necessità di non procrastinare l'attivazione di idonei meccanismi e procedure volti a dare piena attuazione alle disposizioni in tema di accesso ai dati, secondo quanto previsto dall'art. 17 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501. Come si ricorderà, infatti, il comma 9 di tale articolo prevede che i titolari del trattamento debbano agevolare l'accesso ai dati anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad una accurata selezione dei dati che riguardano i singoli soggetti, a semplificare le modalità e a ridurre i tempi per dare riscontro agli interessati anche nell'ambito degli uffici per le relazioni con il pubblico.

Altro grave problema, riscontrato dall'Autorità in ambito pubblico, concerne la non esatta o incompleta individuazione delle figure degli incaricati del trattamento dei dati personali.

L'individuazione di tale figura corrisponde ai dipendenti o ai collaboratori esterni che in ragione del proprio ufficio, servizio o attività, sono legittimati ad accedere a determinati atti e documenti e a trattare dati seguendo le istruzioni del titolare o del responsabile del trattamento e operando sotto la loro autorità (art. 8, comma 5 e 19 della legge n. 675/1996).

Tale individuazione permette quindi di considerare, in generale, legittimo il flusso delle informazioni personali contenute in atti o documenti nell'ambito degli uffici e tra i dipendenti dell'amministrazione titolare del trattamento. In altre parole, senza una formale designazione degli incaricati del trattamento, i soggetti che hanno accesso e trattano dati personali vanno considerati come soggetti estranei all'amministrazione, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e, quindi, per la liceità del trattamento.

Strettamente connessa a tale tema è la problematica dell'individuazione dei responsabili del trattamento acuita dal fatto che i soggetti pubblici si avvalgono per l'adempimento delle proprie finalità istituzionali, anche di organismi privati che devono accedere, quindi, a dati detenuti dalla p.a.

L'amministrazione pubblica deve quindi scegliere se considerare tali soggetti come soggetti esterni che la coadiuvano in un'attività che ricade nell'ambito di titolarità e responsabilità dell'amministrazione stessa o, invece, quali figure del tutto distinte dall'amministrazione che decide, in questo caso, autonomamente in ordine al trattamento delle informazioni e si assume, in concreto, ogni responsabilità in proposito.

Nel primo caso tali figure, designate quali responsabili del trattamento, assumono un ruolo quale parte sostanziale della struttura della pubblica amministrazione e possono quindi trattare i dati detenuti dal soggetto pubblico senza che vi sia necessità di una manifestazione del consenso dell'interessato (indispensabile, invece, se si verificasse la seconda ipotesi e cioè se assumessero la qualità di soggetti "terzi" rispetto all'amministrazione). Tutto ciò è stato ancora una volta ribadito in una pronuncia del Garante, rivolta al Ministero delle finanze, in cui si è chiarito che l'amministrazione finanziaria deve precisare il ruolo assunto dai concessionari della riscossione per poter consentire a questi ultimi l'accesso ai dati detenuti dall'amministrazione (parere del 16 giugno 1999 rilasciato al Ministero delle finanze, in Bollettino n. 9, pag. 19).

Sotto altro profilo, numerose pronunce dell'Autorità hanno ancora una volta ribadito a singole amministrazioni pubbliche che, di norma, esse devono operare senza acquisire il consenso degli interessati al trattamento dei dati personali.

Secondo la legge n. 675, infatti, i soggetti pubblici non operano, di regola, sulla base del consenso dell'interessato, mentre possono effettuare solo i trattamenti connessi all'esercizio delle proprie funzioni istituzionali rispondenti, in caso di comunicazione e diffusione dei dati, a puntuali previsioni di legge o di regolamento (art. 27).

Per quanto riguarda la comunicazione e la diffusione, l'Autorità, dopo aver ricordato nuovamente che la legge n. 675/1996 regola diversamente la comunicazione e diffusione tra soggetti

pubblici (ammesse se previste da norme di legge o di regolamento o qualora risultino comunque necessarie per lo svolgimento di finalità istituzionali) dalla divulgazione di dati da amministrazioni pubbliche nei confronti di soggetti privati, ha analizzato vari casi valutando la loro conformità non solo ai parametri dell'art. 27 della legge n. 675/1996, ma anche al quadro generale delineato dalla normativa relativa ai singoli settori interessati. Ad esempio, il Garante ha constatato che una provincia poteva acquisire dati dai comuni e da altre amministrazioni pubbliche nel rispetto della specifica disciplina applicabile alle singole amministrazioni (parere reso alla provincia di Modena il 14 gennaio 1999, pubblicato in Bollettino n. 7, pag. 53).

Il Garante ha inoltre ribadito più volte la predetta necessità che, qualora la comunicazione e la diffusione dei dati avvengano da parte di soggetti pubblici a soggetti privati o enti pubblici economici, tali operazioni siano previste da norme di legge o di regolamento. La comunicazione e la diffusione dei dati personali può infatti avvenire quando ciò sia previsto da una disposizione normativa di rango primario o secondario; al contrario, la previsione contenuta nel regolamento interno di un ente pubblico economico non può considerarsi fonte idonea a legittimare una comunicazione e diffusione dei dati (cfr. parere rilasciato all'A.C.I. il 16 giugno, 1999, pubblicato in Bollettino n. 9, pag. 61).

Fondamentali sono, infine, le novità apportate dal decreto legislativo n. 135/1999 (di cui si tratterà ampiamente più avanti) concernente il trattamento dei dati sensibili da parte dei soggetti pubblici, che definisce i princìpi generali in base ai quali questi ultimi sono autorizzati a trattare tali dati e quelli attinenti a particolari provvedimenti giudiziari e individua alcune finalità di rilevante interesse pubblico per il cui perseguimento è consentito tale trattamento.

Da ultimo, per quanto concerne l'adozione delle misure minime di sicurezza da parte delle pubbliche amministrazioni, previste all'art. 15 della legge 675/1996 e individuate nel d.P.R. 318/1999 (*"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15, comma 2 della legge 31 dicembre 1996, n. 675"*) si rinvia al capitolo n. 2.14.

2.1.3 Trasparenza dell'attività amministrativa

Il processo di profondo rinnovamento che, come è noto, ha interessato le pubbliche amministrazioni nell'ultimo decennio grazie all'entrata in vigore di provvedimenti normativi innovativi rispetto a quelli precedenti, ha come linee-guida i principi di pubblicità, efficienza ed economicità dell'azione pubblica.

L'intenzione di fare dell'amministrazione una "casa di vetro" si è tradotta, infatti, negli istituti di partecipazione al procedimento, introdotti in via generale dalla legge 7 agosto 1990, n. 241 (la comunicazione di avvio del procedimento, il diritto di intervento, la predeterminazione dei criteri per ausili economici, ecc.) e, ancora, negli ulteriori strumenti apprestati al fine di garantire il massimo della trasparenza nell'agire pubblico (l'obbligo di provvedere, la motivazione obbligatoria, la previa individuazione del termine conclusivo e del responsabile del procedimento, gli accordi sostitutivi e procedimentali) fra i quali, in particolare, il diritto di accesso ai documenti amministrativi ai sensi dell'art. 22 della citata legge.

Nella non facile transizione da un'amministrazione "chiusa" ad una "trasparente" rispetto ai cittadini ed alle istanze da essi rappresentate, un ruolo fondamentale è svolto dalla progressiva informatizzazione dei sistemi pubblici che, quotidianamente, sono in grado di trattare e scambiare fra loro migliaia di dati personali.

Così il valore della trasparenza sembrerebbe poter confliggere con il diritto degli interessati di tutelare la riservatezza e di esercitare un controllo sulle informazioni trattate, in particolare, dai

soggetti pubblici. Al contrario, la stessa legge n. 241/1990 individua nella riservatezza di terzi un limite al diritto di accesso (art. 24, comma 2, lettera d), mentre, dall'altro lato, la legge sulla privacy ammette la comunicazione e la diffusione dei dati personali da parte dei soggetti pubblici a privati o ad enti pubblici economici solo se previste da norme di legge o di regolamento (art. 27, comma 3, legge n. 675/1996).

Contrariamente all'opinione secondo la quale questo regime particolarmente severo avrebbe ripristinato la prevalenza della segretezza sulla trasparenza dell'agire pubblico, fornendo alle amministrazioni un comodo pretesto per negare ai cittadini la conoscenza di documenti che li riguardano, il Garante ha proseguito sulla strada intrapresa in materia sin dalla sua istituzione, della quale si è fornito ampio riscontro nelle due precedenti relazioni per il 1997 e per il 1998.

Infatti, il richiamo ad una precisa disposizione normativa operato dall'articolo 27, comma 3, della legge n. 675 è riferito a tutte le disposizioni vigenti che la legge sulla privacy non ha abrogato e che presuppone, anzi, come limiti legali al trattamento dei dati effettuato dalle amministrazioni pubbliche.

In un parere reso il 16 giugno 1999 (in Bollettino n. 9, pag. 61), in relazione alla possibilità per l'ACI di rendere pubblico l'elenco dei soggetti e dei centri autorizzati alla demolizione di veicoli e rimorchi, il Garante ha ricordato che *"la legge n. 675/1996 non ha introdotto alcun divieto di dare conoscibilità a questi dati, ma in un quadro di maggiore trasparenza stabilisce che le amministrazioni e gli enti pubblici possono diffondere i dati personali quando ciò sia previsto"* da un'apposita disposizione di rango normativo primario o secondario. Di conseguenza, come già accennato, la previsione contenuta in un regolamento meramente interno dell'ente non poteva considerarsi fonte idonea a consentire la diffusione dei dati personali.

Ad analoghe conclusioni è possibile arrivare anche in applicazione del generale principio di legalità, da cui l'attività amministrativa è retta, poiché essa deve svolgersi, in ogni caso, nel rispetto dei limiti previsti dalle leggi.

A questo proposito, in difetto di una specifica disciplina di settore, mentre il trattamento di dati personali "interno" alle singole amministrazioni può comunque avvenire qualora sia necessario per lo svolgimento delle funzioni istituzionali dell'amministrazione (articolo 27, comma 1, legge n. 675/1996), la mancanza di tale disciplina porta a ritenere vietata la comunicazione dei dati stessi a privati (art. 27, comma 3), come precisato in occasione del chiarimento in merito al regime di pubblicità dell'albo professionale degli iscritti all'Ordine degli assistenti sociali, fornito con provvedimento del 29 marzo 1999 (in Bollettino n. 8, pag. 50). Con ciò, tuttavia, il Garante non ha inteso escludere una volta per tutte la possibilità per il soggetto pubblico di divulgare a privati o ad enti pubblici economici i dati personali oggetto di trattamento, ma, al contrario, ha suggerito di integrare la normativa specifica con idonee previsioni, nel senso di rendere maggiormente trasparente l'attività svolta.

Affrontando nuovamente la questione, già trattata nel periodo precedente di attività (cfr. Relazione per l'anno 1998, pag. 14), relativamente al regime di pubblicità delle deliberazioni comunali, il Garante ha preso in considerazione il rapporto della precedente normativa con il d.lg. 11 maggio 1999, n. 135. In particolare, riferendosi all'ipotesi in cui i dati contenuti nelle deliberazioni dell'ente locale abbiano natura sensibile, ai sensi dell'articolo 22 della legge sulla privacy, nel parere del 2 settembre 1999 (in Bollettino n. 9, pag. 9) si è fatto presente che il trattamento di tali informazioni risulta ora espressamente autorizzato dal citato decreto, il quale, tra l'altro, ha riconosciuto la rilevanza a livello di interesse pubblico dei trattamenti di dati personali:

- diretti all'applicazione della disciplina in materia di documentazione dell'attività istituzionale di organi pubblici (art. 8 d.lg. cit.), facendo salvo, anche in questo caso, il divieto di diffusione dei dati idonei a rivelare lo stato di salute previsto in termini generali dall'art. 23, comma 4, della legge n. 675/1996;

- effettuati in conformità alle leggi e ai regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi (art. 16, comma 1, lett. c) d.lg. cit.).

All'amministrazione, pertanto, non rimane che identificare i tipi di dati e le operazioni strettamente necessarie e pertinenti in relazione alle specifiche attività svolte, secondo la disposizione dell'art. 22, comma 3-*bis*, della legge n. 675/1996, poiché *"non vi è alcuna incompatibilità di fondo tra le disposizioni in materia di dati personali e le disposizioni anche previgenti alla legge n. 675/1996 in tema di trasparenza dell'attività della pubblica amministrazione, di accesso ai documenti amministrativi e di pubblicità di taluni atti"*.

Ulteriore applicazione della normativa sui dati sensibili è stata fatta nel parere reso in data 9 giugno 1999 (in Bollettino n. 9, pag.71) in merito al rilascio dell'elenco dei sottoscrittori di una lista elettorale, rilascio di cui è stata riconosciuta la liceità, dovendosi ritenere ricompreso nelle attività in materia di elettorato e di altri diritti politici indicate nell'articolo 8, comma 4, del d.lg. n. 135/1999. Tale norma, infatti, consente la diffusione dei dati per le finalità individuate *"con riguardo alle sottoscrizioni di liste, alle presentazioni delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti"*. In ogni caso, però, il Garante ha sottolineato che i trattamenti in questione devono essere effettuati nel rispetto dei principi fissati dalla legge n. 675/1996 e dal citato decreto legislativo e, in particolare, di quelli di pertinenza e di essenzialità dei dati trattati e del rispetto della finalità perseguita (art. 9, legge n. 675 e artt. 1-4 del d.lg. n. 135). In tal senso è apparso legittimo il rilascio dell'elenco esclusivamente a soggetti che intendano servirsene per l'esercizio dei diritti politici, come nel caso in cui la richiesta pervenga da candidati di liste concorrenti.

Nel corso dell'anno è stato risolto anche il problema della comunicazione e della diffusione da parte delle scuole e degli istituti scolastici, anche a privati e per via telematica, dei dati relativi agli esiti scolastici degli studenti, nonché di altri dati personali diversi da quelli sensibili. L'articolo 17 del d.lg. n. 281/1999, intervenuto a modificare, fra le altre, le disposizioni del testo unico approvato con d.lg. n. 297/1994, ha reso legittima, facendola oggetto di espressa previsione normativa ai sensi dell'art. 27, comma 3, della legge sulla privacy, la divulgazione di dati personali degli studenti a soggetti diversi da quelli pubblici, al fine di agevolarne l'orientamento, la formazione e l'inserimento professionale, come sottolineato dal Garante in un parere del 27 ottobre 1999. La comunicazione e la diffusione non riguardano, comunque, dati sensibili o di carattere giudiziario e sono subordinate alla richiesta dell'interessato. Rispetto ai dati personali raccolti prima dell'entrata in vigore del d.lg. n. 281/1999, il comma 2 del nuovo articolo 330-*bis* del d.lg. n. 297/1994 riconosce poi, espressamente, il diritto degli interessati di opporsi alla loro divulgazione.

2.1.4 Diritto di accesso a documenti amministrativi

Con riferimento al rapporto tra la legge n. 241 del 1990 e la legge n. 675 del 1996 ed in particolare al problema se le due normative interferiscano tra loro, nel 1999 è rimasto confermato il principio secondo cui la legge n. 675 non ha modificato presupposti e ambito di applicazione della citata legge n. 241.

L'Autorità ha, in particolare, ribadito che non v'è alcuna incompatibilità di fondo tra le due normative e che spetta all'amministrazione destinataria della richiesta di accesso il compito di valutare la sussistenza dell'interesse giuridicamente rilevante e degli altri presupposti per accedere ai documenti amministrativi.

L'accesso ai documenti è pur sempre riconosciuto a chiunque abbia un interesse personale e concreto in relazione alla tutela di situazioni giuridicamente rilevanti (art. 22 legge n. 241/1990; art. 2 d.P.R. n. 352/1992) anche dopo l'entrata in vigore della legge n. 675, come testualmente stabilito dall'articolo 43 della stessa legge.

Deve anzi ricordarsi, sotto altro profilo, che, a norma dell'articolo 13 della legge n. 675, l'accesso, in questo caso ai propri dati personali, è uno dei mezzi di tutela della riservatezza, atteso che l'interessato ha diritto di accesso ai dati che lo riguardano per verificarne la correttezza ed il trattamento effettuato.

Sempre relativamente al rapporto tra diritto di accesso e tutela della riservatezza ed all'insussistenza di un rapporto di contraddizione tra i due istituti, non va dimenticato che già la legge n. 241 del 1990, all'articolo 24, comma 2, lettera d), prevede una limitazione al diritto di accesso in relazione alla riservatezza di terzi. E tale limitazione, ovviamente non contrastata dalla legge n. 675 del 1990, trova ora, nella stessa legge, parametri più precisi ai quali ancorarsi.

Con un parere del 4 novembre 1999 sulla richiesta del Ministero delle finanze, volta a conoscere se contrasti con la normativa sulla protezione dei dati personali la richiesta di accesso - avanzata da alcuni concorrenti di un concorso pubblico - alle certificazioni prodotte da altri concorrenti, il Garante ha ribadito quanto già chiarito in precedenti pareri e cioè che le pubbliche amministrazioni, a fronte di domande di accesso agli atti, non devono chiedere il consenso degli interessati alle operazioni di comunicazione dei dati personali, ma devono semplicemente valutare se vi è nel caso concreto l'esigenza di tutelare la specifica posizione di riservatezza di terzi, tenendo presente che la comunicazione che si realizza attraverso l'accesso ai documenti amministrativi è da ritenersi "autorizzata" per legge (in conformità al generale principio di cui all'art. 27, comma 3, della legge n. 675), stante il disposto della legge n. 241/1990.

Nella richiamata occasione, il Garante ha, quindi, nuovamente riconosciuto la possibilità per l'amministrazione di esibire o di consegnare copia di documenti amministrativi a seguito dell'esercizio del diritto di accesso ai sensi dell'art. 22 della legge n. 241/1990 e degli artt. 1 e 2 del d.P.R. n. 352/1992.

Il principio della compatibilità tra l'accesso ai documenti amministrativi e la legge sulla tutela dei dati personali è stato poi ribadito a seguito dell'emanazione del d.lg. n. 135 del 1999 che, all'art. 16, comma 1, lettera c), superando alcuni dubbi emersi tra vari commentatori, consente esplicitamente di applicare la normativa sull'accesso ai documenti amministrativi anche quando questi contengano dati sensibili o riguardanti determinati provvedimenti di carattere giudiziario. Tale principio è stato di seguito ribadito in risposta a diversi quesiti, ad esempio, con il parere del 29 novembre 1999 in riferimento ad una richiesta formulata dal Ministero delle finanze-Dipartimento delle dogane e delle imposte indirette, circa il rapporto tra le due leggi.

L'ordinamento, poi, riconosce uno speciale e più ampio diritto di accesso ai consiglieri comunali e provinciali nei confronti degli atti detenuti dalle rispettive amministrazioni per l'espletamento del proprio mandato (articolo 31, comma 5, della legge n. 142 del 1990).

Con riferimento a tale disposizione, l'Autorità garante ha, però, avuto modo di chiarire che anche questo diritto di accesso può trovare alcuni limiti nella riservatezza di alcuni dati personali contenuti negli atti cui l'accesso stesso è rivolto (ad esempio, in riferimento alla possibile presenza nel cedolino dello stipendio di un dirigente di determinati dati personali ed informazioni di natura sensibile).

Nel parere dell'8 giugno 1999 (Bollettino n. 9 del 1999, pag. 7), reso in risposta ad un quesito del Comune di Viterbo, è stato ribadito che l'accesso ai documenti dell'amministrazione da parte dei consiglieri comunali e provinciali è più ampio di quello previsto dalla legge n. 241, posto che, se detto accesso attiene all'esercizio delle funzioni istituzionali del consigliere medesimo e ne costituisce modalità di espletamento, non è richiesta la sussistenza di un interesse giuridicamente rilevante per l'accesso medesimo.

È stato altresì chiarito, nella medesima circostanza, che il diritto del consigliere comunale di verificare, nell'esercizio delle funzioni consiliari, con piena cognizione di causa, ivi compreso l'accesso ai documenti, la correttezza e l'efficacia dell'operato dell'amministrazione, può essere soddisfatto anche attraverso il regime di pubblicità della situazione patrimoniale dei dirigenti (l. n. 441/1992 e l. n. 127/1997), l'esame dei contratti collettivi, l'accesso alle deliberazioni adottate dalla stessa amministrazione in materia di indennità ed emolumenti ai dipendenti.

2.1.5 Dati sensibili e di carattere giudiziario

Il 1999 ha rappresentato un anno particolarmente significativo per la definizione di una disciplina tendenzialmente organica in materia di trattamento dei dati personali più "delicati" da parte dei soggetti pubblici. Dopo i diversi rinvii che avevano comportato la proroga del regime transitorio previsto dalla legge 675/1996, è stato infatti finalmente approvato il decreto legislativo 11 maggio 1999, n. 135, contenente una serie di disposizioni integrative e modificative della legge n. 675/1996 sul trattamento dei dati sensibili da parte dei soggetti pubblici.

Durante la complessa fase di elaborazione di tale provvedimento, si è realizzata, più di quanto non fosse accaduto in passato, un'effettiva e concreta consultazione del Garante che ha in tal modo potuto formulare diverse osservazioni tendenti a rendere il testo maggiormente conforme ai principi dettati in materia di riservatezza (Comunicato n. 43 del 3 maggio 1999, in Bollettino n. 8, pag. 88).

Il decreto, pur non potendo esaurire la regolamentazione della materia, ha avuto il merito di fissare alcuni principi generali sull'uso di tali informazioni da parte degli enti pubblici, nonché quella di fornire una prima elencazione dei settori all'interno dei quali la pubblica amministrazione può fare uso dei dati sensibili, fissandone al contempo le modalità ed i limiti.

Giova ricordare che i soggetti pubblici, a differenza dei privati, generalmente non sono tenuti a richiedere il consenso degli interessati e fondano invece la loro legittimazione a trattare i dati personali unicamente su disposizioni normative. A causa di ciò, il cittadino non ha il potere di intervenire con una propria manifestazione di volontà per acconsentire o negare l'autorizzazione all'utilizzo dei propri dati da parte della pubblica amministrazione. Da qui l'importanza delle disposizioni che regolano la materia, le quali devono contenere già in sé quel bilanciamento di valori perseguiti e interessi tutelati che, nei rapporti fra privati, scaturisce dal confronto intersoggettivo alla base della manifestazione del consenso. Da qui, anche, l'attenzione che è necessario porre alle specifiche e concrete determinazioni assunte in materia dalle singole amministrazioni, le quali, come si vedrà fra breve, sono spesso chiamate a disciplinare nel dettaglio tali ipotesi.

Si deve tuttavia evidenziare che anche il d.lg. n. 135/1999 è espressione di un'impostazione - propria di gran parte delle disposizioni della legge 675 - basata su una netta separazione di disciplina fra pubblico e privato. In molti casi, essa appare giustificata, oltre che dalla diversità del soggetto agente, da un'innegabile differenza di fini perseguiti e di mezzi utilizzati. Altre volte, però, tale netta separazione potrebbe, in certi casi, essere suscettibile di determinare alcune disparità a causa del sempre più frequente utilizzo di strumenti ed istituti privatistici da parte dei soggetti pubblici, nonché dell'accrescersi della pratica di affidare ai privati la realizzazione di attività svolte fino a ieri da enti pubblici. Per questo, appaiono meritevoli di approfondimento e suscettibili di eventuali sviluppi le tecniche regolative adottate per taluni ambiti di attività, nei quali il trattamento dei dati sensibili viene disciplinato senza assegnare unica rilevanza alla natura pubblica o privata del titolare (il riferimento è, in particolare, ai trattamenti svolti in ambito sanitario e di ricerca scientifica per i quali si rinvia alle apposite sezioni di questa relazione).

Al fine di cogliere le novità introdotte dalla nuova disciplina, ed insieme capirne il significato complessivo, è necessario ricordare che la legge n. 675, sulla scorta di quanto disposto in sede

comunitaria, aveva previsto specifiche garanzie per l'utilizzo da parte delle pubbliche amministrazioni dei dati sensibili, nonché di alcune delle informazioni relative a determinati provvedimenti di carattere giudiziario (artt. 22 e 24, l. n. 675/1996).

Si era infatti stabilito che i soggetti pubblici potessero trattare queste informazioni esclusivamente dietro un'espressa "autorizzazione" di legge, nella quale fossero specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite (art. 22, comma 3). Poiché, nel nostro ordinamento, le leggi in grado di rispondere a tali caratteristiche erano e sono un numero molto esiguo, lo stesso legislatore del '96 aveva previsto un regime transitorio.

Sulla base di esso, questo tipo di trattamenti sono potuti proseguire anche in assenza delle leggi indicate con l'unico onere, per i soggetti pubblici interessati, di dare una preventiva comunicazione sugli stessi al Garante (art. 41, comma 5). Una disciplina in molti aspetti analoga era stata disposta anche per i predetti dati di carattere giudiziario (art. 686, commi 1, lett. a), d), 2 e 3), prevedendosi però che i trattamenti potessero essere autorizzati, oltre che dalle leggi particolarmente dettagliate cui si è fatto riferimento, anche da un provvedimento del Garante con il medesimo livello di specificazione (art. 24, l. 675).

Fin da subito, è però apparso evidente che tale disciplina, dettata esclusivamente per sopperire ad una carenza normativa presente al momento dell'entrata in vigore della legge n. 675/1996, non poteva offrire garanzie pienamente sufficienti per i cittadini e doveva essere integrata in tempi rapidi da una normativa più rispettosa dei diritti delle persone. Tuttavia, anche a causa delle innegabili difficoltà incontrate nell'affrontare le complesse problematiche ad essa legate, la disciplina transitoria è stata prorogata più volte (art. 1 del d.lg. n. 135/1998; e art. 1 del d.lg. 6 novembre 1998, n. 389), fino all'approvazione del decreto legislativo n. 135/1999.

Quest'ultimo - come accennato - da una parte ha voluto fissare alcuni principi generali ai quali devono attenersi i soggetti pubblici che trattano le delicatissime informazioni personali di cui si è detto (capo I) e, dall'altra, ha invece individuato numerose rilevanti finalità di interesse pubblico al fine di autorizzare i trattamenti svolti per il loro perseguimento (capo II). In considerazione della loro particolare posizione nell'ambito dell'ordinamento costituzionale, il legislatore delegato ha invece ritenuto di escludere dall'ambito di applicabilità di tale decreto, oltre ad alcuni trattamenti svolti in ambito pubblico per i quali era già prevista una disciplina differenziata -art. 4, l. 675/1996, art. 1 comma 1, lett. i), l. 676/1996 - anche quelli che divengano oggetto di una nuova disciplina ad opera della Presidenza della Repubblica, del Senato della Repubblica, della Camera dei deputati, nonché della Corte costituzionale.

Molte delle disposizioni di cui al capo I del d.lg., comuni a tutti i trattamenti, costituiscono poi uno sviluppo ed un rafforzamento di alcuni principi generali già sanciti dalla legge n. 675/1996. Si è così previsto, in generale, che i soggetti pubblici devono trattare i dati in discorso con modalità atte ad assicurare il rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato, adottando le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 13 della legge 675/1996.

Al fine di garantire al cittadino una conoscenza adeguata sull'uso che sarà fatto dei propri dati personali, nonché di consentire un più immediato ed efficace controllo sulla legittimità dei trattamenti, è stato altresì stabilito che i soggetti pubblici, nell'informare gli interessati secondo quanto previsto in generale dalla legge (art. 10 l. 675/1996), debbano fare riferimento espresso alla normativa in cui sono previsti gli obblighi o i compiti in base alla quale è effettuato il trattamento.

La particolare delicatezza dei trattamenti disciplinati dal decreto ha inoltre indotto ad un rafforzamento di alcuni principi generali già sanciti dalla legge 675/1996 ed in particolare dal suo art. 9. I soggetti pubblici sono stati infatti autorizzati a trattare esclusivamente i dati essenziali per

svolgere le attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. Gli stessi soggetti sono, inoltre, chiamati a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

Per assicurare che i dati siano strettamente pertinenti e non eccedenti rispetto agli obblighi ed ai compiti loro attribuiti, i soggetti pubblici devono valutare specificamente il rapporto fra le informazioni personali e gli adempimenti. Nel caso in cui da tali verifiche risulti che alcuni dei dati detenuti o comunque utilizzati sono eccedenti, non pertinenti o non necessari, il loro utilizzo è vietato, fatta salva l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Un'attenzione specifica è infine richiesta nella verifica dell'essenzialità delle informazioni riguardanti soggetti diversi da quelli a cui si riferiscono direttamente le prestazioni o gli adempimenti.

L'uso di mezzi elettronici e di quelli comunque automatizzati per creare elenchi, registri o banche dati, consente il trattamento di quantità molto elevate di informazioni personali con il conseguente aumento dei rischi ad esso connessi. Per tale ragione, in tali ipotesi, i soggetti pubblici debbono ricorrere a tecniche di cifratura ed all'utilizzazione di codici identificativi o di altri sistemi che, considerati il numero e la natura dei dati, consentano di identificare gli interessati solamente in caso di necessità.

In considerazione della particolare delicatezza dei dati idonei a rivelare lo stato di salute e la vita sessuale, il loro trattamento è sempre soggetto al rispetto di quest'ultimo obbligo, indipendentemente dall'uso dei mezzi elettronici o automatizzati a cui si è appena fatto riferimento. Tali informazioni personali devono, inoltre, essere sempre conservate separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo. In ogni caso, infine, è fatto divieto di usare i dati sensibili nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato.

Anche con riguardo alle operazioni di trattamento consentite, si è disposto che i soggetti pubblici debbano svolgere unicamente quelle strettamente necessarie al perseguimento delle finalità per le quali il trattamento è permesso. Inoltre, per accrescere il grado di trasparenza sulle operazioni di raffronto, e così anche consentire un più efficace controllo da parte degli interessati, si è previsto che queste debbano essere sempre accompagnate dall'indicazione scritta dei motivi che le giustificano.

Le novità introdotte dal d.lg. n. 135/1999 sono particolarmente rilevanti soprattutto per le modifiche apportate all'art. 22 della legge n. 675/1996, attraverso le quali si è in gran parte ridisegnato il sistema attraverso cui devono essere regolati i trattamenti di dati sensibili da parte dei soggetti pubblici.

Come si è accennato, la legge generale sulla protezione dei dati personali consentiva tali trattamenti solo se autorizzati da una legge particolarmente dettagliata che indicasse, oltre alle finalità di interesse pubblico perseguite ed alle operazioni eseguibili, anche i dati trattati. In seguito alla modifica, tesa anche ad uniformare la disciplina sui dati sensibili a quella dettata per le informazioni di tipo giudiziario, per rendere possibile il trattamento sarà sufficiente che la legge si limiti ad individuare il genere di dati trattati.

Tuttavia, le modifiche sicuramente più rilevanti attengono al fatto che la legge, pur continuando a costituire la base necessaria per ogni trattamento delle delicate informazioni in questione, non rappresenta più l'unica fonte chiamata a disciplinare, fin nei particolari, i trattamenti medesimi. Si è infatti stabilito che tali trattamenti possano avvenire attraverso due nuovi percorsi procedurali.

Il primo richiede una pronuncia del Garante, chiamato ad intervenire in attesa di una successiva specificazione legislativa. Esso riguarda sia i casi in cui manca un'espressa disposizione di legge del tipo prima indicato, sia quelli non previsti dai decreti legislativi di modificazione ed integrazione della legge 675/1996, emanati in attuazione della legge delega n. 676/1996. In queste ipotesi, i soggetti pubblici possono richiedere all'Autorità l'individuazione delle attività -tra quelle demandate ai medesimi soggetti dalla legge- che perseguono rilevanti finalità di interesse pubblico e per le quali è conseguentemente autorizzato il trattamento.

Anche in questo caso, dunque, il legislatore delegato ha voluto uniformare la disciplina sui dati sensibili a quella in vigore per le informazioni di tipo giudiziario rifacendosi anche all'impostazione della direttiva n. 95/46/CE. Si è in tal modo creata una procedura particolarmente flessibile, tesa soprattutto ad evitare ogni rischio di paralisi nell'attività delle amministrazioni pubbliche fino all'adozione dei provvedimenti normativi diretti a dare regolamentazione definitiva ai trattamenti in discorso.

Il d.lg. n. 135/1999 aveva infine previsto che, per le richieste presentate entro la fine del 1999, l'Autorità avesse novanta giorni di tempo per pronunciarsi, stabilendosi altresì che durante tale termine e fino alla sua decisione fosse possibile proseguire i trattamenti in corso.

Tutto ciò ha dunque rappresentato anche un riconoscimento per il ruolo del Garante che in tale quadro ha contribuito, da un lato, a garantire il perdurante rispetto dei diritti della persona legati alla protezione dei dati e, dall'altro, ad individuare le vie attraverso le quali sia comunque possibile perseguire con efficacia e celerità le finalità dei soggetti pubblici di volta in volta interessati.

La seconda nuova via, attraverso cui i soggetti pubblici possono trarre legittimazione per effettuare trattamenti di dati sensibili, trova applicazione nei casi in cui siano state determinate -secondo il disposto del già citato comma 3 dell'art. 22 della legge 675/1996- le finalità di rilevante interesse pubblico, ma non siano stati specificati i tipi di dati e le operazioni eseguibili.

In tali ipotesi, i soggetti pubblici sono chiamati ad identificare e rendere pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando periodicamente tale identificazione.

Il Garante è intervenuto più volte per chiarire che tale "identificazione" deve essere effettuata attraverso atti di rango regolamentare da parte dei soggetti dotati della relativa potestà. Tali atti dovranno intervenire su profili che prima dell'entrata in vigore del decreto erano disciplinati per legge. Si tratta, poi, di atti che assumono una funzione concretamente normativa in una materia delicata, data la natura delle situazioni soggettive coinvolte, e che svolgono una funzione non meramente ricognitiva di operazioni di trattamento e di tipi di dati (Comunicato del 15 dicembre 1999, in Bollettino n. 10, pag. 112).

Al fine di evitare che le modifiche apportate da tale decreto si risolvano –anche contro lo spirito con cui il Governo stesso ha proceduto alla sua approvazione- in un'attenuazione delle garanzie inizialmente previste dalla legge n. 675/1996, il Garante si è impegnato a vigilare affinché le regole in via di introduzione da parte delle pubbliche amministrazioni assicurino anche il rigoroso rispetto dei principi sopra richiamati. Ciò in considerazione del fatto che -come si è detto- tale regolamentazione deve farsi carico di contemperare in maniera adeguata gli interessi delle singole amministrazioni con i diritti fondamentali dei singoli e di organismi collettivi in ordine alla tutela dei propri dati "particolari".

Si deve infine ricordare che il 31 dicembre 1999 ha segnato il termine entro cui tutte le amministrazioni pubbliche, centrali e locali, dovevano quantomeno avviare l'adeguamento dei propri ordinamenti alle disposizioni prima richiamate. I soggetti pubblici sono stati dunque chiamati ad un'attenta disamina dei trattamenti svolti alla luce dei principi che si sono prima ricordati, veri-

ficando in che misura la disciplina relativa alla loro azione fosse adeguata e sufficiente per assicurare le garanzie oggi richieste. Si è già ricordato, in proposito, il regime più favorevole previsto per le pubbliche amministrazioni che hanno presentato al Garante entro la fine del 1999 una richiesta di autorizzazione allo svolgimento dei trattamenti privi della necessaria copertura normativa. Tali enti hanno potuto infatti proseguire gli stessi trattamenti fino alla decisione dell'Autorità, per la quale era previsto un termine di novanta giorni dalla domanda stessa.

Il d.lg. 135/1999 ha anche provveduto ad individuare un numero considerevole di rilevanti finalità di interesse pubblico, autorizzando i trattamenti ad esse legati. Rinviando al testo del decreto legislativo per la completa elencazione di tali settori, nonché per le disposizioni dettate in relazione a ciascuno di essi, in questa sede è sufficiente sottolineare l'ampiezza di tale individuazione, capace di coprire diversi importanti trattamenti di dati sensibili svolti dalla pubblica amministrazione. Essi interessano, in particolare, lo stato civile, l'anagrafe, le liste elettorali, la cittadinanza, l'immigrazione, la condizione dello straniero, l'esercizio dei diritti politici, la pubblicità degli organi rappresentativi. Ed ancora: i rapporti di lavoro, i tributi, le dogane, le verifiche, le ispezioni, i controlli, l'istruzione, i benefici economici, le abilitazioni, le onorificenze, le ricompense, i riconoscimenti, il volontariato, l'obiezione di coscienza, la tutela della salute, l'interruzione volontaria della gravidanza, le tossicodipendenze, l'handicap, le sanzioni, la tutela in sede amministrativa e giurisdizionale, i rapporti con gli enti di culto, la statistica, la ricerca storica e gli archivi.

Dunque, un insieme di settori assai ampio che tuttavia non esaurisce tutte le materie in cui opera la pubblica amministrazione, sia in ragione del fatto che altri trattamenti svolti dalle pubbliche amministrazioni possono essere –ed in linea di fatto sono- autorizzati attraverso le altre procedure che si sono prima evidenziate; sia perché alcuni dei settori appena elencati hanno successivamente ricevuto un'ulteriore regolamentazione attraverso i decreti delegati previsti dalla legge n. 676/1996 (si rinvia, in particolare, alle sezioni di questa relazione dedicate alla sanità, alla statistica, alla ricerca scientifica e storica).

Come si è detto, il decreto n. 135 non aveva, però, individuato un numero di finalità di rilevante interesse pubblico tale da coprire tutte le innumerevoli attività realizzate dalla pubblica amministrazione, trascurando, in particolare, alcuni importanti trattamenti svolti in sede locale. Per tale ragione, il Garante ha autorizzato le amministrazioni pubbliche e gli enti locali, su loro richiesta, ad utilizzare i dati sensibili per una cospicua serie di specifiche attività che non erano state appunto previste dal d.lg. n. 135/1999 (autorizzazione pubblicata in *Gazzetta Ufficiale* n. 26 del 2 febbraio 2000).

L'autorizzazione ha carattere generale e trova pertanto applicazione anche per gli enti che non avevano presentato apposita richiesta. Essa assume particolare importanza per il rilevante interesse dei trattamenti autorizzati: essi attengono infatti, fra l'altro, al collocamento ed all'avviamento al lavoro, alle attività relative alla gestione degli asili nido e delle mense scolastiche, a quelle degli uffici leva presso i comuni, ai servizi in materia di edilizia abitativa pubblica, nonché alle attività ricreative, di promozione della cultura e dello sport.

Col medesimo provvedimento sono state altresì autorizzate diverse attività socio-assistenziali, quali gli interventi di sostegno psico-sociale e di formazione a favore dei giovani e degli altri soggetti che versano in condizioni di disagio sociale, economico o familiare; gli interventi, anche di rilievo sanitario, in favore dei soggetti bisognosi, non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto. Sempre in tale ambito, sono state autorizzate l'assistenza nei confronti di minori, anche in relazione a vicende giudiziarie, le indagini psico-sociali relative ai provvedimenti di adozione, nonché le iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi.

Oggetto di autorizzazione sono state infine le attività di polizia amministrativa locale, quelle in materia di protezione civile, le attività dei difensori civici regionali e locali, con particolare rife-

rimento alla trattazione di petizioni e segnalazioni, nonché quelle svolte dagli uffici per le relazioni con il pubblico.

Per concludere su tali problematiche, sembra doversi rilevare che le numerose novità introdotte nel corso del 1999 in materia di trattamento di dati sensibili e di carattere giudiziario da parte dei soggetti pubblici vanno nella direzione di una maggiore responsabilizzazione di questi ultimi. Essi sono infatti ora chiamati, in molti casi, ad una vera e propria auto-regolamentazione.

Si tratta di una scommessa e di una sfida per le pubbliche amministrazioni alle quali è data un'occasione unica per instaurare un rapporto nuovo con i cittadini, più rispettoso dei loro diritti e conseguentemente più ricco e suscettibile di ulteriori proficui sviluppi. Tutto ciò non comporterà effetti negativi sull'efficienza dell'azione amministrativa che potrà, anzi, esplicarsi con maggiore efficacia grazie al quadro di trasparenza che viene ad introdursi.

Ed è proprio questo lo spirito che ha animato il Garante nei contributi forniti nella fase di elaborazione delle possibili soluzioni normative, nonché in sede di risposta ai sempre numerosi quesiti e segnalazioni che quotidianamente pervengono in relazione alle problematiche sopra evidenziate. Solo partendo dalla piena e rigorosa tutela dei diritti legati alla sfera privata ed alla protezione delle informazioni personali, le amministrazioni potranno migliorare i loro rapporti con i consociati, contribuendo al rafforzamento dello spirito civico e, così, a far nascere una cittadinanza più matura e consapevole.

Si deve però purtroppo registrare che non tutte le amministrazioni sembrano aver compreso l'importanza di tale sfida e, quindi, operato con la necessaria solerzia nella direzione sperata. Si riscontrano infatti casi di enti pubblici che continuano a considerare l'adeguamento alle disposizioni sulla protezione dei dati come un onere sgradito da cui tenersi lontani, almeno ove ciò sia possibile (Comunicato del 15 dicembre 1999, in Bollettino n. 10, pag. 112).

Anche prescindendo da tutti gli aspetti di illegittimità di tali comportamenti -sui quali il Garante è impegnato ad esercitare un controllo rigoroso- resta comunque da sottolineare l'esigenza di un maggiore spirito di collaborazione anche da parte delle amministrazioni che si sono adeguate o si stanno adeguando alla normativa citata. Questa Autorità si è a tal fine dedicata con energia ad un'opera di informazione e formazione degli operatori del settore. Ciò, oltre che per far conoscere meglio il contenuto delle singole disposizioni, soprattutto per diffondere una cultura della privacy e, in tal modo, fare apprezzare il suo significato profondo e le sue potenzialità nel miglioramento delle relazioni reciproche fra cittadini e istituzioni.

2.1.6 Nuovi archivi e grandi banche dati

L'attuale grande e continua evoluzione tecnologica apre sempre nuove possibilità di creazione di archivi e banche dati in grado di contenere un numero crescente di informazioni personali che possono essere poste in relazione fra loro per le finalità più diverse. Tutto questo offre certamente un'opportunità per i cittadini e le imprese, che possono così disporre di nuovi servizi in maniera più efficiente e rapida. E costituisce, altresì, una facilitazione per le pubbliche amministrazioni che possono ridurre i costi della loro azione e rendere più efficaci i controlli.

Tuttavia, questo comporta anche un aumento dei rischi intrinsecamente connessi con tali operazioni, le quali moltiplicano le possibilità che i dati vengano impropriamente comunicati o comunque utilizzati per finalità differenti da quelle consentite o autorizzate. Per tale ragione, il Garante è impegnato in un'opera di attenta vigilanza sulle iniziative relative a nuove banche dati, al fine di verificare il rispetto delle disposizioni in materia di riservatezza.

Le possibilità offerte dalla tecnica, se correttamente utilizzate in questo ambito, possono costituire un'importante risorsa anche per accrescere il livello di partecipazione dei cittadini alla

vita sociale ed alle scelte collettive, innalzando in tal modo lo stesso grado di democraticità del sistema. Al contrario, però, un uso delle grandi potenzialità tecniche che fosse poco rispettoso dei diritti delle persone potrebbe condurre rapidamente ad una pericolosa regressione verso un restringimento degli spazi di libertà individuale e collettiva.

Se veramente si vuole che la società attuale, caratterizzata anche dalla necessità di molteplici flussi informativi e di conoscenza, non si trasformi in una società della sorveglianza e della classificazione, è necessario che tutti i soggetti operanti nei diversi contesti sociali maturino la piena consapevolezza dei rischi legati ad un uso non selezionato o non corretto delle informazioni personali ed insieme delle stesse opportunità di sviluppo e crescita civile legate al rispetto dei diritti connessi alla tutela della riservatezza personale.

Per questo motivo, le rapide trasformazioni in cui siamo immersi non possono essere lasciate alla loro più o meno naturale evoluzione, ma devono essere accompagnate da un'attenta riflessione sulle conseguenze legate ad ogni diversa opzione. Così, il moltiplicarsi degli archivi e delle interconnessioni fra banche dati non può derivare quasi meccanicamente dell'aprirsi di nuove potenzialità tecniche, ma deve presentarsi come il risultato di un cammino consapevole e comunque rispettoso dei diritti personali.

Naturalmente, nel governo di questi incessanti cambiamenti, i soggetti pubblici hanno un ruolo determinante sia per le decisioni di carattere normativo che sono chiamati a prendere, direttamente destinate a regolare il comportamento altrui, sia per le scelte compiute all' interno, attraverso l'organizzazione delle proprie attività.

Negli anni più recenti le pubbliche amministrazioni, impegnate in un meritevole sforzo per ammodernarsi e rendersi più efficienti, hanno mostrato un interesse crescente per tali sviluppi e hanno compiuto passi avanti verso un migliore utilizzo di tali strumenti. Specialmente intorno al progetto per la realizzazione della rete unitaria della pubblica amministrazione, si assiste ad un fiorire di iniziative destinate a creare entro breve tempo una più ampia automatizzazione dei servizi ed una progressiva informatizzazione degli uffici. Tutto ciò grazie in particolare ad un numero accresciuto di interconnessioni fra le diverse banche dati, con però il conseguente grave rischio che possa pensarsi che la mera esistenza dei collegamenti fra le tante e diverse banche dati delle pubbliche amministrazioni possa far prescindere dal rispetto dell'essenziale principio di finalizzazione che caratterizza la legislazione sulla tutela dei dati personali, secondo il quale i dati possono essere raccolti e successivamente trattati per i soli fini determinati dalle diverse normative o con essi compatibili. Normative che possono prevedere la comunicazione ed anche la diffusione dei diversi dati, ma nel rispetto di quanto prescritto dalle disposizioni della legge 675/1996 relative alle diverse categorie di dati personali (si vedano in particolare l'art.27, comma secondo, l'art. 22, comma 3 e 3 bis, l'art. 24).

Il Garante ha avuto modo di occuparsi di tali banche dati in più occasioni durante l'anno trascorso, specie in occasione delle richieste di parere sugli schemi di disposizioni normative predisposte dal Governo.

Limitandosi in questa sede ad un sintetico richiamo ad alcune delle maggiori iniziative intraprese da soggetti pubblici e privati e rinviando, per una loro più puntuale disamina alle altre parti di questa relazione, è qui sufficiente richiamare anzitutto la previsione dell'anagrafe degli assegni bancari prevista dall'art. 36 del decreto legislativo n. 507 del 1999 (su cui cfr. par. 2.6.5) e lo schema di regolamento governativo che istituisce un archivio dei rapporti di conto e deposito, previsto dalla legge n. 413 del 1999 sul potenziamento degli accertamenti fiscali e sulla riforma del contenzioso, sul quale si è espresso criticamente il Garante il 17 novembre 1999 (cfr. par. 2.6.3).

L'Autorità ha altresì partecipato alle attività del Comitato di coordinamento per l'indirizzo ed il controllo della fase di avvio e sperimentazione del Sistema di accesso e interscambio anagrafi-

co - SAIA (art. 8 della Convenzione stipulata in data 4 novembre 1999 tra il Ministero dell'interno e l'Associazione nazionale comuni italiani - A.N.C.I.). Tale Sistema è stato previsto dal Ministero dell'interno in vista del conseguimento della semplificazione burocratica, della riduzione dei costi dei servizi pubblici e del rilascio della carta di identità elettronica (d.P.C.M. 22 ottobre 1999, n. 437), sulla base di un progetto intersettoriale dell'Autorità per l'informatica nella pubblica amministrazione. Il Ministero dell'interno ha posto anche l'esigenza di realizzare, nell'ambito del medesimo Sistema, un Indice nazionale delle anagrafi per l'immediata individuazione del Comune che detiene i dati personali contenuti nelle anagrafi della popolazione di ciascun cittadino, nonché per facilitare l'esercizio dei compiti di vigilanza attribuiti sulla tenuta delle anagrafi comunali.

La rilevante incidenza di quest'ultima progettata innovazione sull'ordinamento anagrafico ed un'assai ampia individuazione dei soggetti legittimati ad accedere all'Indice, hanno originato una prima presa di posizione del Garante, il 2 novembre 1999, nei riguardi del Ministro dell'interno ed una successiva, l'8 marzo 2000, nei riguardi di una pluralità di organi governativi, facendosi presente che la materia sembra esigere un intervento a livello legislativo, che permetta anche di definire con chiarezza le finalità di utilizzo, i soggetti aventi accesso e il contenuto stesso di questo Indice, che comunque non può certo prefigurare la creazione di una vera e propria anagrafe nazionale. Successivamente a questi interventi, sembra che sia in fase di predisposizione un apposito disegno di legge (su tutta la vicenda cfr. par. 2.1.9).

L'Autorità è stata altresì chiamata ad occuparsi delle diverse banche dati costituite nell'ambito del sistema creditizio e finanziario.

Come è noto, presso la Banca d'Italia opera la Centrale dei rischi alla quale sono tenuti a partecipare le banche iscritte all'albo di cui all'art. 13, le società finanziarie di cui all'art. 65, comma 1, lett. a) e b), nonché gli intermediari finanziari iscritti nell'elenco speciale di cui all'art. 107 del testo unico delle leggi in materia bancaria e creditizia, i quali esercitano, in via esclusiva o prevalente, l'attività di finanziamento sotto qualsiasi forma.

Recentemente l'Associazione bancaria italiana (ABI) si è espressa a favore della realizzazione di un sistema di rilevazione degli affidamenti di importo inferiore alla soglia di rilevazione della Centrale di cui sopra. Ciò al fine di ricavare una completa valutazione di tutti i rischi assunti nei confronti della clientela del sistema creditizio e finanziario. Il C.I.C.R., ritenendo che tale iniziativa si iscriva nella logica di sana e prudente gestione e sia coerente con le finalità di vigilanza, ha stabilito l'obbligo, per tutti gli intermediari finanziari che partecipano alla Centrale dei rischi prima citata, di comunicare ad un sistema centralizzato di rilevazione tutti i dati relativi alle esposizioni creditizie di importo inferiore al limite minimo del censimento previsto per la medesima Centrale e superiore al limite massimo stabilito per le operazioni di credito al consumo (attualmente pari a sessanta milioni di lire).

Alla Banca d'Italia è stato affidato il compito di emanare le istruzioni di carattere generale necessarie all'attuazione della delibera del C.I.C.R., prevedendo però che prima essa consulti il Garante per gli aspetti relativi al trattamento dei dati personali e che, successivamente, verifichi il rispetto della relativa disciplina (cfr. par. 2.6.3).

Al fine di offrire un'idea della vastità del fenomeno a cui si è fatto riferimento, può essere utile ricordare altresì alcune altre banche dati di più recente costituzione.

All'interno del Sistema informativo agricolo nazionale (SIAN), integrato con i sistemi informativi regionali, è stata costituita un'anagrafe delle aziende agricole. Essa raccoglie le notizie relative ai soggetti pubblici e privati esercenti attività agricola, agroalimentare, forestale e della pesca, che intrattengano a qualsiasi titolo rapporti con la pubblica amministrazione centrale o locale (art. 1, d.P.R. 1 dicembre 1999, n. 503).

Nell'ambito del riordino delle procedure di collocamento pubblico dei lavoratori dipen-

denti si prevede poi l'istituzione di un Sistema informativo lavoro e di una carta elettronica personale del lavoratore (cfr. par. 2.3.1 di questa relazione).

Più di recente, presso la banca dati dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro e le malattie professionali (INAIL), è stato istituito il registro nazionale delle malattie causate dal lavoro ovvero ad esso correlate. Per ciò che specificamente attiene alla protezione dei dati personali, la disciplina di tale registro richiama la necessità di rispettare quanto disposto dalla legge n. 675/1996, specificando inoltre le categorie di soggetti che possono avervi accesso (art. 10, comma 5, d.lg. 23 febbraio 2000, n. 38).

Con lo stesso provvedimento normativo, si è altresì proceduto al riordino dei compiti e della gestione del Casellario centrale infortuni. Quest'ultimo, posto sotto la vigilanza del Ministero del lavoro e della previdenza sociale, è titolare di una banca dati relativa agli infortuni professionali e non professionali ed alle malattie professionali. Essa viene alimentata e può essere consultata dagli istituti che esercitano l'assicurazione obbligatoria contro gli infortuni sul lavoro, nonché dagli enti che provvedono all'assicurazione contro i rischi di infortunio e contro i rischi derivanti dalla circolazione di automezzi.

Il Casellario dovrà archiviare, conservare e comunicare agli utenti i dati relativi ai casi di infortunio e di malattia professionale che importino invalidità permanente o morte, anche a prescindere da uno specifico evento lesivo. Esso dovrà inoltre elaborare i dati mediante procedure informatiche che consentano l'ottimizzazione del loro uso anche in forma aggregata da parte dei soggetti autorizzati. Suo compito è, infine, quello di favorire l'integrazione ed il raccordo della propria banca dati con altre analoghe a livello nazionale e sovranazionale, nonché con quelle a carattere previdenziale (artt. 15-17, d.lg. 23 febbraio 2000, n. 38).

Da quanto detto e dagli esempi fatti, si desume con chiarezza che l'obiettivo di consentire, attraverso la gestione informatica dei flussi documentali, un più ampio interscambio di dati tra le diverse amministrazioni e fra queste ed i cittadini può svilupparsi solo se viene inserito all'interno di un preciso quadro di garanzie sul rispetto dei diritti fondamentali della persona.

A tal fine, è innanzi tutto necessario avere sempre presenti gli sviluppi complessivi del sistema, così da poterne valutare in modo corretto i rischi e le opportunità, calibrando conseguentemente le misure atte a tutelare i diritti eventualmente messi in pericolo. In tal modo, è anche possibile evitare i pur troppo frequenti casi di duplicazioni e sovrapposizioni fra diversi trattamenti, di impropria diffusione delle informazioni personali o anche solo la costituzione di pericolose concentrazioni di dati, intrinsecamente portatrici di un accrescimento dei rischi.

Occorre evitare poi la creazione di grandi banche la cui disciplina, benché inclusiva di generiche clausole di richiamo della legge n. 675, sia in realtà lacunosa e priva di adeguate garanzie per ciò che riguarda le finalità perseguite, le modalità del trattamento, i flussi di dati e i soggetti legittimati ad utilizzarli.

È in ogni caso necessario che il fiorire non sempre ordinato di disposizioni legislative sulla creazione di nuovi archivi o sulla concentrazione di quelli esistenti rispetti i principi dettati dalla legge 675/1996, essendo questi in gran parte una trasposizione dei contenuti della direttiva 95/46/CE, alla quale il nostro ordinamento è vincolato ad adeguarsi. Tale rilievo assume evidentemente un carattere ancora più pressante per i casi in cui la regolamentazione dei diversi settori avviene attraverso norme di rango regolamentare o, addirittura, mediante circolari ed altri atti amministrativi, comunque privi di carattere normativo (Comunicato del 18 ottobre 1999, in Bollettino n. 10 pag. 88).

Nel corso del 1999, il Garante si è in più occasioni adoperato per sensibilizzare le pubbliche amministrazioni ed i cittadini in ordine a tali problematiche ed ha nel contempo compiuto uno sforzo per far riscoprire le ragioni profonde di quella parte della normativa relativa alla tutela della

riservatezza dalla quale è scaturito il primo nucleo delle leggi più avanzate oggi vigenti. Normativa, che era appunto incentrata sulla regolazione delle banche dati e sui trattamenti realizzati mediante strumenti elettronici.

2.1.7 Documenti elettronici e carte magnetiche

L'evoluzione normativa e la pratica amministrativa mettono in luce una tendenza sempre più diffusa all'utilizzo da parte delle pubbliche amministrazioni di documenti elettronici, di carte magnetiche con funzioni identificative dei cittadini ma anche finalizzate a consentire una più celere erogazione di taluni servizi. Tali strumenti offrono indubbi vantaggi per i cittadini, che in tal modo hanno l'opportunità di ridurre gli oneri di carattere burocratico a cui spesso sono sottoposti e di ottenere con maggiore celerità quanto loro dovuto. Essi comportano anche notevoli risparmi per gli uffici pubblici, che possono contenere i costi sia per la maggiore celerità delle procedure, sia per la possibilità di evitare inutili duplicazioni di documenti ed archivi.

Tutto questo non deve però andare a detrimento della tutela dei diritti delle persone e, in particolare, della riservatezza di ciascuno. Per tale motivo, nel disciplinarne l'utilizzo, è indispensabile porre particolare attenzione al tipo di informazioni che vengono inserite al loro interno, alle operazioni che è possibile fare su di essi ed ai soggetti che hanno accesso alle diverse categorie di dati. È inoltre necessario inquadrare gli interventi diretti alla creazione di nuovi documenti elettronici e carte magnetiche all'interno di un progetto organico, evitando che si creino – come, purtroppo, a volte si verifica – duplicazioni e sovrapposizioni di informazioni ed archivi.

Nella regolamentazione di tali strumenti assume infine particolare rilievo il grado di libertà lasciato agli interessati in ordine alla possibilità di inserire o meno alcuni dati. Al fine di consentire una scelta realmente consapevole, è necessario che siano prospettati in maniera chiara ed esaustiva non solo i trattamenti a cui saranno soggetti in via ordinaria i dati, ma anche tutti i possibili ulteriori usi degli stessi, nonché i rischi legati alla conservazione di tali informazioni all'interno del supporto elettronico (per il parere sulla carta di identità elettronica cfr. par. 2.1.9).

Sotto tutti questi profili, le previsioni relative alle carte sanitarie elettroniche contenute nell'art. 6 del d.lg. n. 282/1999 possono certamente essere considerate un primo importante risultato, frutto anche di un proficuo confronto instaurato fra l'amministrazione interessata ed il Garante. Rinviando per una più approfondita analisi della disposizione in parola al par. 2.2.4 di questa relazione, si deve qui ricordare che, sulla base di esso, gli interessati possono opporsi all'inserimento nelle carte sanitarie dei dati idonei a rivelare lo stato di salute che li riguardano e che eccedono le informazioni relative alla gestione amministrativa e alle situazioni di interventi di urgenza, quali definiti a livello internazionale. Tali disposizioni prevedono inoltre che un decreto ministeriale determini le categorie di incaricati delle aziende sanitarie locali e di operatori che possono accedere ai diversi tipi di dati contenuti nelle carte, le categorie professionali tenute ad inserire i dati, nonché il periodo massimo di conservazione (art. 6, commi 2 e 3).

Conviene, infine, richiamare l'attenzione sulla necessità che i progetti relativi all'introduzione dei documenti elettronici e delle carte magnetiche tengano conto degli sviluppi che si stanno registrando in sede comunitaria. Attualmente, infatti, è in corso un ricco dibattito che mira ad individuare standard tecnici uniformi e regolamentazioni analoghe a livello dell'Unione europea. Regolamentazione, questa, all'interno della quale la tutela della riservatezza rappresenta uno dei capitoli di maggiore rilievo. In tale percorso elaborativo confluiscono perciò le diverse esperienze nazionali in materia, che, fondandosi sulla base comune della citata direttiva n. 95/46/CE, possono condurre a migliori tutele dei diritti della persona, ampliando nel contempo l'ambito di utilizzabilità dei documenti e delle carte in discorso.

In alcuni casi, invece, proprio l'utilizzo delle tecnologie elettroniche può consentire una maggiore tutela della riservatezza, ad esempio permettendo di selezionare le persone che possono avere accesso alle diverse categorie di dati, o facilitando la conservazione separata dei dati fino a che sorga l'effettiva necessità di una loro riunione. Su questo versante si può ricordare il caso inte-

ressante sorto con la proposta di istituire una tessera elettorale cartacea destinata a svolgere la funzione di certificato elettorale per diciotto consultazioni, in attesa di adottare una tessera magnetica (art. 13, l. 30 aprile 1999, n. 120).

La proposta, contenuta in uno schema di regolamento sottoposto al parere del Garante, avrebbe avuto il vantaggio di ridurre le spese per le operazioni di voto, in quanto il costo della distribuzione su tutto il territorio nazionale dei certificati elettorali, ora sostenuto per ogni consultazione, sarebbe stato sostituito dai minori oneri legati alla distribuzione della tessera una sola volta per tutti gli appuntamenti elettorali in essa registrabili. Essa avrebbe inoltre consentito di ridurre il rischio - di fatto ineliminabile col sistema attuale - che qualche persona appartenente alle categorie abilitate a votare anche in sezioni diverse da quelle di iscrizione possa tentare di esprimere un voto doppio o plurimo (la tessera elettorale, avrebbe dovuto contenere, fra le altre informazioni, anche la certificazione dell'avvenuta votazione).

Proprio quest'ultimo dato assume però una particolare delicatezza in quanto - specie in alcune consultazioni quali i referendum abrogativi o votazioni di ballottaggio -, la partecipazione o la mancata partecipazione al voto possono di per sé manifestare una particolare opzione politica dell'elettore. Ed è dunque evidente che la conservazione in un unico documento cartaceo della storia della partecipazione al voto di un elettore espone quest'ultimo al rischio di pressioni di vario genere, che potrebbero ridurre la sua sfera di libertà. Sono, infatti, numerose le persone che potrebbero trovarsi nella condizione di verificare il contenuto di tale documento, sia per ragioni legate al proprio ufficio (è, ad esempio, il caso del personale addetto ai seggi), sia, soprattutto, in conseguenza dei rapporti intrattenuti con l'interessato (si pensi alla famiglia, alle associazioni politiche, all'ambiente di lavoro).

Proprio la considerazione del fatto che lo strumento cartaceo era in ogni caso destinato ad essere superato in tempi rapidi da tessere elettroniche in grado di garantire un più elevato livello di riservatezza, il Garante con il parere del 17 novembre 1999 (in Bollettino n. 10, pag. 19) ha suggerito al Ministero dell'interno di attendere che tali più moderni strumenti possano essere introdotti. Ciò, anche in considerazione delle analoghe iniziative che si stanno sperimentando in ambito comunitario.

In alternativa a ciò, l'Autorità ha comunque segnalato la necessità che fossero adottati accorgimenti atti a ridurre i rischi sopra evidenziati, quali la conservazione separata dei dati identificativi da quelli relativi alla partecipazione al voto, consentendo la loro riunione solo quando questa sia effettivamente necessaria. Il Garante ha inoltre avuto modo di richiamare la necessità di un più attento vaglio della pertinenza dei dati contenuti nella tessera rispetto alle finalità che con essa si intendono perseguire, nonché l'obbligo di adottare le ordinarie misure di sicurezza previste dal nostro ordinamento.

Con particolare riguardo alla possibilità che nella tessera venisse inserito anche un codice di identificazione personale, ed al di là di ogni considerazione sulla pertinenza dello stesso, il Garante ha inoltre voluto ribadire le considerazioni già espresse in un precedente parere relativo alla carta di identità elettronica (parere del 26 febbraio 1998 sullo schema di regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica), relative alla necessità che l'attribuzione ed il trattamento di dati connessi a numeri di identificazione personale siano accompagnati da precise garanzie sui presupposti e sulle condizioni per il loro utilizzo. Garanzie, queste, che devono essere affidate a norme di carattere primario (art. 8, par. 7, direttiva n. 95/46/CE).