16 La sicurezza dei dati e dei sistemi

Anche nel corso del 2005 sono pervenute numerose richieste di chiarimenti circa la disciplina in materia di "misure minime" di sicurezza introdotta dal Codice.

Documento programmatico sulla sicurezza

Il Garante ha in numerose occasioni confermato le indicazioni già fornite agli operatori con una *nota* di carattere generale del 22 marzo 2004 [doc. *web* n. 771307] con riguardo alla natura del documento programmatico sulla sicurezza (d.p.s.). In particolare, si è precisato che: la redazione e/o l'aggiornamento del d.p.s. rientra tra le misure minime di sicurezza; di esso deve dotarsi qualsiasi titolare che effettui un trattamento di dati sensibili e/o giudiziari con strumenti elettronici; è sostenibile affermare che il d.p.s. sia una "nuova" misura minima, con la conseguenza che anche a questo adempimento è applicabile la disciplina transitoria (art. 180, comma 1, del Codice); deve essere conservato dal titolare presso la propria struttura, essendone doverosa l'esibizione o l'invio al Garante in caso di accertamenti ispettivi o su richiesta dell'Autorità (art. 34, comma 1, lett. *g)*, del Codice e regola 19 dell'Allegato B) al Codice).

I principi già affermati dall'Autorità con la citata *nota* del 22 marzo 2004 sono stati, da ultimo, ribaditi nella risposta ad un quesito della Confederazione nazionale dell'artigianato e delle piccole e medie imprese (Cna). Richiamandosi ai contributi già resi dall'Autorità in materia, con specifico riguardo alla redazione di una guida operativa disponibile sul sito del Garante [doc. *web* n. 1007740], volta ad agevolare la stesura e l'aggiornamento di un d.p.s. ancor più semplificato e impostato per le esigenze peculiari delle piccole e medie imprese, l'Ufficio del Garante si è reso disponibile a fornire ulteriori contributi alla categoria, precisando che eventuali provvedimenti di esonero o di deroga non rientrano tra i poteri attribuiti al Garante dal Codice (*Nota* 1 marzo 2005). Si è pertanto sviluppata una proficua collaborazione con la Confederazione che ha portato allo studio e alla definizione di modalità operative semplificate di stesura del d.p.s. reputate dal Cna maggiormente idonee a rappresentare le istanze e le caratteristiche dei piccoli e medi operatori del mercato.

Utilizzo di credenziali biometriche

Un ultimo caso interessante, a riprova del crescente interesse all'impiego di tecniche di autenticazione biometrica, ha riguardato il quesito di una multinazionale operante nel settore della promozione e vendita di prodotti farmaceutici, riguardo al progetto di attivazione di un sistema di credenziali di autenticazione dei propri agenti ed informatori scientifici basato sull'impiego delle loro impronte digitali.

In base alla dettagliata descrizione fornita dalla società è risultato che gli agenti (tutti incaricati del trattamento dei dati del proprio pacchetto clienti) ricevono in dotazione dalla società un *computer* portatile che contiene, come dotazione *standard*, un dispositivo per la rilevazione delle impronte digitali gestito da un *software* installato sul *computer*. Il dispositivo di riconoscimento e il relativo *software*, presenti su ciascun *computer*, sono attivabili solo dall'agente che voglia avvalersene. L'immagine dell'impronta viene registrata esclusivamente su un'area protetta del disco fisso del *computer* stesso ed associata ad una *password* scelta dall'utente e solo dallo stesso modificabile successivamente, senza alcuna centralizzazione in archivi aziendali o possibilità di accesso da parte della società al dato biometrico (anche in caso di malfunzionamento, il *computer* viene reso alla direzione informatica della

società che formatta il disco cancellando l'impronta registrata), il quale resta nell'esclusivo controllo dell'utente-incaricato che può cancellarlo in qualsiasi momento.

Nel caso di specie non è apparsa necessaria la valutazione preventiva del Garante tenuto conto delle caratteristiche del tutto peculiari del progetto e, soprattutto, della finalità di autenticazione informatica perseguita. L'adozione di un sistema di autenticazione informatica (mediante il quale gli incaricati dotati di apposite credenziali possono effettuare specifici trattamenti di dati personali), conforme ai requisiti tecnici indicati dalle regole 1.11. dell'Allegato B) al Codice, costituisce infatti una misura minima di sicurezza che il titolare, il responsabile (ove designato) e l'incaricato sono tenuti ad utilizzare (art. 34, comma 1, lett. *a)*, del Codice). Tali credenziali di autenticazione, come nel caso di specie, possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o a una parola chiave.

17 Registro dei trattamenti

Il registro dei trattamenti previsto dall'art. 37 del Codice ha consolidato la propria veste nel corso del 2005, nella nuova connotazione informatica che ha fornito esiti ancora più positivi in termini di efficienza, efficacia, economicità e rapidità nel monitoraggio.

Nel registro confluiscono come è noto le notificazioni del trattamento di dati personali, le quali pervengono al Garante secondo le procedure previste dall'art. 38. L'intera notificazione (compresa la firma) avviene telematicamente. Il registro è pubblico e chiunque può consultarlo, tramite il sito dell'Autorità, mediante un apposito motore di ricerca.

I contenuti della notificazione sono limitati alle informazioni essenziali sui trattamenti effettuati; rendono però possibile effettuare ampi controlli, estrazioni di dati ed elaborazioni statistiche. Il registro viene pertanto utilizzato dall'Autorità a fini di monitoraggio, controllo e orientamento delle attività ispettive in determinati settori.

Gli obiettivi posti con il nuovo sistema di notificazione (flessibilità del sistema; contenimento delle notizie da richiedere e ai titolari; semplificazione della procedura; pubblicità completa del registro dei trattamenti), la filosofia e il modello posti alla base della procedura, sono stati in seguito tenuti presenti per altre attività legate ai trattamenti che presentano rischi specifici *ex* art. 17 del Codice (verifica preliminare del Garante).

Preme evidenziare, rispetto all'esperienza di applicazione relativa all'anno precedente, il fattivo ausilio offerto all'utenza che ha avuto occasione di sollecitare ed ottenere chiarimenti dal dipartimento dell'Ufficio che vi è preposto.

Tra i momenti istituzionali di contatto con l'utenza si segnala la possibilità, offerta al notificante, di sospendere la notificazione in qualsiasi momento e di continuarla successivamente, utilizzando un codice numerico che viene spedito automaticamente dall'Ufficio, con due vantaggi immediati:

- l'utente può indicare il motivo della sospensione; il dipartimento è messo in grado di intervenire tempestivamente nel caso in cui l'utente stia effettuando una notificazione non dovuta, sia in difficoltà o non abbia compreso alcuni elementi, ovvero semplicemente intenda essere "guidato" o agevolato nella compilazione;
- viene così reso noto all'utente l'indirizzo *e-mail* dell'Ufficio, in seguito utilizzato frequentemente per altre richieste e segnalazioni.

Le difficoltà incontrate dagli utenti nella compilazione della notificazione (trattasi di un fenomeno comunque assai marginale) attengono –salvo quanto si dirà di seguito– quasi esclusivamente all'apposizione della firma digitale (possesso di un certificato scaduto, mancata lettura delle istruzioni, ecc.).

A questi elementi, deve aggiungersi l'esperienza che il dipartimento può continuare ad offrire rispetto ad alcuni dubbi interpretativi emersi nell'individuazione dei soggetti obbligati alla notificazione, anche dopo il provvedimento di esonero del Garante del 2004 e le connesse delucidazioni fornite con una risposta di ordine generale a quesiti (*Provv.* n. 1 del 31 marzo 2004 [doc. *web* n. 852561]; *Nota* 23 aprile 2004 [doc. *web* n. 993385]; *v.* anche *Nota* 26 aprile 2004 [doc. *web* n. 996680], visto che l'art. 37 del Codice descrive il suo ambito di applicazione con una disciplina

generale senza entrare in innumerevoli dettagli legati alle migliaia di diversi titolari del trattamento e di banche dati.

Nel 2005, a parte i picchi registratisi in occasione della scadenza di taluni termini per l'adempimento ad obblighi previsti dal Codice (a volte erroneamente associati all'obbligo di notificazione, come è avvenuto per la redazione del documento programmatico sulla sicurezza), il numero di notificazioni giornaliere ha oscillato tra le sei e le sette.

Le tabelle statistiche riportate in altra parte della presente relazione forniscono altri elementi utili per valutare come il registro si evolve. Ad esempio, dalle tabelle relative alle singole tipologie di trattamenti notificati, si riscontra una netta prevalenza di quelli riferiti alla salute, alla profilazione e alla solvibilità economica rispetto ad altri trattamenti.

Il versamento dei diritti di segreteria (euro 150,00 per ciascuna notificazione) resta possibile utilizzando *on-line* una carta di credito (circa il 22% dei casi) o con altri sistemi quali il bonifico bancario (30 %) o il conto corrente postale (48 %).

Sono stati poi previsti particolari accorgimenti sul piano della sicurezza: un messaggio di avvenuta ricezione della notificazione viene spedito dal dipartimento al notificante, unitamente ad un codice segreto (codice univoco del notificante, Cun) che permette l'eventuale modifica della precedente notificazione o la sua cessazione. Tale aspetto è monitorato costantemente ed eventuali anomalie sono segnalate ad altri dipartimenti dell'Ufficio.

Per agevolare il compito di apposizione della firma digitale, l'Autorità continua inoltre a dare applicazioni ad alcune convenzioni con Poste italiane S.p.A., Unappa (Unione nazionale professionisti pratiche amministrative), Alar (Associazione lavoratori autonomi riuniti) e Comune di Livorno, per permettere la notificazione, tramite l'ausilio di intermediari qualificati, anche a chi non voglia o non possa dotarsi del *kit* di firma digitale. Altri tentativi intrapresi dall'Autorità per estendere le convenzioni ad altri soggetti (banche, comuni, camere di commercio) non hanno per ora riscontrato l'interesse degli interlocutori.

Il notificante può inoltre rivolgersi a soggetti di fiducia (commercialisti, avvocati, notai, conoscenti, purché in possesso di chiave per la firma digitale), senza limitazioni. Il costo del servizio reso dall'intermediario convenzionato, consistente nella stampa della notificazione, nell'apposizione della firma digitale, nell'inserimento di eventuali riferimenti ai diritti di segreteria e nell'invio del *file* è pari ad un massimo di euro 25,00 che l'utente paga direttamente all'intermediario.

Alla data del 31 dicembre 2005, risultavano inoltrate 6.439 notificazioni tramite gli intermediari convenzionati, con prevalenza dell'utilizzo di Poste italiane S.p.A.

Va operato un cenno alla possibilità, consentita dal sistema in uso, di monitorare il flusso dei dati in arrivo e di compiere ricerche ed elaborazioni di statistiche, anche al fine di riscontrare richieste dei dipartimenti dell'Ufficio operanti nel settore giuridico, in particolare allo scopo di coadiuvare l'attività ispettiva. Risultano in particolare interessanti le interrogazioni volte ad estrarre, all'interno delle tabelle descrittive dei trattamenti, le categorie di dati, di interessati, le finalità e le modalità del trattamento, l'eventuale comunicazione dei dati e l'utilizzazione, per il trattamento dei dati, di un sito *web*.

A titolo sperimentale, il dipartimento ha assunto infine l'iniziativa di inviare automaticamente un messaggio di posta elettronica ad alcuni dipartimenti interni (compreso quello ispettivo), segnalando volta per volta l'avvenuta notificazione di trattamenti più significativi (*ad es.*, il trattamento di dati genetici trasferiti all'estero).

18 La trattazione dei ricorsi

18.1. *Considerazioni generali*

Uno strumento di tutela agile e "multiuso": questa definizione, nella sua sinteticità, sembra fotografare efficacemente il ruolo e la funzione che il ricorso, ai sensi degli artt. 145 e ss. del Codice, è venuto ad assumere nel quadro più generale della tutela dei dati personali. L'analisi del numero e della tipologia dei ricorsi proposti nel 2005 attesta la veridicità della definizione a conferma di un *trend* chiaramente emerso già negli ultimi anni. L'esame dell'ampia casistica affrontata in questi mesi dal Garante sottolinea, poi, l'utile funzione di "antenna" di questo strumento di tutela che segnala tempestivamente nuove frontiere della protezione dei dati e, al tempo stesso, evidenzia settori di maggiore "utilizzo" delle opportunità di tutela che il Codice offre.

In questo senso, lo sguardo agli ultimi due anni mette in luce un'autentica "esplosione" dei ricorsi relativi al trattamento di dati effettuato da banche e società finanziarie, con particolare riferimento alla comunicazione e conservazione delle informazioni negli archivi dei Sic (sistemi di informazioni creditizie), già comunemente noti come "centrali rischi private". La vicenda è significativa e rappresenta un interessante esempio di intreccio fra la dinamica sociale ed economica (la crescita esponenziale del credito al consumo in connessione con una fase di limitata disponibilità reddituale delle famiglie) e lo sforzo di disciplina di un settore che era privo di una normativa organica di riferimento.

In questo quadro sono emerse con forza le esigenze di tutela dei dati personali dei consumatori (esattezza dei dati, tempestività degli aggiornamenti, chiarezza informativa dei meccanismi di segnalazione nei citati Sic, definizione dei tempi di conservazione delle posizioni, ecc.) che, in equilibrato contemperamento con le esigenze di garanzia e stabilità degli operatori finanziari, hanno ispirato la disciplina ora affidata, essenzialmente, all'apposito codice di deontologia e di buona condotta di settore (*Provv.* n. 8 del 16 novembre 2004 [doc. *web* n. 1070713] e connesso provvedimento sul bilanciamento di interessi, *Provv.* n. 9 del 16 novembre 2004 [doc. *web* n. 1070779]).

Anche ricorsi presentati in altri campi hanno, parimenti, permesso di far emergere aspetti nuovi. Ne sono testimonianza diverse decisioni che hanno avuto a tema i trattamenti in Internet, così come l'utilizzo dei dati personali da parte degli operatori telefonici o le nuove forme che può assumere, nel quadro tecnologico attuale, il controllo sui lavoratori (*v.* par. 18.3).

18.2. *Profili procedurali*

Venendo in primo luogo a profili più strettamente procedurali, è possibile rilevare alcune linee di tendenza ormai consolidate.

Il ricorso, specie se proposto con l'assistenza di un legale, appare sempre più spesso utilizzato come "tassello" di una più ampia strategia difensiva: diventa, cioè, il veicolo privilegiato per acquisire le informazioni indispensabili alla tutela della posizione di un soggetto o per contestare, sotto lo specifico profilo della protezione

dei dati, operazioni poste in essere, ad esempio, nell'ambito di un rapporto contrattuale. In questo quadro, acquisisce rilievo l'intero "catalogo" dei diritti previsti dall'art. 7 del Codice per la cui tutela il ricorso viene proposto. Lo stesso, quindi, non è più funzionale solamente alla tutela del diritto di accesso ai dati, ma viene frequentemente e consapevolmente utilizzato per accertare l'origine dei dati personali, le finalità o le modalità di uno specifico trattamento o per sollecitare, in caso di violazione di legge, la cancellazione dei dati stessi.

La più ampia conoscenza dei diritti di cui all'art. 7 del Codice e della loro tutelabilità con lo strumento del ricorso ha fatto poi sviluppare, negli ultimi mesi, l'attività di terzi (talvolta associazioni di consumatori, in altri casi soggetti operanti in veste professionale di delegato) che hanno promosso numerose richieste volte ad accedere ai dati e ad ottenere successivamente la loro cancellazione, con particolare riferimento alle informazioni conservate negli archivi dei già citati Sic.

In alcuni casi, peraltro, la procedura del ricorso è dovuta passare attraverso una necessaria fase di regolarizzazione, secondo il disposto dell'art. 148, comma 2, del Codice, in quanto –ad esempio– le procure rilasciate ai soggetti incaricati di presentare ricorso in nome dell'interessato non erano accompagnate dalla necessaria firma autenticata dello stesso. In altri casi, la presentazione del ricorso è avvenuta senza essere stata preceduta dalla doverosa presentazione di un'istanza formulata ai sensi del citato art. 7 del Codice, allegando solamente l'esistenza di generici motivi di urgenza.

Al riguardo, il Garante è pervenuto a declaratorie di inammissibilità (*ad es.*, *Provv.* 14 luglio 2005 [doc. *web* n. 1157708]), ricordando che la presentazione in via di urgenza del ricorso è possibile, ai sensi dell'art. 146, comma 1, del Codice, solo fornendo prova del pregiudizio imminente e irreparabile che avrebbe impedito di procedere all'invio dell'interpello preventivo e di attendere il decorso dei quindici giorni previsti dalle citate disposizioni del Codice.

È stata altresì richiamata più volte l'attenzione degli interessati sul disposto dell'art. 5, comma 3, del Codice secondo il quale "il trattamento dei dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del (…) Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione". Ciò ha reso inammissibile la presentazione di ricorsi incentrati su ipotesi di trattamento di dati relativi, ad esempio, a controversie fra vicini per installare impianti di sorveglianza (*Provv.* 19 ottobre 2005 [doc. *web* n. 1191132]), ferma restando l'applicazione del Codice quando il trattamento è risultato effettuato nell'ambito di un'attività professionale ed economica (*Provv.* 27 ottobre 2005 [doc. *web* n. 1195275]).

Infine, qualche breve annotazione statistica: nel corso dell'anno solare 2005, come evidenziato anche nelle tabelle riportate in altra parte della presente *Relazione*, il Garante ha definito la trattazione di 634 ricorsi.

18.3. *Brevi cenni sulla casistica*

Come in passato, si offre in questo paragrafo una succinta sintesi sui principali temi affrontati con le decisioni in materia di ricorsi, rimandando alle altre parti della relazione per l'ulteriore esame di alcune problematiche sottese alle decisioni stesse.

Diffusione di dati personali tramite siti Internet istituzionali

Meritano anzitutto di essere ricordate due vicende che hanno riguardato la diffusione di dati personali tramite i siti Internet di due autorità amministrative indipendenti.

Nel primo caso (*Provv.* 10 novembre 2004 [doc. *web* n. 1116068]; *cfr.* anche *Newsletter* 21-27 marzo 2005), il ricorso concerneva l'opposizione per motivi legittimi

al trattamento di dati personali contenuti in alcune decisioni (una delle quali risalente nel tempo) adottate dall'Autorità garante della concorrenza e del mercato pubblicate, tra l'altro, sul sito Internet della medesima autorità. Tali decisioni erano state correttamente pubblicate, in adempimento di specifici obblighi normativi, in relazione all'attività di un operatore economico sanzionato per pubblicità ingannevole.

Il provvedimento del Garante ha esaminato le implicazioni della conoscibilità via Internet di tali provvedimenti (specie in relazione alla possibilità di rinvenire agevolmente tali informazioni tramite l'utilizzo di motori di ricerca). Tale forma di diffusione dei dati può comportare infatti un sacrificio sproporzionato dei diritti dell'interessato, specie quando si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le finalità perseguite.

La questione affrontata nel caso di specie è risultata particolarmente delicata, richiedendo il contemperamento fra il dovere di informazione da parte di organi pubblici sulla propria attività, il diritto degli utenti e dei consumatori di conoscere l'esito di determinati provvedimenti sanzionatori e le non convergenti aspettative dei soggetti cui si riferiscono i dati "sanzionatori" diffusi. Con la decisione adottata, il Garante ha tra l'altro riconosciuto il pieno diritto-dovere dell'Antitrust di continuare a pubblicare i propri provvedimenti sul relativo sito *web*, modulando però nel tempo il periodo entro il quale le decisioni del tipo di quella in questione potranno essere direttamente individuabili nel sito Internet dell'Autorità tramite motori di ricerca esterni al sito stesso (non è stato posto in discussione un sistema di ricerca rapida delle decisioni all'interno del medesimo sito).

In un diverso caso, esaminato con decisione del 19 maggio 2005 [doc. *web* n. 1151205], l'Autorità ha invece constatato come non fosse giustificata da un idoneo presupposto normativo la diffusione indifferenziata, tramite il sito Internet dell'Autorità per la vigilanza sui lavori pubblici, di alcune specifiche informazioni contenute nel "Casellario informatico delle imprese qualificate". Per espressa limitazione derivante dalla specifica disciplina applicabile al caso di specie, tali dati devono essere resi agevolmente disponibili, ma solo alle stazioni appaltanti, e non possono essere invece oggetto di una diffusione indifferenziata in rete (*v. amplius* par. 2.5).

Le citate fattispecie, venute ad evidenza in conseguenza delle straordinarie potenzialità diffusive della rete Internet e dei meccanismi di "navigazione" nella stessa, hanno così fatto emergere prepotentemente e il tema del "diritto all'oblìo" e della sua declinazione nel presente quadro tecnologico.

Altri trattamenti svolti da soggetti pubblici

Vari, e molto differenziati tra loro, sono risultati i ricorsi che hanno riguardato trattamenti effettuati da pubbliche amministrazioni. Fra le principali problematiche emerse si può ricordare la decisione del 3 novembre 2005 [doc. *web* n. 1198422] con la quale il Garante ha riconosciuto come lecite e conformi alle disposizioni del Codice le modalità di acquisizione (tramite le liste elettorali) e di successivo utilizzo dei dati personali impiegati per inviare una pubblicazione istituzionale curata dal Ministero della salute.

Con altre decisioni (in particolare, quelle del 16 giugno 2005 [doc. *web* n. 1149999] e del 21 dicembre 2005 [doc. *web* n. 1217532]), sono stati esaminati nuovamente i profili concernenti l'accesso ai dati personali di dipendenti di pubbliche amministrazioni; ciò, richiamando le corrette modalità di riscontro a tali istanze delineate dall'art. 10 del Codice e le linee differenziali rispetto al diritto di accesso ad atti e documenti amministrativi disciplinato dalla l. n. 241/1990.

Sempre con riferimento a problematiche concernenti impiegati pubblici va ricordato il *provvedimento* del 30 novembre 2005 [doc. *web* n. 1215256] con cui è stata esaminata una vicenda relativa alla lamentata diffusione di dati personali sensibili a seguito dell'affissione di una determinazione dirigenziale all'albo pretorio di un

Comune. Con *provvedimento* del 21 dicembre 2005 [doc. *web* n. 1219054] l'attenzione è stata invece rivolta allo svolgimento di un procedimento disciplinare, sempre nell'ambito di un'amministrazione comunale.

I casi in cui i dati personali degli interessati sono stati oggetto di comunicazione ad altri soggetti pubblici o a privati, nonché le ipotesi di diffusione dei medesimi dati (a mezzo affissione all'albo pretorio, pubblicazione a stampa, divulgazione tramite la rete Internet, ecc.), sono stati, quindi, le principali ipotesi che hanno formato oggetto del contenzioso dinanzi all'Autorità in relazione all'attività degli enti pubblici. Ciò, a conferma della particolare sensibilità degli interessati per quelle operazioni di trattamento (comunicazione e diffusione appunto) che moltiplicano le potenzialità lesive di un eventuale uso illecito dei dati.

Trattamenti svolti presso sistemi di informazioni creditizie

Come già ricordato, il settore rispetto al quale si è registrato il maggior numero di ricorsi è stato quello dei Sic. Il 2005 ha rappresentato il primo anno di applicazione delle nuove disposizioni introdotte con il codice deontologico di settore e le decisioni adottate in proposito sono state l'occasione per una verifica del livello di conoscenza e di applicazione delle stesse. Forse in ragione di una non perfetta conoscenza del predetto codice deontologico e del connesso provvedimento di bilanciamento degli interessi, sono pervenuti molti ricorsi incentrati su richieste di "cancellazione totale" delle posizioni riferite ad un interessato, senza che sussistessero, però, i presupposti per un loro accoglimento: ciò, pur in presenza di ritardi o di altre patologie nei rimborsi dei finanziamenti o in ragione di regolarizzazioni molto recenti e destinate quindi a rimanere annotate negli archivi in questione per il lasso temporale previsto dal predetto codice deontologico.

I ricorsi proposti nei confronti dei gestori dei Sic hanno dato luogo spesso a decisioni molto articolate, soprattutto in presenza di numerose posizioni segnalate nelle relative banche dati dei Sic, riferite a prestiti, mutui, carte di credito a saldo o rateali, ecc.

Occorre infatti discernere fra posizioni "positive" (relative a finanziamenti regolari di cui è possibile chiedere la cancellazione previa revoca del consenso al trattamento dei relativi dati) e "negative" (per le quali opera il già richiamato provvedimento sul bilanciamento degli interessi e che possono essere conservate negli archivi dei Sic nel rispetto dell'articolata tempistica che il codice deontologico ha delineato).

Altri archivi contenenti dati relativi ad attività economiche e finanziarie

Numerosi ricorsi sono stati rivolti nei confronti di altri archivi di dati e relativi ad attività economiche.

L'esigenza di assicurare un ordinato svolgimento dei rapporti economici, di permettere una rilevazione puntuale dei rischi creditizi, di garantire la stabilità del sistema finanziario e di prevenire fenomeni di sovraindebitamento ha portato negli ultimi anni sia ad un'estensione del tipo di operazioni e/o di "patologie" finanziarie oggetto di monitoraggio, sia ad un rapido adeguamento alle procedure informatiche dei sistemi di rilevazione, al fine di garantire un maggior livello di affidabilità e trasparenza di questi ultimi.

Il soggetto più antico operante nel settore è, come noto, la "centrale rischi" gestita dalla Banca d'Italia, istituita già nel 1964 per raccogliere le segnalazioni relative ai finanziamenti di importo pari o superiore attualmente a euro 75.000 e ai crediti in "sofferenza". Nei confronti di tale soggetto (art. 8, comma 2, lett. *d)*, del Codice), non è però esperibile il ricorso *ex* art. 145 del Codice, pur rimanendo la possibilità di proporre una segnalazione all'Autorità. Ciò spiega perché alcuni ricorsi pervenuti in ordine a tali trattamenti siano stati dichiarati inammissibili.

Le istanze rivolte *ex* art. 7, e gli eventuali, successivi ricorsi, possono essere invece proposti nei confronti dei trattamenti effettuati presso "la centrale rischi di

importo contenuto" gestita, in conformità alle istruzioni della Banca d'Italia, da S.i.a. S.p.A. cui possono essere rivolte le istanze citate.

Con riferimento ai finanziamenti di più limitato importo ricadenti prevalentemente nel novero del credito al consumo operano, infine, le già indicate disposizioni sui Sic, soggetti rispetto ai quali, come detto, si è concentrato in maggior misura il contenzioso su ricorso del 2005.

Tipologicamente diverso è invece il fenomeno (oggetto di attenzione in numerosi ricorsi) della conservazione in appositi archivi distinti da quelli relativi ai Sic, di altri tipi di informazioni quali dati personali tratti dai registri immobiliari e dagli archivi delle ex-conservatorie, ai quali si applica quindi il disposto dell'art. 24, comma 1, lett. *c)*, del Codice.

A tale riguardo (nei numerosi casi che hanno riguardato richieste di cancellazione rivolte a Crif S.p.A.) l'Autorità ha preso atto della già avvenuta sospensione della loro visualizzazione nella banca dati, anche in relazione alle intervenute modifiche legislative concernenti i nuovi presupposti (oggetto peraltro di ampio contenzioso giudiziario) per la riutilizzazione commerciale di tali dati di cui all'art. 1, commi 368/371, l. n. 311/2004, nonché all'art. 1, comma 5, d.l. 10 gennaio 2006, n. 2, convertito con l. 11 marzo 2006, n. 81.

19 Contenzioso giurisdizionale

19.1. *Considerazioni generali*

Come già osservato nella *Relazione* 2004 (p. 118), l'art. 152 del Codice ha introdotto nel sistema processuale italiano un procedimento a cognizione ordinaria, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali e connotato da una procedura snella, capace di fornire al diritto alla riservatezza una tutela specifica e tempestiva.

L'opportunità di tale impianto normativo ha avuto riscontro nel numero delle azioni proposte direttamente avanti all'autorità giudiziaria, in via alternativa al ricorso presentato in sede amministrativa al Garante. Nel corso del 2005 si è registrata la notifica al Garante, secondo quanto prescritto dal comma 7 dell'art. 152 del Codice, di un numero di ricorsi all'autorità giudiziaria, non coinvolgenti direttamente pronunce dell'Autorità, significativamente superiore a quello registrato nell'anno precedente: a fronte di trentadue controversie introdotte nel 2004, infatti, nel 2005 sono stati notificati al Garante settantaquattro ricorsi, con un incremento quantitativo superiore al 120%.

La crescita dei ricorsi avanti l'autorità giudiziaria, e delle relative decisioni, attribuiscono sicuro rilievo a due novità introdotte dal Codice. L'obbligo imposto dal citato comma 7 di notificare al Garante i ricorsi presentati all'autorità giudiziaria concernenti tutte le controversie relative all'applicazione del Codice (non solo di quelle in cui sia proposta opposizione avverso i provvedimenti dell'Autorità), unitamente alla trasmissione, a cura delle cancellerie, di copia dei provvedimenti emessi a definizione dei relativi giudizi o in materia di criminalità informatica (art. 154, comma 6), consentono al Garante, oltre che di intervenire nelle controversie in cui, pur non essendo direttamente coinvolto, sono in discussione profili di carattere generale, di avere un'ampia informazione sull'evoluzione della giurisprudenza nella materia. Ciò anche al fine di adottare eventuali provvedimenti amministrativi e di segnalare al Parlamento e al Governo gli interventi normativi opportuni per tutelare i diritti e le libertà fondamentali correlati alla protezione dei dati (art. 154, comma 1, lett. *f)*, del Codice).

19.2. *Profili procedurali*

L'art. 152 del Codice ha ribadito che tutte le controversie riguardanti l'applicazione del Codice sono devolute all'autorità giudiziaria ordinaria, precisando che l'azione deve proporsi con ricorso da depositarsi "nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento" (comma 2): nel 2005 si sono però registrati ancora alcuni casi di mancato rispetto del dettato normativo.

Controversie instaurate erroneamente dinanzi al giudice amministrativo

Si è rivolta al Tribunale amministrativo del Lazio una società operante nel settore del *direct marketing* chiedendo l'annullamento, previa sospensione, del *provvedimento* del Garante del 15 luglio 2004 [doc. *web* n. 1032381] concernente l'individuazione delle modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi telefonici cartacei o elettronici. Costituitasi in giudizio, l'Autorità ha eccepito il difetto di giurisdizione del giudice amministrativo, alla luce della ricordata chiara dizione normativa. Con ordinanza del 25 maggio 2005, il

Tribunale ha respinto la domanda di sospensione presentata dai ricorrenti, rimettendo ogni decisione, anche in ordine alla questione della giurisdizione, alla fase di merito.

Foro competente

In ordine al foro competente non sono mancate decisioni con le quali, in accoglimento di eccezioni fondate sul luogo di residenza del titolare del trattamento, i giudizi sono stati rimessi al tribunale competente per territorio. In tal senso si sono pronunciati, fra gli altri, il Tribunale di Roma (sentenza del 10 gennaio 2006) e quello di Viterbo (sentenza n. 767 del 7 settembre 2005). Con analoga decisione il Tribunale di Napoli (sentenza n. 11727 del 25 novembre 2005) ha ribadito la natura esclusiva ed inderogabile del foro stabilito dall'art. 152, dichiarando manifestamente infondata la questione di legittimità costituzionale in ordine alla scelta effettuata dal legislatore ed escludendo, in particolare, che in materia del trattamento dei dati personali possa farsi applicazione alternativa del foro del consumatore di cui all'art. 1469-*bis*, comma 3, c.c., disposizione ora abrogata dal d.lg. 6 settembre 2005, n. 206 (in *G.U.* 8 ottobre 2005, n. 235, *S.O.* n. 162/L) che ha stabilito (art. 63) il foro del consumatore nel luogo di residenza o di domicilio di questi, se ubicato nel territorio dello Stato.

Incompetenza del giudice di pace

Infine, il Garante si è costituito in vari giudizi (introdotti, in particolare, nel 2005 avanti al Giudice di pace di Taranto) al fine di far valere il rispetto della competenza del tribunale ordinario nella materia della protezione dei dati personali.

19.3. *Profili di merito*

Giova in primo luogo ricordare due casi particolarmente significativi, costituiti da decisioni assunte in sede di opposizione a provvedimenti del Garante, che hanno confermato orientamenti di merito sempre sostenuti dall'Autorità.

Con riferimento alle vicende (che hanno dato origine in passato a decisioni contrastanti dell'autorità giudiziaria) relative alla riconducibilità delle valutazioni alla nozione di "dato personale" fornita dalla l. n. 675/1996 e ribadita dal Codice, il Tribunale di Roma, facendo seguito ad una sua precedente analoga decisione, e confermando il provvedimento con cui il Garante aveva ordinato ad una compagnia di assicurazioni di comunicare all'interessato i dati personali, anche di natura valutativa, contenuti in una perizia medico-legale finalizzata alla quantificazione del risarcimento del danno, ha riconosciuto che l'interessato può esercitare il diritto di accesso ai dati personali che lo riguardano anche con riferimento a dati valutativi e, in particolare, alle valutazioni espresse in perizie medico-legali (sentenza n. 1832 del 25 gennaio 2006).

Merita di essere sottolineato che alla questione della riconducibilità dei dati valutativi alla nozione di "dato personale" il legislatore ha dedicato, dopo l'iniziale contenzioso sorto, una specifica disciplina attraverso la soluzione adottata nell'art. 8, comma 4, del Codice.

In altra fattispecie, concernente l'opposizione al provvedimento con cui il Garante, facendo seguito a precedenti decisioni di analogo tenore, ha vietato alla società editrice di un quotidiano l'ulteriore diffusione di fotografie di persone sottoposte a misure restrittive della libertà personale, il Tribunale di Milano, con sentenza n. 12746 del 9 novembre 2004 ha statuito che le foto segnaletiche rientrano nelle immagini indicative e riproduttive dello stato di detenzione del soggetto, quindi non pubblicabili perché idonee a lederne la dignità.

Infine, deve segnalarsi che, con la sentenza n. 14390 del 2005, la Corte di Cassazione ha riaffermato la necessità per i soggetti pubblici di adottare, nei casi previsti dall'art. 20, comma 2, del Codice, gli atti di natura regolamentare che specifichino i tipi di dati sensibili e le operazioni eseguibili, per procedere lecitamente al trattamento dei dati sensibili.

19.4. *Opposizione ai provvedimenti del Garante*

Il 2005 ha registrato quindici opposizioni ad altrettanti provvedimenti del Garante, quattordici delle quali hanno riguardato decisioni adottate su ricorso. In un caso, l'opposizione è stata proposta nei confronti della pronuncia dell'Autorità avente ad oggetto la disciplina dei nuovi elenchi telefonici. L'Autorità si è sempre costituita in questi giudizi.

Quattro opposizioni, di identico tenore, sono state proposte da due società che svolgono attività nel settore della riutilizzazione a fini commerciali dei dati acquisiti dagli archivi catastali o dai pubblici registri immobiliari, tenuti dagli uffici dell'Agenzia del territorio. La materia è stata innovata dalla l. n. 311/2004 (legge finanziaria 2005), che al comma 371 dell'art. 1 ha vietato tale riutilizzazione –precedentemente libera–, salva la stipula di apposite convenzioni con l'Agenzia. In conseguenza di detta innovazione il Garante, nelle more dell'adozione del codice deontologico per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (art. 61 del Codice), cui le convenzioni dovranno ispirarsi, ha accolto i ricorsi con i quali gli interessati avevano chiesto la cancellazione delle informazioni che li riguardavano, conservate presso dette società.

Si deve rilevare che la nuova normativa non ha ancora ricevuto univoca interpretazione da parte della giurisprudenza. Le due opposizioni finora definite hanno infatti registrato esiti contraddittori; nel primo caso il provvedimento del Garante è stato confermato, mentre nell'altro è stato annullato.

Per quanto riguarda le altre opposizioni presentate nel 2005 e quelle relative anche ad anni precedenti, della cui pendenza si è dato conto nella *Relazione* 2004 (p. 121), le decisioni dell'autorità giudiziaria hanno tutte confermato le pronunce dell'Autorità.

In particolare, è stato confermata la validità delle determinazioni adottate con il provvedimento del Garante di divieto all'Inail del trattamento di dati contenuti nei certificati medici, acquisiti dall'Istituto al di fuori delle ipotesi normativamente consentite, nell'ambito della procedura avviata dall'assicurata per il riconoscimento di malattia professionale (Tribunale di Genova, sentenza n. 4982 del 22 dicembre 2005).

In tre occasioni, hanno trovato conferma i provvedimenti con i quali l'Autorità ha ordinato ad alcuni istituti di credito di comunicare i dati richiesti, negati perché relativi a rapporti bancari intrattenuti da persone defunte di cui gli interessati erano eredi o perché subordinati al pagamento di una somma di denaro richiesta ai sensi dell'art. 119 d.lg. n. 385/1993. In questa seconda decisione è stato ribadito, in particolare, che l'esercizio dei diritti attribuiti dal Codice in materia di dati personali è gratuito e non può essere confuso con il diverso diritto di ottenere copia della documentazione bancaria, condizionato al rispetto delle norme poste dal citato d.lg. n. 385/1993.

Sono state parimenti respinte due opposizioni, presentate da altrettante amministrazioni locali, nei confronti di decisioni con le quali il Garante ha censurato, in termini di mancato rispetto del principio di pertinenza, la pubblicazione nell'albo pretorio di deliberazioni contenenti dati anche sensibili degli interessati.

Ancora in senso favorevole all'Autorità, oltre alle già citate opposizioni in materia di diffusione di fotografie di persone sottoposte a misure restrittive della libertà personale e in tema di accesso ai dati valutativi, si è conclusa l'opposizione proposta dall'amministratore di una società il quale aveva chiesto il blocco dei dati del casellario giudiziale che lo riguardavano, acquisiti da un ente pubblico, che in base ad essi aveva escluso la società da una gara d'appalto (Tribunale di Padova, sentenza n. 2454 del 16 settembre 2004). Nei confronti della sentenza è stato proposto ricorso in Cassazione.

È giunto a positiva conclusione per il Garante anche il giudizio introdotto dal ricorso presentato dinanzi al giudice ordinario da Rai S.p.A. e dall'Agenzia delle entrate contro il *provvedimento* adottato il 5 dicembre 2001 [doc. *web* n. 40405] in materia di canone televisivo. Con tale decisione, confermata dal Tribunale di Roma con sentenza n. 10802 del 29 aprile 2005, l'Autorità ha segnalato a Rai S.p.A., individuata quale responsabile del trattamento per conto dell'amministrazione finanziaria, la necessità di interrompere la raccolta, e di astenersi da ogni ulteriore trattamento dei dati personali degli acquirenti in carenza di presupposti giuridici idonei a legittimare la raccolta e il successivo trattamento dei dati stessi.

Infine, va ricordata la già menzionata ordinanza del 25 maggio 2005 con cui il Tribunale amministrativo del Lazio ha respinto la domanda di sospensione del *provvedimento* del Garante del 15 luglio 2004 concernente l'individuazione delle modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi telefonici cartacei o elettronici.

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

Come già riferito, nel 2005 si è registrata la notifica al Garante di settantaquattro ricorsi all'autorità giudiziaria, non coinvolgenti direttamente pronunce dell'Autorità (art. 152, comma 7, del Codice).

A tale proposito occorre evidenziare che il Garante, conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato –che si è pronunciata in termini favorevoli alla costituzione in giudizio del Garante, ritenendo essenziale che l'Autorità possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni–, ha deciso di delimitare la propria presenza attiva in giudizio ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto. Ciò, pur continuando a seguire con attenzione tutti i contenziosi.

In questo quadro, l'Autorità, laddove non ha ritenuto opportuno intervenire, ha pregato i competenti uffici dell'Avvocatura generale dello Stato di seguire periodicamente le vicende processuali.

Per sei ricorsi che le sono stati notificati l'Autorità ha ritenuto opportuno costituirsi. In particolare, si è trattato di tre casi –cui si è fatto già riferimento– nei quali è stato adito il Giudice di pace di Taranto. Si è ritenuto che la questione investisse un aspetto generale relativo alla corretta applicazione del Codice, con particolare riferimento alla individuazione nel tribunale ordinario del giudice competente a trattare la materia.

Uno dei casi di costituzione si è avuto in una causa nella quale il ricorrente ha esposto di essere raggiunto sul proprio telefono portatile da messaggi pubblicitari per la cui ricezione non aveva fornito il preventivo assenso. In questo caso l'Autorità ha inteso ribadire i principi già affermati nel proprio *provvedimento* di carattere generale adottato in tema di invio di *Sms* pubblicitari promozionali il 10 giugno 2003 [doc. *web* n. 29836], con il quale ha inteso fornire agli operatori indicazioni necessarie per conformare il trattamento dei dati personali alla disciplina vigente.

Al fine di ribadire principi più volte espressi, il Garante ha ritenuto necessario costituirsi in due giudizi nei quali si verte in tema di accesso, rispettivamente dell'erede (ai dati relativi a rapporti bancari del *de cuius*) e dell'infortunato (alle informazioni di natura valutativa che lo riguardano contenute in una perizia medico-legale).

20 Attività ispettive e applicazione di sanzioni amministrative

20.1. *Il potenziamento del dispositivo di controllo*

Nel 2005 si è registrato un importante incremento delle attività ispettive (+130% rispetto al 2004) in conseguenza di un complesso di decisioni rientranti nel processo di potenziamento delle attività di controllo dell'Autorità.

Anno	*2002*	*2003*	*2004*	*2005*
Ispezioni	40	69	100	230

Il Garante, per svolgere al meglio i compiti di garanzia dei cittadini e per evitare che, nell'esercizio dell'attività di impresa, soggetti poco virtuosi acquisiscano rendite illecite sulla base di trattamenti di dati personali effettuati in contrasto con la legge, a danno delle altre imprese, ha investito nuovamente in modo significativo sull'attività ispettiva attraverso:

- una revisione e un potenziamento organizzativo del Dipartimento che cura tale attività;
- la firma di un nuovo protocollo di intesa con la Guardia di finanza;
- l'introduzione di una nuova procedura di programmazione delle attività ispettive tesa ad intensificare ulteriormente il controllo su determinati settori di volta in volta individuati in ragione di una più specifica attività di analisi.

Per quanto riguarda il profilo organizzativo, l'esperienza degli anni precedenti ha evidenziato la necessità di accorpare organizzativamente funzioni afferenti all'espletamento dell'attività ispettiva e alla contestazione e all'applicazione delle sanzioni amministrative (spesso connesse all'attività ispettiva stessa), oltre che a diversi rapporti con l'autorità giudiziaria, al fine di orientare in una nuova unità organizzativa istituita internamente all'Ufficio del Garante (Dipartimento attività ispettive e sanzioni) la cura del controllo dell'Autorità di tipo ispettivo nei confronti dei settori che hanno evidenziato, anche a seguito delle sanzioni contestate, il più alto coefficiente di inadempimento, nonché di rendere più spedito il procedimento relativo alle contestazioni delle sanzioni che coinvolge l'operato di più unità organizzative.

Alla medesima, nuova unità organizzativa è stata quindi attribuita la competenza di provvedere alla procedura per il *cd.* "ravvedimento operoso" in relazione all'omessa adozione delle misure minime di sicurezza, punita con una sanzione penale dall'art. 169, comma 2. Trattasi della procedura in base alla quale, una volta accertata la mancata adozione di quelle misure di sicurezza considerate come "minime" e previste dal disciplinare tecnico costituente l'Allegato B) al Codice, il Garante impartisce all'autore del reato le prescrizioni per ripristinare il livello minimo di sicurezza previsto dalla legge. La verifica della congruità dell'adempimento apre la strada per la definizione del procedimento attraverso il pagamento del quarto del massimo dell'ammenda prevista dalla legge, estinguendo così il reato.

Altro elemento determinante per lo sviluppo delle attività ispettive è stato rappresentato dalla firma di un nuovo protocollo di intesa con la Guardia di finanza. Il nuovo accordo, siglato presso il Comando generale l'11 novembre 2005, muove dalla considerazione dell'eccellente livello di collaborazione nell'attività di controllo

raggiunto a seguito del protocollo del 2002 e dell'accresciuta capacità operativa del Corpo conseguente all'istituzione del Nucleo funzione pubblica e *privacy*, reparto specializzato nell'attività di vigilanza in materia di protezione dei dati personali.

In relazione a quanto stabilito nel nuovo protocollo la Guardia di finanza, oltre ad assicurare al Garante la collaborazione nell'attività ispettiva, si impegna a rilevare e a segnalare all'Autorità tutte le situazioni rilevanti sotto il profilo dell'applicazione della legge di cui sia venuta a conoscenza nell'ambito dello svolgimento di attività di controllo, constatate anche con altre finalità (ad esempio, nell'ambito dei controlli tributari).

Altro elemento qualificante dell'attività ispettiva svolta nel 2005 è stato il potenziamento dell'attività di prevenzione attraverso accertamenti *cd.* di iniziativa, ovvero avviati *motu proprio* dall'Autorità anche in assenza di atti di impulso di cittadini (segnalazioni, reclami o ricorsi), i quali hanno costituito la parte più consistente dell'intera attività di controllo (circa il 70%).

A partire dal mese di settembre 2005 è stata messa a punto una procedura di programmazione attraverso la quale il collegio del Garante, con cadenza semestrale, tenuto conto delle risorse disponibili, detta le linee di indirizzo dell'attività ispettiva di iniziativa, individuando i settori e gli ambiti delle ispezioni e determinando il numero delle attività di controllo da effettuarsi in relazione ai diversi settori.

Le linee generali degli indirizzi stabiliti con la programmazione dell'attività ispettiva vengono di volta in volta rese pubbliche.

Questa nuova impostazione dell'attività di controllo consente, attraverso verifiche effettuate nei confronti di più soggetti operanti nello stesso settore o che effettuano tipologie omogenee di trattamento, di acquisire importanti elementi di valutazione in ordine:

- al grado di adeguamento al Codice degli operatori appartenenti ad un determinato settore (*ad es.*, società di selezione e collocamento del personale) o che utilizzano i dati personali per particolari finalità (*ad es.*, profilazione dei clienti attraverso l'uso di tessere di fidelizzazione);
- a fenomeni di ampia portata che possono costituire presupposto per l'adozione di provvedimenti generali (diretti, cioè, ad un insieme indeterminato di operatori);
- alla verifica dell'impatto dei provvedimenti adottati.

Ne deriva una valorizzazione dell'attività di controllo come strumento di governo del sistema in un'ottica non solo repressiva, ma anche conoscitiva e di indirizzo.

20.2. *La collaborazione con la Guardia di finanza*

Anche nel 2005 è risultato determinante, nel settore ispettivo, il rapporto con la Guardia di finanza, che ha consentito all'Autorità di poter disporre di risorse qualificate per espletare l'attività di controllo affidata dalla legge.

Il perfezionamento del nuovo protocollo di intesa consente al Garante di avvalersi del Corpo attraverso:

- la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- l'assistenza nei rapporti con l'autorità giudiziaria;
- lo sviluppo di attività ispettive delegate o *sub*-delegate per l'accertamento delle violazioni;
- la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;

- l'esecuzione di indagini conoscitive sullo stato di attuazione del Codice in determinati settori;
- la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

In pratica il Garante, ogni qualvolta ritenga necessario avvalersi della collaborazione del Corpo, attiva il Nucleo speciale funzione pubblica e *privacy* che, disponendo di personale specializzato, provvede direttamente ad effettuare gli accertamenti avvalendosi anche dei reparti del Corpo territorialmente competenti.

Le informazioni e i documenti acquisiti nell'ambito degli accertamenti vengono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei principi previsti dalla legge. Quando nell'ispezione emergono violazioni penali o amministrative la Guardia di finanza procede direttamente ad inoltrare la notizia di reato all'autorità giudiziaria e a contestare la violazione amministrativa.

Una delle novità più rilevanti del nuovo protocollo consiste nel maggior coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, compagnie e tenenze). L'obiettivo è di disporre di un dispositivo di controllo flessibile ed articolato che consenta, in funzione della complessità degli accertamenti, di effettuarli direttamente a cura del Dipartimento attività ispettive e sanzioni dell'Ufficio del Garante, ovvero attraverso il Nucleo speciale, oppure, nel caso di accertamenti di non elevata complessità che concernono ad esempio la verifica di singoli adempimenti, delegando anche i reparti territoriali della Guardia di finanza.

Al fine di implementare le competenze in materia di protezione dei dati personali, è stato avviato, con il supporto dell'Autorità, già nel mese di dicembre 2005, un complesso piano di formazione del personale appartenente ai comandi territoriali a cui partecipano 120 tra ufficiali e ispettori.

Altro elemento qualificante del nuovo accordo di collaborazione riguarda il supporto che il Corpo si è impegnato ad offrire al Garante per la diffusione delle informazioni sull'applicazione delle norme in materia di protezione dei dati personali, attraverso una stretta interazione tra gli Uffici relazioni con il pubblico. Grazie a questo accordo gli Uffici relazioni con il pubblico della Guardia di finanza potranno costituire, per i cittadini, punti di contatto attraverso i quali ricevere informazioni di prima necessità sulla legge e sui principali adempimenti e reperire materiali esplicativi editi dall'Autorità.

Anche in questo ambito è stato avviato un idoneo percorso formativo per il personale della Guardia di finanza impiegato nel settore delle relazioni con il pubblico.

20.3. *Settori oggetto dei controlli e casi più rilevanti*

I principali settori nei quali sono stati effettuati controlli sono stati:

- aziende sanitarie locali (43);
- società di ricerca e selezione del personale (40);
- società di gestione di alberghi (21);
- società che effettuano sondaggi di opinione (18);
- palestre e centri benessere (12);
- laboratori di analisi che effettuano anche trattamenti di dati genetici (10);
- società che utilizzano tessere di fidelizzazione (10);
- società che utilizzano sistemi di videosorveglianza in luoghi aperti al pubblico (tra cui servizi di trasporto ferroviario, metropolitano e aeroportuale) (7);
- società ed enti che effettuano trattamenti di dati biometrici (5);

- società che gestiscono sistemi di informazione creditizia, *cd.* centrali rischi private (4);
- società che forniscono nuovi servizi televisivi (digitale terrestre e *web* TV) (2);
- operatori telefonici, con riguardo alla *data retention* dei dati di traffico telefonico e telematico (2).

Oltre alle ispezioni di iniziativa di cui sopra, sono state effettuati ulteriori cinquantasei accertamenti in relazione a segnalazioni, reclami e ricorsi pervenuti al Garante o comunque necessari per definire procedimenti aperti dall'Autorità nei confronti di titolari.

I controlli effettuati nei confronti delle aziende sanitarie sono stati volti a verificare l'esatto adempimento alle disposizioni relative alla notificazione al Garante del trattamento di dati genetici e di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria (ai sensi dell'art. 37 del Codice).

Anche se le ispezioni hanno evidenziato un elevato numero di violazioni si è avuto comunque modo di rilevare che alcune realtà hanno avviato interessanti progetti per implementare la protezione dei dati personali attraverso non solo il corretto adempimento degli obblighi di legge, ma anche mediante un'opera di sensibilizzazione e formazione del personale sanitario e amministrativo degli enti, tesa ad accrescere la cultura della *privacy*.

Per quanto riguarda i controlli nei confronti delle società di selezione del personale, sono emerse alcune violazioni relative all'omessa notificazione con riferimento all'art. 37, comma 1, lett. *d)* del Codice –dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato– e alla lett. *e)* del medesimo comma –dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi–.

In generale, si è riscontrato un utilizzo di informative sul trattamento dei dati dei candidati alle selezioni non sempre in linea con i principi del Codice, nonché la diffusione di prassi che non trovano supporto nel dettato normativo, come quella dell'inserimento della locuzione "*autorizzo il trattamento dei miei dati ai sensi del* d.lg. *n. 196/2003*" nell'ambito di *curricula.*

Alcuni accertamenti ispettivi sono stati effettuati a seguito di segnalazioni concernenti accessi illeciti a dati anagrafici detenuti presso il Comune di Roma, al fine di verificare anche il rispetto delle misure di sicurezza nel trattamento dei dati in correlazione a casi di falsa sottoscrizione di candidature alle elezioni regionali del 3 e 4 aprile 2005. L'esito degli accertamenti, effettuati anche nell'esercizio di funzioni di polizia giudiziaria, è stato comunicato alla competente autorità giudiziaria.

Il caso riguardava in particolare accessi effettuati, per finalità e con modalità non consentite, tramite Laziomatica S.p.A. (società per azioni a prevalente capitale regionale istituita dalla Regione Lazio, che le ha affidato la gestione del Sistema informativo regionale), ad una banca dati anagrafica del Comune di Roma che la regione era stata autorizzata a consultare solo per alcune finalità sanitarie, sulla base di un protocollo di intesa. Gli accessi, effettuati in singolari circostanze (utilizzo di *password* altrui; consultazioni in orari non di servizio, notturni e festivi; asseriti interventi di manutenzione straordinaria che hanno determinato la cancellazione di dati di tracciamento di accessi), hanno permesso di consultare ed utilizzare illecitamente vari dati personali inerenti anche a documenti di identità, per finalità diverse da quelle per le quali i dati anagrafici erano stati resi accessibili alla regione (*v.*

amplius par. 2.6). Gli accertamenti effettuati dal Garante sono stati estesi alla sicurezza dei dati presso le banche dati anagrafiche del Comune, ove è emerso il mancato rispetto di alcune misure minime di sicurezza tra le quali l'omesso aggiornamento del documento programmatico sulla sicurezza dei dati, unitamente a talune inosservanze della disciplina applicabile alla gestione dell'anagrafe della popolazione residente. Rispetto ai profili relativi alle misure minime di sicurezza sono stati avviati autonomi procedimenti nei confronti dei responsabili.

Parallelamente a questa vicenda sono stati effettuati accertamenti in relazione a segnalazioni, pervenute nel medesimo periodo, che evidenziavano la possibile utilizzazione illecita, per scopi elettorali, di dati relativi a dipendenti di un ente pubblico e di un'azienda municipale. All'esito dell'attività ispettiva è stata in effetti rilevata la mancata adozione delle misure minime di sicurezza da parte dell'ente pubblico ispezionato e si è proceduto, anche in questo caso, alla segnalazione del reato di cui all'art. 169 del Codice all'autorità giudiziaria competente.

20.4. *L'attività sanzionatoria del Garante*

Le sanzioni amministrative contestate hanno riguardato: l'omessa notificazione al Garante (61); l'omessa o inidonea informativa all'interessato (24); l'omessa risposta alle richieste di informazione del Garante (8) e la mancata acquisizione del consenso preventivo del consumatore per l'utilizzo di sistemi del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax prevista dall'art. 12 del d.lg n. 185/1999 (*v.* ora art. 62 d.lg. 6 settembre 2005, n. 206, recante il Codice del consumo) (1).

A fronte delle sanzioni contestate, sono state riscossi euro 644.000 da parte di enti e società sanzionate che hanno acceduto alla procedura *cd.* di "definizione in via breve", versando il doppio del minimo previsto per la sanzione contestata.

20.5. *Alcuni riferimenti statistici*

Delle 230 attività ispettive effettuate nel 2005, 22 sono state curate direttamente dal Dipartimento attività ispettive e sanzioni del Garante e 208 sono state effettuate su delega dalla Guardia di finanza.

Gli accertamenti hanno riguardato sia l'ambito pubblico (53), sia quello privato (179) e sono stati volti a verificare il rispetto dei principali adempimenti previsti dalla normativa.

Le attività ispettive avviate dal Garante *motu proprio* sono state 169, quelle effettuate nell'ambito di procedimenti conseguenti a segnalazioni pervenute dai cittadini sono state 46; 15 accertamenti sono stati effettuati in relazione ad elementi emersi a seguito di ricorsi, o sono stati tesi a verificare il corretto adempimento dei provvedimenti del Garante.

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

- nord (97);
- centro (62);
- sud (71).

L'incidenza delle violazioni penali e amministrative riscontrate è stato pari a circa al 44% sul totale delle ispezioni effettuate.

Le violazioni penali segnalate all'autorità giudiziaria riguardano ipotesi di trattamento illecito di dati personali (1), omessa adozione di misure di sicurezza (4), inos-

servanza dei provvedimenti del Garante e false dichiarazioni al Garante (2) e hanno comportato la segnalazione di 10 persone all'autorità giudiziaria.

Undici sono stati i procedimenti connessi al *cd.* "ravvedimento operoso" in materia di misure minime di sicurezza, previsto dall'art. 168, comma 2, del Codice, in relazione ai quali sono state impartite dodici prescrizioni, in relazione alle quali sono state ammesse al pagamento del quarto del massimo dell'ammenda prevista dalla legge, in quanto responsabili della violazione, n. 16 persone, per un totale di sanzioni applicate pari a euro 189.145.

Il Dipartimento attività ispettive e sanzioni ha inoltre provveduto, tramite il Nucleo speciale della Guardia di finanza, alla notifica di 70 atti tra proroghe e decisioni di ricorsi e, in generale, provvedimenti dell'Autorità.

21 Relazioni istituzionali

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

Anche nel 2005 l'Autorità ha svolto un ruolo consultivo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo del Parlamento in relazione ad aspetti di specifico interesse in materia di protezione dei dati personali; ha fornito altresì al Governo, ove richiesta, chiarimenti ed indicazioni necessari.

Nell'ambito di tale collaborazione sono stati inoltrati al Governo elementi di valutazione in relazione ad alcuni atti di sindacato ispettivo fra i quali si ricordano, in particolare:

- un'interrogazione a risposta scritta dell'on. Cortiana (n. 4-01434) concernente la diffusione su organi di stampa della vicenda di una ragazza dichiarata adottabile nonostante l'assoluzione del padre dall'accusa di violenza nei suoi confronti (*Nota* 2 agosto 2005). L'Autorità ha richiamato, in proposito, l'applicazione delle disposizioni del Codice (art. 50) e sul processo penale a carico di imputati minorenni (art. 13 d.P.R. 22 settembre 1988, n. 448), che prevedono limiti alla diffusione di notizie e di immagini relative a minori di età o che comunque consentano l'identificazione di minorenni coinvolti in un procedimento giudiziario, anche in materie diverse da quella penale;
- un'interrogazione a risposta orale dell'on. Perrotta (n. 3-3617) concernente l'intestazione ad un utente di più schede telefoniche prepagate, attivate illecitamente a nome e all'insaputa del ricorrente (*Nota* 2 agosto 2005). L'Autorità ha evidenziato di essersi occupata, in più occasioni, dell'attivazione di servizi di telefonia mobile e fissa non richiesti, ivi comprese le schede telefoniche "prepagate", anche in relazione alla vicenda cui si riferiva l'interrogazione, già oggetto di un ricorso presentato all'Autorità per i connessi profili riguardanti la protezione dei dati personali.

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

L'articolo 154, comma 4, del Codice prevede che il Presidente del Consiglio dei ministri e ciascun Ministro consultino il Garante all'atto della predisposizione di norme regolamentari e di atti amministrativi suscettibili di incidere sulla protezione dei dati personali, nell'interesse pubblico e dei cittadini, al fine di prevenire problemi applicativi e in un quadro di collaborazione istituzionale del quale, più volte, vari ministeri hanno riconosciuto l'importanza e l'utilità.

Nel 2005, il Garante ha espresso in questa chiave diversi pareri i quali hanno riguardato, in particolare:

- uno schema di provvedimento dell'Agenzia delle entrate con cui sono state stabilite le specifiche tecniche per l'invio delle richieste e delle risposte in modalità telematica in materia di indagini finanziarie, in attuazione dell'art. 32, comma 3, d.P.R. n. 600/1973 e dell'art. 51, comma 4, d.P.R. n. 633/1972 (*Parere* 21 dicembre 2005 [doc. *web* n. 1210095]). Il provvedimento individua, quale modalità di comunicazione, la posta elet-

tronica certificata, la cui casella è accessibile tramite *password* ed è utilizzabile solo dai titolari degli accertamenti (provvedimento Agenzia delle entrate 22 dicembre 2005, in *G.U.* 10 gennaio 2006, n. 7, *S.O.* n. 6);

- uno schema di regolamento che istituisce presso il Dipartimento per lo sviluppo delle economie territoriali della Presidenza del Consiglio dei ministri una banca di dati informatica denominata "Guida agli investimenti locali" (*Parere* 21 dicembre 2005 [doc. *web* n. 1212504]);
- uno schema di regolamento del Ministro del lavoro e delle politiche sociali, di concerto con il Ministro della salute, concernente gli accertamenti di assenza di tossicodipendenza sui lavoratori destinati a mansioni che comportano rischi per la sicurezza, l'incolumità e la salute dei terzi, adottato ai sensi dell'art. 125 d.P.R. 9 ottobre 1990, n. 309, e successive modificazioni (*Parere* 15 dicembre 2005 [doc. *web* n. 1209068]). Nel parere, dopo aver segnalato che gli esami per accertare l'assenza di tossicodipendenza nell'ambito di particolari categorie di lavoratori devono essere compiuti nel rispetto della dignità e della riservatezza delle persone coinvolte, l'Autorità ha sottolineato la necessità che il regolamento eviti formulazioni generiche o non rispettose del principio di proporzionalità rispetto alle finalità di tali esami. È stato richiesto, in particolare, di specificare la previsione che impone gli esami complementari tossicologici; in considerazione della loro invasività, è stato richiesto di precisare che questo tipo di esami (successivi alla visita medica) vanno eseguiti soltanto quando ci si trovi in presenza di sintomi di una "dipendenza" da sostanze stupefacenti e non solo di un loro uso, magari occasionale. Il Garante ha poi chiesto di individuare con precisione i casi di incidente sul lavoro che possono imporre tali accertamenti e i conseguenti trattamenti di dati, dovendosi fare riferimento solo a quelli che, per le loro caratteristiche e in relazione ai comportamenti dei lavoratori coinvolti, possano derivare da una tossicodipendenza;
- uno schema di decreto del Presidente della Repubblica recante modifiche alla disciplina concernente il sistema matricolare del Corpo della Guardia di finanza, adottato ai sensi dell'art. 5 l. 5 novembre 1962, n. 1695 (*Parere* 19 ottobre 2005 [doc. *web* n. 1185148]);
- uno schema di decreto del Ministro dell'interno, di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, concernente le misure che i titolari o gestori di esercizi pubblici e circoli privati che pongono a disposizione del pubblico apparecchi terminali utilizzabili per comunicazioni, anche telematiche (*cd.* Internet *point*), devono osservare per rispettare l'obbligo di monitorare le operazioni degli utenti e di archiviare i relativi dati, ai sensi dell'articolo 7, comma 4, d.l. n. 144/2005 (decreto *cd.* "antiterrorismo", sul quale *v. amplius* par. 1.1.) (*Parere* 11 agosto 2005 [doc. *web* n. 1170246]). Il decreto adottato ha recepito le osservazioni del Garante (d.m. 16 agosto 2005, in *G.U.* 17 agosto 2005, n. 190);
- uno schema di decreto del Ministro degli affari esteri, per l'istituzione di un nuovo modello di passaporto ordinario atto a contenere dati biometrici (*cd.* passaporto elettronico), in linea con quanto previsto in sede comunitaria (regolamento del Consiglio n. 2252/2004 e decisione della Commissione n. 409/2005) (*Parere* 26 luglio 2005 [doc. *web* n. 1153396]). Il decreto ha recepito le osservazioni del Garante prevedendo, in particolare, che i dati biometrici possano essere utilizzati solo per finalità di verifica dell'identità del titolare e non debbano essere registrati in banche di dati (d.m. 29 novembre 2005, in *G.U.* 17 gennaio 2006, n. 13);

- uno schema di decreto interministeriale, trasmesso dal Ministero dell'interno, per individuare i dati e le informazioni da registrare nell'archivio informatizzato dello Sportello unico per l'immigrazione, ai sensi dell'art. 30-*quater*, comma 3, d.P.R. n. 394/1999, introdotto dal d.P.R. n. 334/2004 (*Parere* 26 luglio 2005 [doc. *web* n. 1152007]);
- uno schema di decreto del Ministro della salute, relativo all'istituzione del registro nazionale delle strutture autorizzate all'applicazione delle tecniche della procreazione medicalmente assistita, degli embrioni formati e dei nati a seguito dell'applicazione delle tecniche medesime, previsto dall'art. 11, comma 1, l. n. 40/2004 (*Parere* 26 luglio 2005 [doc. *web* n. 1151435]; *v.* par. 3.1.4). Il decreto ha recepito le indicazioni del Garante prevedendo che nel registro possano essere inseriti solo dati in forma anonima, anche aggregata, relativi alle coppie che accedono alle predette tecniche, agli embrioni e ai nati (d.m. 7 ottobre 2005, in *G.U.* 3 dicembre 2005, n. 282);
- uno schema di provvedimento del Ministero dell'economia e delle finanze relativo alla trasmissione al Ministero della salute e alle regioni, con modalità telematiche, dei dati relativi alle ricette mediche, ai sensi dell'art. 50, comma 10, d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, dalla l. n. 326/2003 (*Parere* 21 luglio 2005 [doc. *web* n. 1151167]). Il provvedimento è stato adottato in data 9 marzo 2006 ed è stato pubblicato nella *G.U.* 20 marzo 2006, n. 66;
- uno schema di decreto del Ministro dell'interno concernente la modulistica relativa ai procedimenti per l'assunzione di lavoratori stranieri e per il ricongiungimento familiare, di competenza dello Sportello unico per l'immigrazione, ai sensi dell'art. 30-*bis* d.P.R. n. 394/1999 (*Parere* 25 maggio 2005 [doc. *web* n. 1131847]);
- tre schemi di regolamento del Ministro dell'economia e delle finanze concernenti gli obblighi antiriciclaggio per intermediari abilitati, altri operatori non finanziari e alcuni professionisti, in attuazione degli articoli 3, comma 2, e 8, comma 4, d.lg. n. 56/2004 (*Parere* 12 maggio 2005 [doc. *web* n. 1131800]);
- due schemi di decreto del Ministro dell'interno in materia di registrazione di immagini e di titoli di accesso negli stadi, adottati in attuazione dell'art. 1-*quater* d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla l. 2 aprile 2003 n. 88 (*Parere* 4 maggio 2005 [doc. *web* n. 1120732]; *v.* par. 13.1). I decreti prevedono l'utilizzo di strumenti di videosorveglianza presso gli impianti sportivi di capienza superiore alle diecimila unità e l'obbligo di accedere nei medesimi stadi muniti di biglietti nominativi (dd.mm. 6 giugno 2005, in *G.U.* 30 giugno 2005, n. 150);
- uno schema di decreto dirigenziale del Ministero della giustizia, di attuazione in via parziale e transitoria dell'art. 33 d.P.R. 14 novembre 2002, n. 313, concernente il rilascio all'interessato della visura, non avente valore di certificato, dei dati registrati nel casellario giudiziale (*Nota* 6 aprile 2005). Il decreto è stato adottato il 1° agosto 2005 ed è stato pubblicato nella *G.U.* 10 ottobre 2005, n. 185;
- due schemi di decreto del Ministro dell'istruzione, recanti l'individuazione delle modalità e dei contenuti delle prove di ammissione ad alcuni corsi di laurea programmati a livello nazionale (*Nota* 5 aprile 2005; *v.* par. 2.7.1);
- uno schema di convenzione fra il Ministero dell'interno e l'Agenzia del territorio ai sensi dell'art. 54 del Codice, per l'accesso degli organi di polizia agli archivi informatici del catasto terreni, del catasto edilizio urbano e del catasto geometrico, ai fini della consultazione degli atti (*Nota* 4 aprile 2005);

- uno schema di regolamento del Dipartimento per le pari opportunità della Presidenza del Consiglio dei ministri, recante modifiche ed integrazioni al regolamento sulla costituzione e il funzionamento della commissione per le adozioni internazionali (d.P.R. 1° dicembre 1999, n. 492) (*Nota* 4 aprile 2005);
- due schemi di decreti (trasmessi dal Ministero delle attività produttive), concernenti l'utilizzo di strumenti di controllo nel settore dei trasporti su strada (tachigrafi digitali), adottati ai sensi dell'art. 3, commi 7 e 8, d.m. n. 361/2003 (*Nota* 18 febbraio 2005). Le indicazioni fornite dal Garante sono state recepite nei decreti adottati (d.m. 11 marzo 2005, in *G.U.* 11 maggio 2005, n. 108; d.m. 23 giugno 2005, in *G.U.* 26 luglio 2005, n. 172).

L'Autorità, inoltre, nel quadro di una proficua collaborazione istituzionale, ha fornito osservazioni ed elementi di valutazione sugli aspetti di protezione dei dati personali in ordine ad alcuni schemi di decreti legislativi, alle amministrazioni che ne hanno fatto richiesta, con particolare riferimento al codice dell'amministrazione digitale, al sistema pubblico di connettività e all'utilizzo di dati pubblici (*v. amplius* par. 1.4).

A fronte dei pareri espressi sopra menzionati, deve segnalarsi che –anche se in misura ridotta rispetto al 2004– continuano a registrarsi casi di mancata consultazione dell'Autorità. Si riportano le fattispecie più significative:

- decreto del Ministro della salute 30 dicembre 2004 (*"Norme procedurali per l'effettuazione dei controlli antidoping e per la tutela della salute, ai sensi dell'art. 3, comma 1, della legge 14 dicembre 2000, n. 376"*) (*G.U.* 17 febbraio 2005, n. 39);
- provvedimento dell'Agenzia delle entrate 10 marzo 2005 (*"Trasmissione telematica di comunicazioni all'anagrafe tributaria"*) (*G.U.* 21 marzo 2005, n. 66);
- provvedimento dell'Agenzia delle entrate 16 marzo 2005 (*"Comunicazione all'anagrafe tributaria dei dati catastali identificativi degli immobili presso cui sono attivate utenze di energia elettrica, di servizi idrici e del gas"*)(*G.U.* 23 marzo 2005, n. 68);
- decreto del Ministro del lavoro e delle politiche sociali 4 febbraio 2005 (*"Istituzione del Casellario centrale delle posizioni previdenziali attive, presso l'Istituto nazionale della previdenza"*) (*G.U.* 29 marzo 2005, n. 72);
- decreto del Ministro della salute 3 marzo 2005 (*"Protocolli per l'accertamento della idoneità del donatori di sangue di emocomponenti"*) (*G.U.* 13 aprile 2005, n. 85);
- decreto del Ministro della salute 3 marzo 2005 (*"Caratteristiche e modalità per la donazione del sangue e di emocomponenti"*)(*G.U.* 13 aprile 2005, n. 85);
- decreto del Ministro dell'interno 2 agosto 2005 (*"Modificazioni al d.m. 19 luglio 2000, recante: «Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici»*) (*G.U.* 12 agosto 2005, n. 187);
- decreto del Ministro dell'interno 2 agosto 2005 (*"Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione Cie, in attuazione del comma 2 dell'art. 7*-vicies ter *della legge 31 marzo 2005, n. 43"*)(*G.U.* 19 settembre 2005, n. 218);
- decreto del Ministro dell'economia e delle finanze 4 agosto 2005 (*"Modalità di attuazione del progetto Pc ai giovani"*) (*G.U.* 27 settembre 2005, n. 225).

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

L'Autorità ha proseguito, nel 2005, l'attività consultiva sollecitata dalla Presidenza del Consiglio dei ministri sul contenuto di alcune leggi regionali, rispetto agli aspetti riconducibili alla materia della protezione dei dati personali, al fine di segnalare questioni eventualmente rilevanti in sede di conflitto di attribuzioni tra Stato e regioni.

In alcuni casi non si sono ravvisati profili di illegittimità costituzionale; in altri, sono stati invece rilevati aspetti problematici, come avvenuto nel caso della legge della Regione Toscana 15 dicembre 2004, n. 63, recante "*Norme contro le discriminazioni determinate dall'orientamento sessuale o dall'identità di genere*", di cui si è già riferito nella *Relazione* 2004 (p. 136).

In particolare, l'esame degli articoli 7 e 8 di tale legge –che individuano il soggetto competente ad esprimere il consenso ad un determinato trattamento terapeutico per conto di chi si trovi in condizione di incapacità e grave pericolo per la salute o l'integrità fisica– ha evidenziato questioni di legittimità costituzionale attinenti al profilo della potestà legislativa dello Stato in materia di protezione di dati personali, con specifico riferimento alle disposizioni del Codice sull'acquisizione del consenso informato al trattamento dei dati, sulle garanzie a tutela della riservatezza dei pazienti e sulla necessità e proporzionalità della raccolta di informazioni in banche di dati. L'Autorità ha segnalato tali aspetti alla Presidenza del Consiglio dei ministri (*Nota* 11 gennaio 2005) che ha, in seguito, impugnato la legge davanti alla Corte costituzionale.

Di particolare interesse si sono inoltre rivelate le ulteriori vicende della legge della Regione Emilia-Romagna 24 maggio 2004, n. 11 (*Sviluppo regionale della società dell'informazione*). Come riportato nella precedente *Relazione* (p. 135), l'Autorità aveva rilevato importanti profili di illegittimità costituzionale di tale legge, che sono stati poi dedotti dalla Presidenza del Consiglio dei ministri nel contestarne la legittimità dinanzi alla Consulta.

Con sentenza 7 luglio 2005, n. 271, la Corte costituzionale ha sostanzialmente accolto le argomentazioni contenute nel ricorso presentato dalla Presidenza del Consiglio dei ministri, dichiarando incostituzionali gli artt. 12, 13 e 14 della legge regionale in relazione all'art. 117, secondo comma, lettere *l*), *m*) ed *r*), e sesto comma, Cost., e in riferimento ai principi della legislazione statale in materia di protezione dei dati personali.

La Corte ha rilevato che, alla luce del riparto delle potestà legislative di cui al nuovo art. 117 Cost., al legislatore regionale va riconosciuta una limitata competenza *"a disciplinare procedure o strutture organizzative che prevedono il trattamento di dati personali"*, e solo *"nell'integrale rispetto della legislazione statale sulla loro protezione"*; di qui la dichiarazione di illegittimità costituzionale sia dell'art. 12 della legge (che, pur affermando il rispetto delle norme a tutela della riservatezza e delle forme di segreto, risultava in concreto contraddire sotto molteplici profili la legislazione statale vigente in materia di protezione dei dati personali, nonché le stesse direttive europee che ne sono all'origine), sia dell'art. 13, comma 1, della medesima legge (nella parte in cui non richiamava la legislazione statale in materia di protezione dei dati personali).

In seguito alla dichiarazione di incostituzionalità, la Regione Emilia-Romagna, con la legge regionale 22 dicembre 2005, n. 22, ha modificato il testo degli articoli 12 e 13 della predetta l.r. n. 11/2004. L'Autorità ha rilevato che le nuove disposizioni approvate da tale Regione possono ritenersi nel loro complesso sostanzialmente rispondenti ai principi affermati dalla Corte. Il Garante si è peraltro soffer-

21

mato in particolare su una disposizione (il nuovo comma 7 del citato articolo 12), che intende promuovere la comunicazione alla regione e agli altri soggetti pubblici dei dati personali contenuti nei sistemi informativi dei soggetti privati che operano in ambito regionale svolgendo "attività di interesse pubblico", precisando che ritiene possibile interpretarla –conformemente alla prospettiva indicata dalla Corte– nel senso che la regione potrà promuovere la predetta comunicazione di dati relativamente alle sole informazioni pertinenti e non eccedenti rispetto alle attribuzioni regionali. L'Autorità ha rilevato, altresì, che in sintonia con questa interpretazione dovrebbe essere letta anche l'ulteriore previsione, prevista dalla l.r. n. 11/2004, di intese fra la regione stessa e gli enti locali, in relazione alle rispettive attribuzioni dei diversi enti, necessarie per assicurare il rispetto del principio di finalità nel trattamento (*Nota* 10 febbraio 2006).