ti: artt. 12 e 20 l. n. 675), possono effettuare solo i trattamenti di dati connessi all'esercizio delle proprie funzioni istituzionali, nei limiti stabiliti dalle previsioni di legge o di regolamento (art. 27 l. n. 675/1996).

Il trattamento da parte della RAI dei dati relativi agli abbonati è risultato quindi lecito in termini generali, anche per quanto concerne la raccolta, per conto dell'URAR TV, di ulteriori informazioni sui cittadini nell'ambito delle convenzioni che l'amministrazione finanziaria può stipulare per la trasmissione di dati o di documenti (sulla base delle citate disposizioni della l. n. 127/1997 e in tema di scambio dei dati per il recupero di contributi previdenziali), rispettivamente con i comuni (in riferimento agli archivi anagrafici e dello stato civile, con le modalità e nei limiti stabiliti dalle relative discipline normative, su cui il Garante si è più volte pronunciato) e con soggetti erogatori di servizi (ad es., per l'energia elettrica o la telefonia).

Le informazioni personali raccolte possono essere utilizzate dalla società, seppur esclusivamente per le finalità perseguite dall'Amministrazione finanziaria, ai fini della gestione degli abbonamenti e della riscossione dei canoni con adozione, però, di tutti gli accorgimenti richiesti dalla normativa sulla tutela del diritto alla riservatezza (individuazione degli incaricati, informativa, misure di sicurezza, diritti di accesso ai dati personali, ecc.).

Sul piano della corretta e completa attuazione degli adempimenti in materia di protezione dei dati la comunicazione della RAI e le collegate iniziative segnalate dai cittadini, presentano tuttavia diverse lacune ed anomalie.

In considerazione del fatto che varie comunicazioni inviate ai cittadini ed il relativo trattamento di dati sono basati su accertamenti preliminari e valutazioni presuntive, il Garante ha segnalato, anzitutto, l'esigenza che, in linea con il principio di correttezza sancito dall'art. 9 della legge n. 675/1996, la RAI indichi con chiarezza gli obblighi relativi alla detenzione di apparecchi radiotelevisivi e i vantaggi conseguenti ad una regolarizzazione spontanea, riformulando la comunicazione in modo da evidenziare meglio al destinatario le relative finalità, evitando toni ed espressioni con le quali si attribuisca all'interessato una possibile evasione del canone.

Pur restando impregiudicata la doverosa attività di verifica del corretto pagamento del canone, occorre disporre, come ha rimarcato l'Autorità, prima di inviare una comunicazione del tipo di quella segnalata, lo svolgimento di riscontri più attenti ed approfonditi sotto i profili della completezza, dell'esattezza e della pertinenza delle informazioni raccolte. La comunicazione in questione (contenente dati personali raccolti presso terzi) e l'allegato questionario (volto all'acquisizione di dati direttamente dagli interessati) non recavano le informazioni agli interessati necessarie ai sensi dell'art. 10 della legge n. 675/1996; non precisavano, inoltre, la natura facoltativa od obbligatoria del conferimento dei dati, né le conseguenze dell'eventuale rifiuto di fornirli. I destinatari della comunicazione devono essere altresì informati sulla possibilità di esercitare i diritti di accesso ai dati previsti dall'art. 13 della legge n. 675. Deve essere poi agevolato tale accesso anche attraverso opportune misure volte a semplificare le modalità e a ridurre i tempi delle risposte (art. 17, comma 9, del d.P.R. n. 501/1998).

Quanto all'interpretazione secondo cui la società ha fornito un riscontro negativo a talune richieste volte a conoscere l'origine dei dati relativi a nominativi ed indirizzi (ritenendo tali informazioni concernenti atti preparatori di un procedimento tributario, considerati sottratti al diritto di accesso ai sensi degli artt. 13, comma 2, e 24, comma 6, della legge n. 241/1990), l'Autorità ha ribadito le differenze che contraddistinguono, in termini di oggetto e di presupposti, il diritto di accesso di cui alla legge n. 241 (che si riferisce alla documentazione amministrativa e può essere esercitato dal portatore di un interesse personale e qualificato, per la tutela di situazioni giuridicamente rilevanti, salvi i casi di esclusione previsti) e i diritti introdotti dalla legge n. 675/1996. Tali diritti riguardano infatti i dati personali e possono essere esercitati dalle persone cui si riferiscono senza particolari formalità e limitazioni, ad eccezione di taluni diritti che richiedono una specifica situazione e dei casi di esclusione tassativamente indicati dalla legge, nei quali non può però rientrare il trattamento svolto dalla RAI, in qualità di responsabile del Ministero delle finanze, ai fini della gestione degli abbonamenti.

Il Garante ha così confermato l'obbligo, per la società concessionaria e per l'Amministrazione finanziaria, di fornire senza ritardo un riscontro alle richieste avanzate in base al predetto art. 13 della legge n. 675 ricordando che, in caso di mancata risposta o di riscontro negativo, dopo cinque giorni dalla richiesta, gli interessati possono rivolgersi all'autorità giudiziaria o al Garante ai sensi dell'art. 29 della medesima legge.

Infine, il Garante si è occupato di un altro aspetto evidenziato in alcuni reclami, indicando la necessità dell'adozione di misure idonee ad evitare un'inutile divulgazione di dati personali attraverso la restituzione del questionario contenente dati anche di terzi (di familiari o conviventi già abbonati) in una cartolina leggibile da chiunque, anziché in una busta chiusa o con modalità che, comunque, non ne rendano possibile una facile ed immediata consultazione da parte di estranei (*Provv.* del 12 luglio 2000).

Successivamente, il Garante si è espresso in ordine agli schemi di comunicazione e del questionario, riformulati dalla società in conformità al provvedimento (segnalazione del 13 dicembre 2000). In tale occasione, l'Autorità è tornata a chiarire che l'informativa dovrà specificare la possibilità di comunicare dati degli utenti alla Guardia di finanza, per i controlli di competenza, solo sulla base di precisi elementi e riscontri circa la presunta evasione del canone, come richiede la vigente disciplina di riferimento, onde evitare condizionamenti della volontà della persona contattata nel comunicare i dati del terzo cui è intestato l'abbonamento. Il Garante ha quindi segnalato alla società l'opportunità di specificare che la compilazione del questionario facilita l'identificazione dell'abbonamento di riferimento e può rendere superflue ulteriori verifiche.

L'Autorità ha chiesto da ultimo chiarimenti alla società sui presupposti giuridici in base ai quali RAI-radiotelevisione italiana S.p.a. sollecita, nell'ambito di altri tipi di comunicazioni, il rilascio di una dichiarazione sostitutiva dell'atto di notorietà per le situazioni di convivenza con persone titolari di abbonamento al servizio radiotelevisivo, in riferimento a quanto disposto dagli artt. 9 e 10 della legge n. 675/1996.

Il Garante è in procinto di definire conclusivamente tutti i procedimenti attivati sulle varie questioni relative al canone radiotelevisivo, in relazione agli elementi forniti dalla RAI in un quadro di piena collaborazione rispetto alle verifiche effettuate.

14. ARCHIVI RELATIVI A CITTADINI EXTRACOMUNITARI

L'Autorità ha affrontato nel corso dell'anno anche alcune delicate questioni relative alle modalità di costituzione, di gestione e di interconnessione di archivi relativi ai cittadini extracomunitari da parte di soggetti pubblici.

Trattasi di un tema complesso, che può implicare il trattamento dei dati sensibili di persone straniere e che richiede il coordinamento tra l'ampia e articolata legislazione di settore, anche in materia di tutela dell'ordine pubblico e di immigrazione, e le prescrizioni e i principi sulla protezione di dati personali.

Il Garante, nel mese di marzo, ha espresso un parere favorevole sullo schema di decreto poi adottato nel mese di dicembre dal Ministro dell'interno e relativo alle modalità di comunicazione, anche in via telematica, dei dati concernenti i cittadini stranieri fra gli uffici di anagrafe dei comuni, gli archivi dei lavoratori extracomunitari e gli archivi dei competenti organi centrali e periferici del Ministero dell'interno (G. U. 11 gennaio 2001, n. 8).

Il Garante ha poi segnalato al Ministero dell'interno-Dipartimento di pubblica sicurezza la necessità di adeguare i trattamenti dei dati relativi ai permessi di soggiorno per motivi di protezione sociale alla normativa sulla protezione dei dati personali attraverso il ricorso a codici alfanumerici idonei ad identificare la tipologia di permesso ai soli uffici interessati (art. 18, d.lg. n. 286/1998).

L'Autorità ha quindi ritenuto lesive del generale principio di pertinenza e di non eccedenza previsto dall'art. 9 della legge n. 675/1996 le modalità con le quali un ufficio periferico di pubblica sicurezza ha rilasciato alcuni permessi speciali.

In particolare è stata contestata l'apposizione a margine di uno schedario degli estremi della normativa sul soggiorno per motivi di protezione sociale e l'indicazione delle associazioni impegnate nel reinserimento dello straniero. Tale procedura rendeva infatti facilmente desumibile la tipologia del permesso, esponendo gli interessati al rischio di essere facilmente individuati quali persone sottratte ai condizionamenti di organizzazioni criminali.

Il Ministero dell'interno ha recepito le osservazioni formulate dall'Autorità, diramando una circolare con la quale ha disposto che all'atto del rilascio dei permessi di soggiorno per motivi di protezione sociale si debba fare riferimento solo a codici alfanumerici e alla locuzione "motivi umanitari".

Sempre con riferimento a questo argomento, è in via di definizione un procedimento attivato da una segnalazione relativa ad un rilevamento effettuato nelle scuole pubbliche da parte degli insegnanti di religione cattolica. Si tratta di uno studio volto ad acquisire elementi utili per predisporre i nuovi progetti formativi rivolti ad una scuola sempre più multietnica e multireligiosa. I dati raccolti riguardano il numero di studenti immigrati – anche in riferimento alla provenienza geografica – che si avvalgono o meno dell'insegnamento della religione cattolica.

FORZE DI POLIZIA, UFFICI GIUDIZIARI E SERVIZI DI INFORMAZIONE E DI SICUREZZA

15. PROFILI GENERALI

Come è noto, la legge n. 675/1996 prevede, all'art. 4, alcuni trattamenti svolti in ambito pubblico che sono ancora parzialmente sottratti alla disciplina in materia di protezione dei dati personali (ci si riferisce, in particolare, ai trattamenti effettuati per ragioni di giustizia, per finalità di prevenzione e repressione dei reati, a quelli relativi a dati memorizzati o destinati a confluire nel Centro elaborazione dati del Dipartimento della pubblica sicurezza, nonché ai trattamenti effettuati dai servizi di informazione e di sicurezza).

A tali trattamenti, tuttavia, si applicano alcune disposizioni della legge n. 675, in particolare quelle attinenti ai requisiti di liceità e alla sicurezza dei trattamenti di dati personali, nonché quelle che prevedono l'esercizio da parte del Garante di verifiche e controlli (art. 4, comma 2, l. n. 675/1996). Gli uffici giudiziari o di polizia hanno, in particolare, il dovere di rispettare il principio di "proporzionalità" nel trattamento dei dati (in base al quale, fra l'altro, si possono trattare solo i dati *"pertinenti ... e non eccedenti"* rispetto alle finalità istituzionali, secondo quanto previsto dall'art. 9 l. n. 675/1996) e l'obbligo di adottare le cautele necessarie a garantire la sicurezza dei dati trattati (art. 15, commi 1 e 2, l. n. 675/1996 e d.P.R. n. 318/1999 sulle misure minime di sicurezza).

Sulla portata e sui limiti dell'attuale applicabilità di tali disposizioni ai trattamenti dell'art. 4 si è rivolta l'attenzione del Garante, in attesa che sia completato il quadro normativo. La recente legge 24 marzo 2001, n. 127, infatti, al fine di ultimare il processo di piena attuazione dei principi previsti dalla legge n. 675 nell'ambito di specifici settori, già avviato con le leggi-delega n. 676/1996 e n. 344/1998, ha previsto un ulteriore differimento del termine per l'esercizio della delega al 31 dicembre 2001.

16. PROTEZIONE DEI DATI E ATTIVITÀ GIUDIZIARIA

I principi descritti si applicano ai trattamenti di dati personali svolti *"per ragioni di giustizia"*, sebbene la normativa processuale antecedente alla legge n. 675/1996 non sia stata ancora modificata alla luce delle nuove garanzie in materia di trattamento dei dati personali.

Come già riportato nella relazione per l'anno 1999, il Garante si è espresso in tal senso in particolare nel provvedimento del 29 febbraio 2000 rispetto ai trattamenti effettuati nell'ambito di un giudizio instaurato da persone che avevano contratto particolari sindromi a causa della somministrazione di emoderivati infetti.

Data la delicatezza della materia, il legale delle parti aveva richiesto che fossero adottate nel processo misure idonee a tutelare la riservatezza dell'identità dei ricorrenti e, in proposito, l'Autorità ha sottolineato che i principi previsti dalla legge n. 675, benché non ancora compiutamente articolati nelle norme processuali civili e penali, dovrebbero comunque concretizzarsi in misure anche di carattere organizzativo, pur nei limiti delle prerogative dell'autorità giudiziaria. La non integrale adozione in giudizio di efficaci cautele può condizionare, infatti, il diritto del cittadino alla propria difesa o addirittura comportare la rinuncia della parte lesa a chiedere il risarcimento dei danni per timore dell'ampia conoscibilità delle patologie sofferte.

L'Autorità ha comunque segnalato al Governo e al Parlamento l'opportunità che siano introdotte disposizioni processuali volte a contemperare meglio le esigenze processuali con quella di garantire la riservatezza dei soggetti coinvolti in vicende giudiziarie riguardanti aspetti particolarmente delicati della persona.

Sull'argomento il Garante, nel luglio 2000, ha anche avuto un proficuo incontro con l'Associazione nazionale magistrati, nel corso del quale quest'ultima ha sottolineato l'esigenza di integrare, anche sul piano normativo, la disciplina processuale e deontologica al fine di assicurare il pieno rispetto dei dirit-

ti della personalità e in particolare della riservatezza. Il Garante e l'Associazione hanno poi concordato sulla necessità di operare un attento bilanciamento, anche sul piano delle prassi applicative, tra la tutela della riservatezza e la specificità della funzione giudiziaria che è preposta alla tutela di interessi anch'essi costituzionalmente garantiti.

Il Garante non ha rinvenuto, invece, elementi per intervenire in ordine alle disposizioni che un tribunale aveva impartito in tema di accesso degli operatori giudiziari e, in particolare, degli avvocati, alle notizie sullo stato dei procedimenti civili e penali inserite nel sistema informativo del medesimo ufficio giudiziario; ciò anche in considerazione delle precedenti prese di posizione con le quali l'Autorità ha richiamato l'attenzione sul rapporto fra le norme processuali sulla richiesta di atti e di notizie e le disposizioni della legge n. 675.

Sotto il profilo dei controlli sui trattamenti svolti *"per ragioni di giustizia"*, il Garante, anche nel decorso anno, ha precisato che è consentito inviare all'Autorità una segnalazione o un reclamo (art. 31, l. n. 675/1996) per sollecitare il controllo sulla liceità dei trattamenti, ma non è possibile esercitare i diritti nelle forme previste dagli articoli 13 e 29 della legge n. 675 rivolgendosi direttamente all'ufficio giudiziario o presentando un formale ricorso all'Autorità stessa.

Con provvedimento del 14 febbraio 2001, il Garante ha ritenuto tuttavia che i diritti di cui all'articolo 13 si possono esercitare rispetto ai dati contenuti in una nota-circolare del Consiglio superiore della magistratura quale quella esaminata, con la quale si informavano gli uffici giudiziari dell'avvenuta nomina dei referenti per la formazione decentrata. La decisione era ovviamente basata sul presupposto che i trattamenti di dati non erano effettuati per "ragioni di giustizia". Con il relativo ricorso al Garante, il magistrato interessato aveva chiesto il blocco del trattamento dei dati personali e la rettifica delle informazioni diffuse sul proprio conto con la circolare, ritenendo che si trattasse di dati incompleti e non pertinenti e comunque implicanti discredito alla propria persona. Nel merito, l'Autorità ha poi respinto la richiesta di blocco anche in quanto il provvedimento inibitorio non sarebbe comunque risultato necessario alla luce dell'iniziativa assunta dal CSM di sostituire la circolare "impugnata". Ha inoltre respinto anche la richiesta di rettifica in quanto, per le modalità con cui era stata formulata, avrebbe determinato la diffusione di ulteriori dati anch'essi non pertinenti rispetto alla finalità da perseguire; ciò sul presupposto che l'applicazione di un principio previsto dalla legge n. 675 non può comportare un'ulteriore inosservanza degli altri principi di protezione dei dati.

Anche sotto il profilo dei controlli, con l'attuazione della legge-delega n. 127/2001, si avrà la possibilità di sperimentare nuovi strumenti di garanzia per gli interessati volti, ad esempio, a consentire loro un esercizio più immediato dei diritti previsti dall'articolo 13 della legge n. 675, tenendo comunque conto della specificità dei trattamenti svolti per *"ragioni di giustizia"*.

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

– le indicazioni espresse dall'Autorità stessa sullo schema di regolamento recante disposizioni per l'uso di strumenti informatici e telematici nel processo civile (regolamento poi approvato con decreto del Ministro della giustizia 13 febbraio 2001, n. 123);

– il parere reso sullo schema di decreto ministeriale riguardante le regole procedurali relative alla tenuta dei registri informatizzati dell'Amministrazione della giustizia (decreto del Ministro della giustizia 27 marzo 2000, n. 264);

– il provvedimento del 17 febbraio 2000, con il quale il Garante ha riconosciuto la liceità del trattamento di dati personali relativi a minori da parte di un Ufficio per la mediazione penale costituito su iniziativa di alcuni soggetti pubblici, in quanto la normativa di settore consente agli uffici giudiziari di avvalersi della collaborazione di esperti per accertare la personalità di minori e di promuoverne la conciliazione con le persone offese dal reato;

– il provvedimento del 30 marzo 2000 con cui l'Autorità, in risposta ad un quesito posto da un ufficio giudiziario, ha chiarito (in senso diverso da quanto pure ritenuto dall'Ufficio legislativo del Ministero della giustizia) che l'articolo 4 della legge n. 675 si riferisce inequivocamente a tutte le attività comunque effettuate nell'ambito di uffici giudiziari, anche dalla magistratura amministrativa e contabile, ribadendo la diretta applicabilità delle disposizioni della legge n. 675 richiamate nel comma 2 dell'art. 4 a tutti i trattamenti svolti per "ragioni di giustizia" e non solo a quelli amministrativi strumentali alla funzione giurisdizionale, fermi restando, in ogni caso, gli opportuni adattamenti resi indispensabili dalla specificità degli interessi perseguiti previsti dalla più volte ricordata legge delega;

– la nota del 9 novembre 2000 con la quale il Garante ha richiamato l'attenzione del Ministro della giustizia sulla pubblicazione, sul sito Internet di un tribunale, di un avviso relativo all'udienza preliminare di un complesso procedimento penale connesso all'utilizzazione di emoderivati infetti. Nell'occasione l'Autorità ha ribadito che, pur nella consapevolezza che la validità dei relativi atti deve essere verificata nella competente sede giudiziaria, l'applicazione – seppure parziale – della legge n. 675/1996 ai trattamenti di dati per ragioni di giustizia impone agli uffici giudiziari di adottare modalità applicative delle norme processuali più consone alle libertà fondamentali e alla dignità degli interessati.

17. LE MODALITÀ DI NOTIFICAZIONE DI ATTI

La tematica delle cautele da osservare a garanzia della riservatezza delle persone interessate da notifiche di atti giudiziari è, com'è noto, fra quelle cui il Garante ha dedicato maggiore attenzione, sin dal provvedimento del 22 ottobre 1998 (v. Relazione per l'anno 1998, p. 23), considerato il generale interesse dei cittadini manifestato. Il Garante era già tornato sull'argomento nel corso del 1999 chiarendo, con una nota del 26 ottobre 1999, che le cautele richieste nelle notifiche a garanzia della riservatezza della persona interessata, e in particolare nei confronti del terzo cui venga notificato l'atto (ad es. busta chiusa), sono da ritenersi applicabili anche al processo contabile ed amministrativo (v. Relazione per l'anno 1999, p. 62). La questione è stata portata anche all'attenzione del Ministero della giustizia.

Alcune indicazioni dell'Autorità sono state sostanzialmente recepite in un disegno di legge presentato nella decorsa legislatura il quale, tuttavia, è stato approvato solo da un ramo del Parlamento (XIII^ legislatura, AC 6735). Tale iniziativa, che si auspica venga riproposta, opportunamente aggiornata, nel corso della nuova legislatura, prevede alcune soluzioni rispetto alle notificazioni degli atti del processo (si era prevista infatti la modifica di alcune disposizioni dei codici di rito e della normativa sulle notifiche a mezzo posta) e nell'ambito di procedimenti amministrativi, dove il problema è altrettanto sentito (ad es. notifica di sanzioni a carattere amministrativo, cartelle esattoriali, ecc.).

18. ATTIVITÀ DI POLIZIA

Per quanto riguarda i trattamenti svolti per finalità di polizia, hanno assunto un particolare rilievo gli accertamenti svolti dal Garante a seguito di alcune segnalazioni di militari e di cittadini in ordine a taluni trattamenti di dati personali effettuati dall'Arma dei Carabinieri riguardanti, in particolare, le c.d. "pratiche permanenti".

Dagli accertamenti effettuati non sono emersi trattamenti sostanzialmente difformi dalla normativa vigente. Sono stati però evidenziati alcuni problemi che derivano da un quadro normativo non ancora pienamente armonizzato ai principi introdotti dalla legge sulla riservatezza dei dati. In tal senso, il Garante ha segnalato al Governo la necessità di un sollecito intervento normativo, anche in via regolamentare, sia per quanto riguarda i trattamenti a fini amministrativi, sia per quelli attinenti alle attività di polizia.

In particolare, dalle notizie fornite dall'Arma in un quadro di collaborazione, è emerso che alcune prassi da lungo tempo adottate hanno portato alla conservazione di un numero elevato di pratiche e di informazioni ormai in contrasto con i sopravvenuti principi in materia di protezione dei dati. L'Autorità ha pertanto indicato – accanto alle auspicate soluzioni normative – la necessità di interventi anche sul piano organizzativo, volti, fra l'altro, ad individuare termini più adeguati di conservazione dei dati, nonché livelli diversificati di consultazione dei documenti, a consentire verifiche periodiche della pertinenza delle informazioni e ad assicurare idonee cautele rispetto ai dati più risalenti nel tempo, specie se di natura sensibile. L'Arma ha già fornito alcuni primi utili riscontri con due note pervenute nel marzo di quest'anno.

Analogamente a quanto appena descritto in ordine alle "pratiche permanenti" dell'Arma, il Garante non ha rinvenuto elementi di illiceità nei trattamenti di dati effettuati dall'Ufficio per la garanzia peni-

tenziaria del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia, in ordine ai quali un sindacato di categoria aveva segnalato presunte "schedature" del personale con l'asserita creazione di fascicoli riportanti informazioni di carattere privato (*Provv.* del 30 ottobre 2000).

Un'altra problematica della quale il Garante è tornato ad occuparsi è quella delle richieste di informazioni formulate nell'ambito di attività di indagine di polizia giudiziaria o avanzate da pubbliche autorità per altre finalità istituzionali.

Il Garante aveva già chiarito alcuni importanti aspetti applicativi della disciplina in materia allorché, nel 1999, aveva fornito una prima risposta ad una compagnia aerea circa i limiti di acquisibilità da parte delle forze di polizia di dati relativi ai passeggeri dei voli (v. Relazione per l'anno 1999, p. 63).

Più di recente, l'Autorità ha nuovamente distinto due categorie di richieste: a) quelle riconducibili ad un'attività di polizia giudiziaria, cui si applica l'art. 4 della legge n. 675, alle quali deve darsi corso in base al codice di procedura penale non ostandovi l'applicabilità della stessa legge n. 675, salva l'applicabilità, in ogni caso, del principio di pertinenza (per cui le richieste devono, nei limiti del possibile, essere circostanziate sotto il profilo oggettivo e temporale); b) quelle avanzate da forze di polizia o da altre pubbliche autorità non riconducibili all'esercizio di poteri di polizia giudiziaria (o, comunque, alle altre funzioni indicate nell'art. 4), cui si applica l'intera disciplina della legge n. 675 e, in particolare, quella prevista per i flussi informativi fra soggetti pubblici e privati (artt. 27 e 20, l. n. 675).

La questione verrà nuovamente approfondita a breve con particolare riguardo alla richiesta di acquisire sistematicamente dati sui passeggeri di voli aerei.

Per quanto attiene al profilo dei controlli sui trattamenti effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o su trattamenti comunque riconducibili ad attività di polizia considerate nell'art. 4 della legge, il Garante, in relazione ad un ricorso avverso il trattamento dei dati personali utilizzati per un avviso orale del questore, ha ribadito che per i trattamenti effettuati dal predetto C.e.d. o riconducibili a *"finalità ... di prevenzione, accertamento e repressione dei reati"* (art. 4, comma 1, lett. e)) l'interessato può esercitare i suoi diritti di verifica e di rettifica direttamente nei confronti del Dipartimento della pubblica sicurezza, Ufficio per il coordinamento e la pianificazione delle forze di polizia, ovvero sollecitare l'instaurazione da parte del Garante di un autonomo procedimento di verifica su quanto segnalato dall'interessato in ordine ai dati che lo riguardano (art. 31, comma 1, lett. d) e p) e art. 32), ma non può presentare ricorso al Garante ai sensi dell'art. 29 della legge n. 675 e 18 e ss. del d.P.R. n. 501/1998.

Resta ferma l'esigenza che anche attraverso i decreti delegati previsti dalla citata legge-delega, siano introdotte modifiche alle attuali procedure tali da rendere più snelle, ma anche più efficaci le verifiche.

19. Sistema di informazione Schengen

Nel corso dell'anno il Garante, quale Autorità di controllo sulla sezione nazionale del Sistema informativo Schengen (N.SIS), ha ricevuto numerose richieste di verifica dell'eventuale registrazione, nei predetti archivi, di dati personali dei richiedenti e della liceità dei relativi trattamenti in base ai principi contenuti nella Convenzione di applicazione dell'Accordo di Schengen e nella legge n. 675 (art. 11, l. 30 settembre 1993, n. 388).

La gran parte delle richieste sono state presentate dagli interessati direttamente al Garante, mentre in alcuni casi esse sono pervenute dalle omologhe Autorità di controllo degli altri Paesi alle quali i richiedenti si sono rivolti in base alla procedura di consultazione fra Autorità di controllo prevista dall'art. 114, comma 2, della Convenzione.

Si tratta, in molti casi, di istanze relative al diniego del rilascio di visti; altre richieste sono finalizzate a conoscere l'esistenza e le cause di provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno nel nostro Paese ovvero si riferiscono a casi di usurpazione d'identità o di omonimia.

Anche nel decorso anno si è riscontrato un notevole incremento del numero delle richieste pervenute al Garante rispetto all'anno precedente (n. 59 nel periodo 1999-10 aprile 2000), anche a seguito della proficua azione del nostro Paese nell'ambito della campagna informativa sui diritti del cittadino nei confronti del Sistema d'informazione Schengen, a suo tempo deliberata dall'Autorità comune di controllo in tutti i Paesi aderenti all'Accordo.

L'Autorità garante e l'ufficio SIRENE del Dipartimento della pubblica sicurezza, all'esito di proficui incontri su taluni aspetti applicativi della materia, hanno convenuto circa la necessità che sia assicurata una maggiore speditezza alle procedure per il riscontro agli interessati delle verifiche effettuate, in particolare nei casi in cui l'Ufficio del Garante fornisce tale riscontro sulla base degli elementi forniti dal Dipartimento.

Nel quadro delle verifiche effettuate con la piena collaborazione del Dipartimento non sono emerse specifiche violazioni nelle modalità del trattamento dei dati. Il Garante ovviamente proseguirà nell'esercizio delle proprie funzioni di controllo approfondendo, anche sulla base degli orientamenti dell'Autorità comune di controllo Schengen, la piena corrispondenza alla Convenzione di applicazione dell'Accordo di Schengen delle varie modalità di raccolta e trattamento di specifiche categorie di dati.

20. SERVIZI DI INFORMAZIONE E DI SICUREZZA

Il Garante ha svolto anche nel corso del 2000 l'attività di verifica su specifici trattamenti di dati personali effettuati presso gli organismi competenti in materia di informazioni e di sicurezza (SISMI, SISDE e CESIS), effettuando accertamenti rispetto alle segnalazioni dei soggetti interessati, in conformità alla legge n. 675/1996. I controlli sono stati effettuati con le modalità già osservate nel corso dei precedenti anni, anche nei casi più recenti con la piena collaborazione dei predetti organismi.

Al termine di tali accertamenti, che sono stati concentrati nel terzo gruppo di verifiche effettuate dal Garante a decorrere dalla sua istituzione (per un totale di circa trenta persone fisiche e giuridiche che hanno chiesto accertamenti), l'Autorità, nel riscontrare la sostanziale liceità e correttezza del trattamento dei dati personali, ha rivolto alle autorità di Governo, nel maggio del 2000, alcune valutazioni d'insieme sull'applicazione della normativa in materia di protezione dei dati personali. In particolare è stata richiamata l'attenzione sull'opportunità di impartire nuove istruzioni agli uffici periferici per evitare l'acquisizione di informazioni non pertinenti rispetto alle finalità di tutela della sicurezza e difesa dello Stato.

È stata inoltre rilevata l'esigenza di una maggiore attenzione al profilo della conservazione nel tempo dei dati raccolti, raccomandando una maggiore selezione delle informazioni disponibili anche sulla base di tecniche informatiche e un accesso o una conservazione diversificata del materiale riguardante vicende remote.

Un'indicazione ha riguardato il potenziamento delle tecniche di classificazione di fascicoli, che pure sono risultati conservati in modo ordinato e ricostruibile.

Agli interessati che hanno chiesto accertamenti è stato fornito un riscontro nel rispetto di quanto previsto dall'art. 32, comma 6, della legge n. 675/1996.

Infine, anche per quanto attiene ai controlli esercitabili sui trattamenti svolti dagli organismi di sicurezza ovvero su dati coperti da segreto di Stato, il Garante, con un provvedimento del 28 febbraio 2000, ha precisato che è possibile inviare all'Autorità una segnalazione o un reclamo per sollecitarne il controllo sulla legittimità dei trattamenti, ma non è consentito esercitare i diritti previsti dall'articolo 13 della legge n. 675 rivolgendosi direttamente ai predetti organismi ed eventualmente con ricorso al Garante in base all'articolo 29 della stessa legge n. 675.

SANITÀ

21 PROFILI GENERALI

Il nuovo assetto normativo delineato dal legislatore delegato nel 1999 per la disciplina del trattamento dei dati idonei a rivelare lo stato di salute da parte degli organismi sanitari pubblici, nonché degli organismi sanitari e degli esercenti le professioni sanitarie operanti in regime di convenzione o di accreditamento con il Servizio sanitario nazionale, ha incontrato non poche difficoltà applicative.

Invero, l'efficacia delle disposizioni degli artt. 22 e 23 della legge n. 675, così come riformulate a seguito delle integrazioni e modificazioni introdotte dai dd.lg. 11 maggio 1999, n. 135, in materia di "*trattamento dei dati sensibili da parte dei soggetti pubblici*" e 30 luglio 1999, n. 282 recante "*disposizioni per garantire la riservatezza dei dati personali in ambito sanitario*", è rimessa all'adozione di un regolamento del Ministro della sanità con il quale dovranno essere definite le semplificazioni introdotte dall'art. 2, comma 1, del citato d.lg. n. 282.

Alla stesura di tale regolamento, che sarà emanato previo parere della Conferenza Stato-Regioni e del Garante, lavora un'apposita commissione istituita presso il Ministero della sanità. Quest'ultima, nonostante l'impegno, non è ancora addivenuta ad un testo definitivo che, nell'individuare modalità semplificate per il trattamento dei dati sulla salute e, in particolare, per le informative di cui all'art. 10 della legge n. 675 e per la raccolta del consenso, tenga conto delle diverse esigenze di tutti i titolari coinvolti nella "catena sanitaria" – anche in relazione alle diverse finalità – nonché della necessaria previsione di un periodo non breve per la messa a regime del sistema.

Il lavoro è reso peraltro più complesso dal fatto che al medesimo regolamento del Ministero della sanità, anziché alle singole aziende ed organismi sanitari ed ospedalieri, spetta il compito di provvedere alla ricognizione di tutti i trattamenti dei dati sulla salute effettuati nell'ambito del Servizio sanitario nazionale e, quindi, alla specificazione "dei tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi", ai sensi dell'art. 22, comma 3-*bis*, della legge n. 675/1996.

È evidente che, allo stato, la mancata emanazione del suddetto regolamento – che pure sembra poter giungere a rapida definizione – rende priva di concreta efficacia la volontà del legislatore delegato di prevedere, per il trattamento dei dati sulla salute, una disciplina uniforme per i soggetti pubblici e per quelli privati convenzionati o accreditati con il Servizio sanitario nazionale. A tale riguardo deve aggiungersi che la proroga al 31 dicembre 2001 – disposta con legge 24 marzo 2001, n. 127 – per l'esercizio della delega prevista dalla legge n. 676/1999, potrebbe costituire una preziosa occasione per apportare eventuali altri interventi di carattere integrativo e correttivo (art. 2 l. n. 676/1996) alla vigente disciplina sul trattamento dei dati personali in ambito sanitario.

L'assimilazione sopra detta tra soggetti pubblici e privati operanti nell'ambito del Servizio sanitario nazionale non ha invece interessato i professionisti sanitari operanti in regime di libera professione e tutti gli altri soggetti privati per i quali resta valida la regola generale della doppia condizione del consenso scritto e dell'autorizzazione del Garante o, se del caso, la disciplina speciale prevista dall'art. 23, comma 1, della legge n. 675/1996.

Va rammentato tuttavia che la normativa delegata ha preso comunque in considerazione gli organismi sanitari privati e gli esercenti le professioni sanitarie estranei al S.S.N., laddove ha previsto l'emanazione di appositi codici di deontologia e buona condotta da adottarsi ai sensi dell'art. 31, comma 1, lett. h), della legge n. 675/1996. Questi dovranno, da un lato, prevedere una disciplina integrativa dell'emanando regolamento del Ministro della sanità e, dall'altro, in coordinamento con quest'ultimo, introdurre alcune semplificazioni per il trattamento dei dati sulla salute anche da parte degli organismi sanitari ed esercenti le professioni sanitarie non facenti parte del Servizio sanitario nazionale (art. 17, comma 3, d.lg. n. 135/1999, come modificato dal d.lg. n. 282/1999).

In questo intricato quadro normativo il Garante ha proseguito la sua attività autorizzatoria rinnovando anzitutto, con provvedimento del 20 settembre 2000, l'autorizzazione generale per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2000, pubblicata sulla Gazzetta

Ufficiale n. 229 del 30 settembre 2000). La nuova formulazione dell'autorizzazione n. 2/2000 non si discosta sostanzialmente dalla precedente. Il termine di efficacia è stato fissato al 31 dicembre 2001.

Sempre nell'ambito dell'attività autorizzatoria il Garante, con provvedimento del 5 dicembre 2000 (pubblicato nel *Bollettino*, nn. 14/15, p. 10), pronunciandosi in ordine ad una specifica richiesta di autorizzazione, ha accolto soltanto parzialmente la richiesta stessa. In particolare, mentre da un lato ha chiarito che il trattamento dei dati idonei a rivelare lo stato di salute per finalità di gestione degli ordini dei clienti è già autorizzato dal provvedimento n. 2/2000 (punto 1.2 lett. e)) alle condizioni ivi indicate, ha d'altra parte opposto un diniego al trattamento dei dati sulla salute finalizzato ad analisi di *marketing* e di statistica, alla creazione dei profili dei clienti, nonché a proposte commerciali ed offerte di vendita in base alle tipologie di acquisto effettuate da ciascun cliente.

Relativamente a questi ultimi trattamenti, infatti, il Garante ha ritenuto che non sussistessero circostanze particolari o situazioni eccezionali tali da giustificare il rilascio di un'autorizzazione specifica in deroga a quella generale e che la richiesta di autorizzazione non era stata predisposta secondo il modello approvato dall'Autorità ai sensi dell'art. 14 del d.P.R. n. 501/1998.

Un'altra istanza di autorizzazione ha fornito al Garante l'occasione per precisare alcuni aspetti relativi al corretto utilizzo dei dati sulla salute da parte di una società che intendeva fornire ai propri clienti un servizio di messa in rete dei profili sanitari dei clienti stessi in un'area ad accesso riservato di un sito Internet, alla quale poter accedere (in caso di necessità anche dall'estero) tramite un codice identificativo personale.

Al riguardo, con nota del 7 febbraio 2001, il Garante ha chiarito che l'accesso al profilo sanitario dell'interessato via Internet dall'estero configura un'ipotesi di trasferimento transfrontaliero dei dati per il quale è di regola necessario il consenso scritto dell'interessato (art. 28, comma 4, lett. e)), eventualmente cumulato con quello più generale previsto nell'ambito del rapporto contrattuale.

Inoltre, con riferimento ai profili della sicurezza e alle misure minime previste dal d.P.R. n. 318/1999, l'Autorità ha precisato che l'assegnazione del codice identificativo e la sua gestione, anche rispetto all'obbligo di disattivazione in caso di "*mancato utilizzo per un periodo superiore a sei mesi*" (art. 4, comma 1, lett. b), d.P.R. n. 318/1999), riguardano ciascun utente a prescindere dalla circostanza che l'utente medesimo o una persona delegata acceda solo ai dati che lo riguardano. Ne deriva che il rapporto contrattuale dovrà prevedere che all'assegnazione del codice identificativo segua anche l'autorizzazione all'accesso prevista dall'art. 5 del d.P.R.. sopra citato ("*accesso ai dati particolari*").

Il richiamo all'adozione delle misure minime di sicurezza, nonché al rispetto dei principi generali fissati dal d.lg. n. 135/1999, è contenuto anche in un parere reso dal Garante al Ministero della sanità nell'esercizio della sua funzione consultiva (art. 31, comma 2, l. n. 675/1996). Si tratta, in particolare, del parere sullo schema di decreto ministeriale recante modiche al certificato di assistenza al parto (in *Bollettino,* n. 11-12, p. 34), nel quale l'Autorità ha sottolineato la necessità che nei *nuovi* certificati siano adottate misure idonee a garantire la massima riservatezza delle informazioni per le quali già esiste una disciplina speciale (l. n. 194/1978 sull'interruzione di gravidanza e art. 2, comma 1, l. n. 127/1997 sul diritto della madre all'anonimato).

Va fatta menzione, inoltre, di alcune precisazioni fornite dal Garante nell'ambito dell'esame di alcuni ricorsi presentati ai sensi dell'art. 29 della legge n. 675.

In particolare l'Autorità, nel decidere in merito ad una richiesta di accesso con la quale l'interessato intendeva acquisire copia di un'indagine ecografica effettuata presso un presidio ospedaliero realizzata su un supporto che per la tecnologia usata non permetteva l'estrazione di copia ha precisato che l'art. 13 della legge n. 675 non prevede – in linea di principio – la necessaria consegna della documentazione o dei supporti sui quali i dati sono conservati. Tuttavia, il titolare e il responsabile del trattamento sono tenuti ad estrapolare dai propri archivi e documenti tutte le informazioni su supporto cartaceo o informatico che riguardano il richiedente e a riferirle a quest'ultimo con modalità idonee a rendere i dati facilmente comprensibili, specie quando le informazioni, se non messe a disposizione nella loro interezza a mezzo dell'esibizione o consegna di copia di documenti, non siano agevolmente ricostruibili o siano snaturate del loro contenuto (*Provv.* dell'11 aprile 2000, in *Bollettino* 11-12, p. 58). Nel caso di specie, la soluzione è stata quindi individuata nella visione diretta delle immagini riprodotte sull'unico supporto, da parte del medico designato.

Inoltre, esaminando il ricorso con il quale un ricorrente chiedeva la cancellazione dei dati contenuti nella relazione medica stilata da un centro di igiene mentale, perché trattati senza il suo consenso, il Garante ha chiarito che, in base alla disciplina vigente all'epoca in cui si erano svolti i fatti (artt. 22, comma 3, e 41, comma 5, della l. n. 675/1996), la struttura sanitaria pubblica aveva potuto legittimamente svolgere un'attività di trattamento rientrante tra i propri compiti istituzionali senza il consenso del soggetto interessato (decisione del 29 settembre 2000).

In altra occasione l'Autorità ha invece dichiarato la fondatezza del ricorso presentato da due coniugi nei confronti di un'azienda sanitaria e della relativa società assicurativa, che non avevano fornito riscontro alla richiesta di accesso formulata dai ricorrenti ai sensi dell'art. 13 della legge n. 675/1996. In particolare, il Garante ha riconosciuto il diritto dei ricorrenti di accedere alle informazioni personali contenute in alcune relazioni cliniche, purché e nella misura in cui esse siano direttamente o indirettamente riferibili agli interessati. D'altra parte, invece, il diritto di accesso non riguarda altre parti delle relazioni cliniche che siano riferibili soltanto a rapporti interni all'azienda sanitaria o a circostanze attinenti unicamente al personale medico o paramedico coinvolto nella vicenda (decisione del 12 dicembre 2000).

22. DATI GENETICI

Come è noto, anche con riferimento ai dati genetici è intervenuto il legislatore delegato introducendo il principio secondo cui il trattamento dei dati genetici, da chiunque effettuato, dovrà essere oggetto di una nuova ed apposita autorizzazione del Garante (art. 17, comma 5, d.lg. 11 maggio 1999, n. 135, come integrato e modificato dall'art. 16 del d.lg. 30 luglio 1999, n. 281).

Tale autorizzazione, che avrà carattere generale e dunque troverà applicazione senza la necessità di una apposita richiesta, sarà rilasciata dal Garante a seguito di un complesso procedimento nel quale deve essere "*sentito il Ministro della sanità che acquisisce, a tal fine, il parere del Consiglio superiore di sanità*".

Con deliberazione del 2 maggio 2000 (in *Bollettino* n. 13, p. 19) l'Autorità ha avviato tale procedura stabilendo, peraltro, che l'autorizzazione al trattamento dei dati genetici dovrà: *a*) disciplinare le finalità e le modalità di raccolta, di utilizzazione e di eventuale comunicazione di questi dati; *b*) prevedere misure che consentano all'interessato di esprimere in modo consapevole il consenso all'uso dei dati e che possano prevenire discriminazioni nei suoi confronti o di terzi; *c*) garantire il rispetto della volontà dell'interessato di non essere informato sull'esito degli accertamenti e, infine, *d*) disciplinare le cautele da adottare sul piano della sicurezza nel trattamento dei dati e per assicurare il rispetto del segreto professionale.

Fino all'adozione di una regolamentazione più compiuta, il trattamento dei dati genetici resta tuttavia disciplinato dall'autorizzazione n. 2/2000. Il legislatore delegato ha infatti previsto (art. 17, comma 5, sopracitato) che, nelle more dell'autorizzazione specifica, i trattamenti dei dati genetici possono essere proseguiti sulla base dell'attuale autorizzazione generale del Garante (punto 2, lett. *b*), dell'autorizzazione n. 2/2000).

Al momento, sulla base dell'autorizzazione n. 2/2000 (che prevede il consenso scritto ai sensi degli artt. 22 e 23 della legge n. 675, nonché alcune esclusioni soggettive e limitazioni nelle finalità perseguibili), il trattamento dei dati genetici resta temporaneamente consentito sino al 31 dicembre 2001 "*limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività*". La medesima autorizzazione n. 2/2000 non opera, invece (e il titolare del trattamento deve quindi richiedere previamente al Garante un'apposita autorizzazione), se manca il consenso dell'interessato e il trattamento dei dati genetici è finalizzato alla tutela della salute di un terzo o della collettività. L'inosservanza delle prescrizioni impartite dal Garante attraverso lo strumento autorizzatorio resta punita con la sanzione penale (art. 37 legge n. 675/1996).

L'intervento del Garante in materia di dati genetici si è poi avuto in relazione a talune notizie, apparse sulla stampa nazionale ed internazionale, secondo cui alcune popolazioni sarde sarebbero oggetto di indagini genetiche destinate ad essere proiettate sul mercato anche internazionale.

Avvalendosi dei poteri conferitigli dal legislatore (art. 32, comma 1, legge n. 675/1996), l'Autorità è quindi intervenuta chiedendo ai soggetti coinvolti informazioni e precisazioni circa le finalità e le modalità del complesso trattamento di dati genetici denunciato dalla stampa.

Sebbene gli accertamenti e gli approfondimenti siano ancora in corso l'Autorità, che ha proceduto anche ad un sopralluogo, ha potuto registrare la disponibilità dei ricercatori a collaborare e a fornire ogni utile elemento di valutazione.

Occorre infine ricordare che nel giugno 2000 il Garante, in collaborazione con il Comitato nazionale per la bioetica e Legambiente, ha promosso un convegno sul tema "I nostri dati genetici: opportunità, rischi e diritti".

In tale occasione, sulla base di uno studio presentato da Legambiente dal quale è emerso che oltre 50 siti Internet, quasi tutti statunitensi, vendono *on-line* kit "fai da te" per test genetici, tutti i relatori hanno espresso forte preoccupazione per il diffondersi del fenomeno anche nel nostro Paese, dove peraltro negli ultimi anni i test genetici sono aumentati del 99,7%.

In relazione a ciò sono stati sottolineati i rischi connessi all'effettuazione di analisi genetiche indipendentemente dall'intermediazione di medici e specialisti e, quindi, l'importanza della consulenza genetica; la necessità di avviare controlli di qualità sui laboratori di analisi, di stabilire regole per la ricerca e, infine, di scongiurare il pericolo di una commercializzazione anche internazionale di informazioni genetiche. A tale proposito il Presidente di questa Autorità ha rammentato che la normativa in materia di protezione dei dati personali prevede che le informazioni possano essere trasferite solo in Paesi che assicurino un adeguato livello di protezione e che comunque i dati genetici non fanno parte dell'accordo "*Safe Harbor*".

23. Ricerca medica

I riferimenti normativi per il trattamento dei dati sulla salute finalizzati a scopi di ricerca medica ed epidemiologica sono rimasti sostanzialmente immutati: da un lato, la semplificazione introdotta dall'art. 5 del d.lg. n. 282/1999 secondo cui il trattamento può essere effettuato senza il consenso dell'interessato qualora "*la ricerca sia prevista da un'espressa previsione di legge o rientri nel programma di ricerca biomedica o sanitaria di cui all'articolo 12-bis del d.lg. 30 dicembre 1992, n. 502*"; dall'altro, nelle more di eventuali modificazioni conseguenti all'adozione del regolamento del Ministro della sanità di cui si è fatto cenno al paragrafo 17, le prescrizioni contenute e richiamate nel capo 1.2 dell'autorizzazione n. 2/2000 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale.

A queste disposizioni il Garante ha fatto pertanto riferimento nel provvedimento del 18 maggio 2000 (in *Bollettino* n. 13, p. 32), in risposta ad una azienda ospedaliera che chiedeva di verificare la possibilità, per alcune aziende farmaceutiche che sponsorizzano la sperimentazione di farmaci, di accedere alle cartelle cliniche dei pazienti. In particolare l'Autorità ha ricordato che il consenso dei pazienti interessati è sempre necessario, salvo che la ricerca sia svolta al fine di tutelare l'incolumità fisica degli stessi ovvero ricorrano le condizioni previste dall'art. 5 del d.lg. n. 282 sopra richiamato.

Deve rammentarsi inoltre che, per la ricerca medica ed epidemiologica, il quadro normativo dovrà essere integrato dalle disposizioni dei codici di deontologia e buona condotta, il cui rispetto "è condizione essenziale per la liceità del trattamento dei dati".

Sarà infine opportuno un coordinamento con le norme riguardanti la ricerca medica ed epidemiologica contenute nei codici dei deontologia per le attività statistiche e di ricerca scientifica.

24. Tessera sanitaria

Anche in quest'ambito è intervenuto il legislatore delegato, colmando la lacuna esistente nelle disposizioni che disciplinavano l'introduzione della carta sanitaria elettronica (art. 59, comma 50, lett. i) l. n. 449/1997 e d.l. n. 450/1998 convertito, con modificazioni, dalla l. n. 39/1999).

Tali disposizioni infatti, come più volte sottolineato da questa Autorità in diversi pareri espressi nell'esercizio della funzione consultiva (art. 31, comma 2, l. n. 675), non prevedevano alcun quadro di garanzie a tutela della riservatezza dei cittadini interessati.

L'art. 6 del d.lg. n. 282/1999 ha quindi fissato alcuni principi fondamentali in materia di protezione dei dati sanitari, stabilendo alcune limitazioni all'inserimento dei dati nella carta sanitaria elettronica e prevedendo garanzie per la sua corretta utilizzazione.

Successivamente questa Autorità, nel parere reso al Ministero dell'Interno il 12 luglio 2000 sullo schema di decreto ministeriale concernente le regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici, ha rappresentato il rischio di una proliferazione di più documenti elettronici contenenti dati sanitari e di una possibile sovrapposizione con la disciplina delle carte sanitarie elettroniche.

È quindi intervenuta la legge finanziaria 2001 (l. 23 dicembre 2000, n. 388) che ha previsto l'abrogazione delle disposizioni sopracitate delle leggi n. 449/1997 e n. 39/1999 e l'inserimento dei dati sanitari nel "documento d'identità elettronico" (*Provv.* del 7 settembre 2000).

25. AIDS

È noto che l'entrata in vigore della normativa in materia di protezione dei dati personali non ha abrogato le previgenti disposizioni di legge che tutelavano in modo specifico e più rigoroso la riservatezza e la dignità delle persone. Tra queste, in particolare, il legislatore ha espressamente fatto salve, in quanto compatibili, quelle contenute nella legge 5 giugno 1990, n. 135, in materia di Aids (art. 43, comma 2, l. n. 675).

In più occasioni tuttavia, come già evidenziato nelle precedenti relazioni annuali, l'Autorità è stata chiamata ad esprimersi su questioni relative al rapporto tra le disposizioni della legge n. 675 e quelle della normativa in materia di prevenzione e lotta contro l'Aids.

Ancora recentemente, con nota dell'8 febbraio 2001 (in *Bollettino* n. 17, p. 5), l'Autorità ha chiarito che le garanzie di riservatezza previste dalla legge sull'Aids si applicano anche in caso di richiesta di accesso da parte di consiglieri comunali agli atti e ai documenti in possesso di enti locali. Nel provvedimento il Garante ha aggiunto che le medesime garanzie devono essere rispettate quando il trattamento riguardi altre informazioni (tossicodipendenza o malattie mentali) per le quali l'ordinamento prevede un particolare regime di tutela.

Esprimendo preoccupazione per l'inadeguata sensibilità prestata nei confronti della riservatezza e della dignità delle persone offese, l'Autorità si è poi rivolta, come già accennato in un precedente paragrafo, al Ministro della giustizia in occasione della pubblicazione sul sito Internet del Tribunale di Trento di un avviso relativo all'udienza preliminare di un complesso procedimento penale per somministrazione di emoderivati infetti.

In tale nota il Garante ha rammentato la necessità di integrare con urgenza le norme processuali attualmente vigenti; ciò al fine di consentire che persone danneggiate a seguito di emotrasfusioni possano esercitare con piena tranquillità il diritto di difesa e non siano piuttosto indotte a rinunciarvi per evitare ulteriori danni legati ad un'ampia conoscenza della propria condizione di salute.

L'intervento dell'Autorità si è reso infine necessario quando sulla stampa sono state riportate notizie relative alla messa in atto, da parte di alcune strutture sanitarie, di sistemi di sorveglianza delle infezioni Hiv che comportavano l'archiviazione dei dati personali dei soggetti sieropositivi o affetti da Aids.

Il Garante, che ha inviato immediatamente richieste di informazioni alle strutture interessate, sta tuttora svolgendo una serie di approfondimenti sulla conformità dei suddetti sistemi alla specifica disciplina in materia di Aids e di sorveglianza epidemiologica, sulle precise finalità perseguite, sulle modalità di trattamento utilizzate per i flussi di dati e per la conservazione dei dati stessi (anche per ciò che riguarda la sicurezza), sui diritti delle persone interessate e sulle modalità di informazione delle stesse.

LAVORO E PREVIDENZA SOCIALE

26 LA PROTEZIONE DEI DATI NEL RAPPORTO DI LAVORO

Anche nel corso dell'anno 2000, vivo è stato l'interesse del Garante nei confronti delle esigenze di protezione dei dati personali nel settore del lavoro, sia pubblico, sia privato.

Oltre ad aver rinnovato per il periodo 1° ottobre 2000–31 dicembre 2001 le autorizzazioni generali rilasciate negli anni precedenti, rivelatesi strumento idoneo non solo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, ma anche per semplificare gli adempimenti che la legge n. 675/1996 pone a carico di determinate categorie di titolari (tra cui, con specifico riferimento al settore che qui interessa, i datori di lavoro in relazione al trattamento dei dati sensibili e dei dati a carattere giudiziario), il Garante è stato chiamato a pronunciarsi su specifiche problematiche, tra cui quella della conoscibilità delle note di qualifica.

In particolare, il Garante, sviluppando temi e principi già affermati in precedenti occasioni, nel ribadire che la previsione di cui all'art. 13, comma 1, lett. c), n. 1 della legge n. 675/1996 attribuisce a ciascun interessato – e quindi a ciascun lavoratore – il diritto di accedere ai propri dati personali, senza però che ciò possa tramutarsi in un diritto al rilascio di copia integrale degli atti o di altri documenti contenenti tali dati (soltanto ove l'estrazione dei dati personali dai documenti e la conseguente trasposizione su supporto cartaceo o informatico risulti particolarmente difficoltosa, allora l'adempimento alla richiesta di accesso può avvenire anche tramite la modalità dell'esibizione e/o della consegna in copia della documentazione, come già precisato da questa Autorità in tema di diritto d'accesso alle perizie medico-legali nel settore assicurativo e, da ultimo, in materia di lavoro, con *Provv.* del 28 dicembre 2000), ha altresì affermato che, ai sensi dell'art. 13 della legge n. 675/1996 e dell'art. 17 d.P.R. n. 501/1998, il datore di lavoro, quale titolare del trattamento, è tenuto a comunicare al lavoratore i dati relativi alla sua persona in forma completa, "mettendo in chiaro" tutte le informazioni personali comunque collegate al rapporto di lavoro o allo stato giuridico ed economico del dipendente, compresi quelli relativi allo sviluppo di carriera, alla rilevazione delle presenze, alle domande di ferie, ai turni di servizio, alla copia dei ruoli paga, ai certificati di malattia, ai moduli di autorizzazione alle missioni", nonché le informazioni riportate in eventuali progetti formativi (in tal senso, vedi *Provv.* del 17 ottobre 2000). In tale occasione, inoltre, il Garante, a fronte di specifica richiesta, ha avuto modo di chiarire che, tra le pretese azionabili dal lavoratore ex art. 13 legge n. 675/1996, non rientra quella volta a conoscere il nominativo degli eventuali "incaricati" del trattamento dei dati personali, sicché la relativa richiesta deve ritenersi inammissibile.

Sempre in tale ottica, inoltre, va considerato anche il provvedimento adottato il 28 giugno 2000, con il quale il Garante, in consapevole difformità con l'interpretazione fornita dal Tribunale di Fermo con decreto del 26 ottobre 1999, ha ribadito il diritto del lavoratore ad essere posto a conoscenza di tutti i "fattori valutativi" impiegati dal datore di lavoro ai fini della formulazione del giudizio complessivo finale contenuto nelle note di qualifica annuali. Va sottolineato che il caso in questione è identico ad altra precedente fattispecie, nella quale il giudice di merito, adìto da un istituto di credito ex art. 29, comma 6, legge n. 675/1996 (in sede di opposizione avverso una precedente pronunzia del Garante, di tenore analogo a quella oggetto di trattazione), ha affermato che "forma dato personale la valutazione finale del dipendente attribuita dall'amministrazione, ma non le operazioni effettuate al fine di giungere alla valutazione complessiva finale ...".

Al contrario, il Garante, nel ribadire che l'art. 1, comma 2, lett. c), legge n. 675/1996 definisce espressamente dato personale "qualunque informazione relativa a persona fisica, persona giuridica ...", ha affermato che si deve ricomprendere in tale ampia accezione "ogni notizia, informazione od elemento che abbia comunque un'efficacia informativa tale da fornire un contributo di conoscenza rispetto ad un soggetto identificato o identificabile" (principio, questo, già manifestato dall'Autorità in tema di giudizi espressi su docenti e sull'efficacia didattica di determinati corsi, in materia di giudizi su profili della personalità dell'interessato relativamente a test psico-attitudinali, nonché in tema di riscontri diagnostici di tipo medico e, segnatamente, di valutazioni medico-legali), sicché ad ogni elemento valutativo non potrebbe disconoscersi la natura di dato personale; e ciò "a prescindere dal loro successivo confluire nella qualifica sintetica annuale di cui costituiscono presupposti e articolazioni dotati, però, di autonomo significato", e come tali suscettibili di eventuali richieste d'integrazione ex art. 13 della legge n.

675/1996. Ulteriore conferma di tale impostazione, poi, può rinvenirsi nel provvedimento del 19 giugno 2000, con il quale il Garante ha ordinato ad una società di porre a disposizione di un suo ex dipendente gli attestati di qualificazione professionale conseguiti durante il pregresso rapporto lavorativo.

In ogni caso, trattasi di questione giuridica di enorme rilevanza, rispetto alla quale risulteranno di particolare interesse le future valutazioni della Suprema Corte di cassazione, già adita dai lavoratori interessati, che si spera possano tenere presente anche la Risoluzione adottata il 22 marzo 2001 dal Gruppo dei garanti europei, che ha riconosciuto a Bruxelles, appunto, la natura di "dato personale" delle predette valutazioni.

Infine, sempre in tema di "note di qualifica", è opportuno segnalare anche il provvedimento adottato in data 6 febbraio 2001, con il quale il Garante ha avuto modo di chiarire che il diritto del lavoratore (ex art. 13 legge n. 675/1996) ad accedere alle note di qualifica ed ai giudizi può essere esercitato soltanto in relazione ai propri dati personali, e non con riferimento ai dati contenuti in note di qualifica o, comunque, in giudizi relativi ai colleghi di lavoro, a meno che l'istante non sia munito di una delega o di una procura *ad hoc*, all'uopo rilasciatagli dall'interessato.

Analogamente, con riferimento al diritto del lavoratore ad accedere anche ai dati di tipo valutativo e, corrispondentemente, all'obbligo del datore di lavoro di porre a disposizione dell'interessato, "in chiaro", tutte le informazioni personali oggetto di trattamento, meritano di essere richiamati anche i provvedimenti adottati dal Garante in data 9 ottobre 2000, 12 dicembre 2000 e 7 marzo 2001, che si pongono nel già richiamato solco interpretativo.

27. SISTEMI INFORMATIVI E CONTROLLO A DISTANZA DEL PERSONALE

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

In proposito, occorre premettere che in materia trova già applicazione l'art. 4 della legge n. 300/1970 che, nel vietare "il controllo a distanza dell'attività dei lavoratori" (anche come mera possibilità di controllo ad insaputa del prestatore), disciplina distintamente le due ipotesi dell'impianto di apparecchiature finalizzate al controllo a distanza (primo comma) e di apparecchiature per fini produttivi, ma tali comunque da presentare la possibilità di fornire anche il controllo a distanza del dipendente (secondo comma). Mentre le apparecchiature di cui al primo comma sono vietate, data la loro "odiosità", il loro contrasto con i principi della Costituzione e gli stessi effetti che possono arrecare alla produttività, quelle di cui al secondo comma sono consentite a condizione che il datore di lavoro osservi quanto tassativamente previsto nello stesso secondo comma ed, eventualmente, dai successivi.

Il Garante, chiamato nuovamente ad occuparsi della questione, ha anzitutto rammentato che la direttiva comunitaria n. 95/46/CE e la Convenzione n. 108/1981 del Consiglio d'Europa rendono obbligatoria l'applicazione della disciplina sul trattamento dei dati personali anche ai suoni ed alle immagini (quali quelle registrate nei controlli video), qualora permettano di identificare un soggetto anche in via indiretta, evidenziando che la legge n. 675/1996, attuativa della citata Convenzione, ha considerato quale "dato personale" qualunque informazione che permetta l'identificazione, anche in via indiretta, dei soggetti interessati, ivi compresi i suoni e le immagini (art. 1, comma 1, lett. c)).

L'Autorità ha proseguito l'analisi di una problematica già lungamente affrontata nel corso del 1999 e che è bene richiamare anche in questa Relazione. Chiamata infatti ad esprimere un parere in relazione ad un impianto di video-sorveglianza da installare sui mezzi di trasporto di un'azienda comunale, diretto a garantire la sicurezza dei viaggiatori, a prevenire reati ed atti di vandalismo alle fermate, l'Autorità aveva infatti sottolineato la necessità che tali sistemi fossero attivati in presenza di un articolato quadro di garanzie. In particolare, il Garante, nel richiamare i fondamentali divieti sanciti dall'art. 4 della legge n. 300/1970 (con specifico riferimento all'eventuale stabile ripresa della posizione di guida degli autisti), aveva sollecitato il richiedente a determinare la localizzazione delle telecamere e le modalità di ripresa televisiva in aderenza con le finalità sottese all'installazione del sistema stesso, tenendo conto dei principi fissati dall'art. 9 della legge n. 675/1996 in tema di pertinenza e non eccedenza dei dati: di conseguenza, aveva auspicato una predisposizione di modalità di ripresa tali da consentire una visione puramente panoramica dell'interno delle vetture o dell'ambito

della fermata, dovendosi ritenere inibite riprese più particolareggiate, atte a realizzare un'intrusione nella riservatezza delle persone, ovvero una visione di particolari irrilevanti. Inoltre, stante la stretta connessione tra l'eventuale visione "in chiaro" delle immagini (originariamente registrate solo in modo codificato) e la commissione di atti criminosi denunciati all'autorità di polizia, il Garante aveva altresì sollecitato l'installazione di un modulo di accesso ai computer della c.d. "stazione di lettura" secondo un sistema di "doppia chiave" congiunta (una in possesso dell'azienda e l'altra in possesso delle forze dell'ordine), con predeterminazione, tra l'altro, di idonee misure di sicurezza per la salvaguardia dei dati.

Negli ultimi tempi, il problema del controllo a distanza sul luogo di lavoro è tornato all'attenzione del Garante – come pure di altri Paesi e di molte altre autorità di garanzia straniere- in relazione agli accessi alle reti telematiche da parte del personale e all'uso della posta elettronica.

L'Autorità ha già avviato specifici accertamenti richiedendo, sia a società distributrici di appositi software, sia ad aziende risultate utilizzatrici dello stesso, tutte le informazioni utili per una piena valutazione delle caratteristiche del *software* e delle opzioni da esso consentite, nonché delle concrete forme di utilizzazione con specifico riguardo alle modalità di informativa verso i dipendenti, all'istituto del consenso, all'eventuale consultazione delle rappresentanze sindacali aziendali, alle finalità perseguite ed alla conservazione dei dati relativi agli accessi ai siti.

Il Garante si riserva di adottare a breve termine un provvedimento di carattere generale in riferimento ai diversi aspetti emersi nei vari procedimenti, tenendo presenti le nuove implicazioni che la legge n. 675/1996 pone per quanto riguarda l'informativa ai lavoratori interessati, il principio di proporzionalità nel trattamento dei dati, la trasparenza dei controlli e i limiti entro i quali essi sono consentiti, ed eventuali suggerimenti operativi che potranno essere formulati per bilanciare i diritti e le libertà fondamentali degli interessati con le esigenze connesse alla prestazione lavorativa e all'osservanza degli obblighi del rapporto di lavoro.

Il Garante terrà anche conto, a questo riguardo, degli approfondimenti in atto su scala europea, anche alla luce delle prime quattro iniziative intraprese in altri Paesi da altre autorità di garanzia in materia di protezione dei dati, dei risultati dell'apposito Gruppo di lavoro costituito dalle quindici autorità garanti, nonché delle prime riflessioni che l'Autorità italiana ha formulato nel corso della recente Conferenza europea di Atene del 10-11 maggio 2001.

28. Il Sistema informazione lavoro

Nell'ambito dell'attività consultiva (art. 31, comma 2, legge n. 675/1996), il Garante ha avuto modo di proseguire gli approfondimenti relativi ai sistemi informativi in materia di lavoro.

Già in passato l'Autorità aveva espresso un parere in relazione allo schema di regolamento concernente, nell'ambito della delegificazione della materia, il riordino di alcune procedure per il collocamento pubblico; tale regolamento, infatti, avrebbe lo scopo di facilitare l'incontro della domanda e dell'offerta di lavoro nel rispetto della competenza delle Regioni (art. 1 legge 15 marzo 1997, n. 59), attraverso un'efficace attivazione sul territorio nazionale del Sistema informativo lavoro (Sil).

È opportuno richiamare quanto già riportato nella Relazione per l'anno 1999 circa la necessità di chiarire, in via generale, il complessivo rapporto tra flussi di dati previsti e l'organizzazione del SIL, trattandosi di un sistema che, per espressa previsione di legge, dev'essere improntato ai principi di cui alla legge n. 675/1996 (vedi art. 11, comma 1, d.lg. 469/1997).

Analogamente, sono state ribadite le perplessità già sollevate in relazione sia all'istituzione di una "scheda professionale" del lavoratore (non essendo ancora chiara non solo la funzione di tale scheda, ma anche le connesse modalità di trattamento dei dati in essa riportati), sia all'autonomo rilascio, su base regionale, di una "carta elettronica personale" del lavoratore, soprattutto in assenza di un primo quadro normativo d'insieme che poteva essere meglio armonizzato con la recente disciplina della carta d'identità elettronica.

Con provvedimento del 24 aprile 2001, il Garante ha nuovamente ribadito principi analoghi esprimendo il parere su due schemi di decreti ministeriali attuativi del regolamento di semplificazione della disciplina per il collocamento ordinario dei lavoratori con d.P.R. 7 luglio 2000, n. 442. L'Autorità ha

anzitutto evidenziato il mancato recepimento – con il d.P.R. n. 442/2000 - di varie considerazioni formulate con il parere del 30 novembre 1999, in particolare per quanto riguarda il rapporto tra i flussi di dati personali previsti e la peculiare organizzazione del Sil, e la delimitazione degli obblighi di verifica dell'esattezza e della pertinenza delle informazioni, anche in termini di uniformità di disciplina sull'accesso da parte di regioni ed enti locali. Altre osservazioni hanno riguardato la titolarità del trattamento dei dati relativi all'elenco anagrafico delle persone in cerca di lavoro e, sotto altro profilo, alcuni aspetti dello schema di decreto concernente la scheda professionale.

29. CARTELLINI IDENTIFICATIVI

Infine, particolare rilievo merita il provvedimento dell'11 dicembre 2000, con il quale il Garante, sollecitato da molte richieste di parere avanzate da pubbliche amministrazioni, aziende sanitarie, compagnie aeree, aziende di trasporto, servizi di ristorazione e singoli lavoratori, ha affrontato il problema dei c.d. cartellini identificativi.

Alcune norme contrattuali o disposizioni organizzative, in vigore sia nel settore pubblico, sia in quello privato, prevedono che il personale a contatto con il pubblico appunti sull'abito o sulla divisa di lavoro un cartellino identificativo, contenente vari dati personali del dipendente: trattasi di norme aventi lo scopo di migliorare il rapporto tra operatori (pubblici o privati) ed utenti dei servizi o clienti degli esercizi commerciali, comportando una maggiore responsabilizzazione del personale ed una più agevole possibilità di tutela dei terzi.

Però, poiché tale esposizione al pubblico di alcuni dati personali degli interessati risulta anche idonea a determinare un'agevole identificazione dell'operatore che, di fatto, può divenire anche destinatario di improprie pressioni da parte di terzi o di successivi contatti anche per ragioni estranee all'attività lavorativa, il Garante, nel riportarsi ai principi di pertinenza e non eccedenza dei dati rispetto alla finalità perseguita attraverso il trattamento (art. 9 l. n. 675/1996), ha ribadito che la limitazione della riservatezza, anche se collegata al perseguimento di una legittima finalità, dev'essere comunque ridotta al minimo indispensabile. Pertanto, la diffusione dei dati personali dei dipendenti attraverso l'imposizione dei cartellini identificativi può trovare giustificazione, nel settore privato, soltanto in caso di adempimento di un obbligo previsto da una legge, da un regolamento o dalla normativa comunitaria (art. 20 l. n. 675/1996), mentre nel settore pubblico ciò è possibile solo ove sia previsto da norme di legge o di regolamento (art. 27, commi 3 e 4).

Nell'ambito del lavoro privato, l'obbligo dell'apposizione del cartellino identificativo trova fondamento in alcune prescrizioni contenute in accordi sindacali aziendali o in regolamenti aziendali, che hanno esplicito riguardo o a finalità interne all'azienda (controlli sulle entrate e le uscite dall'azienda, riconoscimento del personale, accesso ad aree riservate) ovvero ad altre concernenti i rapporti con gli utenti o con i clienti. Pertanto, proprio con specifico riguardo a quest'ultima finalità, il Garante ha ritenuto che non presenti alcuna utilità l'evidenziazione sul cartellino dei dati dei dipendenti concernenti le generalità o gli estremi anagrafici, mentre risulta senz'altro utile ai terzi che entrino in contatto con il personale la conoscibilità dell'immagine fotografica dell'interlocutore, l'indicazione del ruolo professionale, nonché il nome ed il numero (o la sigla) identificativi.

Analoghe considerazioni, inoltre, valgono anche per il settore pubblico. Infatti, anche ove siano stati emanati atti amministrativi d'organizzazione che prevedano l'adozione, da parte del personale, di cartellini identificativi, la limitazione della riservatezza dei dipendenti dovrà sempre avvenire nel rispetto dei principi di pertinenza e non eccedenza, soprattutto laddove non sussistano precise disposizioni di legge o di regolamento che prescrivano puntualmente il contenuto di detti cartellini.