicurare l'effettivo rispetto della legge.

È stata ribadita da molti, in questa circostanza, l'esigenza di affrontare il tema a livello sovranazionale e con un approccio che tenga conto della tutela dei consumatori, della sicurezza informatica e della protezione dei dati personali. Anche l'elenco delle soluzioni proposte mette in luce la necessità di combinare insieme misure tecniche, legislative, disposizioni di autoregolamentazione e campagne di sensibilizzazione rivolte ad utenti ed imprese. Un forte impegno su scala internazionale in questo settore è fondamentale per preservare la fiducia dei consumatori e delle imprese nello sviluppo di Internet. Lo *spamming* può essere collegato ad altre attività illegali, ciò che comporta il rischio di un arresto nello sviluppo sia dell'*e-commerce* sia dell'*e-government*. Per tali ragioni l'Ocse ha proposto una riflessione comune tra i rappresentanti dei governi, delle imprese e del mondo accademico. In proposito è stata effettuata una raccolta di materiali e documenti frutto dei lavori.

A livello comunitario, il Gruppo dei garanti europei ha di recente ritenuto doveroso adottare un parere (Parere n. 5/2004 WP 90 del 27 febbraio 2004), al fine di fornire un'interpretazione uniforme dell'art. 13 della direttiva n. 2002/58/CE in tema di comunicazioni commerciali non richieste, evitando divergenze nel suo recepimento e nella sua concreta applicazione da parte dei diversi Stati membri. Secondo il Gruppo, il concetto di *e-mail* deve essere interpretato nel senso di ritenere che si configura una comunicazione elettronica ogni qualvolta non sia richiesta la simultanea partecipazione del mittente e del destinatario. Il requisito del previo consenso *("opt-in")*, poi, può essere derogato solo nel caso in cui i dati siano stati già forniti nell'ambito di un rapporto commerciale preesistente ed il *marketing* si riferisca a prodotti o servizi che, eventualmente riguardati anche dal punto di vista obiettivo del destinatario della comunicazione, siano "simili" a quelli oggetto del rapporto, nei termini suggeriti dal parere.

33.3. Il codice deontologico

Sulla base dell'art. 133 del d.lg. n. 196/2003, il Garante, nell'ambito di una più generale collaborazione con i diversi operatori del settore, intende portare a conclusione in tempi rapidi (nonostante la complessità dell'argomento) le attività necessarie per la sottoscrizione del codice di deontologia e buona condotta sui trattamenti dei dati personali effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica. Ciò consentirà di fornire ulteriori criteri per assicurare una più adeguata informazione e consapevolezza agli utenti delle reti di comunicazione elettronica, nonché di favorire una maggiore trasparenza e correttezza nei confronti dei medesimi utenti ed il pieno rispetto dei principi di cui all'art. 11 del Codice.

Nel codice deontologico saranno disciplinati, tra l'altro, i presupposti ed i limiti entro i quali è lecito l'utilizzo della rete di comunicazione elettronica per accedere

33

ad informazioni archiviate nell'apparecchio dell'utente. In tale sede potranno pertanto essere individuate le regole per l'utilizzo lecito dei cd. *cookies*, ai quali fa riferimento anche la Raccomandazione n. 2/2001 del Gruppo dei garanti europei, relativa ai requisiti minimi per la raccolta di dati *on line* nell'Unione europea.

La rilevanza del codice deontologico è accresciuta dal fatto che il rispetto delle disposizioni in esso contenute costituirà condizione di liceità e correttezza del trattamento dei dati personali (art. 12, comma 3, d.lg. n. 196/2003).

Il trasferimento di dati personali all'estero

34 I trasferimenti all'estero di dati

Con il Codice è stata aggiornata la disciplina del trasferimento dei dati personali all'estero (Parte I, Capo VII), completando il recepimento della direttiva comunitaria n. 95/46/CE. È stato ribadito il principio generale in base al quale i flussi di dati verso un Paese situato al di fuori dell'Unione europea sono consentiti solo se tale Paese assicura un adeguato livello di tutela delle persone (v., al riguardo, le autorizzazioni rilasciate negli anni scorsi dal Garante in relazione al livello di adeguatezza del sistema di tutela dei dati personali previsto in Svizzera ed Ungheria, nonché ai principi del Safe Harbor circa il trasferimento dei dati verso gli Stati Uniti), ovvero se sussiste uno dei presupposti di liceità indicati dalla normativa nazionale (consenso dell'interessato, adempimento di obblighi contrattuali, ecc.).

Anche nel corso del 2003 e nei primi mesi del 2004, significativa è stata l'attività svolta dal Garante per dare attuazione ad alcune decisioni comunitarie relative al settore in esame.

Si segnalano, al riguardo:

- la deliberazione n. 6 del 30 aprile 2003, con cui l'Autorità italiana ha dato attuazione alla decisione della Commissione europea del 20 dicembre 2001, con la quale si è ritenuto adeguato il livello di protezione dei dati personali in Canada (v. *Relazione* 2002, p. 128);

- la deliberazione n. 2 del 15 aprile 2004, con cui il Garante ha attuato la decisione comunitaria del 21 novembre 2003 n. 2003/821/CE, recante il riconoscimento del Bailato di Guernsey tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali.

A tale ultimo riguardo va specificato che il Gruppo dei garanti europei istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, nel proseguire la propria attività di valutazione dell'adeguatezza del livello di protezione garantito da Stati non appartenenti all'Ue, si era pronunciato favorevolmente sul Bailato di Guernsey con il parere n. 5/2003 del 13 giugno 2003. Di conseguenza, la Commissione europea ha adottato la citata decisione n. 2003/821/CE con la quale ha stabilito che il livello di protezione dei dati nel territorio di Guernsey è "adeguato" ai fini del trasferimento di dati personali dall'Ue verso soggetti ivi residenti.

Sempre nella materia in esame, è in procinto di essere resa operativa in Italia anche la decisione della Commissione europea n. 2003/490/CE del 30 giugno 2003, riguardante l'adeguatezza del livello di tutela dei dati personali esistente in Argentina, su cui si era già espresso in senso favorevole, con il parere n. 4 del 3 ottobre 2002, il Gruppo dei garanti europei.

34

Infine, una decisione di contenuto analogo è in procinto di essere adottata dalla Commissione europea anche per l'Isola di Man, alla luce del parere favorevole del Gruppo (Parere n. 6/2003 del 21 novembre 2003).

Come anticipato nella *Relazione* per il 2002 (v. ivi, p. 127), il 2003 è stato inoltre caratterizzato da un intenso monitoraggio da parte dell'Autorità sulle attività di trasferimento di dati all'estero effettuate da alcuni operatori italiani, con particolare riguardo al tipo di garanzie adottate per tutelare i diritti degli interessati. Ciò allo scopo di verificare lo stato di attuazione delle disposizioni comunitarie e nazionali sui flussi di dati all'estero, prima di avviare specifici accertamenti relativi a singole società.

Indagine del Garante sulle attività di trasferimento dei dati

Dall'indagine svolta è emerso che:

- circa l'84% delle società interpellate effettua trasferimenti di dati all'estero; le aree geografiche di maggiore interesse sono rappresentate dagli Usa, dall'Europa dell'Est, dall'America centro-meridionale, dall'Africa, dalla Svizzera e dall'Asia;

- nel 40% circa dei casi analizzati, i dati personali oggetto di trasferimento all'estero riguardano principalmente dipendenti e, in misura minore, ma comunque non trascurabile, anche altre società o imprese (in qualità di clienti, concorrenti, fornitori, ecc.);

- i flussi di dati sono stati o sono effettuati, di regola, previa acquisizione del consenso specifico degli interessati o sulla base degli altri presupposti di legge (ad es., per l'esecuzione di obblighi contrattuali);

- soltanto in un numero ristretto dei casi esaminati (il 5% circa), relativi a flussi stabili e più complessi di dati, le società interpellate hanno utilizzato le clausole contrattuali *standard* indicate dalla Commissione europea;

- in alcune limitate ipotesi, caratterizzate dal fatto che la gestione delle risorse umane viene effettuata negli Usa, gli importatori dei dati (società capogruppo o comunque collegate o controllate) hanno aderito all'accordo sui principi del *Safe Harbor*, dichiarandosi in genere disponibili a cooperare con le autorità per la protezione dei dati dei Paesi europei.

L'indagine dimostra che nuovi strumenti, come le clausole contrattuali, cominciano ad essere utilizzati nell'ambito delle prassi economiche e commerciali con aziende di altri Paesi e che tali strumenti possono essere ancora migliorati, in particolare con riguardo alla disciplina di fenomeni più complessi e frequenti a livello internazionale, quali quelli relativi a gruppi societari, a rapporti multilaterali tra imprese, o al conferimento a terzi, all'estero, di attività o servizi precedentemente svolti in proprio (cd. *outsourcing*).

In argomento, il Gruppo di lavoro istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE ha evidenziato l'opportunità di introdurre eventuali correttivi, prevedendo ulteriori garanzie e regole di comportamento in aggiunta alle clausole contrattuali tipo già predisposte (v. il paragrafo seguente).

35 Le clausole contrattuali tipo

Diverse imprese e gruppi societari, operanti a livello internazionale, si sono rivolti al Garante per ottenere informazioni e chiarimenti sulla corretta applicazione della normativa in materia di trasferimento all'estero dei dati personali.

In particolare, l'Autorità ha esaminato un caso relativo alla realizzazione a livello internazionale di un sistema informativo centralizzato di gestione delle risorse umane di diverse società situate in vari Stati dell'Ue, tra cui l'Italia, affidato in *outsourcing* ad una società con sede negli Usa (ipotesi frequente in questi ambiti).

Contratto globale

Al fine di rendere lecito il trasferimento all'estero dei dati dei dipendenti nell'ambito di questa operazione, è stato sottoscritto, anche per conto delle società appartenenti ai gruppi societari coinvolti nella gestione di tali dati, un contratto cd. globale basato sulle clausole contrattuali-tipo relative ai flussi transfrontalieri di dati tra autonomi titolari del trattamento (cfr. decisione della Commissione europea del 15 giugno 2001, n. 2001/497/CE, attuata in Italia attraverso l'autorizzazione generale del Garante n. 35 del 10 ottobre 2001).

Le clausole contrattuali-tipo consentono alle imprese di trasferire dati personali nel rispetto dei principi della direttiva anche quando il Paese di destinazione non abbia una legislazione adeguata, prevedendo idonee garanzie attraverso strumenti negoziali.

Sulla base delle osservazioni formulate dal Garante e dalle altre Autorità di controllo europee interpellate, è stato predisposto poi uno schema di contratto integrativo del precedente, basato sulle clausole contrattuali-tipo indicate nell'autorizzazione generale n. 3 del 10 aprile 2002 e relative al trasferimento dei dati a responsabili del trattamento residenti in Paesi terzi.

L'Autorità si è, inoltre, espressa favorevolmente circa il mantenimento, nel contratto integrativo, della previsione di una responsabilità disgiunta e solidale dell'esportatore e dell'importatore dei dati per i danni subiti dagli interessati a causa della violazione delle regole contrattuali. Le imprese od enti che si avvalgono dei contratti *standard* possono infatti inserire ulteriori clausole pertinenti, purché non risultino limitative o incompatibili con le clausole-tipo approvate dalla Commissione europea. Si è ritenuto pertanto opportuno conservare nello schema di contratto la clausola sulla responsabilità appena descritta, in quanto espressiva di una maggiore garanzia per il risarcimento dei danni eventualmente causati agli interessati: questi ultimi potrebbero così attivare direttamente un'azione legale nei confronti di entrambe le parti contrattuali.

L'Autorità ha sottolineato, infine, la necessità che lo schema di contratto stipulato tra le società interessate anche in nome e per conto delle rispettive società controllate e collegate venga sottoscritto da ciascuna di queste società o, comunque, dalla maggior parte di quelle per le quali la capogruppo non abbia uno specifico mandato o procura a rappresentarle.

L'Autorità è anche giunta alla conclusione di considerare applicabile allo schema di contratto in esame l'autorizzazione generale n. 3 del 10 aprile 2002: non è,

35

quindi, necessario il rilascio di una specifica autorizzazione del Garante per trasferire all'estero i dati in questione.

Sempre in tema di trasferimento dei dati verso Paesi non appartenenti all'Ue (cd. Paesi terzi), il Gruppo dei garanti europei ha approfondito e sviluppato il lavoro sulle clausole contrattuali-tipo.

Binding corporate rules

Il Gruppo ha avviato una riflessione su quest'ultimo punto con riferimento al livello di tutela che può essere garantito dall'adozione di norme che possono apportare un vincolo nell'impresa (cd. *binding corporate rules*), una sorta di codici di condotta elaborati nell'ambito di un gruppo di imprese e impegnativi per tutti i soggetti che ne fanno parte. Con un documento di lavoro (WP del 3 giugno 2003) sono state formulate alcune indicazioni preliminari sulle condizioni in base alle quali questi speciali codici di condotta possono offrire garanzie sufficienti ai fini del trasferimento di dati verso Paesi terzi che non dispongano di un livello adeguato di protezione dei dati, con particolare riferimento ai trasferimenti fra società appartenenti ad uno stesso gruppo multinazionale.

Un modello alternativo di clausole contrattuali-tipo rispetto a quelle approvate con la decisione della Commissione n. 497/2001/CE ha formato oggetto di un successivo parere (Parere 8/2003 del 17 dicembre 2003). Il Gruppo ha espresso una valutazione positiva su un progetto di clausole contrattuali presentato dalla Camera di commercio internazionale e da altre organizzazioni commerciali, suggerendo alcune modifiche al fine rendere il livello di tutela equiparabile a quello delle clausole approvate dalla Commissione.

La sicurezza pubblica e privata

36 Il trasferimento dei dati *Pnr (Passenger name record)* dei passeggeri

Anche nel corso del 2003 il trasferimento dei dati personali dei passeggeri alle autorità doganali di Paesi non appartenenti all'Ue ha rappresentato uno dei punti chiave dell'attività del Gruppo costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE. Tali tematiche, già affrontate nel 2002 in relazione agli Stati Uniti (Parere 6/2002 WP 66 del 24 ottobre 2002), hanno assunto speciale rilevanza nell'ultimo anno anche per le istanze presentate in proposito da Canada ed Australia, alimentando il dibattito europeo ed internazionale sul giusto equilibrio fra misure di controllo delle frontiere e di lotta al terrorismo e tutela del diritto fondamentale alla protezione dei dati personali.

Il trasferimento dei dati *Pnr* da e verso gli Stati Uniti

Il confronto con gli Stati Uniti si è aperto quando, in seguito agli eventi dell'11 settembre 2001, sono stati adottati leggi e regolamenti che impongono alle compagnie aeree di trasferire alle autorità doganali degli Usa i dati personali dei passeggeri e dell'equipaggio in volo da o verso il territorio statunitense. In particolare, le autorità americane hanno chiesto l'accesso elettronico ai dati contenuti nei sistemi di prenotazione e distribuzione delle compagnie aeree (cd. dati *Pnr-Passenger name record*), prevedendo in caso contrario controlli minuziosi e lunghi dei passeggeri e dei membri dell'equipaggio all'arrivo, nonché pesanti sanzioni pecuniarie, e disponendo persino la perdita dei diritti di atterraggio. Secondo il sistema proposto, un numero ingente di dati riguardante la totalità dei passeggeri dei voli transatlantici dovrebbe essere raccolto elettronicamente nei *database* delle compagnie aeree e dei sistemi di prenotazione, e poi analizzato e conservato per lunghi periodi dalle autorità statunitensi. Le autorità doganali potrebbero poi comunicarli ad altre autorità degli Usa o di altri Paesi al fine di valutare la pericolosità dei passeggeri, negando eventualmente l'imbarco ai soggetti ritenuti pericolosi (cd. sistema *"Capps II"*). Tutto ciò avverrebbe, però, in assenza di un quadro normativo negli Stati Uniti che garantisca ai passeggeri europei una tutela dei dati personali equivalente a quella assicurata dalla direttiva n. 95/46/CE.

La posizione del Gruppo dei garanti europei

Il Gruppo si è pronunciato nuovamente sul tema sia nel giugno 2003 (Parere 4/2003 WP 78 del 13 giugno 2003), sia nel gennaio 2004 (Parere 2/2004 WP 87 del 29 gennaio 2004), seguendo con attenzione gli sviluppi dei negoziati fra la Commissione europea e le autorità statunitensi e cercando di fornire elementi utili alla configurazione di meccanismi di trasferimento compatibili con il diritto alla protezione dei dati personali. Le carenze di tutela, evidenziate già nel parere del giugno 2003, e le conseguenti perplessità sulla possibilità di considerare adeguata la protezione prevista per i dati personali dei passeggeri europei, sono state confermate nel parere del gennaio 2004, adottato al termine dei negoziati fra Commissione e Stati Uniti.

36

In tale occasione il Gruppo ha tenuto conto sia dell'ultima versione degli impegni statunitensi ("Dichiarazione d'intenti dell'Ufficio doganale e di protezione dei confini *(Cbp)* del Dipartimento per la sicurezza interna" del 12 gennaio 2004), sia della comunicazione della Commissione europea ("Trasferimento dei dati contenuti nel *Passenger name record*: un approccio globale dell'Ue" COM(2003) 826 *final* del 16 dicembre 2003). In quest'ultimo documento, la Commissione manifesta l'intenzione di associare alla decisione sull'adeguatezza un accordo internazionale bilaterale che autorizzerebbe le compagnie aeree a considerare la richiesta degli Stati Uniti un obbligo di legge, imponendo nel contempo agli Usa di garantire ai cittadini europei l'esercizio dei propri diritti.

Nel sottolineare come anche nella lotta contro il terrorismo occorra tutelare le libertà individuali e i diritti fondamentali, compresi il rispetto della vita privata e la protezione dei dati, il Gruppo ha ribadito che il sistema deve rispettare almeno i principi fondamentali stabiliti dalla direttiva europea, ossia:

- principio di finalità. I dati del *Pnr* devono essere utilizzati soltanto per contrastare il terrorismo ed altri specifici reati connessi al terrorismo; inoltre, devono essere specificati chiaramente i soggetti ai quali i dati possono essere comunicati e non deve essere ammessa l'utilizzazione dei dati in rapporto ad altri sistemi, come ad esempio il *Capps II*;

- principio di proporzionalità. Devono essere trasferiti solo i dati necessari per le finalità indicate, evitando la raccolta di informazioni eccessive o non pertinenti;

- conservazione per un periodo di tempo limitato;

- divieto di trattare dati sensibili;

- esercizio dei diritti degli interessati. I passeggeri devono ricevere informazioni chiare e accurate su chi tratterà i loro dati e sugli scopi del trattamento, nonché sulle modalità per l'esercizio dei diritti riconosciuti dalla direttiva n. 95/46/CE e dalle leggi nazionali (accesso, rettifica, ecc.). Restano perplessità sui poteri del *Chief Privacy Officer* creato presso il *Department of Homeland Security*, anche alla luce dei problemi sul grado di vincolatività giuridica degli "impegni" assunti dall'Amministrazione degli Stati Uniti.

La posizione del Parlamento europeo

L'inadeguatezza dell'attuale configurazione del sistema di trasferimento dei cd. dati *Pnr* verso gli Usa è stata sostenuta dal Parlamento europeo che ha approvato una serie di risoluzioni in cui, nell'invitare la Commissione europea a definire un quadro giuridico chiaro per il trasferimento dei dati dei passeggeri verso gli Stati Uniti, ha rilevato varie lacune nelle garanzie offerte dal sistema statunitense e nella soluzione proposta dalla Commissione. Il Parlamento europeo ritiene pertanto che, per tutelare il diritto alla protezione dei dati personali sancito dall'art. 8 della Carta dei diritti fondamentali dell'Ue, sia necessario un accordo internazionale, possibilmente a carattere multilaterale, in cui chiarire il ruolo svolto dalle compagnie aeree e le garanzie offerte ai passeggeri.

Da ultimo il Parlamento europeo, con un'apposita risoluzione, ha censurato la

soluzione proposta della Commissione europea, invitando quest'ultima a ritirare il progetto di decisione sul trasferimento dei dati personali dei passeggeri aerei negli Stati Uniti e riservandosi il diritto di adire la Corte di giustizia per verificare la legalità dell'accordo raggiunto. Ciò in quanto gli impegni (cd. *undertakings*) assunti dall'Amministrazione statunitense sono stati giudicati una base giuridica inadeguata per la decisione della Commissione europea (*Comunicato stampa* 31 marzo 2004).

L'opportunità di un negoziato multilaterale, già evidenziata dal Gruppo nei propri pareri, si desume anche dalle richieste di trasferimento dei dati dei passeggeri recentemente formulate dalle autorità doganali canadesi ed australiane, oltre che da quanto sta emergendo in relazione a Paesi quali il Sudafrica e la Corea del Sud. Il Gruppo, in proposito, ha constatato che l'obiettivo di prevenire il terrorismo può essere efficacemente perseguito anche attraverso sistemi più rispettosi del diritto alla protezione dei dati personali dei passeggeri.

Così, un approccio certamente più equilibrato caratterizza il sistema australiano, rispetto al quale il Gruppo ha espresso un parere sostanzialmente favorevole, pur se condizionato ad alcune modifiche e miglioramenti (Parere 1/2004 WP 85 del 16 gennaio 2004). Tale sistema prevede, infatti, la trasmissione di un numero più limitato di dati personali. Inoltre, le finalità della raccolta sono circoscritte alla prevenzione del terrorismo e dei reati connessi, non è prevista la conservazione sistematica dei dati raccolti ed i diritti dei passeggeri sono garantiti da un quadro normativo ed istituzionale più conforme alle esigenze di tutela della vita privata.

Per quanto riguarda il Canada, il Gruppo ha adottato un ulteriore parere (Parere 3/2004 WP 88 del 11 febbraio 2004) in cui si evidenziano le questioni da risolvere e le modifiche da apportare al sistema canadese prima che possa essere approvata una pronuncia di adeguatezza da parte della Commissione europea.

La questione dell'utilizzazione dei dati dei passeggeri ad opera delle autorità di frontiera continua ad occupare un ruolo di primo piano non solo nell'agenda del Gruppo e delle istituzioni comunitarie, ma anche di altri organismi internazionali, quali l'Ocse e l'Icao, che più di recente hanno inteso contribuire allo sviluppo di un approccio globale a tale tematica (cfr. *infra*, parag. 41.2.).

37 Videosorveglianza

Il parere del Gruppo dei garanti europei

Il Gruppo dei garanti europei, nel parere n. 4/2004 (WP 89 dell'11 febbraio 2004), ha fornito specifiche indicazioni in materia di videosorveglianza e protezione dei dati personali, con l'obiettivo di fissare regole e garanzie comuni sull'installazione di telecamere, anche in vista di eventuali interventi legislativi in materia. Il parere, adottato su particolare impulso della delegazione italiana, contiene un "decalogo" sulle cautele ed i principi da osservare in materia di videosorveglianza, che si applicano anche ai trattamenti che non sono soggetti espressamente alle disposizioni della direttiva europea (ad esempio, trattamenti effettuati per scopi di sicurezza pub-

blica o per il perseguimento di reati, oppure effettuati da una persona fisica per scopi esclusivamente privati o familiari). I Garanti hanno tenuto conto in proposito anche di alcuni commenti pervenuti attraverso la consultazione pubblica conclusasi il 31 maggio 2003.

37.1. La videosorveglianza in ambito pubblico

L'incremento delle risorse finanziarie a disposizione degli enti locali derivanti da fonti comunitarie, dal Piano operativo nazionale sulla sicurezza e dalle leggi regionali tese a finanziare gli investimenti per promuovere legalità e sicurezza sociale ha probabilmente contribuito a determinare un incremento nell'utilizzo di sistemi di rilevazione di immagini in ambito pubblico.

Ancora numerosi sono stati i reclami e le segnalazioni pervenuti al Garante in merito a possibili violazioni delle norme sulla protezione dei dati personali derivanti dall'installazione di sistemi di videocontrollo ad opera, in particolare, di amministrazioni locali, attivati per finalità di sicurezza urbana, tutela del patrimonio, monitoraggio del traffico, asserite competenze in tema di prevenzione e repressione dei reati, disciplina dei rifiuti urbani. Numerosi sono stati pure i reclami e le segnalazioni nei confronti di impianti installati dagli esercenti attività commerciali o artigianali per ridurre il "rischio criminalità".

Parallelamente, sono stati posti al Garante moltissimi quesiti sul tema da parte di soggetti pubblici titolari del trattamento (enti locali, aziende sanitarie locali, istituti scolastici e prefetture).

Il Garante ha ricordato in primo luogo che l'installazione di sistemi di videosorveglianza non è subordinata ad una formale autorizzazione preliminare. Non è quindi stabilito alcun termine decorso il quale i progetti sottoposti all'Autorità dai titolari possano ritenersi conformi alla normativa sulla protezione dei dati personali o comunque autorizzati dal Garante, poiché al riguardo non è previsto il formarsi del cd. silenzio-assenso. Ciò, tenuto oltretutto conto che i progetti trasmessi all'Autorità spesso non descrivono tutte le caratteristiche che permetterebbero di verificare l'applicazione del principio di proporzionalità nei singoli aspetti del trattamento.

Già in passato, con il provvedimento generale del 29 novembre 2000 (cd. decalogo sulla videosorveglianza), l'Autorità aveva fornito alcune prime indicazioni per garantire un equo contemperamento tra le esigenze di sicurezza ed il rispetto della normativa sulla protezione dei dati personali nella rilevazione di immagini e suoni.

Le prescrizioni, gli accertamenti e le garanzie indicate in tale documento dovevano essere necessariamente aggiornate, in ragione dell'evoluzione delle tecnologie disponibili, dei nuovi strumenti giuridici elaborati in sede comunitaria ed internazionale e del nuovo Codice.

Il Garante ha perciò portato a compimento un nuovo procedimento, adottando nell'aprile 2004 un ulteriore provvedimento generale per individuare principi e cautele più specifici da rispettare in materia di videosorveglianza a pena di illiceità del trattamento, in vista del relativo codice deontologico.

L'art. 134 del d.lg. n. 196/2003 impegna infatti l'Autorità a definire a breve i lavori preparatori di un apposito codice deontologico per disciplinare il trattamento dei dati personali effettuato con strumenti automatizzati di rilevazione di immagini.

Nel merito delle questioni analizzate dall'Autorità nel 2003, va tra l'altro evidenziato il quesito formulato da un'agenzia investigativa sulla possibilità di installare telecamere in luoghi pubblici in connessione con il mandato ricevuto da un comune e finalizzato alla raccolta di prove di eventuali atti di vandalismo, danneggiamenti o altri atti criminosi, affinché si potessero perseguire penalmente e civilmente i relativi autori. In proposito, l'Autorità ha rilevato la mancanza del presupposto della proporzionalità nell'uso dello strumento rispetto alla finalità perseguita. Si è pure notato che l'ente pubblico committente (un comune) era privo di funzioni istituzionali in materia di prevenzione ed accertamento dei reati. L'adozione di un sistema di videosorveglianza avrebbe potuto giustificarsi solo in presenza di una comprovata inidoneità di altri sistemi o cautele (impianti di allarme, specifica vigilanza, ecc.) e con un ruolo ben diverso del titolare del trattamento, ovvero con l'attivazione delle forze di polizia.

Il Garante è intervenuto a richiesta affinché la realizzazione di un "sistema integrato di sicurezza territoriale" presso il quartiere Eur di Roma avvenga in piena conformità a quanto previsto dalla normativa sulla protezione dei dati personali e, in particolare, in stretto ossequio al principio di proporzionalità tra mezzi impiegati e scopi perseguiti (che si specifica nei principi di pertinenza e non eccedenza) e nel rispetto delle competenze degli organi coinvolti. Sotto questo aspetto, saranno perciò oggetto di ulteriore e preventivo esame le modalità di registrazione delle immagini, il tempo della loro conservazione, nonché la predisposizione di un'adeguata informativa alla cittadinanza.

37.2. La videosorveglianza nel settore privato

Anche nel settore privato l'utilizzo di impianti di videosorveglianza ha dato luogo, nel 2003, a frequenti interventi del Garante, a conferma della progressiva diffusione del fenomeno e della crescente attenzione e sensibilità dei cittadini al riguardo.

Nei numerosi casi analizzati, in attesa della definizione del codice di deontologia previsto dall'art. 134 del d.lg. n. 196/2003, sono stati ribaditi i principi già affermati nel provvedimento generale del 29 novembre 2000.

Videosorveglianza per fini di sicurezza individuale

Diverse sono state le istanze riguardanti l'installazione di impianti per finalità di sicurezza in ambito condominiale e in spazi antistanti le porte d'ingresso ad abitazioni private. Al riguardo, fermo restando il divieto sanzionato penalmente di interferire illecitamente nella vita privata altrui, si è nuovamente constatata l'inapplicabilità della vigente normativa sulla protezione dei dati personali ai trattamenti di dati effettuati per fini esclusivamente personali (art. 5, comma 3, d.lg. n. 196/2003): tuttavia, si è rilevato che questa esclusione per le apparecchiature di videosorveglianza installate al solo fine della sicurezza individuale non riguarda quelle attivate da condomini o più gruppi familiari e presuppone, comunque, che le immagini registrate non siano oggetto di successiva comunicazione sistematica o diffusione (*Provv.* 22 dicembre 2003).

Nei casi in cui la legge non sia applicabile perché ad esempio il sistema è attivato da un solo condomino che non registra i dati, ciò non comporta che i terzi siano

37

privati di garanzie in sede civile e penale. A parte la possibilità di ottenere tutela sulla base dell'art. 615-*bis* c.p., i terzi devono essere comunque salvaguardati nei loro diritti (riservatezza, tranquillità individuale) attraverso la delimitazione dell'angolo visuale, in modo da non riprendere l'uscio altrui o da attivare indebite forme di controllo su aree comuni.

Varie segnalazioni e reclami hanno poi riguardato il trattamento di dati effettuato tramite sistemi di videosorveglianza più complessi, installati ad opera, ad esempio, di studi professionali, esercizi commerciali, società ed enti *no-profit*, per i quali si è reso necessario eseguire accertamenti *in loco* in collaborazione con la Guardia di finanza (per il protocollo d'intesa siglato dalle due istituzioni il 26 ottobre 2002, v. *Relazione* 2002).

In un caso, poi, di installazione da parte di una farmacia, a seguito di alcuni episodi criminosi, di apparecchiature di videosorveglianza a protezione dei dipendenti e delle cose custodite nei relativi locali, si è reso necessario richiamare il titolare ad una più scrupolosa osservanza dei principi del cd. decalogo.

In altre ipotesi sono state invece contestate sia l'omessa notificazione al Garante del trattamento effettuato mediante impianti di videosorveglianza installati dai titolari per motivi di protezione del patrimonio e delle persone, sia la mancata adozione di un'idonea informativa agli interessati circa la presenza di tali impianti. In questi casi è stato infatti accertato che la qualità delle immagini consentiva l'identificazione delle persone che entravano nel campo di visuale delle telecamere e che i relativi titolari avevano completamente disatteso gli obblighi vigenti in materia, soprattutto per quanto concerne l'omessa informativa, comprovata dall'assenza di avvisi o cartelli recanti le indicazioni prescritte dalla normativa.

Altri procedimenti, scaturiti da reclami proposti da organismi sindacali aziendali (Rsa o Rsu) di diverse società avverso l'installazione di sistemi di videosorveglianza potenzialmente configurabili come strumenti di controllo a distanza dell'attività dei lavoratori, sono sfociati anch'essi nel richiamo al rispetto delle prescrizioni di cui all'art. 4 della legge n. 300/1970 (la cui vigenza è fatta salva dal d.lg. n. 196/2003).

Videosorveglianza sui treni

Di particolare interesse è risultato inoltre un progetto sperimentale di Trenitalia S.p.A. per installare sistemi di videosorveglianza su taluni vagoni di treni che transitano su specifiche tratte ferroviarie oggetto di ripetuti atti vandalici e di episodi di microcriminalità a danno dei passeggeri. Al riguardo la società ha dichiarato di aver già adottato taluni primi accorgimenti per la protezione dei dati, come ad esempio l'effettuazione delle riprese con modalità volte ad escludere sia un avvicinamento dell'immagine sia (per quanto riguarda le carrozze–cuccette) la ripresa degli scompartimenti dei passeggeri, nonché la memorizzazione delle immagini riprese in forma criptata e la predisposizione di un'informativa agli interessati.

Dopo un approfondito esame, l'Autorità ha richiamato l'attenzione di Trenitalia S.p.A. sui seguenti punti: necessità di individuare con precisione e nell'ambito di una ristretta cerchia di persone i responsabili e gli incaricati del trattamento; riduzione al minimo, ove tecnicamente possibile, dei tempi di conservazione giornaliera delle immagini prima della loro cancellazione; adozione di idonee misure di sicurezza dei sistemi e dei dati raccolti. Il Garante ha inoltre chiesto di conoscere, entro il mese di giugno 2004, l'esito della prima sperimentazione del progetto e lo stato di attuazione delle misure di protezione dei dati.

38 Rilevazioni biometriche

I dati biometrici recano informazioni particolarmente delicate ed il loro uso, se, da un lato può svolgere un ruolo utile nella previsione di misure di sicurezza per l'accesso a dati, apparecchiature e sistemi, riducendo il ricorso ad altri dati personali più direttamente identificativi quali nome, indirizzo o domicilio, dall'altro, può comportare gravissimi rischi legati all'uso indebito o indiscriminato di informazioni desunte da connotati particolari quali le impronte digitali lasciate dalla persona interessata.

La posizione dei garanti europei

La diffusione crescente dei sistemi biometrici ha spinto il Gruppo dei garanti europei ad adottare uno specifico documento di lavoro sul tema (WP 80 del 1° agosto 2003).

Secondo il Gruppo, l'impiego di tecniche biometriche è ammissibile solo se realmente proporzionato agli scopi che si vogliono raggiungere e se non comporta di regola la creazione di archivi centralizzati e l'utilizzazione di informazioni desunte da "tracce fisiche" (come le impronte digitali) che una persona può lasciare anche senza rendersene conto. I garanti si sono riservati di tornare sul tema in futuro per far sì che le imprese, le pubbliche amministrazioni e i soggetti interessati all'impiego di sistemi biometrici sviluppino dispositivi realmente rispettosi della *privacy*; in particolare, il Gruppo ha richiamato l'attenzione sull'opportunità di redigere anche appositi codici deontologici che fissino i criteri da seguire nello sviluppo e nell'utilizzo di sistemi biometrici.

Il Wpisp

Anche il *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse ha rivolto particolare attenzione al tema delle tecnologie biometriche, in considerazione del notevole interesse che tali tecnologie stanno assumendo in svariati ambiti, quali il settore bancario, l'istruzione, i servizi pubblici, la sicurezza dei viaggi ed il controllo dell'immigrazione. Il gruppo, coadiuvato da consulenti esperti in materia di *privacy*, ha pertanto elaborato un documento che, dopo un'introduzione generale in cui vengono esaminate le differenti tecnologie biometriche, analizza le diverse possibili configurazioni e funzionalità dei sistemi biometrici, evidenziandone le implicazioni in materia di protezione dei dati e sicurezza dell'informazione.

38.1. Dati biometrici: gli interventi del Garante

In considerazione dei rischi connessi all'utilizzo di sistemi biometrici, l'Autorità ha potenziato la propria attività di verifica e di vigilanza in tale settore. Attenzione particolare è stata dedicata ad esempio alla possibilità di installare questi sistemi a fini di controllo degli accessi ai luoghi di lavoro o a servizi di mensa universitaria.

Tramite tali verifiche, il Garante intende accertare se l'uso di un sistema così invasivo, come quello di rilevazione delle impronte digitali, sia effettivamente e obiettivamente proporzionato rispetto alle finalità che si vogliono perseguire.

Le pubbliche amministrazioni nei cui confronti sono stati avviati accertamenti, sono state chiamate a documentare le ragioni dell'inidoneità di altri sistemi o procedure da cui deriverebbero minori pericoli o rischi per i diritti e le libertà fonda-

38

mentali degli interessati, nonché le finalità perseguite con l'impiego di tali sistemi di rilevazione.

Inoltre, è stato chiesto di indicare le modalità di concreta rilevazione e/o registrazione dei dati biometrici ed il successivo confronto delle impronte digitali eventualmente registrate con quelle rilevate dai lettori ottici. Ancora, i destinatari degli accertamenti sono stati invitati a specificare i tempi di conservazione, le misure di sicurezza adottate e le modalità di consultazione dei dati da parte dei soggetti autorizzati.

Tra gli accertamenti effettuati va in particolare evidenziato quello nei confronti di un ente regionale per il diritto allo studio universitario che, secondo notizie di stampa, intendeva bandire una gara di appalto per 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 (ad esempio, studenti vincitori di borse di studio o in particolari condizioni di reddito). A seguito dell'intervento del Garante, l'ente ha comunicato la rinuncia a realizzare il progetto in quanto non conforme al principio di proporzionalità tra i mezzi impiegati e le finalità di controllo della spesa perseguite.

Il progetto *S-Travel*

Con riferimento all'utilizzo di dati biometrici da parte di operatori privati, merita di essere poi ricordato l'esame di un progetto pilota, curato da un gruppo di organizzazioni e società operanti a livello internazionale (cd. *S-Travel Consortium*).

Attraverso tale progetto si intendeva avviare, presso gli aeroporti di Atene e di Milano Malpensa, la sperimentazione dell'uso di tecniche di autenticazione biometrica (impronte digitali e/o immagine dell'iride) nel settore del trasporto aereo, con particolare riguardo alle operazioni di *check-in* e di imbarco. Il progetto, seguito in Italia da Alitalia-Linee Aeree Italiane S.p.A., avrebbe coinvolto, in una prima fase, i dipendenti Alitalia e avrebbe dovuto essere esteso in una seconda fase ai passeggeri abituali della medesima compagnia che vi avessero aderito spontaneamente.

Dopo un primo contatto con tale compagnia, il Garante ha richiamato l'attenzione sulle cautele imposte dalla normativa comunitaria e nazionale in materia, ed in particolare sull'opportunità di un formale interpello al Garante stesso (ai sensi dell'art. 24-*bis*, legge n. 675/1996; v. ora, art. 17, d.lg. n. 196/2003) per permettergli di effettuare gli approfondimenti del caso e di prescrivere le necessarie garanzie, anche in vista dell'ipotizzata estensione della sperimentazione ai passeggeri abituali.

Il progetto poneva, infatti, delicati problemi in merito al rispetto dei principi di necessità e proporzionalità del trattamento, nonché di pertinenza e non eccedenza dei dati. L'utilizzo di tecniche di sperimentazione biometriche di riconoscimento rispondeva solo in parte al perseguimento dell'obiettivo di rafforzamento della sicurezza nei controlli aeroportuali, mirando anche alla semplificazione degli attuali adempimenti ed all'accelerazione del flusso dei passeggeri negli aeroporti.

La raccolta di dati biometrici relativi sia alle impronte digitali, sia all'immagine dell'iride di entrambi gli occhi è risultata eccedente e sproporzionata rispetto alle finalità del trattamento anche all'Autorità greca per la protezione dei dati personali, la quale, nel novembre 2003, è intervenuta bloccando lo sviluppo del progetto.

Dopo un ulteriore incontro con l'Ufficio del Garante nel quale sono stati illustrati questi punti problematici, il Consorzio e Alitalia non hanno fornito ulteriori notizie circa l'intenzione di avviare in Italia la sperimentazione.

Rilevazioni biometriche in banca

Nel corso dell'anno sono inoltre pervenute all'Ufficio numerose richieste da parte di cittadini relative all'installazione, effettuata da alcune banche, di sistemi di rilevazione biometrica per l'accesso alle filiali. In proposito è stato ribadito l'orientamento già espresso dall'Autorità in precedenza: si è così confermato, anzitutto, che l'accesso con tali modalità deve avvenire solo ed esclusivamente sulla base di un consenso realmente libero ed informato e prevedendo modalità di ingresso alternative agevoli e non lesive della dignità della persona, anche in caso di indisponibilità al rilascio dei propri dati biometrici. Si è poi ricordato che, per il principio di proporzionalità tra gli strumenti impiegati e le finalità perseguite, resta non consentito l'utilizzo indiscriminato di sistemi di rilevazione biometrica all'ingresso di banche a fronte di una generica esigenza di sicurezza.

Sono pervenute, altresì, talune segnalazioni circa l'impiego, da parte di alcune società, di tecniche di autenticazione biometrica (impronta palmare o facciale) per la rilevazione delle presenze del personale dipendente. Si tratta di ipotesi sulle quali il Garante sta concludendo accertamenti specifici, in considerazione del fatto che il trattamento di dati biometrici in tale ambito non risulta allo stato lecito in base ai principi di necessità e proporzionalità.

È necessario, ancora, ricordare la partecipazione del Garante al cd. Gruppo passaporto elettronico costituito presso il Ministero degli affari esteri al fine di affrontare i problemi connessi all'inserimento di dati biometrici nei passaporti. L'Autorità ha fatto presente costantemente l'esigenza di individuare un'adeguata base giuridica che consentisse l'inserimento dei dati biometrici nei passaporti, sottolineando, altresì, la necessità di rispettare comunque i principi di finalità, di pertinenza e di non eccedenza nel trattamento dei dati.

Per quanto riguarda, infine, l'attività consultiva svolta dall'Autorità su richiesta del Ministero dell'interno in merito al nuovo modello elettronico per i permessi di soggiorno, specifiche indicazioni sono state formulate relativamente alla necessità di un'adeguata base giuridica per l'utilizzo di dati biometrici, alle tecniche di registrazione dei dati (verificazione o autenticazione), nonché alla conservazione separata dei dati biometrici rispetto a quelli raccolti ai sensi del testo unico delle leggi di pubblica sicurezza per persone pericolose o sospette (cfr. sul punto anche *infra*, parag. 45.2.).

39 Attività di polizia

Anche nel 2003 sono pervenute a questa Autorità alcune segnalazioni, a volte presentate direttamente al Garante, ovvero a seguito di istanze di accesso rivolte al Dipartimento della pubblica sicurezza, con le quali gli interessati lamentano la registrazione, nel C.e.d. (Centro elaborazione dati) di tale Dipartimento, di dati inesatti, incompleti o non aggiornati, per lo più in riferimento a provvedimenti giudiziari o amministrativi adottati e non registrati (art. 10 legge n. 121/1981, modificato dall'art. 42 legge n. 675/1996 e, da ultimo, dall'art. 175, comma 3, d. lg. n. 196/2003).

Il C.e.d. del Dipartimento della pubblica sicurezza

L'Autorità aveva già sottolineato in passato (*Provv.* 17 gennaio 2002) 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 comunque effettuati nel rispetto dei principi di liceità, pertinenza e non eccedenza previsti dall'art. 9 della legge n. 675/1996 (ora, art. 11 d.lg. n. 196/2003). Si era poi richiamata l'attenzione degli uffici sulla necessità di verificare con cadenza periodica la rispondenza a tali principi dei dati trattati, apportando senza ritardo le modifiche richieste o necessarie e cancellando i dati detenuti, specie in ragione degli esiti processuali eventualmente documentati dagli interessati.

In linea con le indicazioni del Garante, questi profili hanno trovato ulteriore rafforzamento nel Codice.

Il d.lg. n. 196/2003 ha infatti previsto che il C.e.d. del Dipartimento della pubblica sicurezza debba assicurare in maniera più incisiva l'aggiornamento periodico, la pertinenza e la non eccedenza dei dati trattati anche attraverso interrogazioni del casellario giudiziale e di quello dei carichi pendenti del Ministero della giustizia o di altre banche di dati di forze di polizia, al fine di garantire la costante rispondenza delle informazioni registrate nel C.e.d. a quelle conservate in altri archivi (art. 54, comma 3, d.lg. n. 196/2003).

Analogamente, la verifica periodica del rispetto dei principi dettati dall'art. 11 del Codice è prevista come specifico obbligo per i singoli organi, uffici e comandi di polizia, i quali potranno avvalersi anche delle risultanze del C.e.d. (aggiornate come appena precisato) procedendo pure, in caso di trattamenti di dati effettuati con mezzi diversi da quelli elettronici, ad annotare o integrare i documenti cartacei che li contengono (art. 54, comma 4, d.lg. n. 196/2003).

L'importanza di queste garanzie è testimoniata anche dalla disposizione del Codice che demanda ad un regolamento governativo lo sviluppo di taluni principi applicabili ai trattamenti effettuati per finalità di polizia. In un regolamento previsto dovranno essere infatti contemplati, fra l'altro, appositi e più specifici termini di conservazione dei dati, nonché determinate modalità per il loro aggiornamento periodico, per la comunicazione degli aggiornamenti ad altri soggetti cui le informazioni sono state, eventualmente, comunicate in precedenza, e per la verifica della pertinenza dei dati rispetto alla specifica finalità perseguita (art. 57 d.lg. n. 196/2003).

Il Codice ha inoltre chiarito che la disciplina vigente in materia di accesso ai dati conservati nel C.e.d. (art. 10, commi 3, 4 e 5, legge n. 121/1981) si applica anche

ai dati 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. (art. 56 d.lg. n. 196/2003).

Particolare attenzione dovrà essere prestata ai trattamenti di dati che presentano maggiori rischi di danno all'interessato (trattamenti riferiti a dati genetici, biometrici o effettuati mediante tecniche basate su dati relativi all'ubicazione) per i quali l'Autorità intende individuare, anche su comunicazione degli organi interessati, particolari misure ed accorgimenti a garanzia dell'interessato (artt. 55 e 17 d.lg. n. 196/2003). L'Autorità ha già segnalato la necessità di determinare tali misure, anche in conformità alle indicazioni che potranno pervenire dalle stesse amministrazioni interessate, in relazione alla raccolta dei rilievi dattiloscopici effettuata in occasione del rilascio o del rinnovo del permesso di soggiorno agli stranieri ed all'eventuale inserimento dei dati biometrici nel documento di soggiorno elettronico.

L'Autorità è, poi, intervenuta nuovamente sulla diffusione da parte di organi di polizia di immagini e, specialmente, di foto segnaletiche di persone coinvolte in attività di polizia, in relazione ad una recente vicenda giudiziaria, che ha coinvolto anche alcuni personaggi del mondo dello spettacolo.

In merito a tale caso, già ricordato in un'altra parte della *Relazione* (cfr. parag. 15.2.), il Garante ha rilevato 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.

40 Problemi applicativi e possibili sviluppi del sistema di informazione Schengen

Il Sistema di informazione Schengen (su cui, v. pure *infra*, parag. 49.) è assoggettato ad un'attività di verifica e controllo del suo funzionamento da parte dell'Autorità comune di controllo (Acc), alla quale compete vigilare sull'applicazione della Convenzione di Schengen. Nel biennio 2002-2003 tale Autorità è stata presieduta dal segretario generale del Garante, che aveva già ricoperto la carica di vice presidente nel precedente biennio.

Il sesto Rapporto dell'Acc

Nel dicembre 2003 l'Autorità comune ha approvato il sesto Rapporto, in cui sono evidenziate le attività intraprese per una nuova campagna di informazione nei confronti dei cittadini, per l'apertura di un sito *web* della stessa Autorità comune *(http://www.schengen-jsa.dataprotection.org)* e per l'attuazione di una *newsletter*.

Il Rapporto è dedicato, in particolare, al potenziamento degli strumenti di indagine attraverso le modifiche proposte al sistema informativo attuale. Si tratta del cd. Sis II, che prevede un significativo ampliamento delle categorie di informazioni registrabili nel sistema, il possibile inserimento di dati biometrici e la modifica di alcuni meccanismi di accesso e utilizzazione dei dati.

40

Il Rapporto sottolinea i vari sforzi compiuti dall'Autorità di controllo per far sì che tali modifiche siano pienamente conformi alla Convenzione di applicazione dell'Accordo di Schengen. In particolare, nel rispondere alle sollecitazioni di alcuni Stati membri rispetto agli sviluppi del Sis, si è evidenziato che le modifiche proposte (il Sis II dovrebbe essere attuato entro il 2006) comporterebbero un sostanziale mutamento della natura del sistema informativo. Dando a strutture come Europol o Eurojust la possibilità di accedere direttamente ai dati in esso contenuti, il Sis verrebbe utilizzato per scopi investigativi leciti senza, però, una revisione complessiva delle sue finalità: invece, la Convenzione del 1990 aveva previsto un'utilizzazione "più statica" del Sis, sostanzialmente per vietare l'ingresso nella cd. Area Schengen a soggetti segnalati come indesiderabili dalle competenti autorità nazionali e quale strumento utile per alcune misure cd. compensative.

Alle proposte di modifica del Sis l'Autorità comune ha dedicato nel biennio 2002-2003 diversi pareri, nei quali si è sottolineata la necessità di chiarire le nuove modalità di accesso di altri organismi (Europol, Eurojust) e si è ribadita l'inopportunità di inserire dati biometrici nel sistema (ad esempio, rilievi dattiloscopici) qualora tali dati non siano effettivamente indispensabili ai fini della specifica segnalazione. In merito alla proposta di inserire nel Sis le informazioni contenute nel cosiddetto "mandato di arresto europeo", l'Autorità comune, in un altro parere, ha sollecitato chiarimenti da parte del competente Comitato presso il Consiglio Ue, sottolineando che l'utilizzo del Sistema informativo Schengen quale veicolo di trasmissione delle informazioni contenute nel mandato di arresto europeo comporterebbe, ancora una volta, una modifica sostanziale della natura del Sis e dei suoi meccanismi di funzionamento, che va previamente discussa ed impostata organicamente sul piano normativo. Tra le diverse altre questioni riassunte nel Rapporto vi è quella dell'integrazione con altre banche dati.

Anche il Parlamento europeo ha sollecitato un riesame della questione, attraverso alcune audizioni pubbliche e seminari tenuti a Bruxelles, cui è stato chiamato a partecipare il segretario generale del Garante, in qualità di presidente dell'Autorità comune di controllo.

L'art. 96 della Convenzione Schengen

Sotto altro profilo, è stato avviato dall'Autorità comune uno studio per verificare le discrepanze eventualmente esistenti fra i vari Paesi nell'interpretazione ed applicazione dell'art. 96 della Convenzione Schengen, relativo alle segnalazioni ai fini della non ammissione sul territorio comune. In base ai criteri previsti da tale norma, nessuna segnalazione relativa ad una persona può essere inserita nel Sis se non in base ad una richiesta delle competenti autorità nazionali successiva all'adozione di un formale provvedimento (in genere di espulsione) delle autorità amministrative o giudiziarie concernente la medesima persona. Si è quindi avviata una verifica comune in tutti i Paesi, che dovrà portare entro breve termine anche in Italia a controlli almeno a campione sulle migliaia di interessati segnalati dal nostro Paese e sulle procedure di immissione di tali informazioni.

In merito, infine, ai tempi di conservazione delle segnalazioni inserite nel Sis, l'Autorità comune ha ritenuto, in un parere, che il termine di tre anni previsto dall'art. 112 della Convenzione Schengen per il riesame delle singole segnalazioni si applichi a tutti i dati personali contenuti nel Sis, indipendentemente dalle specifiche finalità (reperimento di una persona, divieto di ingresso nei confronti di tale persona).

41 Gli interventi dell'Ocse in materia di sicurezza

41.1. Attuazione delle linee-guida sulla sicurezza

Ad un anno dall'approvazione delle linee-guida sulla sicurezza, l'Ocse ha organizzato un seminario internazionale cui ha partecipato anche questa Autorità, per mettere a confronto le esperienze applicative nei singoli Paesi.

Le relazioni hanno evidenziato una notevole difformità nelle misure attuative a livello nazionale ed hanno fatto emergere la mancanza di chiarezza sui soggetti che dovrebbero promuovere l'attuazione dei principi contenuti nelle linee-guida. Tutti i partecipanti hanno affermato la necessità di incrementare lo scambio di *best practice* e di sviluppare metodologie capaci di valutare l'impatto delle misure di sicurezza informatica. Altre esigenze assai sentite sono quelle di sviluppare ulteriormente la condivisione delle informazioni *(Warning, Advice and Reporting WARP)* e di incoraggiare le industrie a conformare sempre di più i loro *hardware* e *software* alla sicurezza ed alla *privacy*, individuando soluzioni che evitino di far affidamento solo sui consumatori finali.

Particolare attenzione è stata rivolta anche alla necessità di promuovere politiche di istruzione e formazione per i Paesi non membri dell'Ocse, anche in ragione dell'interdipendenza crescente fra Paesi sviluppati e Paesi in via di sviluppo, che obbliga a pensare la sicurezza in termini "globali". È stata inoltre sottolineata la necessità di passare dal concetto di sicurezza a quelli di responsabilità e affidabilità.

La discussione si è conclusa con la decisione di creare un *Global Culture of Security Web Site (www.oecd.org/sti/cultureofsecurity)*, che possa costituire uno strumento di scambio di esperienze reciproche fra i Paesi membri e, allo stesso tempo, una fonte di informazione per i Paesi non membri.

41.2. Sicurezza dei viaggi internazionali (Travel Security)

Alla luce dei numerosi dibattiti non solo europei, l'Ocse ha deciso di rivolgere particolare attenzione a tale argomento, ritenendolo un importante terreno di confronto tra le rinnovate esigenze di sicurezza ed i principi di protezione dei dati personali.

Nel settembre del 2003, l'Ocse e l'Icao (Organizzazione internazionale dell'aviazione civile) hanno organizzato a Londra un incontro, cui ha partecipato anche questa Autorità, volto ad esaminare i tipi di controlli e di sistemi che potrebbero migliorare la sicurezza dei viaggi internazionali, garantendo al contempo un elevato grado di tutela dei dati personali.

L'esame dei metodi sottoposti alla discussione, tra i quali figurano l'inserimento di dati biometrici nei passaporti e la previsione di sistemi di trasmissione dei dati dei passeggeri, ha confermato che questa materia costituirà un elemento cruciale del dibattito anche futuro su sicurezza e *privacy*.

Per tali ragioni il *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse, avendo competenze in materia di sicurezza, *privacy* e biometria –i tre ele-

41

menti centrali della *travel security*– ha recentemente dato vita ad un gruppo di esperti che, unitamente a rappresentanti dell'Icao, si occuperà del tema. Il gruppo, basandosi sulle raccomandazioni dell'Icao e sulle linee guida dell'Ocse, avrà come compito principale l'elaborazione di indicazioni agli Stati membri sugli aspetti di sicurezza dell'informazione e di tutela della *privacy* nella raccolta e scambio dei dati relativi ai passeggeri che intraprendono viaggi internazionali. Di tale gruppo farà parte anche un rappresentante del Garante.

Le informazioni genetiche

42 I compiti e gli interventi del Garante

Con riferimento ai dati genetici, il Codice ha confermato il principio stabilito dalla disciplina previgente secondo cui il trattamento di queste informazioni, da chiunque effettuato, dovrà essere oggetto di un'apposita autorizzazione del Garante (art. 90).

Tale autorizzazione sarà rilasciata nel 2004 sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità. Nelle more di questa nuova ed apposita autorizzazione, che avrà carattere generale, i trattamenti di dati genetici possono essere allo stato iniziati o proseguiti osservando le prescrizioni contenute nell'autorizzazione n. 2/2002, come ad es. il divieto di comunicare le informazioni genetiche a terzi.

Sempre in tema di dati genetici, il Garante è intervenuto a seguito di una segnalazione proveniente dall'estero rispetto ad una vicenda che aveva avuto eco anche sulla stampa straniera. Il caso riguarda un'articolata ricerca genetica su popolazioni isolate in Alto Adige. L'Autorità, avvalendosi dell'esperienza acquisita a seguito di analoghi accertamenti svolti in merito a ricerche attivate in altre regioni, ha curato ispezioni *in loco*, ottenendo informazioni e documenti relativamente alle modalità di raccolta dei dati bio-genetici e all'osservanza delle garanzie a tutela della riservatezza degli interessati in materia di informativa e consenso.

Dal procedimento svolto con la collaborazione dei professionisti preposti alla ricerca è già scaturita, pur in presenza del rispetto di parte dei principi di legge, una denuncia di reato per violazione di norme in materia di misure di sicurezza e un connesso provvedimento di prescrizione di misure idonee ai sensi dell'art. 169 del Codice.

È poi attualmente allo studio dell'Autorità il trattamento di dati personali connesso alla realizzazione di *test* genetici. L'esame avviato dal Garante concerne i *test* finalizzati alla prevenzione, diagnosi o terapia di malattie genetiche, quelli di paternità e/o maternità utilizzati per scopi probatori in sede civile o penale, nonché quelli di tipo "informativo" o "confidenziale", basati cioè su una mera comparazione dei profili genetici ottenuti da due o più tracce biologiche anonime, al fine di fornire indicazioni sulla loro compatibilità genetica.

Procreazione assistita

Per quanto riguarda la materia della procreazione assistita, si è parlato in altra parte della *Relazione* dell'audizione del presidente del Garante nell'ambito dei lavori preparatori della legge n. 40/2004 (cfr. parag. 2.). Va aggiunto che l'Autorità è stata investita da numerosi interpelli e segnalazioni a proposito delle modalità inizialmente ipotizzate per attuare l'art. 17 di tale legge, 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"*.

Di seguito alla prima circolare del Ministro della salute del 10 marzo 2004, l'Ufficio del Garante ha curato alcuni approfondimenti in collaborazione con il Ministero.

All'esito di tali approfondimenti, con nota ministeriale del successivo 25 marzo, si è ottenuta conferma che non si sarebbe più sollecitata una comunicazione nominativa di tutti gli interessati che avevano fatto ricorso alla procreazione assistita presso i centri, ma 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). La vicenda ha trovato così un giusto punto di bilanciamento di cui il Governo ha anche dato atto nella successiva risposta ad alcuni atti di sindacato ispettivo in Parlamento.

43 Il documento di lavoro del Gruppo art. 29

Sul trattamento dei dati genetici deve essere ricordato, inoltre, il documento di lavoro adottato il 17 marzo 2004 dal Gruppo dei garanti europei costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

L'inarrestabile progresso tecnologico nel settore della genetica ha indotto il Gruppo ad occuparsene, viste le sue ripercussioni nel campo della riservatezza. In particolare si è cercato di individuare i settori in cui il trattamento dei dati genetici determina maggiori preoccupazioni, considerando comunque la protezione dei dati genetici un presupposto indispensabile del principio di uguaglianza e del diritto alla salute.

Dopo aver fornito le definizioni di dato genetico ed elaborato il concetto di "gruppo biologico", in linea con quanto stabilito in materia dal Consiglio d'Europa e dall'Unesco, vengono descritti il campo di applicazione della direttiva n. 95/46/CE, nonché le caratteristiche che rendono unici questi dati e le finalità più rilevanti per le quali vengono trattati negli ordinamenti dei quindici Paesi membri (tra le quali l'assistenza sanitaria e la terapia medica, l'occupazione, le assicurazioni, la ricerca medica e scientifica e l'identificazione). In tutti questi casi è necessario raggiungere un approccio uniforme e un punto di vista condiviso, al fine di stabilire adeguate garanzie.

Qualsiasi trattamento di dati genetici non connesso alla salvaguardia della salute dell'interessato e alla ricerca scientifica può avvenire solo se previsto da una norma di legge conforme alla direttiva e, in particolare, al principio di finalità e proporzionalità. Ne discende il divieto di *screening* genetici generalizzati.

Nei settori dell'occupazione e delle assicurazioni il trattamento dovrebbe essere consentito solo in casi eccezionali e comunque previsti da norme di legge.

In relazione ai campioni di materiali genetici, viene ribadita la necessità di garantire pienamente i diritti degli interessati durante il trattamento, così come l'opportunità di distruggere o rendere anonimi i campioni non appena ottenute le informazioni necessarie, anche in considerazione del loro eventuale impiego per fini di clonazione. Tutti i dati genetici devono inoltre essere trattati solo da professionisti qualificati, sulla base di specifiche autorizzazioni e regole.

Il documento si chiude invitando le autorità nazionali a svolgere un ruolo attivo nei rispettivi Paesi, con la previsione di forme di *prior checking* (in particolare per le cd. bio-banche) e ponendo l'accento sulla necessità di applicare i principi di proporzionalità e finalità.

La Conferenza di Sydney

44 La Conferenza e le Risoluzioni

Il Garante ha partecipato a numerose conferenze internazionali (su cui *infra,* parag. 52.3.): in questa sede va ricordata in particolare la partecipazione alla 25ª Conferenza internazionale delle autorità per la protezione dei dati personali, svoltasi a Sydney dal 10 al 12 settembre 2003.

La conferenza australiana ha rappresentato, infatti, un momento significativo nella discussione su una serie di temi emersi recentemente con piena evidenza: i prossimi passi nella regolamentazione della protezione dei dati personali, gli effetti che le normative sulla *privacy* producono a livello globale su imprese e consumatori, gli organismi, le tecnologie e gli incentivi per sostenere e sviluppare la difesa del diritto alla riservatezza, le implicazioni della protezione dei dati personali in campo giuridico, i rapporti tra tutela dell'ordine pubblico e rispetto delle persone, il ruolo svolto dalla *privacy* nella società contemporanea.

Alla Conferenza, che ha visto riuniti rappresentanti delle autorità per la protezione dei dati personali, esperti, imprese e rappresentanti governativi di oltre quaranta Paesi, l'autorità italiana ha partecipato con una delegazione guidata dal presidente prof. Stefano Rodotà, dal componente del collegio, on. Mauro Paissan e dal segretario generale, Giovanni Buttarelli. Il prof. Rodotà ha presieduto la sessione inaugurale dedicata alle nuove prospettive di regolamentazione della *privacy*. La Conferenza è stata preceduta da seminari di formazione e conferenze su diversi argomenti: tra queste va segnalata quella svoltasi l'8 settembre 2003 a Melbourne, dedicata a corpo fisico, corpo elettronico e dati personali, aperta dallo stesso prof. Rodotà.

La Conferenza si è conclusa con l'approvazione di cinque risoluzioni che richiamano l'attenzione su aspetti attuali e significativi della vita privata dei cittadini.

44.1. Trasferimento dei dati dei passeggeri

Una risoluzione riguarda il trasferimento di dati personali riguardanti i passeggeri da parte delle compagnie aeree alle autorità statunitensi. In essa viene affermato che nella lotta contro il terrorismo e la criminalità organizzata gli Stati devono osservare i principi fondamentali in materia di protezione dei dati, e che le informazioni sui viaggiatori diretti negli Usa possono essere acquisite e trasferite solo all'interno di un contesto che tenga conto delle esigenze di protezione dei dati ed in base ad un accordo internazionale. Questo accordo dovrebbe contenere norme adeguate in relazione ad alcuni profili: limitazione delle finalità, non eccedenza dei dati raccolti, tempi di conservazione, informativa, diritto di accesso, previsione di un'autorità di controllo indipendente.

44.2. Informativa

Al tema dell'informativa e, in particolare, all'esigenza di migliorarne insieme la chiarezza e l'efficacia dei contenuti è stata dedicata un'altra risoluzione, in cui è stato affermato che l'informativa deve essere il più possibile chiara e concisa. Le autorità garanti si sono impegnate ad elaborare un modello *standard* che soggetti pubblici e privati potranno utilizzare per fornire informazioni essenziali sul trattamento con un linguaggio semplice, inequivocabile e diretto. Nel modello deve essere specificato il soggetto che tratta i dati e le finalità per le quali li tratta. Inoltre, deve essere spiegato come contattare tale soggetto e quali sono i diritti riconosciuti agli interessati e deve indicarsi l'autorità di controllo alla quale rivolgersi. Nell'informativa sintetica saranno poi forniti gli elementi per reperire ulteriori informazioni, secondo le esigenze del singolo interessato. Questa informativa deve essere fornita prima di richiedere qualsiasi dato personale e, per quanto riguarda il settore telematico, possibilmente in maniera automatizzata (su questo punto la Conferenza si è richiamata espressamente al lavoro svolto in materia dal Gruppo di cui all'art. 29 della direttiva europea n. 95/46/CE).

Le autorità hanno anche ribadito la propria disponibilità a collaborare con tutti i soggetti impegnati a migliorare la comunicazione fra imprese, pubblica amministrazione e cittadini, in un'ottica di trasparenza e di rispetto per la vita privata.

44.3. Organizzazioni internazionali

Una terza risoluzione si è occupata degli organismi internazionali e sovranazionali. Le autorità hanno invitato questi ultimi ad impegnarsi nell'osservare le regole compatibili con i principi fissati a livello internazionale nella materia della tutela della *privacy* (direttive Ue, raccomandazioni del Consiglio d'Europa, linee-guida Ocse), tra le quali la creazione di autorità di controllo interne, effettivamente indipendenti sul piano operativo. È poi necessaria, a giudizio delle autorità garanti, una valutazione preliminare dell'impatto in materia di riservatezza di qualsiasi norma o regolamento elaborato da un organismo internazionale e che abbia riflessi sulla legislazione dei singoli stati.

44.4. Aggiornamenti automatici di software

Gli aggiornamenti automatici di *software* hanno formato oggetto di un'altra risoluzione adottata a Sydney. In particolare è stato rilevato che le case produttrici di *software* ricorrono sempre più a meccanismi non trasparenti per trasferire aggiornamenti di *software* nei computer dei singoli utenti. Per evitare i rischi derivanti dalla possibilità di leggere e raccogliere dati personali memorizzati nel *computer* dei singoli utenti senza che questi ne abbiano consapevolezza, e per non esporre gli utenti stessi al rischio di commettere involontariamente un illecito, la Conferenza ha invitato le società:

- ad aggiornare il *software on line* solo su richiesta dell'utente, secondo procedure trasparenti;

- a non richiedere dati personali se non assolutamente necessari per effettuare l'aggiornamento, anche in tal caso solo con il consenso informato dell'utente.

La risoluzione ha inoltre sottolineato l'opportunità di offrire forme alternative di distribuzione del *software* (ad esempio, attraverso specifici *Cd-Rom*).

44.5. Radio frequency identification

L'ultima risoluzione, adottata non contestualmente allo svolgimento della Conferenza, si è occupata del tema dell'identificazione attraverso radiofrequenze *(Rfid)*.

I dispositivi basati su tale sistema, che vengono utilizzati sempre più spesso, comportano significative implicazioni anche in materia di tutela della *privacy*. La tecnologia impiegata, infatti, potrebbe ricostruire le attività di singoli individui e istituire collegamenti fra le informazioni raccolte e banche dati preesistenti.

Per tali motivi le autorità garanti hanno invitato i titolari di trattamenti ad utilizzare, laddove possibile, approcci alternativi rispetto alla raccolta di dati personali o alla profilazione della clientela. Quando tale tecnologia risulta indispensabile, per scopi legittimi, la raccolta deve essere comunque chiara e trasparente, i dati devono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati raccolti e conservati solo fino al raggiungimento di tale scopo, e gli interessati dovrebbero avere la possibilità di cancellare i dati e di disattivare o distruggere le etichette *Rfid*. Viene inoltre sottolineata l'importanza di tener conto dei principi enunciati in materia di dati personali anche nella fase di progettazione e nell'utilizzazione di prodotti cui siano applicabili tecnologie basate su *Rfid*.

Il Garante

VI - L'attività del Garante

45 La collaborazione fornita dal Garante alle attività del Parlamento e del Governo

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

Anche nel corso del 2003 l'Autorità ha seguito con attenzione l'attività di sindacato ispettivo e di indirizzo esercitata dal Parlamento, in relazione agli aspetti di specifico interesse in materia di protezione dei dati personali, fornendo al Governo, laddove richiesto, i chiarimenti e le indicazioni necessarie.

Sono stati pure inviati al Governo gli elementi richiesti in relazione ad alcuni atti di sindacato fra i quali, in particolare, un'interrogazione a risposta immediata presentata dall'on. Folena (3-02832), relativa all'acquisizione da parte degli Usa dei dati dei passeggeri conservati nella banca dati dell'Alitalia (*Nota* 4 novembre 2003). In tale occasione il Garante ha ricordato, fra l'altro, che la richiesta formulata dalle autorità americane alle compagnie aeree di accedere a tutti i dati contenuti nel *Pnr* (*Passenger name record*, su cui cfr. *supra*, parag. 36.) relativi ad individui diretti, provenienti o in transito verso gli Stati Uniti, va valutata alla stregua delle disposizioni comunitarie in materia (in particolare, l'art. 25 della direttiva n. 95/46/CE).

Va infine ricordato che due mozioni analoghe della maggioranza (1-00304 Leone ed altri) e dell'opposizione (1-00215 Folena ed altri), poi approvate all'unanimità dal Parlamento il 14 gennaio 2004, con riferimento alle problematiche inerenti alla conversione del d.l. n. 354/2003 hanno impegnato il Governo a rimuovere tutte le norme potenzialmente lesive dei diritti di riservatezza e a regolamentare in modo più efficace il trattamento dei dati di traffico della telefonia mobile, al fine di tutelare il diritto degli individui (sul punto, cfr. più diffusamente parag. 1.11.).

45.2. L'attività consultiva del Garante sugli atti del Governo

L'articolo 154, comma 4, del d.lg. n. 196/2003 (che riproduce l'art. 31, comma 2, della legge n. 675/1996) stabilisce che il Presidente del Consiglio dei ministri e ciascun ministro debbano consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere in materia di protezione di dati personali.

In relazione a tale competenza, nel corso dell'anno il Garante ha espresso vari pareri anche in importanti materie, fra cui, in particolare, quelli riguardanti:

- due schemi di regolamento in attuazione della legge n. 189/2002 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, lo sviluppo e la razionalizzazione dei sistemi informativi delle pubbliche amministrazioni coinvolte nell'applicazione della legge, in particolare ai fini del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (*Parere* 4 marzo 2004);

Il permesso di soggiorno elettronico

- 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 tra rappresentanti dell'Autorità e del Ministero dell'interno, in cui sono stati forniti chiarimenti sul piano applicativo, il Garante ha formulato un secondo parere il 4 marzo 2004 con il quale ha, fra l'altro, indicato 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. Al riguardo, l'Autorità ha anche confermato la propria disponibilità a proseguire la cooperazione con il Ministero al fine di approfondire i problemi ed i rischi derivanti dalle differenti tecniche di identificazione e di autenticazione, descritte dai Garanti europei a proposito dei dati biometrici nel parere del 1° agosto 2003 (su cui, *supra*, parag. 38.). Ciò anche allo scopo di individuare le cautele necessarie nella fase di attivazione del documento elettronico e di consegna dei documenti o di accesso selezionato ai dati, nonché le migliori garanzie di sicurezza disponibili. L'esito di tali approfondimenti potrebbe essere trasfuso nelle misure e negli accorgimenti che, in materia di dati biometrici, devono essere individuati dal Garante ai sensi dell'art. 55 del Codice;

- 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 (C.e.d.) della Corte di cassazione (*Parere* 27 febbraio 2004).

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

- uno 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* 28 gennaio 2004).

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 28 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.

Consultazione ed utilizzo dei dati del casellario giudiziale da parte delle p.a.

Le osservazioni del Garante hanno tenuto conto anche del ricorso presentato da un privato interessato all'aggiudicazione di un appalto, che lamentava l'utilizzo da parte della pubblica amministrazione, ai fini dell'esclusione dalla gara, di dati contenuti in un certificato generale del casellario, contestando che quest'ultimo potesse essere rila-

sciato ad un soggetto pubblico, considerata l'equiparazione dei certificati rilasciabili ai privati interessati e alle pubbliche amministrazioni. L'Autorità ha ritenuto infondate le tesi del ricorrente, alla luce della normativa vigente, che consente alla pubblica amministrazione di acquisire dal casellario i dati necessari per accertamenti d'ufficio o per il controllo delle autodichiarazioni presentate dai privati (il ricorrente ha impugnato la decisione davanti all'autorità giudiziaria: v. pure *supra*, parag. 27.). Tuttavia, sia nella decisione del ricorso, sia nel parere del 28 gennaio scorso, il Garante ha richiamato l'attenzione del Ministero della giustizia sulla necessità di completare al più presto ed in via definitiva la messa a punto del sistema di consultazione in via telematica del casellario da parte delle pubbliche amministrazioni e dei gestori di pubblico servizio, superando l'attuale fase transitoria così da consentire un utilizzo selettivo delle informazioni necessarie nell'ambito dello specifico procedimento avviato;

- lo schema di d.P.C.M. recante regole tecniche per la generazione, apposizione e verifica delle firme digitali, adottato ai sensi del testo unico in materia di documentazione amministrativa (d.P.R. n. 445/2000), in sostituzione del d.P.C.M. 8 febbraio 1999 (Parere 19 novembre 2003);

- lo schema di regolamento recante disposizioni per il diritto di accesso agli atti delle imprese di assicurazione, in attuazione dell'art. 3 della l. 5 marzo 2001, n. 57 (*Parere* 13 agosto 2003). A tal proposito, si sottolinea che le indicazioni fornite dal Garante in merito alla necessità di mantenere chiara la distinzione tra il diritto di accesso agli atti delle imprese di assicurazione ed il diritto di accesso ai dati di cui al d. lg. n. 196/2003, sono state recepite nel d.m. 20 febbraio 2004, n. 74 (v. in particolare l'art. 1, comma 2);

- lo schema del regolamento di attuazione ed organizzazione della banca dati relativa ai minori dichiarati adottabili istituita dall'articolo 40 della legge 28 marzo 2001, n. 149 (*Parere* 11 luglio 2003); il regolamento è stato poi adottato con d.m. 24 febbraio 2004, n. 91 in *Gazzetta Ufficiale* 9 aprile 2004, n. 84;

Carta nazionale dei servizi

- lo schema di d.P.R. recante il regolamento sulle caratteristiche e le modalità per il rilascio della Carta nazionale dei servizi (*Parere* 9 luglio 2003). In tale parere il Garante ha richiesto un'attenta valutazione, da parte dell'amministrazione procedente, circa la pertinenza dei dati da inserire nella carta, che in ogni caso non potrebbero essere dati sensibili; si è inoltre espresso in favore della loro utilizzazione da parte delle amministrazioni esclusivamente a fini di identificazione dell'interessato e di legittimazione al servizio offerto. L'Autorità ha poi richiesto che le disposizioni dello schema relative all'utilizzo dell'Indice nazionale delle anagrafi (Ina) fossero rese coerenti con la funzione propria di tale indice, che è quella di mero strumento per l'individuazione agevole del comune di residenza degli interessati e non di sostanziale anagrafe nazionale;

- lo schema di regolamento per la tenuta dei fascicoli personali della carriera diplomatica ai sensi dell'art. 113 del d.P.R. n. 18/1967 (*Parere* 19 giugno 2003). Il regolamento è stato poi adottato con il decreto del Ministro degli affari esteri 13 ottobre 2003, n. 311;

- lo schema di regolamento concernente le modalità di istituzione e tenuta presso la Presidenza del Consiglio dei ministri della banca dati informatica dei componenti degli organi di amministrazione attiva, consultiva e di controllo dello Stato e degli enti pubblici a carattere nazionale e delle relative modalità di nomina (*Parere* 9 aprile 2003);

- lo schema di regolamento in materia di estensione delle disposizioni antiriciclaggio ad attività non finanziarie particolarmente suscettibili di utilizzazione a fini di riciclaggio, in attuazione dell'art. 4, comma 8, del d.lg. 25 settembre 1999, n. 374 (*Parere* 12 marzo 2003).

46 La cooperazione a livello europeo

46.1. L'attività del Gruppo istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE

Nel 2003 è proseguita la tendenza ad un ampliamento del ruolo e delle competenze del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

Intenso è stato il lavoro svolto da tale Gruppo per interpretare, segnalare ed indirizzare l'attività della Commissione europea in relazione all'applicazione dei principi della direttiva generale in materia. Il rischio che potrebbe presentarsi al riguardo è che il Gruppo sia però considerato, anche presso uffici comunitari, alla stregua di un gruppo di lavoro specializzato, anziché un organismo consultivo indipendente.

A causa dell'attuale esiguità della struttura di segretariato, che svolge una funzione di supporto al Gruppo, la predisposizione degli elementi per la discussione e la successiva valutazione delle proposte della Commissione è stata a volte compiuta direttamente dagli uffici della stessa Commissione che avevano chiesto l'avviso del Gruppo. I pareri sono stati, inoltre, talora sollecitati non già in fase di predisposizione di misure comunitarie, bensì a volte dopo la presentazione delle relative proposte al Consiglio.

In proposito, un'iniziativa della Commissione tuttora in corso di elaborazione, sulla quale il Gruppo dei garanti europei ha fornito un parere preliminare, ha riguardato la proposta di una direttiva in materia di protezione dei dati dei lavoratori. Nel settore della protezione dei dati sono inoltre da segnalare le proposte della Commissione relative all'introduzione di modelli per il rilascio di visti e permessi di soggiorno, nonché di passaporti che prevedono l'inserimento obbligatorio di dati biometrici.

In ogni caso, come detto, il ruolo dei garanti europei in ambito comunitario ha acquisito un rilievo più forte.

Il Gruppo, che fino al 16 marzo scorso è stato presieduto dal prof. Rodotà, è stato più volte coinvolto ufficialmente nell'ambito di vari incontri, seminari, audizioni e lavori parlamentari, coordinati dal Parlamento europeo per discutere ed approfondire temi di particolare rilevanza: è quanto avvenuto, ad esempio, in relazione a

numerose proposte volte ad intensificare la creazione di basi di dati a livello europeo e a rendere accessibili, al di là delle previsioni delle singole convenzioni istitutive, i trattamenti di dati effettuati nell'ambito della cooperazione di polizia e giudiziaria.

Alla luce di ciò, potrebbe diventare necessario ridefinire la collocazione istituzionale del Gruppo nel quadro della complessa compagine comunitaria, come pure del suo segretariato. Questo anche in considerazione delle numerose proposte in corso di elaborazione su materie di confine tra il primo ed il terzo pilastro, la cui predisposizione compete ad uffici della Commissione diversi da quelli ai quali è affidata l'attuazione della direttiva n. 95/46/CE (D.g. mercato interno).

Nel corso del 2003, l'attività del Gruppo ha riguardato un'ampia gamma di tematiche, attinenti sia ai diversi ambiti di applicazione delle direttive n. 95/46/CE e n. 2002/58/CE, sia al trasferimento dei dati personali verso Paesi terzi.

Il Gruppo ha dedicato particolare attenzione alle richieste di alcuni Stati (Australia, Canada, Stati Uniti) di ottenere da parte delle compagnie aeree i dati personali dei passeggeri in viaggio da e verso il loro territorio. Tali richieste sono state motivate con la necessità di prevenire il terrorismo e di facilitare i compiti delle autorità doganali. Il Gruppo, nel ribadire l'esigenza di un approccio equilibrato alla lotta contro il terrorismo (v. Pareri n. 10/2001 e n. 6/2002), ha sottolineato la necessità di rispettare e di applicare correttamente anche in tale settore i principi sulla protezione dei dati personali (per maggiori dettagli sul punto, v. *supra*, parag. 36.).

Si ricorda, infine, un primo documento di lavoro (WP 86 del 23 gennaio 2004) sui dispositivi proposti dal consorzio *Trusted Computing Group* per incentivare la sicurezza delle transazioni elettroniche mediante strumenti non solo *software*, ma anche *hardware*.

46.2. La partecipazione ad altri comitati e gruppi di lavoro

Il Gruppo di Berlino

Sempre nell'ambito della definizione delle forme di collaborazione e scambio tra le autorità di protezione dei dati, va ricordata l'attività dell'*International Working Group on data protection in telecommunications* (cd. Gruppo di Berlino), in quanto sede di discussione ed approfondimento, non solo a livello europeo, su temi quali Internet, cifratura e comunicazioni elettroniche, tra esperti in materia di tecnologie ed informazione.

Nella riunione di Berlino del 2-3 settembre 2003 sono stati discussi numerosi temi, fra cui meritano di essere menzionati in particolare il *media privilege*, la *Radio frequency identification* (identificazione attraverso radio frequenze), il tempo di conservazione dei dati di traffico e lo *spamming*.

Con riferimento ai *media*, sono stati analizzati gli esiti dei questionari compilati a livello nazionale e sono state presentate le innovazioni introdotte in materia nella normativa nazionale dal d.lg. n. 196/2003.

È stato inoltre illustrato il contenuto del provvedimento del Garante relativo ai *Multimedia message systems (Mms)*, il quale potrà contribuire all'elaborazione di una dichiarazione che il Gruppo adotterà durante la prossima riunione.

46

Con riguardo alla *Radio frequency identification*, il Gruppo ha elaborato un documento che è successivamente servito come base per la risoluzione adottata dalle autorità di garanzia riunite a Sydney nel settembre del 2003 (v. *supra*, parag. 44.5.).

I *Complaints Handling Workshop*

Sono proseguiti gli incontri (cd. seminari in materia di *Complaints Handling*) organizzati ai fini dello scambio di informazioni e della definizione di linee operative comuni per la trattazione delle segnalazioni e dei ricorsi presentati alle autorità nazionali per la protezione dei dati, con particolare riguardo ai casi che, per la loro rilevanza o per la natura delle parti interessate, travalicano l'ambito nazionale.

Ai due incontri, tenutisi rispettivamente a Roma (VIII *Complaints Handling Workshop*, 23-24 ottobre 2003) ed a Stoccolma (IX *Complaints Handling Workshop*, 11-12 marzo 2004), hanno partecipato oltre quarantacinque delegati dei Paesi Ue e di quasi tutti i Paesi in via di adesione all'Unione.

Nel seminario di Roma è stata dedicata specifica attenzione al tema della biometria, con la discussione dei risultati di un questionario presentato dalla delegazione portoghese. Il tema della ricerca farmacologica e delle modalità di prestazione del consenso da parte dei pazienti e/o candidati è stato esaminato in relazione a un questionario predisposto dalla delegazione belga. La delegazione italiana ha impostato la discussione di due casi concreti di bilanciamento di interessi, evidenziando numerose difformità negli approcci seguiti dai singoli Paesi in rapporto, soprattutto, all'esistenza o meno di norme settoriali che indichino già criteri operativi. Sono stati pure presentati gli aggiornamenti relativi all'indagine conoscitiva condotta dal Garante nel 2002 sui meccanismi utilizzati dalle maggiori imprese italiane per trasferire dati personali (di clienti e/o dipendenti) verso Paesi terzi. La discussione ha poi preso in considerazione possibili linee-guida per assicurare che i seminari in materia di *"Complaints Handling"* continuino ad essere focalizzati su casi concreti e su positive modalità operative già in sperimentazione.

Alcuni dei temi affrontati durante l'incontro di Roma sono stati approfonditi in occasione del seminario di Stoccolma, con particolare riguardo alla biometria. Ciascuna delegazione ha, infatti, presentato un caso nazionale emblematico, prospettando le soluzioni volta per volta individuate. La delegazione portoghese ha segnalato l'esistenza di un "decalogo" emanato dall'autorità nazionale di protezione dati per regolamentare l'impiego di dispositivi biometrici ai fini del controllo dell'accesso a locali pubblici e/o privati. Sono state analizzate, inoltre, le strategie seguite dalle varie autorità nazionali per sollecitare l'attenzione dell'opinione pubblica. In particolare, l'autorità svedese e quella del Land di Brandeburgo hanno illustrato l'attività di sensibilizzazione ed educazione svolta rispetto ai cd. incaricati della protezione dei dati, cioè i soggetti che i titolari possono designare ai sensi dell'art. 18(2) della direttiva n. 95/46/CE con il compito, fra l'altro, di tenere un registro dei trattamenti, evitando così l'invio della notificazione all'autorità di controllo. I partecipanti hanno anche esaminato le priorità eventualmente individuate dalle rispettive autorità in relazione alle attività ispettive. Infine, è proseguita la discussione sulla configurazione futura dei seminari e, in particolare, sullo spostamento del nucleo centrale di attività dalla trattazione di casi che coinvolgono più Paesi al confronto su casi concreti affrontati dalle singole autorità. Un documento in merito è stato presentato per la discussione all'*European Spring Conference of Data Protection Commissioners* (Rotterdam, 21-23 aprile 2004).

46.3. EUROPOL: l'attività dell'Autorità comune di controllo e i primi casi di contenzioso

L'Autorità comune di controllo prevista dall'art. 24 della Convenzione Europol ha continuato la sua attività di verifica e controllo sulla gestione degli archivi Europol, che dal luglio 1999 comprendono gli archivi di analisi.

Tale Autorità ha seguito con attenzione i progetti di negoziato sottoposti dal Direttore dell'Europol per ottenere il consenso ad iniziare le trattative volte allo scambio di dati con alcuni Paesi terzi. Sono stati inoltre espressi pareri in merito all'apertura di *file* di analisi e alla nozione di dato personale nel contesto Europol, compresa la possibilità di includervi anche le persone decedute.

L'Autorità comune si è inoltre occupata degli sviluppi applicativi dell'accordo Europol-Stati Uniti per la trasmissione di dati personali a seguito della ristrutturazione del *Department of Homeland Security* ed ha espresso le sue preoccupazioni riguardo ai lavori per la revisione dei sistemi di informazione esistenti nel cd. terzo pilastro, che si svolgono presso il Consiglio dell'Unione europea ed ai quali partecipa il segretariato comune delle autorità comuni di controllo in tale ambito.

Nell'ottobre del 2003 sono stati rinnovati diversi componenti dell'Autorità comune di controllo e del Comitato ricorsi, per scadenza del rispettivo mandato, ed è iniziata un'attività di definizione delle regole per l'accesso agli atti e ai documenti detenuti dall'Autorità comune. Ciò anche in relazione all'apertura di uno specifico sito *web (http://europoljsb.ue.eu.int/home/default.asp?lang=it)* ed alla scelta dei documenti da mettere a disposizione del pubblico (oltre al rapporto di attività e al testo dei pareri adottati, anche informazioni sulla composizione dell'Autorità, sui compiti attribuiti, nonché sul funzionamento del comitato ricorsi).

Una discussione approfondita è stata dedicata alla bozza di accordo predisposta per lo scambio di dati ed informazioni tra Europol ed Eurojust.

Alle riunioni erano presenti, in veste di osservatori, i rappresentanti degli organismi incaricati della protezione dei dati dei Paesi in via di adesione all'Unione europea.

È stata anche svolta l'annuale ispezione alla sede dell'Europol incentrata sugli archivi di analisi e sugli sviluppi tecnologici del sistema, ed è stata effettuata una visita di controllo per verificare il grado di adempimento di Europol alle raccomandazioni impartite a seguito dell'ispezione.

La prima relazione di attività dell'Autorità comune

La prima relazione di attività, riguardante il periodo ottobre 1998-ottobre 2002, è stata ufficialmente presentata dal Presidente agli organi competenti ed è stata resa disponibile nelle diverse versioni linguistiche, sia in formato cartaceo (cfr. l'allegato alla presente Relazione), sia in formato elettronico sul sito *web* dell'Autorità comune.

Va, infine, ricordata la modifica della Convenzione Europol adottata dal Consiglio dei ministri giustizia e affari interni, che amplia il ruolo di Europol rispetto agli specifici scopi conferitigli inizialmente dalla Convenzione.

46

46.4. Il sistema informativo doganale

Il Sistema informativo automatizzato comune (Sistema informativo doganale-S.i.d.) è stato istituito dalla Convenzione sull'uso dell'informatica nel settore doganale del 26 luglio 1995, elaborata in base all'articolo K3 del Trattato Ue e ratificata dall'Italia con la legge 30 luglio 1998, n. 291.

La Convenzione mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'Ue, specie attraverso lo scambio di dati personali. A tal fine è appunto prevista la creazione del Sistema informativo doganale, che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La Convenzione istituisce, inoltre, un'autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati, che ha iniziato i suoi lavori nel corso della primavera del 2002. Nel periodo in esame l'Autorità ha definito il proprio regolamento interno e i metodi di lavoro. Ha espresso, inoltre, il parere sull'istituzione di un archivio di identificazione dei fascicoli a fini doganali (cd. Fide). Nelle ultime riunioni, l'Autorità comune di controllo si è occupata in particolare di definire gli aspetti relativi all'effettuazione di ispezioni *in loco*.

46.5. Eurodac

A seguito della nomina e costituzione dell'Autorità di controllo indipendente, avvenuta con la decisione del Parlamento e del Consiglio del 22 dicembre 2003, l'Autorità comune di controllo Eurodac per il confronto delle impronte digitali di coloro che richiedono l'asilo ha esaurito le sue funzioni.

La nuova Autorità di controllo su Eurodac

Il controllo su tale sistema informativo, costituito e gestito dalla Commissione, spetterà infatti in via definitiva alla predetta autorità di controllo indipendente prevista dall'art. 286, par. 2, del Trattato di Amsterdam, che ha il compito di controllare la correttezza dei trattamenti di dati effettuati dalle istituzioni e dagli organismi dell'Ue.

La nuova cornice normativa in materia di protezione dati è stata illustrata dai servizi giuridici della Commissione nel corso dell'ultima riunione dell'Autorità comune di controllo, in cui sono state esposte, in particolare, le funzioni e i legami fra i differenti organi di controllo competenti in materia. In tale occasione sono stati pure presentati i regolamenti che stabiliscono i criteri e i meccanismi di determinazione dello Stato membro responsabile dell'esame di una domanda di asilo e le modalità attuative, in particolare il funzionamento della rete DubliNET.

È stato inoltre evidenziato che la banca dati dell'Unità centrale aumenta costantemente di dimensioni, e che vengono alla luce anche doppie e triple "identificazioni positive", ciò che prova la reale utilità del sistema. La Commissione ha sottolineato l'alta qualità dei dati contenuti nella banca dati centrale ed ha evidenziato la necessità di un'analoga qualità in ambito nazionale al momento della raccolta delle impronte digitali inviate ad Eurodac per l'accertamento.

47 L'attività dell'Autorità nell'ambito del Consiglio d'Europa

47.1. I gruppi di esperti

Il Protocollo addizionale alla Convenzione n. 108 del 1981, che prevede l'istituzione di autorità di controllo indipendenti con compiti di verifica e controllo dei trattamenti, e disciplina i flussi transfrontalieri di dati, aperto alla firma l'8 novembre 2001, avendo raggiunto il numero di ratifiche necessario, entrerà in vigore il 1° luglio 2004.

L'Italia è tra i Paesi firmatari, ma non ha ancora presentato in Parlamento il disegno di legge di ratifica.

Per quanto riguarda le modifiche alla ricordata Convenzione n. 108 per consentire alle Comunità europee di aderirvi, l'Italia non ha firmato il relativo Protocollo emendativo. Essendo necessaria l'accettazione degli emendamenti da parte di tutti i Paesi dell'Unione europea, tali modifiche non sono quindi ancora entrate in vigore.

Nel quadro dell'attività del Consiglio d'Europa meritano di essere menzionati i lavori dei cd. gruppi di esperti: il Comitato CJ-PD, nato nell'ambito del Comitato per la cooperazione giudiziaria e soppresso a seguito del processo di razionalizzazione delle risorse utilizzabili, è riuscito comunque, nel corso della sua ultima riunione, svoltasi nel dicembre 2003, a portare a compimento i lavori sulle linee guida per l'uso delle carte intelligenti *(smart card)*.

Il Comitato T-PD

Il Comitato T-PD cd. convenzionale, in quanto costituito direttamente dalla Convenzione n. 108 e quindi non sopprimibile per decisione amministrativa, nell'unica riunione plenaria svoltasi anch'essa nel mese di dicembre 2003, si è trovato a valutare le problematiche derivanti dalla soppressione del CJ-PD e, in particolare, le modalità di prosecuzione dei lavori sul trattamento di dati biometrici, che il CJ-PD non ha potuto completare.

Proprio a causa dell'inserimento nei suoi lavori delle problematiche legate alla biometria, il TP-D ha poi dovuto rivedere le priorità stabilite per il 2003 e per il 2004, programmando un approfondimento sui seguenti temi:

- l'applicazione dei principi della Convenzione in relazione agli sviluppi tecnologici. Il Comitato si propone così di esaminare meglio, alla luce della Convenzione, come un indirizzo di posta elettronica o il numero di un telefono cellulare sia da considerare "dato personale". Intende inoltre valutare i rischi che derivano dalla diffusione di nuove tecnologie (molteplicità dei fini, conservazione dei dati da parte dei "nuovi media") come pure le opportunità che ne possono discendere in merito alla protezione dei dati personali (PETs, tecnologie non invasive, ecc);

- l'applicazione dei principi di protezione dei dati ad Internet, in relazione ai quali il TP-D ha preparato un progetto di mandato per uno studio preliminare da far effettuare ad un consulente.

48 Altre iniziative in ambito internazionale: Ocse

Nel periodo di riferimento il Garante ha continuato a seguire i lavori del *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse, sottogruppo del *Committee for Information Computer and Communication Policy (Iccp)*.

Fra i problemi di maggior rilievo affrontati negli incontri svoltisi nel 2003 in relazione al trattamento dei dati personali, si debbono ricordare l'attuazione delle linee-guida sulla sicurezza, lo *spamming*, la biometria, e la creazione di un apposito gruppo che si occuperà di sicurezza nei viaggi internazionali *(travel security)*, gruppo a cui parteciperà questa Autorità. Le conclusioni raggiunte in sede Ocse su tali temi sono già state esposte in appositi paragrafi della *Relazione*, ai quali pertanto si rinvia per un'analisi dettagliata (v. parag. 41.1. e 41.2.).

49 Il sistema di informazione Schengen (Sis)

Nel corso dell'anno sono state sottoposte al Garante, quale autorità di controllo sulla sezione nazionale del Sistema informativo Schengen (Sis), numerose richieste di verifica in merito all'eventuale o corretta registrazione, negli archivi del Sis, di dati personali dei soggetti interessati ed alla liceità dei relativi trattamenti. Si tratta, in gran parte, di domande che attengono al diniego di visto, per lo più adottato a causa di segnalazioni, ai fini della non ammissione nella cd. area Schengen, di persone nei cui confronti sono stati emessi provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno (espulsione, respingimento alla frontiera).

Si è registrato anche quest'anno un notevole incremento delle richieste pervenute, da attribuire pure alla procedura di regolarizzazione di cittadini extracomunitari introdotta dalla legge n. 189/2002; le richieste provengono soprattutto da Paesi dell'Est europeo e, in particolare, dalla Romania.

Nell'arco temporale che va dal 1° gennaio 2003 al 31 marzo 2004 le richieste sono state 480, di cui 464 già definite.

Per svolgere al meglio i propri compiti e fronteggiare più rapidamente anche le domande di chiarimenti sulla normativa di riferimento, nel febbraio 2003 il Garante ha nuovamente riassunto l'esatto ambito delle proprie competenze: ha così precisato che gli interessati possono rivolgere a questa Autorità richieste di verifica dei dati che li riguardano inseriti nel Sis, ovvero di aggiornamento, di rettifica o di cancellazione dei medesimi dati. Al Garante, invece, non sono conferiti compiti di adozione, revoca o controllo dei provvedimenti amministrativi che sono alla base delle segnalazioni contenute nel Sis.

Per rimediare poi a problemi insorti nei casi in cui erano state segnalate usurpazioni d'identità o omonimie, è stata ulteriormente sperimentata nel 2003, in colla-

borazione con il Dipartimento della pubblica sicurezza, una procedura di comparazione degli elementi identificativi della persona oggetto di usurpazione d'identità con quelli, anche dattiloscopici, della persona effettivamente segnalata nel Sis.

Sempre allo scopo di rilevare più agevolmente i casi di omonimia, è stata poi rafforzata la collaborazione con il Centro visti del Ministero degli affari esteri e con le divisioni Sirene ed N.Sis del Dipartimento della pubblica sicurezza.

La nuova disciplina di accesso al Sis

Su tale quadro complessivo si sono innestate, con effetto dal 1° gennaio 2004, le modifiche introdotte dal Codice circa le modalità di esercizio del diritto di accesso al Sis e degli altri diritti connessi (rettifica, integrazione o cancellazione), che possono essere ora esercitati direttamente nei confronti dell'autorità di polizia (cd. accesso diretto) e non più solo per il tramite del Garante (cd. accesso indiretto).

Il d.lg. n. 196/2003 ha infatti modificato la legge n. 388/1993, lasciando sostanzialmente inalterato il sistema dei controlli del Garante attribuiti all'Autorità dalla Convenzione e dalla legge n. 675/1996 (ora, artt. 53, 154, comma 2, lett. *a)*, e 160 d.lg. n. 196/2003), ma disciplinando in maniera innovativa il diritto dell'interessato di conoscere l'esistenza nel Sis di una segnalazione che lo riguarda ed i dati detenuti, nonché di ottenerne l'eventuale aggiornamento, rettifica o cancellazione (art. 173 d.lg. n. 196/2003).

In base alla nuova disciplina l'interessato ha il diritto di ottenere in tempi rapidi una risposta direttamente dall'autorità che ha la competenza centrale per la sezione nazionale del SIS, ai sensi dell'art. 108 della Convenzione, che in Italia è il Dipartimento della pubblica sicurezza, anziché per il tramite del Garante. Se necessario, all'esito di un intempestivo, mancato o inidoneo riscontro alla richiesta formulata al Dipartimento, l'interessato può proporre una segnalazione o un reclamo al Garante.

La scelta operata dal Codice è in linea con quella effettuata da gran parte dei Paesi dell'area Schengen ed introduce una procedura analoga a quella prevista per l'accesso diretto ai dati inseriti nel Centro elaborazione dati del Dipartimento della pubblica sicurezza.

L'Autorità ha richiamato l'attenzione del Ministero dell'interno sulla necessità di assumere ogni iniziativa utile ad assicurare a quanti richiedono l'accesso un riscontro idoneo e tempestivo, anche in relazione alla possibilità per l'interessato, confermata dal Codice, di richiedere, sulla base dei dati conosciuti, un'ulteriore tutela dei propri diritti rispetto all'aggiornamento, rettifica, o cancellazione dei dati, anche in sede giudiziaria (art. 11, comma 2, legge n. 388/1993 e art. 10, comma 5, legge n. 121/1981).

A tal riguardo il Garante ha pure indicato l'opportunità di alcuni accorgimenti per l'inoltro delle richieste e il loro riscontro, che possono risultare vantaggiosi per le stesse persone interessate.

Il Garante ha infine richiamato l'attenzione dell'Ufficio visti del Ministero degli affari esteri sulla necessità di sensibilizzare efficacemente in materia le ambasciate e le cancellerie consolari nei Paesi interessati, anche attraverso il ricorso a moduli prestampati o ad apposite diciture che orientino quanti richiedono il visto sulle modalità di esercizio del diritto di verifica delle segnalazioni esistenti nel Sis.

50 La trattazione dei ricorsi

50.1. Il ricorso come strumento diffuso di tutela

La crescita progressiva del numero dei formali ricorsi pervenuti al Garante, che già era stata registrata nelle relazioni degli ultimi anni, ha trovato conferma nel 2003, anno nel quale si può parlare addirittura di una vera e propria esplosione dell'utilizzo di questo strumento di tutela, come dimostrato dalle statistiche.

Mentre nel 2001 le decisioni sui ricorsi sono state 169, nel 2002 sono stati esaminati 390 ricorsi, per arrivare ai 608 ricorsi decisi nell'anno solare 2003 (per il periodo di riferimento 1° gennaio 2003-31marzo 2004 il numero totale dei ricorsi decisi è 775). Un esame più approfondito del contenuto dei ricorsi dimostra che ormai, grazie anche all'attenzione che molte decisioni hanno ottenuto sulla stampa, così come nella letteratura specializzata, questo strumento di tutela è entrato nella coscienza sociale e costituisce parte del bagaglio professionale degli operatori forensi.

Varie sono le ragioni di questo incremento: la celerità della procedura, i costi contenuti, la possibilità per gli interessati di tutelare i propri diritti senza obbligo di assistenza da parte di un legale, ma soprattutto l'estrema duttilità dello strumento del ricorso che ha dimostrato di poter essere applicato ai campi più diversi. Ciò vale in particolare per il diritto di accesso ai dati personali, che trova ormai larga e comune applicazione ai settori più disparati (pubblica amministrazione, ambito sanitario, settori assicurativo, finanziario e creditizio, trattamenti connessi alla gestione del rapporto di lavoro, ecc.).

Le opposizioni ai provvedimenti del Garante

Per quanto concerne, invece, le opposizioni proposte contro le decisioni assunte dall'Autorità nell'anno trascorso, ne sono state proposte in numero estremamente contenuto, e comunque, sono state in larghissima parte rigettate dai tribunali o contraddette da una successiva giurisprudenza.

La competenza territoriale

Sul piano della corretta instaurazione del contraddittorio, merita di essere segnalata la decisione del Tribunale di Firenze (depositata in cancelleria il 15 aprile 2003), con la quale è stata accolta l'eccezione di incompetenza territoriale sollevata dall'Autorità, confermandosi il principio secondo cui, avverso i provvedimenti espressi del Garante sui ricorsi, nonché nelle ipotesi di rigetto tacito, il titolare o l'interessato possono proporre opposizione al tribunale del luogo ove risiede il titolare del trattamento (art. 29, comma 6, legge n. 675/1996; ora, artt. 151 e 152, d.lg. n. 196/2003).

Analoga eccezione, sollevata sotto altro profilo dall'Autorità in un giudizio instaurato dinanzi al Giudice di pace di Amantea con opposizione ad ordinanza di applicazione di sanzione amministrativa, è stata accolta dall'adito giudice che si è pertanto dichiarato incompetente.

Dati contenuti nelle perizie medico-legali

Altra significativa questione definita in sede di impugnativa davanti al giudice ordinario di una decisione del Garante su un ricorso (al termine, peraltro, di un complesso *iter* processuale), è stata quella della riconducibilità delle valutazioni espresse nelle perizie medico-legali alla nozione di dato personale (Tribunale di Roma, sentenza 17 luglio 2003). Allineandosi agli orientamenti espressi in alcune altre sedi giudiziarie e conformi a quelli enunciati dal Garante in più occasioni

(cfr. *supra,* parag. 7.9.), l'adito giudice si è discostato da alcuni circoscritti precedenti ed ha affermato che anche i giudizi valutativi devono considerarsi dati personali, in quanto, riferendosi ad un persona determinata, sono dotati di un'efficacia informativa tale da fornire un elemento aggiuntivo di conoscenza rispetto all'interessato. Una questione di legittimità costituzionale delle disposizioni relative alla nozione di dato personale e al diritto di accesso, sollevata con riferimento agli artt. 2 e 21 della Costituzione, è stata dichiarata quindi manifestamente infondata.

Si è pertanto riconosciuto che anche rispetto ai "dati valutativi" l'interessato può esercitare il diritto di accesso e alcuni altri diritti previsti dalla normativa in materia di protezione dei dati personali, ad esclusione dei diritti di rettificazione o integrazione (in tal senso dispone ora, come già detto, l'art. 8, comma 4, del Codice).

Gradi del giudizio di opposizione

Con la medesima pronuncia il tribunale ha inoltre ritenuto manifestamente infondata l'eccezione di costituzionalità delle disposizioni che disciplinano l'opposizione ai provvedimenti dell'Autorità, sollevata in relazione alla riconosciuta natura di rimedio non giurisdizionale (Cass. civ. 20 maggio 2002, n. 7341) del ricorso al Garante ai sensi dell'art. 29 della legge n. 675/1996 (ora, art. 145 del Codice). Da tale natura la giurisprudenza ha fatto derivare, infatti, la legittimazione di questa Autorità ad essere parte nei giudizi instaurati a seguito di opposizione ad un suo provvedimento. Di qui la proposizione, nella vicenda in esame, della questione di costituzionalità, per asserita violazione della regola del giusto processo, in quanto 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.

Nel respingere tale questione, il tribunale 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.

Va infine ricordata, sebbene non sia stata proposta avverso una decisione su ricorso, l'impugnazione del provvedimento del Garante del 19 marzo 2003 concernente la pubblicazione di foto segnaletiche. Di tale impugnazione, accolta dal Tribunale di Milano, si è già parlato in altra parte di questa *Relazione* (cfr. *supra*, parag. 15.2.). Qui occorre sottolineare che, nel relativo decreto, l'adito tribunale ha invece rigettato l'eccezione dei ricorrenti nella parte in cui lamentavano di non esser stati sentiti da questa Autorità prima dell'emissione del provvedimento, ritenendo infondata al riguardo ogni doglianza di costituzionalità. Secondo il tribunale, infatti, in certe situazioni possono essere necessari interventi immediati del Garante, salva la possibilità di contestarli e di ottenerne se del caso la sospensione degli effetti. Inoltre, sono state ritenute inapplicabili in via analogica all'intervento d'ufficio dell'Autorità le regole procedurali da osservare in sede di ricorso al Garante di cui all'art. 29 della legge n. 675/1996 (ora, art. 149 del Codice).

50.2. Le novità introdotte dal Codice in materia di protezione dei dati personali

Il d.lg. n. 196/2003 è intervenuto anche sulle disposizioni relative ai ricorsi, che sono ora contenute negli artt. 145 e s. del Codice.

50

Alla luce dell'esperienza maturata nei primi quattro anni di vigenza delle disposizioni attuative in materia di ricorsi, sono state apportate alcune importanti modifiche riguardanti, essenzialmente, l'ampliamento dei termini di durata del relativo procedimento, in funzione di prevenzione del contenzioso.

Anzitutto, l'art. 146 ha portato a quindici giorni (aumentabili fino a trenta in caso di riscontro di particolare complessità) il termine a disposizione del titolare o del responsabile per rispondere all'interpello preventivo che l'interessato deve necessariamente formulare prima di poter presentare il ricorso.

La modifica mira a consentire al titolare e al responsabile del trattamento di poter riscontrare adeguatamente le richieste di accesso ai dati personali presentate dall'interessato; ciò anche tenuto conto che le richieste riguardano a volte una complessa serie di dati, non sempre riportati, come pure sarebbe dovuto, su documenti o supporti prontamente reperibili per l'estrazione di tutte le informazioni rilevanti.

Il termine in precedenza fissato indirettamente in cinque giorni non agevolava in questi casi un riscontro tempestivo o adeguato e favoriva talora la presentazione del ricorso.

L'art. 150, comma 2, ha anche fissato in sessanta giorni il termine per la decisione sul ricorso: tale ampio spazio temporale a disposizione delle parti e dell'Autorità permette di articolare meglio, quando è necessario, gli accertamenti istruttori e consente di dare quindi maggiore effettività al principio del contraddittorio.

In questo quadro si colloca pure la nuova possibilità per l'Autorità di disporre una proroga fino a quaranta giorni dei termini per la decisione sul ricorso, non subordinata, come la più breve proroga prevista in precedenza, all'assenso di entrambe le parti.

Il Codice è poi intervenuto su due profili procedurali che avevano dato luogo ad alcuni problemi interpretativi.

È stata in questo quadro confermata la necessità dell'autenticazione della sottoscrizione apposta dal ricorrente in calce al ricorso, superando, con l'esplicita indicazione contenuta nell'art. 147, comma 4, le perplessità insorte in alcuni circa la compatibilità di tale obbligo con la disciplina in tema di autocertificazione.

Un'altra precisazione utile è venuta infine dal comma 6 dell'art. 150 del Codice il quale, in riferimento all'eventuale pronuncia sulle spese del procedimento, ha stabilito che la decisione del Garante costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 c.p.c.; resta invece ferma l'inammissibilità della proposizione innanzi a questa Autorità delle richieste di risarcimento dei danni.

50.3. Brevi cenni sulla casistica

Per sottolineare l'ampio spettro di questioni affrontate dal Garante in sede di decisione sul ricorso, è utile un cenno sommario ai settori in cui si è avuta la proposizione del maggior numero di ricorsi, rinviando comunque, per una trattazione più analitica delle relative problematiche, alle specifiche sezioni di questa Relazione.

Trattamenti svolti in ambito bancario e finanziario. A partire dalla seconda metà del 2003 in questo settore si è indirizzato il maggior numero di ricorsi, che si sono incentrati soprattutto sull'accesso degli interessati ai dati personali detenuti dagli istituti di credito o dalle società finanziarie. È importante notare come delicate vicende che hanno interessato il mondo finanziario nell'ultimo anno (i casi Cirio e Parmalat e la vicenda dei *bond* argentini) abbiano trovato immediata eco dinanzi all'Autorità, in conseguenza della presentazione di numerose richieste di accesso, mirate a conoscere l'insieme dei dati personali trattati nelle operazioni finanziarie in questione (profili di rischio, logica e modalità del trattamento, ecc.).

Settore bancario e finanziario

Trattamenti svolti dalle cd. centrali rischi private. È, questo, uno dei settori dove si riscontra una maggiore attenzione da parte dell'opinione pubblica, anche in conseguenza del forte impatto che ha avuto il provvedimento generale del Garante intervenuto in materia (*Provv.* 31 luglio 2002). Sono stati infatti proposti molti nuovi ricorsi in cui se ne lamentava l'inosservanza, chiedendo l'applicazione dei principi in esso affermati, con particolare riguardo ai tempi di conservazione dei dati.

"Centrali rischi"

Sono emersi peraltro, anche profili ulteriori, quali il problema della conservazione nelle banche dati delle "centrali rischi" private di dati concernenti le cd. segnalazioni positive o gli effetti della revoca del consenso al trattamento dei dati espressa dall'interessato nell'interpello o direttamente nell'ambito del ricorso (v., tra i tanti, *Provv.* 22 dicembre 2003).

Trattamenti di dati da parte di operatori di telecomunicazioni e problematiche relative ai trattamenti in rete. Il settore ha visto pervenire un numero elevato di ricorsi, anche in conseguenza di importanti decisioni dell'Autorità che hanno richiamato l'attenzione sulle garanzie in materia. Ciò con particolare riguardo all'invio di messaggi promozionali indesiderati e non sollecitati ad indirizzi di posta elettronica (cd. *spamming*), tenuto oltretutto conto che gli indirizzi di posta elettronica sono spesso acquisiti tramite rastrellamento in rete a mezzo di appositi *software*.

Comunicazioni elettroniche e telefonia

Peraltro, l'Autorità ha talora dichiarato inammissibili alcuni ricorsi in quanto formulati da soggetti non legittimati a proporli, trattandosi di persone diverse da quelle cui si riferivano i dati concernenti gli indirizzi di posta elettronica dei quali era lamentato l'illecito trattamento.

In materia di telefonia fissa e mobile, i casi più frequenti di ricorso hanno riguardato le richieste di accesso ai dati relativi al traffico in entrata e in uscita e le opposizioni al trattamento consistente nell'invio di comunicazioni promozionali e pubblicitarie (anche a mezzo di *sms*) in assenza di consenso dell'interessato. Con riferimento alla telefonia fissa, alcuni casi hanno riguardato anche l'opposizione alla divulgazione, da parte del gestore, di numeri telefonici per i quali era stato richiesto il carattere di numero riservato.

Dati conservati nelle perizie medico legali in ambito assicurativo. L'argomento, esaminato dal Garante fin dal 1999 ed oggetto anche di significative pronunce giurisprudenziali, si è riproposto in misura più contenuta rispetto agli anni precedenti. Nei casi esaminati l'Autorità è stata chiamata più volte a decidere sull'applicabilità della disposizione che, a certe condizioni, consente di differire l'esercizio del diritto di accesso in caso di pregiudizio all'esercizio del diritto di difesa del titolare del trattamento. Una riduzione del contenzioso al riguardo è probabilmente derivata pure dalla più moti-

Ambito assicurativo

vata e condivisibile giurisprudenza alla quale si è fatto riferimento poc'anzi (cfr. *supra*, parag. 50.1.), e dalle precise scelte operate dal Codice, cui ha fatto rinvio il d.m. 20 febbraio 2004, n. 74 sull'accesso agli atti delle imprese assicurative.

Trattamenti effettuati dalle pubbliche amministrazioni. I ricorsi proposti nei confronti delle pubbliche amministrazioni coprono una serie molto vasta e differenziata di ipotesi di trattamento dei dati, che sono già state ampiamente analizzate nei capitoli II e IV. In questa sede merita comunque di essere ricordato che in tale settore hanno assunto specifico rilievo alcune opposizioni formulate dagli interessati.

51 Attività ispettive e applicazione di sanzioni amministrative

51.1. Profili generali – Tipologia degli accertamenti ispettivi e criteri adottati

L'art. 154 del Codice consolida, in capo al Garante, il compito di controllare se i trattamenti siano effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione. A tal fine, l'Autorità continua ad esercitare anche una funzione ispettiva per mezzo del Dipartimento vigilanza e controllo, il cui personale riveste, nell'esercizio dei poteri attribuiti dalla legge, la qualifica di ufficiale/agente di polizia giudiziaria.

Le attività ispettive sono costituite anzitutto da accertamenti effettuati nei luoghi dove si svolgono i trattamenti, utilizzando i poteri previsti dal Codice (artt. 157–160).

In generale, le ispezioni possono essere originate da segnalazioni o reclami ricevuti dall'Autorità, da esigenze di approfondimento emerse nell'ambito dell'esame di ricorsi, d'iniziativa dell'Autorità in relazione, ad esempio, alle verifiche degli adempimenti da parte di determinate categorie di titolari o, ancora, sulla base di notizie comunque acquisite direttamente dal Garante.

Anche nella vigenza del Codice, l'esercizio dell'attività di controllo resta informato ai principi di proporzionalità, adeguatezza e gradualità, tenendo presente, di volta in volta, il contesto operativo di riferimento (rischio di dispersione o di alterazione degli elementi di prova) e la disponibilità o meno del soggetto controllato ad una collaborazione per lo svolgimento delle verifiche.

I controlli possono essere effettuati pure mediante richieste, sul posto o meno, di informazioni o di esibizione di documenti; possono inoltre svolgersi anche mediante accessi a banche di dati o altre ispezioni e verifiche nei luoghi dove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo stesso.

Ispezioni

Le ispezioni previste dall'art. 158 del Codice sono disposte quando, per acquisire gli elementi necessari alla definizione della vicenda, non sia idonea una mera richiesta di informazioni o di esibizione di documenti, nonché nei casi in cui non siano state fornite tempestivamente le informazioni o i documenti richiesti (o, se pervenuti, siano incompleti o non veritieri).

Si tratta di una potestà con caratteri inquisitori e i soggetti interessati agli accertamenti sono quindi tenuti a farli eseguire: l'accertamento è infatti eseguito anche in caso di rifiuto e in tale ultima ipotesi le eventuali spese sono poste a carico del titolare. Durante l'accertamento il titolare o il responsabile possono farsi assistere da persone di loro fiducia.

Autorizzazione dell'a.g.

L'autorizzazione da parte dell'autorità giudiziaria, diversamente da quanto stabilito dalla previgente disciplina, che contemplava in ogni caso tale autorizzazione, è oggi opportunamente richiesta dal Codice solo nel caso di accessi "svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze" (art. 158 cit.).

All'autorizzazione è equiparato l'assenso informato, che viene anche documentato per iscritto (cfr. *Provv.* n. 2 del 30 gennaio 2001).

Le attività effettuate durante l'ispezione sono riportate in un sommario verbale, nel quale sono registrati tutti gli elementi rilevanti occorsi durante le operazioni e menzionate le informazioni e la documentazione eventualmente acquisita.

Esiti del procedimento ispettivo

Nel corso o al termine del procedimento nel cui ambito vengono svolte le ispezioni, l'Autorità:

- prescrive ai titolari o responsabili del trattamento dei dati le modificazioni necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti (la disciplina previgente contemplava un potere analogo in forma di segnalazione);

- adotta ove necessario uno dei provvedimenti di divieto o blocco del trattamento (v. artt. 143, 144 e 154 del Codice);

- contesta le violazioni amministrative eventualmente constatate;

- nei casi più gravi previsti dalla legge, procede alla comunicazione di notizia di reato all'autorità giudiziaria per l'accertamento delle violazioni costituenti reato.

51.2. La collaborazione con gli organi dello Stato

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 di quest'ultima nel campo delle attività di controllo in ambito amministrativo.

Collaborazione con la Guardia di finanza

Nell'ottica del potenziamento dell'attività di vigilanza e controllo, pertanto, nel mese di ottobre 2002 il Garante e la Guardia di finanza hanno siglato un protocollo d'intesa in base al quale è stata potenziata l'attività di collaborazione tra le due istituzioni (cfr. *Relazione 2002*, p. 145).

Successivamente al perfezionamento del protocollo di intesa, nel mese di gennaio del 2003 è stata effettuata un'intensa attività di formazione del personale del Corpo destinato a svolgere in via continuativa l'attività di collaborazione (venti unità circa

tra ufficiali, ispettori e sovrintendenti). Ciò ha consentito di avviare più rapidamente la collaborazione con la Guardia di finanza, che si è dimostrata estremamente proficua sia nella fase preparatoria degli interventi più delicati, grazie alle capacità investigative proprie del Corpo, sia nella fase realizzativa. Sono stati eseguiti, in particolare, 33 interventi, di cui 7 congiuntamente a personale dell'Autorità.

La collaborazione ha investito anche gli sviluppi investigativi dei casi oggetto di segnalazione all'autorità giudiziaria, i quali hanno comportato, nel 2003, l'esecuzione di 177 sommarie informazioni testimoniali, la ricezione di 12 querele e la segnalazione di 5 persone all'autorità giudiziaria.

I risultati raggiunti e l'esigenza di rispondere in maniera sempre più adeguata alle istanze di tutela provenienti da cittadini hanno indotto l'Autorità a chiedere per il 2004 un ulteriore rafforzamento del rapporto di collaborazione con la Guardia di finanza, allo scopo di potersi avvalere anche di personale, adeguatamente formato, in ogni regione.

Assai significative sono risultate pure le collaborazioni con la Polizia di Stato (specie per accertamenti nelle reti telematiche) e l'Arma dei carabinieri.

La collaborazione con le forze di polizia si è quindi confermata come un elemento essenziale di incremento dell'efficacia dell'azione di tutela dei diritti dei cittadini, che passa anche attraverso una più intensa attività di vigilanza e controllo.

51.3. I casi più significativi

Attivazione di schede telefoniche

Un caso rilevante tra quelli emersi ha portato alla segnalazione all'autorità giudiziaria dell'illecito trattamento di dati personali connesso all'attivazione di carte telefoniche effettuato da una società che gestisce numerosi punti vendita, situati nell'Italia centrale.

L'attività di accertamento dell'Autorità è partita dalla segnalazione di una persona che, dopo aver acquistato una scheda telefonica ricaricabile, era venuta casualmente a conoscenza di essere intestataria di altre sei utenze attivate a suo nome presso il medesimo esercizio commerciale.

L'attenzione del Garante si è concentrata quindi sulle attivazioni di schede telefoniche da parte di tali punti vendita, e in particolare sulle modalità e sulle finalità del trattamento dei dati personali forniti dai clienti.

Dalle ispezioni presso la sede della società, nonché da riscontri incrociati con i dati in possesso della società telefonica, è emerso che, nel solo breve periodo esaminato, presso i punti vendita erano state attivate quasi 800 schede telefoniche ricaricabili nei confronti di circa 200 persone, a loro insaputa. Tale prassi illecita è stata seguita nel quadro dei "piani di incentivazione per i rivenditori" che prevedevano, al superamento di determinate soglie di attivazioni prestabilite, il riconoscimento ai rivenditori stessi di un ulteriore compenso per ogni attivazione effettuata in più rispetto a quanto programmato. La società sarebbe pertanto riuscita a lucrare, pur nel solo breve periodo preso in esame, premi per oltre quarantamila euro.

Gli interessati avevano spesso acquistato una prima scheda telefonica presso uno degli esercizi della società ed erano ignari di essere intestatari di altre schede, utilizzabili in vari modi, anche illeciti. I dati personali erano stati ovviamente trattati senza il loro consenso espresso.

La vicenda, sulla quale l'autorità giudiziaria competente ha effettuato poi ulteriori accertamenti, si lega ad un'analoga indagine svolta dalla Guardia di finanza di Rovigo sotto la direzione della locale procura della Repubblica, i cui esiti sono stati comunicati al Garante. Dalla stessa emerge che, almeno in un certo periodo di tempo, rivenditori poco scrupolosi hanno adottato comportamenti lesivi dei diritti di molte persone, a nome delle quali sono state attivate migliaia di carte telefoniche.

Spamming

Un altro dei settori rilevanti dell'attività ispettiva del Garante è quello relativo al cd. *spamming*.

In uno degli accertamenti effettuati in tale settore è stato denunciato alla magistratura il titolare di un'impresa operante nel campo delle arti grafiche.

Alcuni cittadini avevano presentato ricorso al Garante lamentando di essere stati raggiunti da *e-mail* commerciali inviate dal titolare della tipografia senza il previo consenso informato dei destinatari. Nell'accogliere tutti i ricorsi pervenuti, il Garante ha ordinato al titolare dell'impresa di cancellare i nominativi dei ricorrenti e ha disposto il blocco dei dati personali trattati illecitamente, per prevenire ulteriori possibili violazioni della legge. L'Autorità ha poi disposto che l'impresa fornisse informazioni sull'origine dei dati, sull'avvenuta cessazione degli illeciti e sui nominativi dei responsabili del trattamento eventualmente designati.

Acquisiti elementi che dimostravano la continuazione dei comportamenti illeciti da parte del titolare del trattamento successivamente alla notifica del blocco, l'Autorità ha comunicato alla competente procura della Repubblica la notizia di reato in relazione all'inosservanza alle prescrizioni del Garante e all'illecito trattamento dei dati personali.

Servizi di *e-banking*

Un ulteriore settore di intervento ha riguardato le misure di sicurezza delle banche dati, con particolare riguardo ai servizi di *e-banking*. Tali servizi consentono a ogni cliente abilitato, previo inserimento di codici di autenticazione, di consultare via Internet i movimenti del proprio conto corrente e di visualizzare i dati che lo riguardano e gli estratti conto, creando un prospetto delle ultime operazioni effettuate da memorizzare o stampare.

Il Garante si è attivato a seguito del ricorso di un cliente di una banca *on line* che, nel consultare via Internet la propria posizione contabile, aveva avuto accidentalmente accesso ad informazioni riservate di altri correntisti ignari. Il caso, che ha assunto un notevole interesse per i suoi riflessi sul rapporto dei clienti con la banca, è stato già analizzato in altra parte di questa Relazione (cfr. *supra*, parag. 11.). Qui occorre solo puntualizzare che il Garante ha inoltrato denuncia alla magistratura ordinando contestualmente, con apposito provvedimento, di adottare adeguate misure di sicurezza per prevenire il ripetersi di tali illeciti. L'adempimento di tale prescrizione ha consentito alla banca di beneficiare dell'ammissione al pagamento di una ammenda con conseguente possibilità di beneficiare dell'estinzione del reato, così come previsto dal Codice (art. 169).

51

51.4. Riferimenti statistici

Grazie all'apporto fornito anche dalla collaborazione con la Guardia di finanza, l'attività ispettiva effettuata nel periodo fino al 31 marzo 2004 ha avuto un incremento significativo rispetto a quella svolta nel precedente periodo di riferimento.

Nell'ambito delle centinaia di procedimenti di controllo avviati dall'Autorità, 69 sono stati svolti anche mediante necessari accertamenti ispettivi *in loco*.

Le attività ispettive sono state avviate sulla base di:
- segnalazioni pervenute all'Ufficio (45%);
- autonomi accertamenti a seguito di ricorsi presentati al Garante (36%);
- accertamenti avviati di iniziativa (19%).

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;
- le misure di sicurezza.

Le ispezioni sono state effettuate:
- in 61 casi mediante richieste di informazioni ed esibizione di documenti, formulate sul posto;
- in 8 casi mediante accessi a banche dati.

Con riferimento all'ambito territoriale la ripartizione è stata:
- nord (41%);
- centro (43%);
- sud (16%).

L'incidenza delle violazioni penali sui procedimenti amministrativi di controllo avviati è pari circa al 16%. 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.

In generale le ispezioni hanno consentito di rilevare che nel settore privato le aziende più grandi stanno assumendo specifiche iniziative per adeguarsi alla normativa e agli indirizzi dell'Autorità, anche attraverso la costituzione di unità organizzative con deleghe specifiche e veri e propri "uffici *privacy*", mentre le aziende medio-piccole dimostrano un livello inferiore di adeguamento.

Nella pubblica amministrazione stenta di più ad affermarsi una vera e propria cultura della *privacy* applicata ai processi di lavoro e alla gestione delle pratiche di ufficio. Talvolta, ad un assetto formalmente corretto non corrisponde una piena consapevolezza dei doveri e delle responsabilità connesse al trattamento dei dati personali. Alcune delle attività ispettive hanno rivelato ancora preoccupanti fenomeni di superficialità nel trattamento dei dati, soprattutto per quanto riguarda la gestione degli archivi e le connesse misure di sicurezza.

Si è pure rilevata, nelle amministrazioni pubbliche, la frequente mancanza di articolazioni dedicate all'attuazione della normativa, dotate di autonomie decisionali e gestionali indispensabili per tradurre in pratica i programmi formalmente delineati.

51.5. L'attività sanzionatoria del Garante

Anche nel settore delle sanzioni amministrative il Codice in materia di protezione di dati personali ha introdotto novità di assoluto rilievo.

Le novità introdotte dal Codice

In modo significativo, il d.lg. n. 196/2003 inserisce nella Parte III, "Tutela dell'interessato e sanzioni" un apposito titolo dedicato alle "Sanzioni", a sua volta suddiviso nel Capo I ("Violazioni amministrative") e nel Capo II ("Illeciti penali", distinguibili in delitti e contravvenzioni).

Le violazioni amministrative previste dal Codice sono: 1) omessa o inidonea informativa all'interessato (art. 161); 2) cessione dei dati in violazione dell'art. 16, comma 2, o di altre disposizioni in materia di disciplina dei dati personali (art. 162, comma 1); 3) violazioni delle disposizioni in tema di comunicazione dei dati personali idonei a rivelare lo stato di salute, di cui all'art. 84, comma 1 (art. 162, comma 2); 4) omessa o incompleta notificazione del trattamento (art. 163); 5) omessa informazione ed esibizione di documenti al Garante (art. 164).

La nuova normativa mostra così di voler rafforzare ulteriormente, in termini di effettività della tutela degli interessati, gli strumenti idonei a sanzionare una serie di comportamenti illeciti sul piano amministrativo, che possono essere commessi sia nei confronti degli interessati, sia nei confronti del Garante.

Si è scelto quindi, da un lato, di dare maggior risalto (anche visivo) rispetto al passato ai comportamenti, omissivi e non, da cui può conseguire la contestazione solo di una violazione amministrativa, concentrandoli in un apposito capo, distinti da altri tipi di illeciti; dall'altro, di aggiornare gli importi delle relative sanzioni nei limiti consentiti dalla delega legislativa conferita al Governo.

Nel caso di omessa o incompleta notificazione, oltre alla sanzione pecuniaria amministrativa, è stata prevista specificamente la pena accessoria della pubblicazione dell'ordinanza-ingiunzione. Per le altre violazioni, l'applicazione della pena accessoria della pubblicazione è invece in facoltà dell'Autorità che può disporla quando il suo utilizzo risulti opportuno per le modalità e le finalità del trattamento, oltre che per la natura dei dati, ai fini della tutela dei diritti degli interessati.

Per quanto attiene al procedimento di applicazione, il Codice non ha invece apportato nessuna modifica rispetto a quanto già stabilito dalla disciplina previgente, fatto salvo il conferimento *ex novo* all'Autorità della competenza a contestare e applicare la sanzione amministrativa già prevista in materia di vendite a distanza (art. 179, comma 3, in riferimento al d.lg. n. 185/1999).

L'attività operativa svolta nel corso del 2003 relativamente alle contestazioni di violazioni amministrative è stata caratterizzata da un intenso ricorso allo strumento sanzionatorio. Ciò anche a seguito di indagini effettuate dall'Autorità in specifici settori e che hanno coinvolto, in qualità di titolari, soggetti pubblici e privati. Di

51

Tipologia delle violazioni amministrative contestate

rilievo sono stati anche gli autonomi procedimenti di verifica del rispetto della normativa sui dati personali avviati a seguito di decisione sui ricorsi proposti innanzi all'Autorità, all'esito dei quali è stata spesso prevista la preliminare contestazione di violazione amministrativa.

L'analisi in dettaglio delle violazioni contestate permette di individuare le operazioni di trattamento e le modalità che sono state oggetto di constatazione di infrazioni.

L'informativa all'interessato, in particolare, 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 modalità e finalità del trattamento perseguite di fatto in concreto dal titolare. Significativo, in proposito, è ad esempio il caso nel quale, a seguito della segnalazione di un interessato, si è accertato che i dati raccolti per mezzo della prenotazione ed acquisto di biglietteria marittima (per le operazioni effettuabili sul sito della compagnia di navigazione) venivano utilizzati anche per attività ulteriori rispetto a quelle per le quali era stata fornita l'informativa presente sul sito stesso. Altre violazioni in tema di informativa sono poi state accertate nell'ambito delle attività di promozione commerciale per mezzo di strumenti di comunicazione elettronica, a causa di trattamenti effettuati in modo difforme dalla previsione normativa, che prevede in argomento il rispetto del principio di *opt-in* (cfr. ora, art. 130, comma 4).

Per quanto riguarda invece i trattamenti di dati personali effettuati per mezzo di sistemi di videosorveglianza, si continuano ad accertare e sanzionare violazioni connesse ad informative assenti o carenti di qualsiasi riferimento alle modalità e finalità del trattamento in tal maniera effettuato.

A seguito di un ricorso proposto dall'interessato, è stata anche accertata e contestata la violazione, da parte di imprese assicuratrici, del principio più volte affermato dal Garante (ora disciplinato in modo parzialmente diverso dal Codice), in base al quale i dati personali in possesso delle imprese stesse e contenuti nelle perizie medico-legali dovevano essere comunicati all'interessato esclusivamente tramite un medico, designato dall'interessato stesso o dall'impresa che detiene i dati (art. 23, comma 2, legge n. 675/1996).

In tema di mancato riscontro alle richieste di informazioni ed esibizione di documenti, rivolte dall'Autorità (ora, ai sensi dell'articolo 157 del Codice), i soggetti pubblici –quali titolari del trattamento– sono risultati purtroppo spesso inadempienti e sono stati pertanto oggetto di varie contestazioni di violazione amministrativa ora prevista dall'articolo 164 (omessa informazione o esibizione al Garante). Merita di essere quindi ribadito in questa sede che la richiesta di informazioni o documenti in tali casi va inquadrata, nell'ambito dei rapporti tra istituzioni pubbliche, come attività strumentale all'imparzialità dell'azione amministrativa: per ben operare l'Autorità ha infatti necessità, nel valutare la fondatezza delle segnalazioni che ad essa pervengono ed al fine di accertare l'eventuale violazione degli obblighi di legge, di assumere una serie completa di elementi, tali da consentire una corretta decisione.

Sempre con riferimento ai trattamenti effettuati da soggetti pubblici, sono state pure accertate, all'esito della verifica presso il registro dei trattamenti sulla notificazione inviata all'Ufficio, violazioni concernenti l'omessa od incompleta notifica-

zione; di conseguenza, sono state predisposte anche in questo caso alcune contestazioni di violazioni amministrative.

Per quanto attiene poi ai provvedimenti di ordinanza-ingiunzione al pagamento di somme, nell'anno 2003 si sono predisposte, ai sensi dell'articolo 17 della legge n. 689/1981, alcune decine di rapporti necessari all'eventuale e successiva adozione del provvedimento medesimo.

Tale dato lascia prevedere che per il futuro, così come si è già verificato per il periodo preso in considerazione, sia ipotizzabile un ulteriore aumento delle attività relative al contenzioso amministrativo dell'Autorità, tra le quali anche quella di obbligatoria audizione delle parti (art. 18 l. n. 689 cit.).

52 L'attività di informazione e comunicazione

52.1. Profili generali

Il rischio di muoversi rapidamente verso una società della classificazione e della sorveglianza, la permanente attenzione ai problemi della sicurezza collettiva, nazionale ed internazionale, il ricorso sempre più massiccio a tecnologie di raccolta e conservazione di dati, il potenziale uso indiscriminato delle informazioni più delicate relative alle persone, hanno indotto il Garante, nel corso del 2003, ad intensificare la sua azione di informazione e comunicazione specie su queste tematiche. Un compito non facile, ma necessario in considerazione dell'obiettivo istituzionale di promuovere un diritto, quello alla protezione dei dati personali, che si è andato affermando come uno dei cardini della nuova cittadinanza elettronica fino ad essere riconosciuto nella sua piena autonomia dalla Carta dei diritti fondamentali dell'Unione europea e, in due disposizioni (artt. I-50 e II-8), dal progetto di Costituzione europea.

L'Autorità ha cercato di raggiungere un livello sempre più alto di produzione informativa riguardo all'intero spettro delle tematiche sulle quali si incentra la sua azione: la tutela della libertà e della dignità della persona, la gestione trasparente delle banche dati, l'uso non discriminatorio delle informazioni personali, specie di quelle sanitarie, fornendo al contempo a cittadini, imprese e istituzioni contributi esplicativi ed indicazioni operative per l'attuazione delle norme, specialmente in presenza del Codice entrato in vigore il 1° gennaio 2004.

Particolare significato ha assunto l'impegno costante rivolto dall'Autorità alla definizione di regole per il corretto utilizzo dei nuovi sistemi di comunicazione, così come l'attenzione posta ai rischi che possono derivare per la libertà delle persone dalle indagini genetiche, dall'uso sproporzionato delle tecniche biometriche, dalla raccolta dei dati *on line*, dalla localizzazione, dall'elaborazione dei profili dei consumatori.

Non è mancata l'attenzione alla promozione della *privacy* come "valore aggiunto" per imprese e pubbliche amministrazioni, al fine di instaurare un rapporto nuovo con cittadini, clienti, utenti e consumatori.

52

La ricerca di un corretto equilibrio tra diverse esigenze e tra diritti equivalenti ha caratterizzato, anche nel 2003, gli interventi del Garante, con particolare riguardo al diritto di cronaca e alla dignità delle persone.

Trasparenza, correttezza, tempestività, esaustività sono valori ai quali il Garante ha da sempre improntato la sua azione di informazione.

In linea con questi obiettivi, l'Autorità ha confermato la scelta di affidare la sua informazione ad un linguaggio rigoroso, ma attento ad una funzione divulgativa. Nel dar conto della propria attività e delle tematiche all'ordine del giorno, l'Autorità ha richiamato l'attenzione di quanti trattano dati personali sugli obblighi da attuare, sui rischi di violazione e sugli illeciti messi in atto.

52.2. I prodotti informativi ed editoriali del Garante

La tipologia dei prodotti informativi ed editoriali è ampia e differenziata, ma comunque nettamente caratterizzata, alla luce della precisa connotazione istituzionale dell'Autorità, e si fonda su 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*.

Nel periodo dal 1° aprile 2003 al 15 marzo 2004, sulla base della rassegna stampa prodotta dall'Ufficio, le pagine dei maggiori quotidiani e periodici nazionali ed internazionali e dei media *on line* che hanno dato spazio alle tematiche riguardanti generalmente la *privacy* sono risultate circa 7500, delle quali oltre 1700 dedicate specificamente all'attività del Garante. Le prime pagine dedicate ai temi della protezione dei dati personali sono state circa 700 (di cui oltre 300 riguardanti la sola Autorità). Numerose sono state le interviste pubblicate sulla carta stampata (83), su tv e radio nazionali e locali (130 nel complesso), e diverse su pubblicazioni *on line*.

I prodotti informativi

I prodotti informativi hanno offerto un ventaglio ampio di risposte alle esigenze informative dei cittadini.

La *Newsletter*

La *Newsletter* settimanale, al suo quinto anno di pubblicazione (per un totale complessivo di 205 numeri), è diventata ormai lo strumento di riferimento dell'attività di comunicazione del Garante. In particolare, essa riesce a coniugare un'illustrazione, in chiave giornalistica, dei provvedimenti e dell'attività dell'Autorità con l'esigenza di un'informazione di tipo più ampio ed approfondito. Nel corso degli anni, la *Newsletter* ha infatti dedicato una crescente attenzione a quanto avviene in campo comunitario ed internazionale, riguardo non solo ai temi della protezione dei dati, ma anche al più ampio ambito della tutela dei diritti fondamentali, fornendo un vasto panorama di questioni e problematiche.

La possibilità di consultare la *Newsletter on line* ha facilitato la diffusione delle informazioni.

Le *Newsletter* diffuse tra il 1° gennaio 2003 e il 31 marzo 2004 sono state 54, mentre i comunicati stampa 39.

Il *Cd-Rom*

Nel 2003 è giunto alla sua decima edizione l'archivio digitale ipertestuale "Cittadini e Società dell'informazione", che contiene in forma integrale e nell'originale

veste editoriale i provvedimenti del Garante, il Codice, la documentazione relativa alla normativa nazionale ed internazionale di riferimento e le pubblicazioni realizzate. Il *Cd-Rom*, che consente una consultazione con funzioni di ricerca *full-text*, rappresenta uno strumento ormai conosciuto e costantemente richiesto da parte di amministrazioni pubbliche, imprese, liberi professionisti e cittadini. Le recenti edizioni presentano caratteristiche di multimedialità, con l'inserimento di video divulgativi e dello *spot* televisivo e radiofonico, trasmesso dalle tre reti Rai nel marzo 2003, nonché miglioramenti tecnici e di contenuto che ne rendono ancora più funzionale l'uso.

Il Bollettino

Tra le attività di comunicazione resta il Bollettino che raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa ed altra documentazione significativa, e che dal gennaio 2004 ha aggiornato la propria veste editoriale.

La necessità di sviluppare una sempre maggiore conoscenza delle norme sulla *privacy* e dei diritti 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, *Newsletter*, conferenze stampa, incontri periodici con la stampa) a quelli multimediali ed interattivi– l'Autorità ha realizzato nuovi significativi prodotti.

L'impegno per una comunicazione agile, immediata e diretta in primo luogo al cittadino ha trovato concreta attuazione nella realizzazione di *depliant* divulgativi in grado di illustrare, secondo un percorso ben preciso, i diversi aspetti connessi con la protezione dei dati. I pieghevoli finora pubblicati sono dedicati: il primo all'esercizio dei diritti riconosciuti dalla normativa; il secondo, all'attività e al ruolo del Garante; il terzo a come difendere la *privacy* in Internet.

Il progetto di comunicazione istituzionale proseguirà con la realizzazione di un quarto *depliant* sulla *privacy* nella telefonia.

I prodotti editoriali

Notevole sviluppo hanno avuto poi, nel periodo considerato, i prodotti editoriali dell'Autorità.

Il notiziario bimestrale

Il notiziario bimestrale, *"Garanteprivacy.it"*, che ha preso avvio nel dicembre 2002, è giunto al suo settimo numero. Il bimestrale è una pubblicazione destinata in particolare a personalità del mondo istituzionale ed imprenditoriale, caratterizzata da una comunicazione agile ed essenziale, in grado di sottolineare l'attività dell'Autorità nei diversi settori di intervento.

Allo scopo, inoltre, di contribuire all'approfondimento dei temi legati alla *privacy* e ai principi posti dalla normativa nazionale e comunitaria, il Garante ha deciso di dar vita ad un nuovo prodotto editoriale, la collana "Contributi". Sono attualmente disponibili i primi due volumi, il "Massimario 1997-2001", a cura di Luigi Pecora e Giuseppe Staglianò, relativo ai provvedimenti adottati dal Garante nel primo quadriennio di attività, e "Privacy e giornalismo", a cura di Mauro Paissan.

"Massimario 1997-2001"

Nel primo libro, l'attività di massimazione in chiave tecnico-giuridica dei provvedimenti assunti nel corso degli anni è stata preordinata alla formazione di una rassegna di "giurisprudenza" del Garante che, attraverso un'articolazione in voci e sottovoci, permetta la rapida e corretta individuazione degli argomenti trattati e delle decisioni assunte. L'opera, che arricchisce il panorama delle pubblicazioni curate dal

52

"Privacy e giornalismo"

Garante e la cui edizione è imminente anche su supporto informatico, si indirizza in particolar modo ad una platea di utenti costituita da giuristi, operatori del diritto, ordini professionali, imprese ed istituzioni pubbliche e private.

Il secondo volume raccoglie, invece, un'ampia scelta delle decisioni adottate dall'Autorità in materia di tutela della persona e libertà di manifestazione del pensiero. I provvedimenti sono organizzati per grandi temi e preceduti da un breve sommario che ne riassume i contenuti e mettendo in luce gli aspetti più significativi. 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.

È in preparazione un terzo volume, che affronterà il tema della protezione dei dati nelle attività produttive, a cura di Gaetano Rasi.

52.3. La partecipazione a manifestazioni e conferenze

L'attività dell'Autorità collegata con seminari, convegni ed altre iniziative ha visto, nel corso del 2003 e nei primi mesi del 2004, la conferma di un grande interesse da parte del pubblico. 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.

Forum P.A. 2003

Nell'ambito del *Forum* P.A.-edizione 2003, svoltosi a Roma dal 5 al 9 maggio, il Garante è stato chiamato ad affrontare il tema dei rapporti tra sicurezza 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. Gaetano Rasi, componente dell'Autorità, è intervenuto al convegno dedicato a "La sicurezza dei cittadini nello Stato federale". Affrontando il tema dei rapporti tra sicurezza e *privacy*, Rasi ha sottolineato che la tutela della collettività e le garanzie di libertà del singolo individuo sono certamente conciliabili, come sta a dimostrare, in particolare nel campo della videosorveglianza, la fattiva collaborazione con il Ministero dell'interno.

Il segretario generale dell'Autorità, Giovanni Buttarelli, ha tenuto un corso su "La gestione dei dati sensibili e la tutela della *privacy* nei rapporti tra cittadini e amministrazioni". Il corso al quale hanno partecipato centinaia di persone, si è articolato in una prima parte, a carattere illustrativo, dedicata alla evoluzione normativa e in una seconda parte, a carattere pratico, nella quale si è effettuata una verifica dell'applicazione della normativa sulla *privacy* nei diversi settori della p.a.

Com-p.a. 2003

L'Autorità garante è stata presente anche al Com-p.a. 2003, Salone della comunicazione pubblica di Bologna (dal 17 al 19 settembre). Nell'ambito della manifestazione dedicata al tema "Per il buon Governo. Dieci anni di Comunicazione Pubblica", il vice presidente del Garante, Giuseppe Santaniello, ha partecipato al convegno su "Comunicazione e diritto" con un intervento sul tema della protezione dei dati in quanto elemento costitutivo dell'informazione.

Il Com-p.a. ha offerto l'occasione per affrontare i temi legati alla protezione dei dati come elemento costitutivo dell'informazione resa al cittadino e per approfondire le novità più significative introdotte dal recentissimo Codice in materia di protezione dei dati personali.

Nell'ambito della manifestazione, l'Autorità garante ha ricevuto anche quest'anno, per la seconda volta consecutiva, il "Premio Qualità". Il premio è stato assegnato per "i progetti integrati di comunicazione al cittadino".

Smau 2003

L'Autorità ha partecipato inoltre alla 40ª edizione di Smau 2003, Esposizione internazionale di *ICT & Consumer Electronics*, che si è tenuta alla Fiera di Milano dal 2 al 6 ottobre.

L'Autorità è stata presente in tutte e tre le 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.

La partecipazione alle conferenze internazionali

Per quanto riguarda l'attività internazionale, va ricordata anzitutto la partecipazione del Garante alla Conferenza di primavera delle autorità europee per la *privacy*, svoltasi dal 3 al 4 aprile 2003 a Siviglia. I temi affrontati nella Conferenza hanno riguardato il settore delle telecomunicazioni; il trasferimento internazionale dei dati; il ruolo delle Autorità di garanzia l'attuazione della direttiva "madre" sulla *privacy* del 1995; la situazione dei Paesi che entreranno a breve a far parte del Gruppo dei garanti Ue.

Stefano Rodotà, in qualità di presidente del Gruppo dei garanti europei, ha fatto il punto sull'attuazione della direttiva-madre europea e sul lavoro svolto dalle Autorità in un periodo che ha visto sul tappeto questioni rilevanti, quali la conservazione dei dati di traffico telefonico, i sistemi di autenticazione *on line*, la richiesta di accesso da parte delle autorità statunitensi alle banche dati delle compagnie aeree europee, nonché, ancora, sulle iniziative che il Gruppo intende prendere in futuro.

Giuseppe Santaniello ha tenuto un'articolata relazione sul nuovo Codice e sulla specifica novità, nel quadro delle fonti, dei codici deontologici italiani.

Mauro Paissan ha tenuto una relazione sulle più importanti decisioni adottate dal Garante in materia di telecomunicazioni, in particolare sull'uso di *Sms* e *Mms*, sul fenomeno dello *spamming* e sulle nuove tecnologie di comunicazione.

Infine, dal 10 al 12 settembre del 2003, l'Autorità ha partecipato alla 25ª Conferenza internazionale delle Autorità Garanti, svoltasi a Sydney. Della Conferenza, conclusasi con l'approvazione di cinque risoluzioni (riguardanti rispettivamente: il trasferimento dei dati dei passeggeri di voli aerei diretti negli Usa; il miglioramento delle informative ai cittadini; la protezione dei dati personali e il ruolo degli organismi internazionali; gli aggiornamenti automatici dei *software*; *Rfid)*, si è già parlato in modo approfondito nei paragrafi. 44.-44.5., ai quali si rinvia.

52

52.4. Il sito Internet dell'Autorità, il progetto NormeInRete *e le attività editoriali*

Per quanto riguarda il sito Internet del Garante, nell'anno appena trascorso si è consolidata la piattaforma tecnologica del nuovo sito e sono stati attivati alcuni nuovi servizi per il cittadino.

Va in primo luogo segnalata la procedura *web* per la notificazione per via telematica con firma digitale e per la connessa operazione di transazione con carta di credito ai fini del pagamento dei diritti di segreteria. A tale scopo sono state stipulate convenzioni con quattro tra i maggiori emettitori di carte, che potranno essere in futuro utilizzate anche in altre circostanze.

Come annunciato nella Relazione per l'anno 2003, l'Autorità ha poi aderito al progetto intersettoriale nazionale *NormeInRete* promosso dal Cnipa (Centro nazionale per l'informatica nella pubblica amministrazione, su proposta del Ministero della giustizia.

Il portale *www.normeinrete.it*

Il portale *www.normeinrete.it* offre un punto di accesso unitario alla normativa italiana ed europea pubblicata sui siti delle istituzioni aderenti e che (una volta marcata sulla base delle regole espresse in vari *Dtd-Document type definition* –utilizzando il linguaggio informatico *Xml-Extensible markup language*–), oltre a valorizzare ciascun documento per il suo contenuto giuridico, assegna una *Urn* (*Uniform resource names*), ovvero un "nome" univoco al singolo documento. Dal portale nazionale l'utente è così indirizzato verso i siti istituzionali che pubblicano l'informazione richiesta e risulta quindi amplificata la distribuzione della documentazione d'interesse per i cittadini.

La redazione del sito *web* del Garante si è posta peraltro l'ulteriore obiettivo di contribuire fattivamente al progetto *NormeInRete* studiando –in collaborazione con il gruppo di lavoro di *NormeInRete*– un nuovo e specifico standard *Dtd* per marcare i provvedimenti del Garante con modalità che potranno essere all'occorrenza utilizzate da altre autorità indipendenti, al fine di sfruttare l'amplificazione del portale *NormeInRete* ed incrementare le potenzialità del motore di ricerca interno.

Il sito *web* del Garante costituisce inoltre uno strumento volto ad offrire, in conformità all'art. 154, comma 1, lettera *h)* del Codice, la massima conoscenza tra il pubblico della disciplina del trattamento dei dati personali. Per questo, attraverso le sintetizzate tecniche di marcatura, verranno diffusi i testi normativi di riferimento nella versione consolidata.

La pubblicazione sul sito delle norme, dalla versione originaria della legge n. 675/1996 al Codice e agli ulteriori sviluppi normativi, consentirà di ottenere una rappresentazione completa delle modifiche intervenute sulle norme stesse nel tempo, nonché di visualizzare, sempre all'interno del sito, il *link* del provvedimento pubblicato con la versione vigente della norma alla data del documento.

A tal fine, l'anno appena trascorso ha visto la redazione del sito impegnata in uno studio di fattibilità per la piena integrazione tra la piattaforma tecnologica del sito e le peculiari necessità tecniche dettate da *NormeInRete*, nella predisposizione di un apposito capitolato tecnico-esecutivo e nella ricerca e selezione di un *partner* scientifico in grado di fornire un competente ausilio nella marcatura di un volume così alto di documenti. Il *partner* istituzionale ora individuato è il Cirsfid (Centro inter-

dipartimentale di ricerca in storia del diritto, filosofia e sociologia del diritto e informatica giuridica) dell'Università di Bologna che ha acquisito una consolidata esperienza scientifica nel trattamento dell'informazione giuridica in Internet.

Corollario di questo piano di lavoro è, poi, la completa messa *off-line* della precedente versione del sito *web* e il completamento del trasferimento di tutta la copiosa documentazione già disponibile.

Sul piano internazionale è stato inoltre progettato, realizzato e arricchito di contenuti normativi e documentali, il sito dell'Autorità di controllo comune Schengen, durante il periodo di presidenza italiana di tale organismo. Progettato per ospitare contenuti in tutte le lingue dei Paesi che applicano la Convenzione Schengen, il sito è già disponibile in lingua inglese (indirizzo attuale, in vista di nuovi domini in ambito comunitario: *www.schengen-jsa.dataprotection.org*). Nello stesso contesto è stata anche prodotta la versione grafica, sempre in lingua inglese, della *"Newsletter JSA-ACC Schengen"* e del *depliant* della campagna informativa dell'Autorità Schengen.

Il sito dell'Acc Schengen

Presso la redazione *web* continua ad essere infine seguita, oltre ai prodotti dell'editoria tradizionale con particolare riferimento alle relazioni annualli e al Bollettino ufficiale dell'Autorità, la cura editoriale –sino alla pre-stampa tipografica– delle pubblicazioni dell'Autorità (con particolare riferimento ai volumi cui si fa cenno in altre parti di questa *Relazione*, cfr. parag. 52.2).

52.5. Il rapporto con il pubblico: l'Urp e l'attività di formazione

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, attenta alle nuove frontiere della protezione dei dati personali e dei nuovi diritti della persona. La messa a disposizione sul sito di una notevole quantità di documentazione, con continui aggiornamenti e *dossier* tematici, ha rappresentato uno strumento di informazione e "formazione" del pubblico.

L'interesse che suscita il diritto alla *privacy* è sempre maggiore e, per conseguenza, i motivi di contatto con il pubblico si moltiplicano: da tale riflessione è derivata la scelta dell'Autorità per un modello organizzativo che consenta di tenere adeguatamente conto della funzione di comunicazione, anche come momento di confronto e di dialogo continuo con i cittadini.

In questo quadro, ha assunto un rilievo fondamentale l'entrata in funzione a pieno regime, nel corso del 2003, dell'Ufficio per le relazioni con il pubblico, istituito nell'ambito della segreteria generale, che ha rivestito da subito un ruolo centrale nell'attuazione del progetto di sviluppo della comunicazione tra il Garante ed il pubblico: la sua centralità dipende, in effetti, dal rilevante fabbisogno degli utenti e dalla costante crescita delle aspettative ed esigenze degli utilizzatori di questo tipo di comunicazione ed informazione.

L'attivazione di tale Ufficio ha pure contribuito a garantire la qualità dell'azione amministrativa, permettendo all'Autorità di percepire il grado di soddisfazione dell'utenza per le risposte da essa date alle molteplici problematiche avanzate. Inoltre, ha creato un canale che permette di cogliere con immediatezza quali sono le tematiche di cui è più avvertita l'importanza da parte della collettività.

52

In proposito, le materie che nel periodo preso in esame hanno formato più spesso oggetto di quesiti rivolti all'Ufficio (o per le quali più di frequente è stato richiesto materiale informativo) sono state lo *spamming*, il trattamento dei dati da parte delle "centrali rischi" private, l'esercizio dei diritti previsti dall'art. 13 della legge n. 675/1996 (ora, dall'art. 7 del d.lg. n. 196/2003), la videosorveglianza, il trattamento dei dati nell'ambito del rapporto di lavoro e il trasferimento di dati all'estero.

Per le pubbliche amministrazioni, particolare rilievo dominante ha assunto il rapporto tra la normativa in materia di *privacy* e la legge n. 241/1990, nonché, per gli enti locali, quella del diritto di accesso dei consiglieri comunali e provinciali.

Peraltro, sebbene l'attività dell'Ufficio sia stata rivolta prevalentemente a fornire elementi su questioni per le quali si era già formato un consolidato orientamento del Garante, non sono mancate risposte a quesiti su aspetti di novità.

Nel corso del 2003 l'affluenza del pubblico in cerca di un contatto diretto con l'Autorità è aumentata in modo costante. I mezzi di comunicazione utilizzati per le risposte sono stati le lettere, l'invio di *fax*, le risposte telefoniche e le *e-mail*: questi ultimi due strumenti sono stati privilegiati, laddove possibile, per la loro agilità e speditezza.

In particolare, sono pervenuti allo specifico indirizzo di posta elettronica dell'Ufficio diverse migliaia di quesiti e richieste di documentazione; allo stesso modo, i riscontri forniti a mezzo *e-mail*, *fax* o lettera sono quantificabili in svariate migliaia. Ancora più numerosi sono stati i contatti telefonici (stimabili in oltre dodicimila), per brevi questioni o richieste di chiarimenti ed informazioni, cui è stata sempre data puntuale e rapida risposta.

Vi sono stati, poi, momenti di "picco" nei contatti del pubblico con l'Urp, che si sono verificati anche in occasione dello *spot* televisivo e radiofonico trasmesso nel marzo 2003 dalle reti Rai o di trasmissioni televisive su profili di interesse.

Rilievo particolare ha poi assunto il nuovo Codice che, sin dalla sua emanazione (giugno 2003), ha dato luogo ad un'intensa attività di comunicazione incentrata su aspetti interpretativi e applicativi, soprattutto per quanto riguarda le misure di sicurezza e gli adempimenti connessi alla notificazione. Tale attività, via via incrementatasi con l'avvicinarsi della data di entrata in vigore della nuova normativa, ha portato l'Ufficio a fornire sempre più spesso risposte, pur se con la necessaria prudenza, a questioni di carattere innovativo.

Infine, proprio attraverso il contatto diretto con i cittadini ha assunto ulteriore incisività il potere del Garante di intervenire tempestivamente in occasione di situazioni particolarmente lesive della *privacy* (ad esempio, con la misura cautelare del blocco dei dati trattati in violazione di legge, oppure con accertamenti e controlli).

I corsi di formazione

L'impegno, infine, di contribuire in maniera fattiva alla promozione della cultura della protezione dei dati presso aziende e pubbliche amministrazioni, nonché all'applicazione delle norme e alla corretta attuazione degli adempimenti nell'at-

tività quotidiana, ha portato il Garante ad avviare un'attività di formazione. L'iniziativa si è concretizzata nel primo corso, organizzato con successo il 2 aprile 2004, rivolto al mondo dell'impresa, al quale seguiranno presto quelli dedicati ad amministrazioni pubbliche e sanità da un lato, e alle comunicazioni elettroniche dall'altro.

VII - La gestione amministrativa dell'Ufficio

53 Le novità legislative e l'organizzazione dell'Ufficio

Il d.lg. n. 196/2003, nel capo II dedicato all' Ufficio del Garante, ha confermato l'impianto normativo già previsto dalla legge n. 675/1996 e successive modificazioni, conferendogli un ordine sistematico più razionale.

Nel nuovo quadro resta demandata ai regolamenti del Garante la definizione dell'organizzazione e del funzionamento dell'Ufficio, del trattamento giuridico ed economico del personale –pur con le limitazioni previste dal Codice–, nonché della gestione amministrativa e contabile.

L'organico dell'Autorità viene confermato nel limite senz'altro esiguo di cento unità.

L'art. 182 del Codice prevede che il Garante, in sede di prima applicazione e comunque non oltre il 31 marzo 2004, possa individuare i presupposti per inquadrare in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilità di organico, il personale in posizione di fuori ruolo o di comando presso l'Autorità in servizio presso l'Ufficio alla data di pubblicazione del Codice nella *Gazzetta Ufficiale* (29 luglio 2003). Di tale facoltà il Garante si è avvalso individuando i criteri in data 31 marzo 2004. Il Codice dispone inoltre che il Garante possa prevedere riserve di posti nei concorsi pubblici, nel limite del 30% dei posti disponibili in organico, per il personale non di ruolo che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

Le predette disposizioni sono finalizzate ad assicurare il buon andamento dell'Autorità, ma nel rigoroso rispetto dell'art. 97 Cost., evitando che vada disperso un patrimonio di conoscenze ed esperienze acquisite. Il personale interessato all'inquadramento è integralmente composto da dipendenti pubblici, reclutati esclusivamente tramite concorso pubblico.

In attuazione di tale disciplina il Garante ha pertanto bandito due nuovi concorsi pubblici (oltre quelli già banditi nel 2003 e che si potrebbero ulteriormente bandire nel 2004), riservando il 30% dei posti al personale non di ruolo (in posizione di fuori ruolo o a contratto) che abbia maturato i requisiti previsti (cfr. *infra*, parag. 55.).

La modifica della pianta organica

La pubblicazione dei bandi è stata preceduta da una riflessione sulle esigenze funzionali e organizzative dell'Autorità, a conclusione della quale si è deciso di ridurre l'area esecutiva da 9 a 3 unità e di redistribuire le residue 6 unità tra l'area direttiva (5 unità) e quella operativa (1 unità), con provvedimento di modifica della pianta organica pubblicato sulla *Gazzetta Ufficiale* e allegato alla presente *Relazione*.

La parziale modifica delle dotazioni organiche è finalizzata a potenziare e rafforzare l'Ufficio, dotandolo di personale di elevata qualificazione da destinare prevalentemente all'area giuridica, in considerazione dei nuovi compiti demandati all'Autorità dal Codice.

Il processo di consolidamento della struttura organizzativa dell'Autorità, avviato negli anni precedenti e continuato nel 2003, è confermato in particolare dalle nuove immissioni di personale reclutato all'esito delle procedure concorsuali e selettive indette dall'Autorità stessa.

Avvalendosi delle convenzioni Consip S.p.A., sono state conferite in *outsourcing* e *insourcing* alcune attività di natura esecutiva. È inoltre proseguita la gestione di un servizio di *inbound* telefonico, con funzioni di centralino.

Parallelamente, al fine di poter meglio adempiere ai nuovi e delicati compiti assegnatigli dal Codice, il Garante ha provveduto al rinnovo degli incarichi (previsti per la durata di due anni rinnovabili) ai dirigenti dell'Ufficio.

Per una migliore funzionalità dell'Ufficio e nel rispetto delle priorità istituzionali sono stati avviati graduali avvicendamenti negli incarichi dirigenziali, finalizzati anche alla valorizzazione delle esperienze dei singoli dirigenti.

Mediante l'istituzione di un'unità temporanea di vigilanza e controllo si è perseguito l'obiettivo di incrementare l'attività ispettiva, già notevolmente cresciuta nel 2003 con significativi risultati.

Il documento programmatico per il 2004

Nel quadro delle iniziative per migliorare efficienza, efficacia ed economicità dell'azione amministrativa, contestualmente all'approvazione del bilancio di previsione, il Garante ha come di consueto definito nel documento programmatico i principali obiettivi e le priorità per il 2004. La direttiva del Garante sarà seguita da ulteriori atti di indirizzo del segretario generale tendenti a specificare tempi e modalità di attuazione dei programmi di lavoro di ciascuna unità organizzativa e delle articolazioni interne all'Ufficio.

Per la definizione di parametri di valutazione e di indicatori per la verifica dei risultati dell'attività dell'Ufficio, oltre che per un controllo di regolarità della gestione contabile, è operante un servizio di controllo interno (al quale partecipano un magistrato contabile e due dirigenti di provata esperienza e competenza) ed è in fase di avanzata definizione un efficiente sistema di controllo di gestione, cui occorre ora accennare.

53.1. Gli interventi per il miglioramento dell'azione amministrativa

Nel corso del 2003 sono proseguiti gli interventi per il miglioramento dell'assetto organizzativo e degli obiettivi di efficacia, efficienza ed economicità dell'azione amministrativa, specialmente in considerazione dell'aumentato volume di compiti affidati dal Codice all'Ufficio del Garante, che è peraltro rimasto invariato nel suo assetto organico.

Gli interventi, attuati sulla base degli studi effettuati nell'anno precedente anche sulla base dei contributi di due società di consulenza, hanno riguardato in particolare:

53

- la costituzione, con delibera del gennaio 2003, del servizio di controllo interno;

- l'immissione in servizio dal mese di luglio di una nuova figura dirigenziale presso la segreteria generale con compiti delegati di coordinamento di talune attività amministrative (direttore di gestione);

- la progettazione di un sistema informativo direzionale per il controllo di gestione (Sid) coerente con il metodo della programmazione per funzioni obiettivo.

Il progetto Sid

Il progetto Sid è stato predisposto con risorse interne e si basa sulla cd. gestione per obiettivi, che costituisce un metodo di analisi largamente usato per la valutazione della gestione di ogni tipo di organizzazione, comprese le pubbliche amministrazioni.

Il sistema utilizza il criterio del grado di raggiungimento degli obiettivi per guidare ogni fase della gestione e per valutare, misurandole, le prestazioni delle unità organizzative e dei dirigenti ad esse preposti: per "obiettivi" si intendono, infatti, i risultati in termini di efficacia, economicità e qualità, espressi in numeri finiti, che si decide di conseguire in un tempo determinato.

I diversi livelli dell'Autorità sul piano strategico, direzionale ed operativo riceveranno flussi di informazione costanti e di elevata qualità sulla "produzione" realizzata e sull'assorbimento delle risorse umane e finanziarie. I *report* verranno forniti con brevi cadenze periodiche, in modo che sia possibile stimare tempestivamente gli scostamenti dai programmi e disporre in tempo utile gli interventi correttivi.

Si è scelto di basare la valutazione del sistema su prodotti e risorse, piuttosto che sulle attività, in quanto si tratta degli oggetti che più facilmente ed attendibilmente si prestano ad essere rilevati e contabilizzati. Viceversa, sui processi di lavoro verranno svolte in modo trasparente alcune analisi, utilizzando anche, laddove possibile, tecniche comparative *(benchmarking)*, per l'eventuale reingegnerizzazione dei processi e comunque per indurre miglioramenti in termini di qualità, costi e tempi di esecuzione. La progettazione è stata svolta partendo dalla considerazione della situazione attuale dell'Autorità, con particolare riferimento ai compiti istituzionali delineati dall'art. 154 del d.lg. n. 196/2003, al disegno della struttura organizzativa, alle caratteristiche quantitative e qualitative del personale dipendente, alla struttura delle spese e alle infrastrutture tecnologiche disponibili.

Peculiare attenzione è stata dedicata alle tipologie di processi di lavoro ed all'individuazione delle categorie di servizi offerti al pubblico. I processi di lavoro sono stati raggruppati nelle seguenti funzioni-obiettivo: informazione e regolazione preventiva, controllo e tutela, registro dei trattamenti, comunicazione istituzionale, cui si debbono aggiungere l'indirizzo politico-amministrativo e le attività per il funzionamento della struttura. L'archivio dei processi è configurato come un sistema che rileva l'assorbimento delle risorse umane nelle diverse linee di attività per centri di costo e per centri di responsabilità.

È previsto che la prima versione del Sid entri a regime entro il primo semestre del 2004 e che il sistema sia aggiornato periodicamente, in modo da consentirne la

crescita graduale e facilitare i dirigenti nella comprensione ed utilizzazione consapevole del nuovo strumento.

È importante sottolineare che il sistema non ha carattere ispettivo, ma mira espressamente a fornire un supporto ai processi decisionali, a favorire la crescita dell'organizzazione e ad ottenere la massima valorizzazione del personale, nonché a stimolare la collaborazione, l'automiglioramento e la condivisione delle conoscenze.

53.2. Lo sviluppo del sistema informativo e l'attività in ambito tecnologico-informatico

L'operato dell'Ufficio nel settore tecnologico e informatico è stato caratterizzato nel 2003, per quanto attiene alle attività negoziali, da un maggiore ricorso a servizi rispetto all'acquisizione di beni e attrezzature, nel segno di una progressiva integrazione dei sottosistemi precedentemente sviluppati e che nel loro insieme costituiscono il sistema informativo dell'Ufficio.

Nello stesso tempo si è sviluppata notevolmente la capacità di integrazione basata su risorse interne e tecnologie *software* di tipo *open source*. Questi strumenti sono stati utilizzati per significative realizzazioni, quali il sito *web* per il supporto al lavoro cooperativo del Servizio studi e documentazione, in precedenza, il sistema di gestione del contenzioso amministrativo.

Il Dipartimento risorse tecnologiche ha inoltre continuato a svolgere i propri compiti di gestione delle infrastrutture, di assistenza nei confronti degli utenti interni, di consulenza nei confronti dei dipartimenti giuridici e di altre articolazioni dell'Autorità, di contributo alla vita amministrativa dell'Ufficio, di progettazione e sviluppo di sistemi *software* di *database*, di *reporting*, di documentazione.

Il sistema informativo si è arricchito di nuove funzionalità o ha visto realizzate quelle che erano state delineate o progettate nell'anno precedente, nell'ottica del perseguimento di ancora più elevati livelli di efficienza, a vantaggio dell'azione amministrativa dell'Autorità.

Molte risorse sono state assorbite dalla manutenzione e dallo sviluppo dei sistemi di sicurezza a protezione della rete e delle risorse dell'Ufficio. Strumenti quali gli *antivirus* per le postazioni individuali, per i *gateway* di posta elettronica, per i *proxy server*, sono stati ulteriormente affinati, così come i sistemi di rilevamento delle intrusioni e i sistemi di protezione da accessi indesiderati.

È stata progettata e sviluppata internamente la procedura di notificazione telematica tramite *web* prevista dal Codice, che ha comportato la realizzazione di servizi *web* sicuri, con crittografia forte, avvalendosi di una autorità di certificazione ufficiale, al fine di garantire la riservatezza delle transazioni e la sicurezza dei pagamenti dei diritti di segreteria. Per la parte di sviluppo del *database* ci si è avvalsi del supporto di una ditta specializzata che ha curato la programmazione delle relative procedure. Questa attività è stata svolta in coordinamento con il Dipartimento registro dei trattamenti, con cui si è sviluppata una specifica collaborazione all'atto della definizione dei requisiti del nuovo sistema e nella successiva fase di realizzazione.

La procedura di notificazione telematica si avvale delle capacità di riconoscimento e controllo delle firme digitali previste dal nuovo sistema di gestione del pro-

53

tocollo informatico, la cui definizione ha impegnato il Dipartimento per tutto il secondo semestre del 2003, consentendo di avviare il nuovo sistema il 1° gennaio del 2004, in aderenza al dettato normativo.

L'introduzione del nuovo sistema di gestione del protocollo ha facilitato l'opera di controllo dello stato delle pratiche da parte dei dirigenti assegnatari. Il nuovo protocollo informatico consente anche una maggiore trasparenza amministrativa, sia per gli *standard* di sicurezza che garantiscono l'immodificabilità dei documenti registrati, sia per la possibilità di fare accedere per via telematica, con i cosiddetti codici Urp, il pubblico interessato e avente diritto a conoscere lo stato delle pratiche che lo riguardano. L'intera procedura è infatti di tipo *web oriented* ed è utilizzabile tramite un comune *browser*.

In parallelo all'adozione del nuovo sistema di protocollo si è proceduto alla registrazione dell'Autorità nell'indice delle pubbliche amministrazioni gestito dal Cnipa, accessibile con protocolli *Ldap* e interrogabile anche tramite interfaccia *web*.

A supporto del protocollo informatico, è stato realizzato in collaborazione con il Cnipa un sistema di posta elettronica certificata che consente l'interazione tramite posta elettronica, con pieno valore legale, con altre amministrazioni o cittadini che utilizzino servizi *e-mail* in un dominio di posta certificata.

Il Dipartimento ha poi dedicato un rilevante impegno alle procedure amministrative nell'ambito del procedimento di gara europea per aggiudicare il servizio di scansione ottica delle notificazioni di trattamento dei dati personali pervenute nel periodo 1997-2003.

Si è trattato di un lavoro molto impegnativo sia per la valutazione della complessità del servizio, che include l'archiviazione sostitutiva e la successiva eliminazione degli originali cartacei, sia per l'esigenza di un'approfondita ed equa comparazione dei progetti presentati.

Una delle più rilevanti innovazioni realizzate dal Dipartimento è l'introduzione di un servizio di posta elettronica per l'Ufficio che viene ora gestito interamente con risorse interne e con strumenti in dotazione. Il servizio svolto in proprio ha consentito infatti di pervenire ad elevatissimi livelli di efficienza, all'estensione delle funzionalità, all'incremento della sicurezza e della protezione dei dati, alla possibilità di gestire con la massima flessibilità tutte le politiche di trattamento dello *spam* e dei contenuti dannosi *(virus, warm, trojan)*. Tutto ciò con risparmio di risorse economiche da dedicare a servizi specialistici di diverso tipo relativi alle metodologie e alle procedure di sicurezza *(security assessment)*.

È stato portato in produzione l'ulteriore sistema informatico per la gestione amministrativo-contabile (Sigac) che, interagendo con altri sottosistemi, come il protocollo e il sistema di gestione del personale, costituisce il nucleo del complessivo sistema informativo dell'Ufficio. Con il Sigac è stato possibile predisporre in modo più efficiente la previsione di bilancio per l'esercizio 2004 e attivare le piene funzionalità del sistema, in modo da avviare il 1° gennaio 2004 la contabilità in modalità totalmente automatizzata.

Il personale del Dipartimento ha infine contribuito all'attività istituzionale del Garante in sede internazionale, in particolare partecipando al lavoro della *Internet Task Force* a supporto del Gruppo istituito ai sensi dell'art. 29 della direttiva europea, interessandosi in particolare dei sistemi di autenticazione a *single sign-on* e dei problemi di *privacy* derivanti dalla gestione dei servizi di *directory* di tipo *whois* associati alla gestione dei nomi a dominio.

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

Il bilancio di previsione del 2003, riferito al settimo 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 quei settori individuati nel documento programmatico di accompagnamento al bilancio di previsione che ha fissato gli obiettivi dell'Ufficio per l'esercizio 2003.

Il bilancio di previsione del 2003 è stato predisposto tenendo conto di tutto ciò e l'intensa attività del Garante è stata resa possibile, nel periodo considerato, non solo dalle risorse finanziarie assegnate ai servizi più impegnati su tali fronti, ma anche in relazione all'incremento delle risorse umane a disposizione dell'Ufficio, poiché a seguito dei concorsi espletati nel 2002 l'organico è stato implementato, dall'inizio dell'anno, di ventitré unità (cfr. parag. 55.).

Inoltre, con le due prime delibere adottate nel 2003, il Garante ha istituito il servizio di controllo interno previsto dall'art. 8, comma 5, del regolamento 1/2000 ed ha nominato i tre componenti che ne fanno parte. Il servizio interno, oltre ai compiti propri di un organo di controllo contabile, dovrà fornire al Garante elementi di valutazione dei risultati dell'attività dell'Ufficio e per la verifica della corretta ed economica gestione delle risorse pubbliche.

Le risorse a disposizione del Garante per il 2003 sono state accertate, nell'esercizio, per euro 11.709.701,00 di cui provenienti dal contributo dello Stato per euro 10.252.000,00. Le restanti risorse finanziarie sulle quali ha potuto contare l'Autorità per entrate proprie si riferiscono ai diritti di segreteria per le notificazioni, per i ricorsi e le autorizzazioni, ai rimborsi spese provenienti dal Consiglio d'Europa e dalle istituzioni comunitarie per la partecipazioni di rappresentanti del Garante a riunioni a Bruxelles e nelle altre sedi comunitarie, agli interessi maturati sui fondi relativi agli avanzi pregressi, alle entrate derivanti dalla sublocazione di alcuni locali dell'edificio di piazza di Monte Citorio 115, e ad entrate accertate per sanzioni pecuniarie. Il contributo dello Stato per il 2003 è stato ridotto rispetto al 2002 di quasi 600 mila euro e poiché il complesso delle uscite previsto per l'anno 2003 è stato superiore a circa 1.600 mila euro rispetto all'anno precedente, dovuto questo in gran parte agli oneri derivanti dai nuovi assunti, tali minori entrate, aggiunte alle maggiori spese, sono state compensate con un circoscritto ricorso all'utilizzo dell'avanzo di amministrazione. Nell'esercizio 2003 la spesa per il personale in servizio ha registrato un incremento del 4% sul totale delle spese, passando dal 61% del

54

2002 al 65% del 2003. Inoltre, l'esercizio che si è chiuso al 31 dicembre ha registrato per la prima volta un'eccedenza del totale delle spese impegnate sul totale delle entrate accertate. Come detto in precedenza lo sbilancio è stato coperto ricorrendo all'utilizzo dell'avanzo di amministrazione.

Le spese di funzionamento sono state ulteriormente contenute e razionalizzate, e seguitano ad essere limitate all'indispensabile poiché l'Autorità, dalla fine del 2002 e a seguito dell'emanazione del decreto legge n. 194 (convertito con la legge n. 246/2002) concernente la limitazione degli impegni di spesa non aventi carattere obbligatorio, ha proseguito nella politica di contenimento delle spese aventi tali finalità. Infatti, benché l'attività del Garante si sia notevolmente incrementata in qualità e in quantità, la percentuale delle spese di funzionamento sul totale delle spese in bilancio è leggermente diminuita passando dal 26,9% del 2002 al 26,4% del 2003.

Il costante decremento nello stanziamento pubblico per il Garante, passato da euro 11.362.000 del 2000 a 10.081.000 del 2004 e compensato parzialmente dall'incremento delle entrate proprie, induce l'Autorità a perseguire attualmente una politica di bilancio molto attenta che, per il momento, non intacca i servizi che sono giudicati prioritari, come l'elevato livello del sistema informatico e della sua rete interna. Tuttavia, come emerso anche dal dibattito parlamentare su una recente mozione, la dotazione di fondi e altre risorse a sostegno dell'Autorità non potrà non essere incrementata.

Il Dipartimento contratti e risorse finanziarie nel corso del 2003 ha dato seguito a molteplici richieste tese all'approvvigionamento di beni e servizi pervenute su indicazione dei vari uffici.

Gran parte di questa attività è stata dedicata al potenziamento delle strutture tecnologiche.

L'Autorità ha dato notevole impulso allo sviluppo del sistema informativo seguendo un programma di acquisizione curato dal Dipartimento risorse tecnologiche.

Il Dipartimento contratti e risorse finanziarie, su attivazione del Dipartimento registro dei trattamenti, anche sulla base delle nuove necessità emerse con l'emanazione del d.lg. n. 196/2003 in materia di notificazioni dei trattamenti al Garante, ha attivato le procedure necessarie a consentire l'automazione delle lavorazioni e velocizzare l'accesso alle notificazioni memorizzate, nonché a procedere all'adeguamento tecnologico necessario a consentire l'uso della firma digitale per tali adempimenti.

Nel 2003 è stata espletata la gara per l'acquisizione del servizio di scansione ottica delle notificazioni del trattamento dei dati personali e di memorizzazione di file contenuti nei *floppy disk*. La gara è stata bandita ai sensi del decreto legislativo 17 marzo 1995, n. 157, è stata pubblicata nella *Gazzetta Ufficiale C.E.* 28 novembre 2002, n. S231e nella *Gazzetta Ufficiale* 29 novembre 2002, n. 280. L'avviso di aggiudicazione è stato pubblicato nella *Gazzetta Ufficiale* 30 luglio 2003, n. 175. Il servizio ha reso possibile la visualizzazione diretta tramite registro dell'intera notificazione compresi gli allegati.

Inoltre, si è proceduto a sviluppare il *software* necessario per attivare il nuovo registro dei trattamenti con l'obiettivo di inviare telematicamente la notificazione superando i problemi connessi alla compilazione e all'invio dei modelli cartacei.

Tra le varie attività contrattuali espletate nel corso del 2003 è da citare anche la gara svolta per l'affidamento del servizio di noleggio delle autovetture con conducente. Il bando è stato pubblicato nella *Gazzetta Ufficiale*, parte seconda, 30 luglio 2003, n. 175 e nella *Gazzetta Ufficiale C.E.*, 2 agosto 2003, n. S147 (affidamento del servizio di noleggio di autoveicoli con conducente per il trasporto di persone per conto dell'Autorità, mediante il ricorso alla licitazione privata di cui all'art. 6, comma 1, lett. *b)*, d.lg. n. 157/1995). L'avviso di aggiudicazione è stato invece pubblicato nel Foglio delle inserzioni della *Gazzetta Ufficiale* 17 dicembre 2003, n. 292.

Come previsto dalla finanziaria 2003, nel quadro delle iniziative di razionalizzazione della spesa per beni e servizi della p.a., l'Autorità si è anche rivolta alla Consip S.p.A., che cura lo sviluppo e la gestione operativa del relativo programma, per acquisire alcuni beni e servizi necessari per le esigenze dell'Ufficio con la stessa appositamente concordati. Si è così proceduto a stipulare appositi contratti per i servizi di pulizia, per la raccolta e lo smaltimento dei rifiuti speciali, per la disinfestazione dei locali, la manutenzione degli impianti antincendio, nonché per reperire alcuni servizi quali quello di guardiania e *reception*. Sempre nell'ambito della convenzione Consip S.p.A. si è proceduto a rinnovare la convenzione per la fornitura dei buoni pasto e si è aderito alla convenzione Consip per alcuni servizi di telefonia.

Infine, nell'ambito del piano di razionalizzazione della spesa dell'Autorità, è da citare l'avvenuta adesione dell'Autorità al primo mercato elettronico della p.a. attivato da Consip S.p.A. su incarico del Ministero dell'economia e delle finanze e dal Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri.

55 Il personale e i collaboratori esterni

Nel periodo considerato è proseguito il processo di consolidamento dell'Autorità con l'immissione in servizio, agli inizi del 2003, dei vincitori di quattro concorsi pubblici espletati dall'Autorità per la copertura di complessivi 21 posti (dei quali 19 coperti), di cui n.1 per dirigente informatico, n. 2 per dirigente, n. 10 per funzionario e n. 8 per impiegato operativo (vedi *Relazione 2002*). Tale processo è stato rafforzato dal contemporaneo inserimento in servizio di altre 4 unità con contratto di specializzazione a tempo determinato, selezionate con una procedura bandita nell'agosto 2002.

Sono stati inoltre stipulati 4 contratti di *stage*, all'esito di una selezione che ha portato alla formazione di una graduatoria alla quale attingere periodicamente, al fine di offrire a giovani laureati la possibilità di un periodo di tirocinio presso il Garante.

Come accennato nel paragrafo 53., il Garante ha bandito di recente due nuovi concorsi pubblici per complessivi 13 posti, di cui 9 nel ruolo di funzionario, e 4 nel ruolo di impiegato operativo, riservando il 30% dei posti a concorso al personale non di ruolo in servizio presso l'Autorità che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno. A garanzia dell'imparzialità delle procedure concorsuali il Garante, come per il passato, ha chiesto e ottenuto dal Consiglio di presidenza della giustizia amministrativa la nomina dei presidenti delle due commissioni esaminatrici.

Contestualmente il Garante ha indetto una selezione per il reclutamento di un massimo di 3 giovani laureati in materie giuridiche, da assumere con contratto di specializzazione a tempo determinato.

Con i concorsi appena banditi, l'organico dell'Autorità sarà coperto al 90% circa. Attualmente infatti l'Ufficio dispone di 93 unità, di cui 59 appartenenti al ruolo organico, 18 (n. 2 a *part-time*) assunte con contratto a tempo determinato e 16 in posizione di fuori ruolo o comando da altre amministrazioni ed enti pubblici, come da prospetto allegato:

Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	Personale a contratto	TOTALE
Dirigenti	26	17	5		**22**
Funzionari	40	27	6		**33**
Operativi	25	15	5		**20**
Esecutivi	9				**0**
Personale a contratto	20			18	**18**
TOTALE	**120**	**59**	**16**	**18**	**93**

Personale in servizio

L'Autorità allo stato non si avvale della collaborazione di consulenti esterni. Nel periodo considerato si è peraltro reso necessario acquisire occasionali consulenze qualificate, per le problematiche concernenti il sistema informativo interno e il sito *web* del Garante, per l'attuazione del nuovo programma di gestione del bilancio e della contabilità e per la definitiva sistemazione della biblioteca e dell'ampio materiale documentale acquisito e prodotto dall'Autorità nel corso della sua attività. Sono da ultimo in corso due brevi incarichi di studio per necessari approfondimenti in alcune tematiche giuridiche.

56 La notificazione ed il registro dei trattamenti

La notificazione del trattamento dei dati personali ha subito profondi cambiamenti nella sua *ratio*, nei suoi contenuti e nelle sue modalità di compilazione a seguito dell'emanazione del Codice. Prima di affrontare questo aspetto, occorre soffermarsi sull'attività svolta nel 2003 e nei primi mesi del corrente anno in relazione al vecchio registro dei trattamenti istituito ai sensi dell'abrogata legge n. 675/1996.

Un profilo significativo è stato in primo luogo quello della sottoposizione a scansione ottica dell'enorme archivio cartaceo custodito nel magazzino messo a disposizione dalla Presidenza del Consiglio dei ministri-Dipartimento della protezione civile presso il centro polifunzionale di Castelnuovo di Porto. Tale attività comporterà indubbi vantaggi per il Garante, rendendo immediato il riscontro delle notificazioni, agevolando le attività tese alla regolarizzazione delle pratiche e consentendo il risparmio di spese di gestione e di manutenzione dell'archivio stesso.

Nel 2003 l'attività del Dipartimento registro generale dei trattamenti si è sviluppata su quattro direttive: proseguimento della memorizzazione delle notificazioni pervenute entro il 31 dicembre dello stesso anno; regolarizzazione delle notificazioni incomplete; riscossione dei diritti di segreteria inevasi; progettazione del nuovo registro dei trattamenti.

In particolare, il recupero dei diritti di segreteria inevasi ha fatto affluire nel bilancio del Garante più di 80.000,00 euro. Le richieste di regolarizzazione sono state circa 12.000. Si stanno tuttora esaminando alcune migliaia di posizioni, per le quali la verifica dovrebbe concludersi entro il mese di aprile del 2004.

La nuova notificazione

Per quanto riguarda la nuova notificazione, come già accennato, l'esperienza di sei anni ha indotto il Garante a rivederne completamente le caratteristiche.

Come si è già detto (cfr. *supra,* parag. 1.6.), a differenza di quanto previsto dalla legge n. 675/1996, dove tutti coloro che effettuavano il trattamento dei dati personali erano obbligati a notificare, salvo i casi di esonero per taluni titolari, con il nuovo sistema notificano solo i titolari dei trattamenti che sono elencati nell'art. 37 del Codice: si tratta di casi che, per la particolare delicatezza dei dati, le modalità di trattamento o le finalità perseguite, presentano rischi per i diritti e le libertà dell'interessato. In particolare, il Codice ha individuato sei categorie di trattamenti sottoposti ad obbligo di notificazione ed ha altresì attribuito al Garante il potere di incrementare o ridurre l'elenco dei trattamenti sottoposti a tale obbligo, con proprio provvedimento. A tal riguardo, il 31 marzo scorso il Garante ha emanato il provvedimento teso ad esonerare alcuni trattamenti dall'obbligo di notificazione, su cui cfr. *supra*, parag. 12.

Non sono stati previsti modelli differenziati di notificazione, essendosi scelto un'unico modello di notificazione, di semplice compilazione e di contenuto ridotto agli elementi davvero significativi.

L'attuale istituto della notificazione e le connesse procedure, fruibili solo *on line*, si ispirano ai seguenti obiettivi: grande flessibilità nell'individuazione di contenuti e tipologie dei trattamenti sottoposti ad obbligo di notificazione; richiesta delle sole notizie essenziali ed effettivamente utili all'attività di controllo da esercitare; semplificazione della procedura di notificazione; possibilità per gli interessati di consultare direttamente il registro.

I contenuti della notificazione sono stati determinati dal Garante stesso al momento in cui ne ha delineato il modello. Ciò consente un'estrema flessibilità e rapidità nell'adattare il modello di notificazione alle esigenze di tutela dei dati personali, senza dover ricorrere allo strumento normativo.

56

Per quanto riguarda la modalità di notificazione, l'art. 38 del Codice consente solo la compilazione e la trasmissione per via telematica, direttamente sul *server* del Garante. I diritti di segreteria possono essere corrisposti utilizzando *on line* la carta di credito (oppure tramite bonifico bancario o conto corrente postale). Infine, alla notificazione, prima della spedizione, deve essere apposta la firma digitale.

La procedura della notificazione

La procedura si sviluppa attraverso una sequenza di moduli *on line* che l'utente richiama entrando nel sito *web* del Garante e che sono corredati di spiegazioni, sia a carattere generale, sia sui singoli campi da compilare. L'utente può scegliere se consultare il registro, accedere alle istruzioni generali, procedere ad una notificazione (o modificarla), consultare le cd. *Faq*, accedere ad altri siti di interesse per la notificazione (es. elenco dei certificatori, organismi convenzionati).

La semplificazione per il notificante consiste nel fatto che, in qualsiasi Paese si trovi, può predisporre la notificazione, sospenderla, portarla a termine. In caso di mancanza di firma digitale, l'utente può recarsi presso operatori convenzionati (intermediari) ed utilizzare la loro firma digitale. Per permettere la notificazione tramite intermediari qualificati, il Garante ha stipulato apposite convenzioni con Poste S.p.A., l'Unione nazionale professionisti pratiche (Unappa) e l'Alar (Associazione lavoratori autonomi riuniti). È in fase di studio la stipula di altre convenzioni.

In caso di sospensione della notificazione, l'utente è in grado di riprenderla successivamente utilizzando un codice personale, che viene di volta in volta assegnato automaticamente. La procedura è validamente conclusa qualora sia stata completata l'apposita maschera con gli estremi del pagamento –il che permette di risolvere il problema del recupero dei diritti di segreteria non versati– e sia stata apposta la firma digitale.

La notificazione è *una tantum* e deve sempre precedere il trattamento; solo per i trattamenti di dati personali iniziati antecedentemente al 1° gennaio 2004, in sede di prima attuazione, è previsto il termine del 30 aprile per l'invio (art. 181, comma 1, lett. *c)* del Codice).

Al 31 marzo 2004 risultano regolarmente inviate n. 320 notificazioni, delle quali la gran parte sono prime notificazioni e provengono da soggetti privati.

Ovviamente i dati esposti sono provvisori e, allo stato attuale, non ancora altamente significativi; è difficile, infatti, fare al momento previsioni analitiche circa il preciso numero di notificazioni che andranno a costituire il registro dei trattamenti.

Il nuovo registro

Il nuovo registro, con la facoltà di interrogare l'intero archivio e di incrociare i dati dei singoli campi, offre un ausilio indispensabile al Garante per monitorare in maniera efficace il panorama dei trattamenti oggetto di notificazione, allo scopo di consentire sia il controllo da parte degli interessati, sia quello da parte della stessa Autorità, che può sfociare anche nell'adozione di specifici provvedimenti ad opera del Garante.

57 Il Servizio studi e documentazione

Il Garante ha ripreso e potenziato l'attività del Servizio studi e documentazione anche allo specifico scopo di promuovere indagini conoscitive volte all'acquisizione di informazioni provenienti dai diversi attori dei settori interessati all'applicazione della normativa sulla protezione dei dati.

L'Autorità considera infatti importante instaurare un dialogo con gli stessi operatori. Tale scambio consente, da una parte, a questi ultimi di ottenere chiarimenti sul sistema normativo in materia di tutela dei dati personali anche per orientare i propri investimenti in maniera conforme alla legge; dall'altra, è assai utile al Garante stesso per conoscere più approfonditamente le problematiche derivanti dall'applicazione della normativa sulla *privacy* nei diversi settori.

L'Autorità ha inoltre potenziato l'attività di documentazione e di ricerca promuovendo la formazione di *dossier* informativi su materie di interesse del Garante; la circolazione di tali *dossier* potrebbe, in prospettiva, essere pure allargata all'esterno dell'Ufficio.

L'attività di ricerca, tra l'altro, ha un ruolo determinante anche al fine di acquisire le conoscenze necessarie ogni qualvolta l'Autorità ritenga opportuno agire di proprio impulso, piuttosto che su attivazione esterna. Interventi di iniziativa propria del Garante appaiono del resto quanto mai opportuni alla luce dei molteplici eventi che ai vari livelli (normativo, scientifico, tecnologico) hanno delle ripercussioni sulla disciplina in materia di *privacy*.

È in questa prospettiva, ad esempio, che nel corso del periodo in esame si è ritenuta utile l'elaborazione di analisi variamente articolate in tema di *Radio frequency identification*, televisione interattiva, banche del cordone ombelicale e localizzazione.

58 Prospetto analitico (*)

Attivitò Garante / Atti e provvedimenti

Richieste di informazione e quesiti telefonici	38.180
Segnalazioni e reclami pervenuti	7.109
Quesiti pervenuti	994
Richieste di parere pervenute (parere *ex* art. 31 comma 2)	22
Richieste di autorizzazione pervenute	21
Notificazioni dei trattamenti previste dagli articoli 7, 16 e 28	9.791
Autorizzazioni generali al trattamento dei dati sensibili (art. 22) rilasciate per categorie di titolari e di trattamenti (art. 41, comma 7)	7
Autorizzazioni rilasciate a singoli destinatari	2
Risposte a quesiti	834
Risposte a segnalazioni/reclami	4.080
Pareri rilasciati in base all'art. 31, comma 2	14
Provvedimenti istruttori ai sensi dell'art. 32 comma 1	227
Procedimenti contenziosi definiti sulla base di ricorsi (art. 29)	775
Elementi forniti per la risposta del Governo a interrogazioni parlamentari	5
Comunicati stampa e dichiarazioni alla stampa	39
Notiziari settimanali pubblicati dal Servizio relazioni con i mezzi di informazione	54
Richieste di accesso e/o di verifica di dati esistenti nel Sistema d'informazione Schengen	480
Procedimenti relativi alle richieste di accesso e/o di verifica di dati esistenti nel Sistema d'informazione Schengen già definiti	464
Seminari e conferenze internazionali	10
Procedimenti ispettivi	69
Segnalazioni all'autorità giudiziaria	16

Servizi ispettivi

Ispezioni effettuate:	69
sopralluoghi ex art. 32, comma 1	61
accessi alle banche dati con decreto dell'autorità giudiziaria	7
accessi alle banche dati con assenso informato	1
Segnalazioni all'autorità giudiziaria:	16
per trattamento illecito (art. 35)	5
per omessa adozione misure minime di sicurezza (art. 36)	6
per false dichiarazioni al Garante	2
per inosservanza dei provvedimenti al Garante (art. 37)	3

Ufficio relazioni con il pubblico

Risposte fornite nel 2003 con *e-mail*, fax o lettera	5.754
Totale chiamate telefoniche ricevute	12.600
Richieste *e-mail* evase	4.338
Richieste con lettera evase	144
Richieste con fax evase	90
E-mail pervenute alla casella urp	6.060

(*) I riferimenti normativi sono relativi alla legge n. 675/1996
Periodo di riferimento 1° gennaio 2003 - 31 marzo 2004

Registro generale dei trattamenti

Legge 31 dicembre 1996, n. 675:	
notificazioni presenti nel Registro	330.000
lettere inviate per la regolarizzazione dei versamenti in conto corrente	11.832
richieste di accesso al Registro	210
richieste di copie della notificazione	410
somma relativa ai diritti di segreteria recuperati (in euro)	83.000
Decreto legislativo 30 giugno 2003, n. 196:	
nuove notificazioni telematiche validamente effettuate	320
nuove notificazioni telematiche sospese e in via di completamento	853

Servizio ricorsi

Decisioni al termine del procedimento	775
Tipo di decisioni adottate:	
non luogo a provvedere	331
inammissibilità	149
accoglimento	128
parziale accoglimento	110
infondati	57

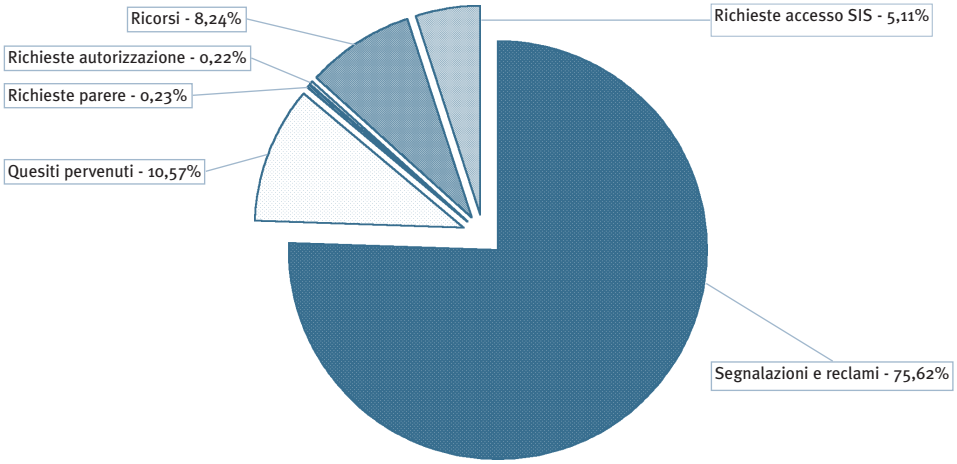
Call-center (1)

Quesiti sul nuovo codice	
Notificazioni (Obbligo, Compilazione, Modalità, etc.)	21
Documento programmatico sulla sicurezza	19
Quesiti sul codice in generale	13
Centrali Rischi Finanziarie	
Provvedimenti, richieste di cancellazioni, etc.	14
Tabulati telefonici in chiaro	
In entrata	8
In uscita	3
Richieste di accesso al S.I.S.	5
***Spamming* e comunicazioni commerciali e/o indesiderate**	
Provvedimenti e informazioni su cosa fare	9
Informazioni sulle pratiche	
In attivo	10
Concluse	4
Denunce su presunte violazioni	6
Informazioni su concorsi banditi	7
Varie richieste	
Partecipazione a seminari, convegni, corsi, etc.	2
Interviste, partecipazioni TV, etc...	1
Comunicare con segreterie e dipendenti dell'ufficio	14
Numeri telefonici, fax, *e-mail*	10
Informazioni sulle pubblicazioni (*Cd-Rom*, Bollettini, Libri, etc...)	5
Info generiche su ricorsi e notifiche (modulistica, c/c postali, etc...)	12
Altro	3

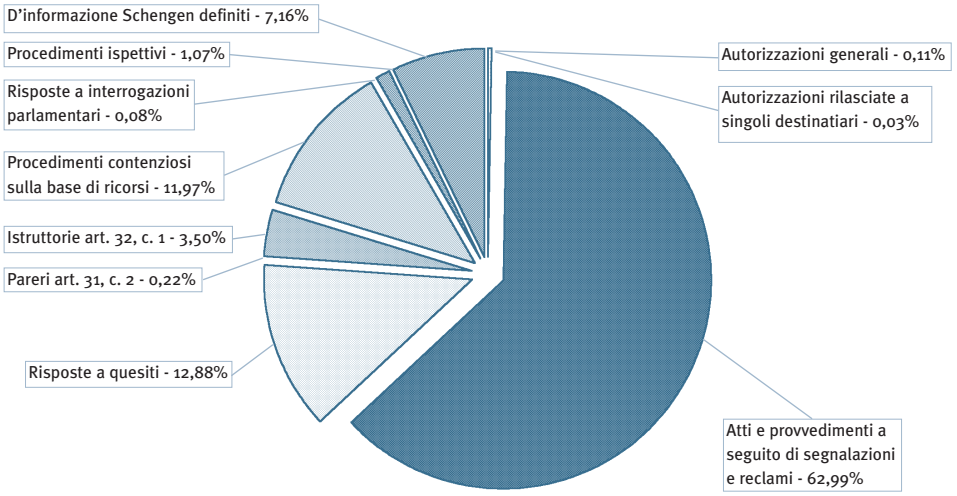
(1) Tipologia delle richieste medie su base giornaliera

58

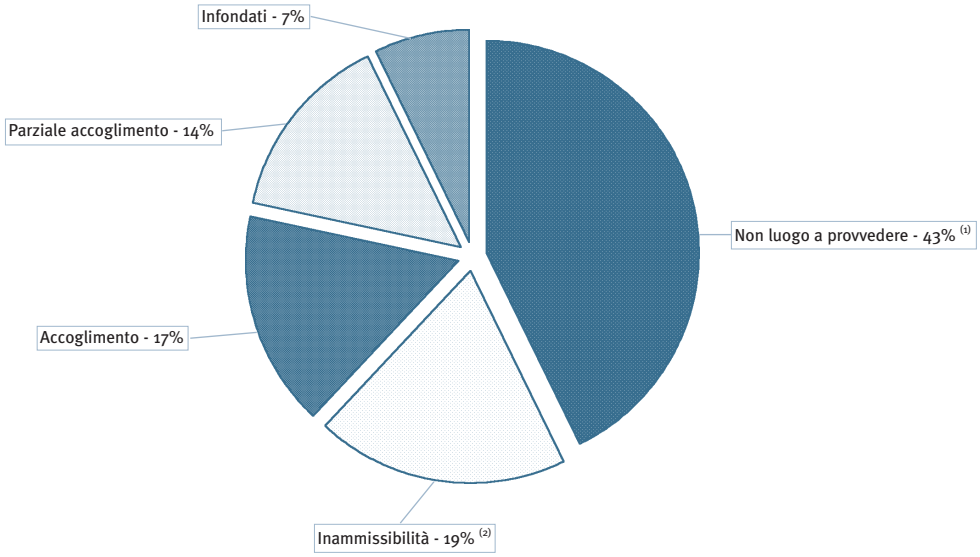
Atti e Provvedimenti richiesti
(esclusa assistenza telefonica e notificazioni)



Attività espletate



Statistica dei ricorsi



(1) Decisioni quasi integralmente riferite a casi nei quali il titolare/responsabile del trattamento ha aderito tardivamente alle richieste dell'interessato, nel caso del procedimento

(2) Casi di ricorsi formalmente irregolari e non regolarizzati, o nei quali il titolare/responsabile del trattamentro non era stato preventivamente interpellato; casi di richieste non previste dalla legge o di trattamenti cui non si applica la disciplina sui ricorsi

Servizi ispettivi