DIPARTIMENTO DELLA FUNZIONE PUBBLICA

per l'efficienza delle amministrazioni

Presidenza del Consiglio dei Ministri
DIPARTIMENTO DELLA FUNZIONE PUBBLICA

La tutela della Privacy del personale delle pubbliche amministrazioni

La Direttiva del Ministro per la Funzione Pubblica dell'11 febbraio 2005 "Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, con particolare riguardo alla gestione delle risorse umane"

a cura

Ufficio per il Personale delle Pubbliche Amministrazioni

ANALISI E RICERCHE PER LA GESTIONE DELLE RISORSE UMANE

La tutela della Privacy del personale delle pubbliche amministrazioni

La Direttiva del Ministro per la Funzione Pubblica dell'11 febbraio 2005 "Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, con particolare riguardo alla gestione delle risorse umane"

a cura
dell'Ufficio per il Personale delle Pubbliche Amministrazioni

INDICE

PREFAZIONE

Il decreto legislativo 30 giugno 2003, n. 196 ha posticipato l'entrata in vigore delle proprie disposizioni al primo gennaio 2004 anche in considerazione della complessità dello sforzo innovatore che l'applicazione delle sue disposizioni comporta per le pubbliche amministrazioni.

L'aver introdotto nell'ordinamento un nuovo diritto fondamentale, quale quello alla protezione dei dati personali, comporta la necessità che gli operatori pubblici, a tutti i livelli, mutino il proprio approccio alle tematiche della riservatezza. Ciò anche in considerazione degli obblighi che gravano sul nostro paese in forza della sua appartenenza all'Unione, la quale ha scritto tale diritto fra quelli enunciati dalla Carta dei diritti fondamentali dell'Unione europea.

Già in precedenza le pubbliche amministrazioni avevano mostrato non poche difficoltà nell'adeguarsi alle previsioni contenute nei decreti legislativi 11 maggio 1999, n. 135 e 31 dicembre 1996, n. 675. La situazione era stata puntualmente rilevata dall'Autorità garante per la protezione dei dati personali già nelle relazioni annuali al Parlamento del 2002 e del 2003. Ora l'adozione di uno strumento normativo unitario, che coordina efficacemente il complesso delle norme interne sulla materie con le nuove convenzioni e direttive comunitarie, offre l'opportunità alla pubblica amministrazione di ripensare la propria attività all'interno di un sistema di regole certe e semplificate.

I principi posti dal Codice, ed evidenziati nella direttiva del Ministro per la funzione pubblica, costituiscono un'esigenza trasversale che deve guidare l'azione amministrativa in ogni sua manifestazione, prescindendo da un approccio formale e burocratico per ripensare, invece, la propria organizzazione ed i propri processi.

In questa ottica deve essere letta l'introduzione, operata dal Codice, del comma 1-bis all'articolo 2 del decreto legislativo 30 marzo 2001, n. 165. Ciò comporta, infatti, che i criteri di organizzativi ivi dettati debbono tenere conto della disciplina vigente in materia di trattamento dei dati personali, così informando profondamente l'ordinamento del lavoro alle dipendenze delle pubbliche amministrazioni.

L'adozione di codici di deontologia e di buona condotta per i soggetti interessati al trattamento dei dati effettuato per finalità previdenziali e per la gestione dei rapporti di lavoro, prevista dall'articolo 111 del Codice e che ad esso saranno successivamente allegati, costituisce uno strumento già noto alle pubbliche amministrazioni ed loro ordinamento in quanto già il decreto n. 29 del 1993, ed ora il decreto n. 165 del 2001 all'articolo 54, prevedeva la necessità di adottare un codice di comportamento dei dipendenti quale strumento organizzativo finalizzato ad assicurare la qualità dei comportamenti, anche in relazione alle necessarie misure organizzative da adottare al fine di assicurare la qualità dei servizi resi ai cittadini.

È proprio nella sua veste di datore di lavoro che la pubblica amministrazione può imprimere la spinta necessaria al sistema per rivedere le proprie attività, poiché è forse proprio da un'efficace politica interna che può partire quel processo di crescita culturale che solo realizza l'effettività dei diritti affermati in sede normativa.

Francesco Verbaro
Direttore dell'Ufficio per il personale
delle pubbliche amministrazioni

INTRODUZIONE

L'adozione da parte del Ministro per la funzione pubblica di una direttiva per l'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel Codice sulla privacy, con particolare riguardo alle tematiche relative alla gestione delle risorse umane, è dovuta all'attenzione che il legislatore ha posto sul tema dei rapporti fra datori di lavoro pubblici e lavoratori ed ai frequenti richiami allo Statuto dei lavoratori, che si applica anche al lavoro pubblico per esplicito richiamo dell'articolo 51 del decreto legislativo n. 165 del 2001.

Infatti al Titolo VIII, dedicato al lavoro ed alla previdenza sociale, ed in particolare all'articolo 112, sono individuate le finalità di rilevante interesse pubblico quali l'instaurazione e la gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito, che consentono il trattamento dei dati personali, sensibili e giudiziari. Con atto di natura regolamentare le amministrazioni, in relazione alle finalità di rilevante interesse pubblico già definite dal legislatore e per le quali sia necessario acquisire e trattare i dati sensibili e giudiziari, specificheranno i tipi di dati e le operazioni eseguibili.

Anche gli altri adempimenti previsti dal Codice a carico delle pubbliche amministrazioni, e ricordati nella Direttiva al paragrafo 3, toccano i rapporti fra le amministrazioni ed il personale da esse dipendente, così come al paragrafo 6 sono ricordate alcune tematiche di interesse in materia di gestione del personale che vanno dalle fasi dell'accesso al lavoro pubblico, alla gestione dei fascicoli personali, al divieto del controllo a distanza dell'attività lavorativa fino ai temi più attuali della vigilanza sulle comunicazioni elettroniche e sull'utilizzo di internet sul posto di lavoro.

Fa da sfondo a tutte le attività delle amministrazioni l'informatizzazione delle procedure e la raccolta ed il trattamento di informazioni con tecnologie informatiche le quali comportano la necessità di osservare le misure di sicurezza indicate dal Codice fra le quali l'adozione del Documento programmatico sulla sicurezza.

La Direttiva contiene, inoltre, un paragrafo dedicato alla relazione fra

diritto di accesso agli atti amministrativi e diritto alla tutela della riservatezza, nel quale vengono sinteticamente richiamati gli orientamenti giurisprudenziali che hanno guidato le amministrazioni ogni qualvolta tali diritti si siano trovati in contrapposizione.

La finalità che sottende tutta la Direttiva sta nel richiamo ai dirigenti ed ai funzionari preposti alle unità organizzative perché adottino tutte le misure utili a garantire il rispetto e la piena attuazione dei principi sanciti dal Codice. Questi, infatti, si trovano a giocare, per così dire, un doppio ruolo operativo in materia di tutela della riservatezza poiché la garantiscono sia per quanto concerne l'esercizio delle funzioni proprie dell'amministrazione di appartenenza che nella gestione delle risorse umane.

Stefania de Paulis

LA DIRETTIVA DEL MINISTRO PER LA FUNZIONE PUBBLICA DEL 11 FEBBRAIO 2005 "MISURE FINALIZZATE ALL'ATTUAZIONE NELLE PUBBLICHE AMMINISTRAZIONI DELLE DISPOSIZIONI CONTENUTE NEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196, RECANTE CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, CON PARTICOLARE RIGUARDO ALLA GESTIONE DELLE RISORSE UMANE"

1. Premessa

Il primo gennaio del 2004 è entrato in vigore il decreto legislativo 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali", d'ora in poi denominato "Codice", nel quale sono raccolte, in forma di testo unico, tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ed alle attività connesse.

Il Testo rappresenta il primo modello di codificazione organica della privacy in Europa e tiene conto sia del quadro normativo comunitario (direttive n. 95/46/CE e n. 2002/58/CE) che di quello internazionale.

La disciplina del Codice, analogamente a quella dettata dalla normativa previgente, si innesta in un contesto prevalentemente orientato alla pubblicità dell'azione amministrativa, ad opera della legge 7 agosto 1990, n. 241 e delle altre disposizioni di settore, e conferma la graduazione dei differenti livelli di tutela previsti all'interno della generale categoria dei dati personali predisponendo garanzie più rigorose in relazione ai dati sensibili.

Il Codice offre al cittadino un sistema di garanzie articolato e al contempo semplificato che, nell'individuare tutti gli strumenti idonei ad una piena realizzazione del diritto alla protezione dei dati personali, costituisce

il presupposto per la fruizione di tutti gli altri diritti fondamentali dell'individuo che a quel diritto sono naturalmente collegati.

In tale quadro i principi ricordati nel Testo unico informano tutti gli aspetti della vita sociale e dell'azione delle pubbliche amministrazioni ed in particolare, per quanto interessa in questa sede, anche gli aspetti relativi alla gestione delle risorse umane in tutti gli aspetti organizzativi, di sicurezza e di benessere.

2. I principi e gli obblighi

Appare opportuno ricordare in questa sede i principi che derivano dal Codice in materia di protezione dei dati personali ai quali l'azione amministrativa dovrà ispirarsi e che sono destinati ad esercitare una grande influenza sull'esercizio della potestà organizzativa delle pubbliche amministrazioni.

Il "diritto alla protezione dei dati personali" quale prerogativa fondamentale della persona, è stato introdotto nell'ordinamento in attuazione dell'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea del 7 dicembre 2000 e deve considerarsi quale diritto autonomo e distinto rispetto al diritto alla riservatezza sostanziandosi nel diritto del suo titolare di conoscere e controllare la circolazione delle informazioni che lo riguardano.

Il Codice, che ha dunque affermato, all'articolo 1, il diritto alla protezione dei dati personali, mira a garantire che il trattamento di queste informazioni "si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 2).

Un principio generale del sistema di garanzie approntato dal Codice che deve guidare l'azione amministrativa è costituito dal principio di "necessità del trattamento dei dati personali", da intendersi quale principio che integra quello di "pertinenza e non eccedenza" dei dati trattati (già individuato dalla legge n. 675 del 1996) con riferimento alla configurazione di sistemi informativi e programmi informatici. Tale regola prescrive di predisporre i sistemi informativi e i programmi informatici in modo da utilizzare al minimo dati personali ed identificativi escludendone il trattamento quando le finalità perseguite possono essere raggiunte mediante l'uso di dati anonimi o di modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3). Deve essere, inoltre, ricordato che il principio di necessità costituisce un presupposto di liceità del trattamento dei dati personali ed il mancato rispetto di questo e degli altri presupposti comporta conseguenze rilevanti per l'amministrazione. Infatti il Codice, nel dettare le regole per tutti i trattamenti ha sancito l'inutilizzabilità dei dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (articolo 11, comma 2).

Il diritto alla protezione dei dati personali potrà, pertanto, essere garantito solo se le amministrazioni titolari dei trattamenti ispireranno la loro attività ai principi sanciti dal Codice e conseguentemente, oltre ad ottemperare agli obblighi espressamente previsti, adotteranno una serie di comportamenti concreti, azioni e provvedimenti organizzativi coerenti con i principi che regolano la materia.

In particolare, il trattamento dei dati personali da parte delle pubbliche

amministrazioni è consentito solo qualora sia necessario per lo svolgimento delle funzioni istituzionali rispettando gli eventuali altri presupposti e limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti. Al riguardo è il caso di sottolineare che, salvo quanto previsto per i trattamenti posti in essere dagli esercenti le professioni sanitarie e gli organismi sanitari pubblici (parte II del Codice), le pubbliche amministrazioni non devono chiedere il consenso dell'interessato.

I dati sensibili possono, invece, essere trattati soltanto se il trattamento risulta autorizzato da un'espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite (artt. 18, 19, 20 e 22 del Codice. Per i dati sensibili v. più diffusamente *infra* la parte relativa ai "Regolamenti").

E' inoltre, imposto alle amministrazioni l'obbligo di garantire la sicurezza nella gestione dei dati e dei sistemi in modo da ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Pertanto le amministrazioni, o i soggetti affidatari di servizi e sistemi per conto delle stesse, dovranno adottare tutte le cautele consentite dalle moderne tecnologie prevenendo i rischi derivanti dall'organizzazione e gestione delle banche dati e dei sistemi informativi (artt. 31-35 e disciplinare tecnico contenuto nell'Allegato B) al Codice). Analoghe cautele dovranno essere adottate nella gestione di tutti gli atti ed i provvedimenti che comportano l'utilizzo di dati personali e sensibili.

Nell'ambito del predetto obbligo generale di contenere nella misura più ampia possibile determinati rischi, i titolari del trattamento sono tenuti in ogni caso ad assicurare un livello minimo di protezione dei dati mediante l'adozione delle "misure minime" di sicurezza individuate nel Titolo V, Capi I e II, della Parte II del Codice o che saranno individuate ai sensi dell'articolo 58, comma 3, in relazione ai trattamenti effettuati per finalità di difesa o coperti da segreto di Stato.

La disciplina del Codice, infine, è informata dal principio di semplificazione in base al quale l'elevato grado di tutela dei diritti è assicurato nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità di esercizio del diritto alla protezione dei dati personali e degli altri diritti e libertà fondamentali dell'interessato e degli adempimenti in capo ai titolari del trattamento (art. 2, comma 2).

Disposizioni in deroga o ad integrazione della disciplina generale sono poste dal Codice in relazione a specifici settori di interesse per l'attività amministrativa, quali l'ambito giudiziario, negli articoli da 46 a 52, i trattamenti eseguiti dalle forze di polizia, negli articoli da 53 a 57, e quelli attinenti alla difesa e sicurezza dello Stato, di cui all'articolo 58.

3. Finalità della direttiva

La presente direttiva è finalizzata a richiamare l'attenzione delle amministrazioni sulle prescrizioni del Codice che incidono maggiormente nel settore pubblico, richiedendo l'adozione di efficaci scelte organizzative per tradurre sul piano sostanziale le garanzie previste dal legislatore, nonché sulle conseguenze connesse alla loro mancata attuazione.

L'entrata in vigore del nuovo Codice comporta, per le pubbliche amministrazioni, la necessità di ripensare le proprie attività e la propria organizzazione al fine di consentire una piena ed effettiva garanzia dei diritti in esso affermati.

Infatti, le tematiche relative alla privacy investono le amministrazioni nella quasi totalità delle proprie attività, assumendo significativo rilievo nello svolgimento di molti dei compiti istituzionali loro affidati dall'ordinamento, come ad esempio, la gestione delle risorse umane.

In considerazione di ciò, il Codice (art. 176) ha aggiunto il comma 1-bis al comma 1 dell'articolo 2 del decreto legislativo 30 marzo 2001, n. 165. Pertanto le amministrazioni dovranno attuare le linee fondamentali di organizzazione degli uffici nel rispetto della disciplina in materia di trattamento dei dati personali, in aggiunta ai criteri indicati nella medesima disposizione .

Da quanto premesso emerge la necessità di provvedere all'adozione degli strumenti necessari per l'attuazione pratica delle previsioni del Codice, quali:

– regolamenti indicanti i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere eseguite su di essi in relazione al perseguimento di finalità di rilevante interesse pubblico qualora manchi una specifica indicazione legislativa (artt. 20, 21 e 22);
– le informative all'interessato (art. 13);
– la notificazione al Garante nei casi previsti dall'art. 37;
– le eventuali comunicazioni al Garante (art. 39);
– le misure minime di sicurezza e, in particolare, il documento programmatico sulla sicurezza (art. 34, comma 1, lett. g) e regola n. 19 dell'Allegato B) al Codice)).

Occorrerà, inoltre, procedere a puntuali ricognizioni dei dati trattati alla luce delle disposizioni vigenti e alla revisione delle modalità di gestione degli stessi, ponendo particolare attenzione alla necessità di garantire agli interessati l'esercizio del diritto di accesso ai dati che li riguardano e degli altri diritti sanciti dall'art. 7 del Codice, nonché alle problematiche relative all'accesso ai documenti amministrativi ed alla necessità di contemperare le esigenze di trasparenza dell'azione amministrativa con quelle di tutela del diritto alla protezione dei dati personali.

Pertanto ci si rivolge ai dirigenti ed ai funzionari preposti alle unità di loro competenza perché nell'ambito delle attività di direzione, coordinamento e controllo degli uffici dei quali sono responsabili adottino tutte le misure utili a garantire il rispetto e la piena attuazione dei principi sanciti dal Codice, prevengano i rischi presenti nelle singole attività e adottino, conseguentemente, tutti gli atti, le soluzioni organizzative ed i comportamenti necessari.

4. Classificazione dei dati e tipologia dei relativi adempimenti

4.1 Dati personali

L'articolo 4, comma 1, lettera b) del Codice definisce dati personali "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

Alle pubbliche amministrazioni è consentito il trattamento dei dati personali quando risponda alla necessità di esercitare le proprie funzioni istituzio-

nali. Pertanto, salvo quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici (si vedano le disposizioni della parte II del Codice), le medesime non debbono chiedere il consenso dell'interessato ai sensi dell'articolo 18.

In particolare, il trattamento dei dati diversi da quelli sensibili e giudiziari è consentito anche in assenza di una specifica previsione normativa purché sia finalizzato allo svolgimento delle funzioni istituzionali dell'amministrazione, mentre la comunicazione di questi dati da una pubblica amministrazione ad un'altra o a privati oppure la loro diffusione è possibile solo quando vi sia una espressa previsione normativa, come indicato all'articolo 19.

Nel caso in cui le amministrazioni abbiano necessità di fornire tali informazioni ad un altra pubblica amministrazione, sempre ai fini dello svolgimento delle attività istituzionali, ma in assenza di idonea previsione normativa, possono però informarne preventivamente il Garante, ai sensi dell'art. 39 del Codice. In base a tale nuovo meccanismo, decorsi quarantacinque giorni dalla comunicazione al Garante, l'operazione di comunicazione dei dati può essere avviata, ferma restando la possibilità di una diversa determinazione dell'Autorità adottata anche successivamente al decorso del termine.

Deve essere effettuata una preventiva comunicazione al Garante, a norma dell'articolo 39, anche nel caso di trattamento di dati idonei a rivelare lo stato di salute previsto da un programma di ricerca biomedica o sanitaria, conformemente a quanto dispone l'art. 110 del Codice.

Sulle amministrazioni titolari del trattamento grava inoltre l'obbligo di notificare al Garante i trattamenti di dati personali che sono elencati nel comma 1 dell'articolo 37 del Codice. Tale adempimento deve essere effettuato prima dell'inizio del trattamento ed una sola volta, a prescindere delle operazioni che debbono essere effettuate (salvo, ovviamente, l'obbligo di notificare le eventuali modifiche del trattamento o la sua cessazione). In base agli articoli 37 e 38, la notificazione si intende validamente effettuata solo se inviata telematicamente utilizzando le modalità indicate dal Garante tramite il modello all'uopo predisposto e disponibile sul sito dell'Autorità (www.garanteprivacy.it). Al riguardo si segnala che, con provvedimento n. 1 del 31 marzo 2004, disponibile anch'esso sul sito dell'Autorità, sono stati individuati alcuni trattamenti di dati non suscettibili, in concreto, di recare pregiudizio agli interessati e quindi sottratti all'obbligo di notificazione di cui al citato articolo 37.

Si rammenta infine che sulla base della disciplina del Codice configura una "comunicazione" di dati personali il dare conoscenza di tali informazioni ad uno o più soggetti diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Non può considerarsi tale, invece, la comunicazione effettuata nei confronti dell'interessato, del rappresentante del titolare nel territorio dello Stato, del responsabile o dell'incaricato (art. 4, comma1, lett. l).

4.2 Regole generali per il trattamento dei dati

Le regole generali, comuni a tutti i trattamenti di dati, sono rinvenibili negli articoli da 11 a 17 del Codice.

4.2.1 Modalità del trattamento e requisiti dei dati

In particolare, l'articolo 11, nell'indicare le modalità del trattamento e i requisiti dei dati, individua anche i presupposti di liceità del trattamento. Secondo la disciplina introdotta dal Codice, il mancato rispetto dei presup-

posti sanciti da tale disposizione e delle altre norme rilevanti in materia trattamento di dati personali comporta l'inutilizzabilità dei dati (art. 11, comma 2).

4.2.2 Titolare, responsabile, incaricati

Per quanto riguarda i soggetti che effettuano il trattamento, l'articolo 28 chiarisce che il "titolare del trattamento", nel caso delle pubbliche amministrazioni, coincide con l'entità nel suo complesso ovvero con l'unità o l'organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, anziché con la persona fisica incardinata nell'organo o preposta all'ufficio.

Per le strutture amministrative complesse si suggerisce di avvalersi della facoltà accordata al titolare dall'art. 29 del Codice di designare uno o più "responsabili del trattamento", fra i soggetti che, per qualità professionali e personali, forniscano idonea garanzia del rispetto delle disposizioni vigenti in materia. Tale designazione deve essere accompagnata dalla specificazione analitica per iscritto dei compiti affidati e dalla vigilanza periodica sulla puntuale osservanza delle istruzioni impartite e sul generale rispetto delle norme in materia di protezione dei dati personali, come previsto dal comma 5 dell'articolo 29.

A chiusura del sistema è posta la previsione relativa agli "incaricati del trattamento", i soli che possono materialmente effettuare le operazioni di trattamento di dati personali. Gli incaricati operano sotto la diretta autorità del titolare o del responsabile, previa designazione espressa per iscritto, contenente la puntuale individuazione dell'ambito del trattamento loro consentito e l'indicazione delle istruzioni cui devono attenersi nello svolgimento del trattamento. Per semplificare tale adempimento, in considerazione della frequenza con cui il personale viene soggetto a rotazione e avvicendamento all'interno delle strutture amministrative, il Codice considera equivalente alla designazione nominativa degli incaricati, la preposizione del personale ad un'unità organizzativa (ad esempio, tramite un ordine di servizio) per la quale venga altresì individuato per iscritto l'ambito del trattamento consentito agli addetti che operano all'interno della medesima unità.

4.2.3 Informativa agli interessati

A tutela dell'esercizio del diritto alla protezione dei dati personali il Codice pone in capo ai titolari del trattamento l'obbligo, previsto dall'articolo 13, di fornire agli interessati un'adeguata informativa. L'interessato o la persona presso la quale sono raccolti i dati personali deve pertanto essere informato oralmente o per iscritto, fra l'altro, delle finalità e delle modalità del trattamento dei dati, della eventuale obbligatorietà del loro conferimento, delle conseguenze relative al rifiuto di fornire i dati, dei diritti esercitabili dal medesimo interessato, nonché dei dati identificativi del titolare del trattamento e del responsabile. Nel caso di designazione di più responsabili, il Codice introduce un'ulteriore semplificazione dando possibilità di riportare nell'informativa all'interessato gli estremi identificativi di un solo responsabile indicando contestualmente le modalità attraverso le quali è conoscibile l'elenco completo e aggiornato dei responsabili (ad esempio, attraverso l'indicazione del sito istituzionale dell'amministrazione in cui l'elenco è eventualmente pubblicato).

4.3 Dati sensibili

L'articolo 4, comma 1, lettera d) del Codice definisce dati sensibili "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

Il trattamento dei dati sensibili è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite. Qualora una disposizione di legge non specifichi i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere svolte su di essi, le amministrazioni sono tenute ad identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili, in relazione al perseguimento di finalità ritenute dalla legge di rilevante interesse pubblico, aggiornando ed integrando tale identificazione periodicamente (art. 20, commi 1, 2 e 4, del Codice). Al riguardo, la parte II del Codice individua alcune attività di rilevante interesse pubblico, tra le quali assumono rilievo per le pubbliche amministrazioni, a titolo esemplificativo, le attività finalizzate all'applicazione della disciplina sull'accesso ai documenti amministrativi (art. 59), o della normativa in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti o abilitazioni (art. 68), le attività socio-assistenziali (art. 73) e quelle volte all'instaurazione e alla gestione da parte di soggetti pubblici di rapporti di lavoro (art. 112).

Nel caso in cui invece le amministrazioni intendano porre in essere un trattamento di dati sensibili che non risulti previsto espressamente da una disposizione normativa di rango primario, esse possono richiedere al Garante se siano ravvisabili i presupposti di rilevante interesse pubblico che ne autorizzano il trattamento, secondo il meccanismo previsto dall'articolo 26, comma 2, del Codice. In tal caso, il trattamento è consentito soltanto se l'amministrazione interessata provveda altresì ad identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili con un atto di natura regolamentare (art. 20, comma 3, del Codice, al riguardo, v. più diffusamente infra la parte relativa ai "Regolamenti").

4.4 Dati giudiziari

L'articolo 4, comma 1, lettera e) del Codice definisce "dati giudiziari" i dati personali idonei a rivelare provvedimenti iscrivibili nel casellario giudiziale indicati dall'articolo 3, comma 1, lettere da a) ad o) e da r) ad u) del .decreto del Presidente della Repubblica del 14 novembre 2002, n. 313, o la qualità di imputato o di indagato ai sensi degli articolo 60 e 61 del codice di procedura penale.

È possibile per le pubbliche amministrazioni trattare tali informazioni quando ciò sia previsto da una norma di legge oppure da un provvedimento del Garante che specifichi espressamente le rilevanti finalità di interesse pubblico perseguite, i dati personali che possono essere utilizzati e le operazioni di trattamento eseguibili. Nel caso in cui la legge specifichi soltanto le finalità di rilevante interesse pubblico, valgono le prescrizioni relative al trattamento dei dati sensibili, di cui all'articolo 20, commi 2 e 4, del Codice per quanto riguarda la necessità di individuare e rendere pubblici attraverso un atto di natura regolamentare i tipi di dati utilizzabili e le operazioni eseguibili (art. 21).

4.5 Regolamenti

Gli articoli 20, comma 2, e 21, comma 2, del Codice prevedono che, quando una disposizione di legge abbia specificato le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere svolte su di essi, le amministrazioni dovranno adottare un apposito regolamento con il quale identificare e rendere pubblici, a cura dei soggetti che ne effettuano il trattamento, i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dall'articolo 22 del Codice. L'adozione di tali provvedimenti postula la previa ricognizione di tutte le attività poste in essere dal soggetto pubblico che comportano un trattamento di dati sensibili o giudiziari, nonché la valutazione della indispensabilità dei dati utilizzati e delle operazioni svolte nell'ambito di tali attività rispetto alle finalità di volta in volta perseguite. I dati trattati vanno indicati per categorie (ad esempio, dati sulla salute, vita sessuale, sull'origine razziale, sull'origine etnica, ecc.), tenendo conto che le tipologie di dati non individuate nel regolamento non potranno essere trattate.

In altri termini, tramite tali regolamenti dovrà risultare chiaro ai cittadini il collegamento tra le finalità di rilevante interesse pubblico perseguite dalle amministrazioni in relazione ai compiti ad esse attribuiti dall'ordinamento e le modalità con cui vengono effettivamente utilizzate le informazioni che li riguardano. Al fine di dare efficacia al sistema di garanzie delineato dal Codice per i dati sensibili e giudiziari è pertanto necessario che le amministrazioni provvedano a tale identificazione, ove mancante, tramite atti di natura regolamentare, entro il 31 dicembre 2005, previa acquisizione del parere di conformità del Garante ai sensi dell'articolo 154, comma 1, lettera g), del Codice (art. 3, decreto legge del 24 giugno 2004, n. 158 convertito con l. 27 luglio 2004, n. 188 che modifica l'art. 181, comma 1, lettera a) del Codice). L'identificazione dei tipi di dati e di operazioni è poi aggiornata e integrata periodicamente, come indicato dall'articolo 20 del Codice.

Per rendere più agevole e rapida l'adozione di tali atti, il Codice prevede che il parere del Garante possa essere formulato anche su schemi tipo. Nel caso in cui gli schemi regolamentari predisposti dalle amministrazioni corrispondano ai modelli su cui il Garante ha reso un parere conforme, non sarà quindi necessario sottoporli caso per caso allo specifico esame da parte dell'Autorità.

A tal fine, si esortano le amministrazioni ad avviare ogni iniziativa utile ad identificare settori di attività, comuni a più amministrazioni, per i quali si possa procedere ad un'elaborazione congiunta di schemi tipo da sottoporre all'attenzione del Garante, anche attraverso i progetti che questo Dipartimento avvierà in collaborazione con il Formez.

4.6 Criteri applicabili al trattamento dei dati sensibili e giudiziari

L'articolo 22 indica i criteri applicabili al trattamento dei dati sensibili e giudiziari. In primo luogo, le pubbliche amministrazioni devono prestare particolare attenzione alla prevenzione di possibili danni per l'interessato, conformando il trattamento di queste informazioni in modo da prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

In tale contesto assume uno specifico rilievo il principio di indispensabilità, in base al quale possono essere trattati soltanto i dati sensibili e giudiziari indispensabili allo svolgimento di funzioni istituzionali che non potrebbero

essere adempiute altrimenti (mediante il ricorso a dati anonimi o dati personali di diversa natura).

Analogamente, sui dati sensibili e giudiziari indispensabili, le amministrazioni possono effettuare unicamente le operazioni di trattamento strettamente necessarie al raggiungimento delle finalità consentite nei singoli casi.

Rispetto alla normativa previgente, è confermato infine il divieto di diffondere i dati idonei a rivelare lo stato di salute.

4.7 Sicurezza dei dati

Una particolare attenzione è posta dal Codice, negli articoli 31 e seguenti, alle tematiche della sicurezza dei dati e dei sistemi.

Il Codice distingue in proposito le misure di sicurezza da adottare in:

misure idonee e preventive volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31);

misure minime, indicate negli articoli 34 e 35 secondo le modalità applicative analiticamente specificate nell'Allegato B) al Codice e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici, ovvero da individuare, ai sensi dell'articolo 58, comma 3, in relazione ai trattamenti effettuati per finalità di difesa o coperti da segreto di Stato (art. 33).

La distinzione rileva ai fini sanzionatori perché, mentre l'inosservanza delle misure "minime" configura una condotta penalmente rilevante, ai sensi dell'art. 169 del Codice, l'inosservanza delle misure "idonee" rende il trattamento illecito e, nel caso in cui si cagioni un danno all'interessato, espone l'autore del danno ad eventuali azioni risarcitorie da parte del soggetto leso (art. 15 del Codice).

In particolare, l'omessa adozione delle misure minime di sicurezza è punita con l'arresto sino a due anni o con l'ammenda da 10 mila euro a 50 mila euro. In questo caso è però previsto il meccanismo del "ravvedimento operoso" applicabile a coloro i quali adempiano puntualmente alle prescrizioni impartite dal Garante una volta accertato il reato ed effettuino un pagamento in sede amministrativa di una somma pari al quarto del massimo dell'ammenda, ottenendo così l'estinzione del reato.

4.8 Documento programmatico sulla sicurezza

Fra le misure minime di sicurezza previste dal Codice rientra anche il Documento programmatico sulla sicurezza (Dps), obbligatorio per chi effettua un trattamento di dati sensibili e giudiziari con l'ausilio di strumenti elettronici. Tale documento deve contenere, in particolare, l'analisi dei rischi che incombono sui dati personali, l'individuazione degli accorgimenti da adottare per prevenire la loro eventuale distruzione, perdita accidentale o gli accessi abusivi e la pianificazione degli interventi formativi nei riguardi del personale. Il Dps deve essere adottato, dall'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento dell'amministrazione e predisposto (o aggiornato per le amministrazioni che erano già tenute a redigere o ad aggiornare il Dps in base alla previgente disciplina) al più tardi entro il 30 giugno 2005 (art. 6, decreto legge del 9 novembre 2004, n. 266 che modifica l'articolo 180 del Codice). Decorso il periodo transitorio connesso all'entrata in vigore del Codice, secondo quanto precisato dal Garante nel parere del 22 marzo 2004, e, quindi a partire dal 2006, il termine per aggiornare annualmente il Dps

rimarrà fissato alla scadenza del 31 marzo di ogni anno, come dispone la regola tecnica n. 19 dell'Allegato B) al Codice.

Le amministrazioni che per obiettive ragioni di natura tecnica non possono, in tutto o in parte, applicare entro il 30 giugno 2005 le misure minime introdotte dalla nuova disciplina con riferimento agli elaboratori elettronici e ai programmi utilizzati possono avvalersi di un termine più ampio per l'adeguamento (30 settembre 2005, secondo quanto dispone l'art. 6 del decreto legge citato), purché predispongano un documento, avente data certa, nel quale sono descritti tali impedimenti tecnici e lo conservino presso la propria struttura. Nell'attesa di adeguare la propria dotazione tecnologica, l'amministrazione è però tenuta ad adottare ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti, in modo da evitare i rischi, indicati dall'articolo 31 del Codice, di distruzione, perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta .

5. Accesso ai dati e accesso ai documenti

5.1 Accesso ai dati personali

È opportuno rammentare alcuni elementi di rilievo introdotti dal Codice in materia di accesso ai dati personali.

Com'è noto, il Codice riconosce all'interessato vari diritti nei confronti delle pubbliche amministrazioni che trattano i suoi dati personali, tra cui, in particolare, il diritto di accedere ai dati che lo riguardano, di ottenerne l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi (art. 7).

Per esercitare tali diritti l'interessato deve presentare una richiesta all'amministrazione titolare del trattamento (o al responsabile, qualora l'amministrazione si sia avvalsa di tale facoltà) senza particolari formalità (art. 9). La richiesta, se non fa riferimento ad un particolare trattamento o a specifici dati o categorie di dati personali, deve ritenersi riferita a tutti i dati personali che riguardano l'interessato comunque trattati dall'amministrazione (art. 10) e può riguardare anche informazioni di tipo valutativo, salvo per quanto attiene alla loro rettifica o integrazione (art. 8, comma 4).

L'amministrazione destinataria della richiesta è tenuta a fornire un riscontro compiuto ed analitico all'interessato nel termine di 15 giorni dal suo ricevimento, ovvero di 30 giorni, dandone comunicazione all'interessato, se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo (art. 146). Il riscontro può essere fornito anche oralmente, tuttavia, in presenza di una specifica istanza, l'amministrazione è tenuta a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica (art. 10).

Si esortano pertanto le amministrazioni a predisporre idonei meccanismi e procedure volti a dare piena attuazione alle disposizioni del Codice in materia di accesso ai dati, in modo da agevolare l'accesso da parte degli interessati alle informazioni che li riguardano, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad una accurata selezione dei dati relativi a singoli soggetti, e da semplificare le modalità e ridurre i tempi per il riscontro agli interessati anche nell'ambito degli uffici per le relazioni con il pubblico.

5.2 Accesso ai dati e accesso ai documenti amministrativi

Occorre sottolineare, infine, alcuni elementi che differenziano il diritto di accesso ai dati personali e gli altri diritti introdotti dalla disciplina sulla protezione dei dati personali dal diritto di accesso ai documenti amministrativi previsto dagli artt. 22 ss. della legge n. 241/1990 e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione. Si tratta, infatti, come ricordato più volte dal Garante, di due diversi ed autonomi diritti di accesso che differiscono in termini di oggetto e di presupposti del loro esercizio.

Il diritto di accesso ai dati personali e gli altri diritti sanciti dal Codice riguardano i dati personali (anziché ad atti e documenti) e possono essere esercitati dalle persone cui i dati si riferiscono senza particolari formalità e limitazioni, ad eccezione di taluni diritti che richiedono una specifica situazione (ad esempio, la rettifica può essere richiesta solo in relazione a dati inesatti e la cancellazione solo nei confronti di dati utilizzati in violazione di legge) e dei casi di esclusione tassativamente indicati dal Codice (art. 8). In particolare, ai fini dell'esercizio del diritto di accesso ai dati, l'interessato non è tenuto ad esplicitare le ragioni della sua richiesta di accesso, che può concernere soltanto le informazioni riferite alla propria persona e non può essere estesa ai dati relativi a terzi.

Il diritto di accesso ai documenti è, invece, garantito solo in riferimento a documenti della pubblica amministrazione e di determinati altri soggetti da parte di chiunque sia portatore di in un interesse personale e qualificato per la tutela di situazioni giuridicamente rilevanti, nonché da parte di amministrazioni, associazioni e comitati portatori di interessi pubblici o diffusi.

Per ciò che concerne le modalità di riscontro al richiedente, nel caso di esercizio del diritto di accesso ai dati, l'amministrazione è tenuta ad estrapolare dai propri archivi e documenti tutte le informazioni di carattere personale che riguardano l'interessato, riportate anche su supporto informatico, e a comunicarle a quest'ultimo in forma idonea a renderle facilmente comprensibili. A differenza dell'accesso ai documenti, l'amministrazione non pertanto è obbligata ad esibire o a consegnare copia all'interessato di atti o documenti contenenti le informazioni che lo riguardano o (eventualmente) anche dati relativi a terze persone, a meno che l'estrazione dei dati risulti particolarmente difficoltosa e le informazioni relative ai richiedenti e ai terzi siano intrecciate al tal punto da risultare incomprensibili se scomposte o private di alcuni elementi (art. 10, commi 4 e 5).

5.3 Tutela giurisdizionale

Per quanto riguarda la tutela in sede giudiziaria del diritto di accesso ai dati personali e degli altri diritti sanciti dal Codice, la nuova disciplina prevede che "tutte le controversie riguardanti, comunque, l'applicazione delle disposizioni del Codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione" competono all'autorità giudiziaria ordinaria (art. 152).

In relazione alla tutela in sede giudiziaria del diritto di accesso agli atti amministrativi, la legge 241/90 ha disposto, invece, all'articolo 25, comma 5, che contro le determinazioni amministrative concernenti il diritto di accesso e nei casi di rifiuto, espresso o tacito, o di differimento dell'accesso è dato ricorso, nel termine di trenta giorni, al tribunale amministrativo regionale.

Al riguardo è emerso un indirizzo nella giurisprudenza amministrativa,

in via generale condiviso anche dalla Corte di Cassazione (si veda Cassazione Civile, sez. un., 28 maggio 1998, n. 5292), in base al quale si deve riconoscere l'esistenza di una giurisdizione esclusiva amministrativa per quanto riguarda le valutazioni di legittimità degli atti amministrativi che decidono sulla richiesta di accesso, a prescindere dalla consistenza della posizione giuridica fatta valere e ciò anche nei casi in cui l'amministrazione, nel perseguire i propri interessi abbia agito quale soggetto di diritto privato (si veda Consiglio di Stato, sez. IV, 3 agosto 1995, n. 589).

6. Tematiche di interesse in materia di gestione del personale

Com'è noto poiché la pubblica amministrazione si caratterizza per essere una organizzazione produttiva basata sul lavoro, la gestione delle risorse umane, fra le attività da essa compiute, riveste un ruolo essenziale che si interseca con la potestà organizzativa attribuita alle amministrazioni. In tale ambito, occorre porre una particolare attenzione ai principi posti dal Codice.

I profili relativi alla tutela della riservatezza sono ben noti alle pubbliche amministrazioni ed in particolare agli uffici cui compete la gestione del personale. Questi ultimi detengono ed acquisiscono un numero elevato di informazioni relative ai dipendenti dell'amministrazione. Da ciò deriva la necessità di una preliminare ricognizione delle proprie attività alla luce delle norme vigenti che deve essere costantemente aggiornata. Al riguardo, vale la pena di ricordare alcuni dei problemi emersi in questi ultimi anni ed evidenziati in diverse occasioni dal Garante.

Dal momento che le pubbliche amministrazioni raccolgono, sempre più spesso attraverso tecnologie informatiche, un numero rilevante di dati, sia in relazione ai compiti di istituto, sia in relazione alla gestione del personale dipendente (per tutte le fasi relative al rapporto di lavoro, dall'accesso all'estinzione), occorre rammentare in primo luogo che la configurazione e la gestione di queste banche dati deve essere realizzata nel rispetto del principio di necessità sancito dall'art. 3 del Codice (v. più diffusamente *supra* la parte relativa ai "Principi e gli obblighi").

In via generale, nel titolo VIII della Parte II del Codice, intitolato "Lavoro e previdenza sociale", l'art. 112, considera di rilevante interesse pubblico una serie di trattamenti di dati sensibili e giudiziari attinenti ai lavoratori e finalizzati all'instaurazione e alla gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato. Tra tali trattamenti sono compresi, in particolare, quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, o la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio (art. 112, comma 2, lett. c)), di adempiere agli obblighi connessi alla definizione dello stato giuridico ed economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili (lett. d)), di adempiere a specifici obblighi o compiti previsti in materia di igiene e sicurezza del lavoro (lett. e)), di svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile dei dipendenti (lett. g)).

In particolare, in tema di pubblicazione di graduatorie delle procedure di selezione del personale, si sottolinea la necessità di verificare che le indicazioni contenute nelle graduatorie non comportino la divulgazione di dati idonei a rivelare lo stato di salute e di utilizzare, piuttosto, diciture generiche o codici numerici, in modo da non incorrere nel divieto di diffondere i dati attinenti alla salute sancito dall'articolo 22, comma 8, del Codice.

Analoghe cautele devono essere adottate nella redazione di graduatorie relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti o abilitazioni. L'inserimento in tali atti, destinati alla pubblicazione, di informazioni riguardanti lo stato di salute degli iscritti (ad esempio relative allo stato di disabilità di un componente il nucleo familiare di uno dei beneficiari) contrasta, infatti, con la disciplina sulla protezione dei dati personali che vieta ai soggetti pubblici, autorizzati a concedere specifici benefici connessi all'invalidità civile, di diffondere i dati relativi allo stato di salute dei soggetti beneficiari (art. 68 del Codice). L'adozione di tali accorgimenti, peraltro, non deve pregiudicare la possibilità per le persone a ciò legittimate di accedere ad eventuali altre informazioni relative agli iscritti in graduatoria, anche sensibili, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa.

Un altro aspetto che, oltre ad impegnare particolarmente le amministrazioni, ha suscitato alcuni interventi giurisprudenziali, riguarda le richieste di accesso agli elaborati concorsuali. Sul punto si rimanda, più in generale, alla parte successiva nella quale si richiamano gli attuali orientamenti giurisprudenziali in tema di diritto di accesso agli atti detenuti dalle pubbliche amministrazioni.

Sul versante della gestione dei dati personali dei dipendenti molti sono gli aspetti di rilievo. Per quanto concerne i dati contenuti nei fascicoli personali, il Garante ha avuto modo in alcune occasioni di sottolineare che le certificazioni mediche rese a giustificazione di assenze per malattia devono contenere soltanto la prognosi e non la diagnosi relativa alla patologia sofferta dal lavoratore. L'amministrazione, che non è legittimata a trattare questi dati, deve quindi adoperarsi per oscurare le diagnosi eventualmente riportate su certificati medici già detenuti ed adottare opportuni accorgimenti anche verso lavoratori e medici affinché vengano prodotti soltanto certificati dai quali risulti la sussistenza e la durata dello stato di incapacità del lavoratore, senza alcuna indicazione diagnostica.

Inoltre l'articolo 113 del Codice richiama il disposto dell'art. 8 della legge 20 maggio 1970 n. 300, il quale stabilisce che "è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".

Altro tema di grande attualità è quello della vigilanza sulle comunicazioni elettroniche e sull'utilizzo di Internet sul posto di lavoro rispetto al quale si richiama il documento di lavoro delle autorità europee di protezione dei dati riunite nel Gruppo dei garanti europei, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, adottato il 29 maggio 2002, nonché la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'articolo 8 della Convenzione europea dei diritti dell'uomo.

Riguardo al tema del controllo dei lavoratori, occorre rammentare il divie-

to di controllo a distanza dell'attività lavorativa e le altre garanzie previste in materia di lavoro dall'art. 4 della legge n. 300/1970 richiamato dal Codice. Tali garanzie devono essere rispettate, in particolare, nel caso di installazione nei locali dell'amministrazione di impianti di videosorveglianza per motivi di sicurezza o per esigenze organizzative e dei processi produttivi, tenendo presente l'obbligo di informare, anche con formule sintetiche, i dipendenti ed i visitatori che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione (art. 13 del Codice).

Sulla specifica questione si ricordano gli indirizzi formulati dal Gruppo dei garanti europei, nel parere del 11 febbraio 2004 n. 4 sul trattamento dei dati personali tramite videosorveglianza e il provvedimento del 29 aprile 2004 del Garante con cui sono state indicate le condizioni di liceità della installazione di sistemi di videosorveglianza. In particolare, l'Autorità ha ribadito che i soggetti pubblici possono attivare sistemi di videosorveglianza solo in quanto siano strumentali allo svolgimento delle loro funzioni istituzionali e ha affermato che tale installazione è lecita solo se è proporzionata agli scopi che si intendono perseguire (art. 11, comma 1, lett. d) del Codice), essendo altre misure realmente insufficienti e inattuabili (ad esempio, sistemi d'allarme o misure di protezione agli ingressi).

Al riguardo, occorre altresì valutare se sia realmente necessario raccogliere immagini dettagliate, definendo di conseguenza la dislocazione e la tipologia delle apparecchiature da installare (fisse o mobili), e limitare rigorosamente la creazione di banche dati quando, per le finalità perseguite, è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini senza registrazione (ad esempio, per il controllo del flusso ad uno sportello). In armonia con il principio di necessità sancito dal Codice (art. 3), attraverso tali sistemi è poi possibile riprendere persone identificabili soltanto se, per raggiungere gli scopi prefissati, non possono essere utilizzati dati anonimi. I cittadini che transitano nelle aree sorvegliate devono inoltre essere informati della rilevazione dei dati (art. 13 del Codice). In proposito, si rammenta che con il provvedimento citato il Garante ha messo a disposizione un modello semplificato di informativa, la quale deve essere chiaramente visibile ed indicare chi effettua la rilevazione delle immagini e per quali scopi.

Infine, sulla base dell'articolo 111 del Codice, è prevista l'adozione, attraverso un procedimento che coinvolgerà le categorie interessate, di un codice di deontologia e buona condotta relativo al trattamento dei dati personali in materia di gestione del rapporto di lavoro. Le disposizioni del codice deontologico una volta pubblicate nella Gazzetta Ufficiale a cura del Garante, previa verifica della loro conformità alle leggi e ai regolamenti, acquisiranno efficacia giuridica vincolante, poiché il loro rispetto costituirà "condizione essenziale per la liceità e correttezza del trattamento dei dati personali" effettuato anche da parte dei soggetti pubblici nell'ambito della gestione del rapporto di lavoro (art. 12 del Codice).

7. L'accesso agli atti amministrativi e la tutela della riservatezza: il contemperamento degli interessi e gli orientamenti giurisprudenziali

Come noto il problema di fondo relativo all'applicabilità della normativa sulla tutela della riservatezza alle pubbliche amministrazioni è basato sulla possibile contrapposizione fra il principio della trasparenza dell'azione ammi-

nistrativa, e quindi della pubblicità e conoscibilità degli atti delle pubbliche amministrazioni, sancito dalla l. n. 241/90, ed il principio della tutela della riservatezza. Entrambi i principi derivano dalla Carta costituzionale essendo rispettivamente espressione dell'imparzialità e del buon andamento e della tutela dei diritti inviolabili della persona. Tali principi assumono una rilevanza assoluta per le pubbliche amministrazioni, poiché le norme che ne hanno dato attuazione concreta hanno permeato profondamente e diretto incisivamente l'attività amministrativa.

Nell'impianto della l. n. 241/90 la tutela della riservatezza costituisce un limite al diritto di accesso (si veda l'art. 24, comma 2, lett. d)), quale eccezione alla regola della accessibilità agli atti amministrativi. Tale intendimento è stato successivamente riconfermato dal decreto del Presidente della Repubblica del 27 giugno 1992, n. 352 recante il regolamento sulla disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, nel quale si prevede che l'interessato possa avere visione degli atti relativi al procedimento amministrativo quando ciò sia necessario per curare e difendere i propri interessi giuridici.

Negli anni successivi il dibattito si è dipanato intorno al tema della comparazione dei valori contrapposti, articolandosi essenzialmente sulla contrapposizione fra tutela del diritto alla riservatezza da un lato e tutela del diritto di accesso ai documenti per la difesa di un interesse giuridicamente rilevante.

La possibilità che i regolamenti di delegificazione, ai quali la legge 241/90 aveva demandato la disciplina dei limiti oggettivi all'esercizio del diritto di accesso, fornissero elementi efficacemente dirimenti, non si è verificata, poiché questi si sono limitati, essenzialmente, ad indicare i documenti sottratti all'accesso.

Le amministrazioni, pertanto, per lungo tempo si sono trovate nella situazione di dover valutare caso per caso quale fosse l'esigenza prevalente, di fatto svolgendo una funzione di composizione degli interessi.

Alcuni punti di riferimento sono stati elaborati, soprattutto, dalla giurisprudenza del Consiglio di Stato, il quale ha sempre ritenuto che dovesse sempre soccorrere la disciplina legislativa (si veda ad esempio Consiglio di Stato, sez. V, 5 maggio 1999, n. 518).

L'Adunanza plenaria del Consiglio di Stato, con la decisione n. 5 del 4 febbraio 1997, in linea con lo spirito della disciplina sulla trasparenza amministrativa, ha affermato che tale disciplina accorda prevalenza al principio di pubblicità rispetto a quello di tutela della riservatezza, consentendo l'accesso anche nei confronti di documenti contenenti dati riservati, sempre che l'istanza ostensiva sia sorretta dalla necessità di difendere i propri interessi giuridici e con il limite modale della sola visione, non essendo percorribile la modalità più penetrante e potenzialmente lesiva dell'estrazione di copia.

Con riferimento, invece, all'accesso a documenti amministrativi contenenti dati sensibili, il decreto legislativo 11 maggio 1999, n. 135, integrando la normativa sul trattamento di questi dati da parte dei soggetti pubblici (art. 16), aveva già colmato il vuoto normativo determinato dall'assenza di una espressa previsione legislativa relativa all'accesso a documenti contenenti informazioni sensibili .

Rispetto alla normativa previgente, il Codice conferma la compatibilità delle disposizioni sull'accesso ai documenti amministrativi con quelle in materia protezione dei dati personali, stabilendo che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi conte-

nenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla legge 241/1990 e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso (art. 59). La nuova disciplina, inoltre, riproduce la previsione già contenuta nell'art. 16 del Decreto legislativo. n. 135/1999, in materia di trattamenti di dati sensibili da parte di soggetti pubblici, considerando le attività finalizzate all'applicazione della disciplina in materia di accesso ai documenti amministrativi di rilevante interesse pubblico.

Per ciò che concerne i limiti al diritto di accesso, nel caso in cui i documenti amministrativi oggetto della richiesta di accesso contengono dati attinenti la salute e la vita sessuale, il Codice, risolvendo alcuni dubbi interpretativi sorti sulla base del citato art. 16 del Decreto legislativo. n. 135/1999 ed in linea con l'orientamento interpretativo espresso al riguardo dalla giurisprudenza amministrativa (Consiglio di Stato, sez. VI, n. 1882/2001), dispone che il trattamento dei dati sensibili finalizzato a permettere l'accesso è consentito soltanto se la situazione giuridica che si intende tutelare con la richiesta di accesso è "*di rango almeno pari ai diritti dell'interessato*", ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile (art. 60).

In proposito il Consiglio di Stato ha sostenuto che tale valutazione deve essere fatta in concreto "in modo da evitare il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica dei diritti in contesa" (Consiglio di Stato, Sez. VI, 30 marzo 2001, n. 1882 e 9 maggio 2002, n. 2542; cfr. anche Consiglio di Stato, Sez. V, 31 dicembre 2003, n. 9276).

Con il provvedimento del 9 luglio 2003, il Garante ha affrontato la questione, riferendosi in particolare alle richieste di accesso a cartelle cliniche, ma fornendo indicazioni utili anche per altri tipi di documenti detenuti in ambito pubblico, la cui ostensibilità a persone diverse dall'interessato impone comunque una valutazione sul rango dei diversi diritti coinvolti da parte dell'amministrazione destinataria della richiesta di accesso.

In tale provvedimento, l'Autorità ha precisato, in particolare, che occorre avere presente, quale elemento di raffronto per il bilanciamento degli interessi, non già il diritto alla tutela giurisdizionale, che pure è costituzionalmente garantito, bensì il diritto soggettivo sottostante, che si intende far valere sulla base del materiale documentale di cui si vorrebbe avere conoscenza. La comunicazione di dati che rientrano nella sfera di riservatezza dell'interessato può ritenersi giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti fondamentali ed inviolabili.

Per ciò che riguarda invece l'accesso agli elaborati concorsuali, si rammenta che la giurisprudenza amministrativa propende per la tesi favorevole all'accesso. Ciò in considerazione del fatto che, essendo gli elaborati concorsuali, per loro natura destinati ad una valutazione e ad una comparazione, la riservatezza delle prove non può essere ritenuta prevalente rispetto all'esigenza di difesa di interessi giuridici. Pertanto il diritto all'accesso può essere fatto valere anche prima che si verifichi una lesione concreta e si esplica fino al diritto ad avere copia degli elaborati e dei titoli degli altri candidati (si vedano Consiglio di Stato, sez. IV, 13 gennaio 1995, n. 5; Consiglio di Stato, sez. VI, 13 settembre 1996, n. 1221). Più recentemente la giurisprudenza amministrativa ha affermato un principio di maggiore cautela, cioè quello della per-

tinenza, in base al quale l'accesso agli atti di una procedura concorsuale deve essere consentito, previa garanzia dell'anonimato degli altri concorrenti, in relazione alle stesse prove sostenute dal richiedente (si veda TAR Toscana, sez. I, 9 marzo 1999, n. 146).

Le amministrazioni avvieranno tutte le iniziative di informazione e formazione dirette ad accrescere la conoscenza del Codice e della presente direttiva al fine di favorire, in particolare, l'attuazione delle regole per il trattamento dei dati personali, sensibili e giudiziari.

I Ministeri provvederanno a sollecitare le amministrazioni da esse vigilate perché predispongano, nei termini previsti, gli atti regolamentari di cui agli articoli 20, comma 2, e 21, comma 2, del Codice.

La presente direttiva è inviata all'Ispettorato per la funzione pubblica al quale è demandata dall'ordinamento l'attività di vigilanza e verifica dell'attuazione e corretta applicazione delle riforme amministrative, con particolare riferimento alle innovazioni più significative in tema di rapporti tra cittadini e amministrazioni pubbliche, secondo quanto previsto dal decreto sull'organizzazione interna del Dipartimento della funzione pubblica in corso di pubblicazione.

Il Ministro per la Funzione Pubblica
on. Mario Baccini

REGOLAMENTI CONCERNENTI I TRATTAMENTI ESEGUIBILI IN RELAZIONE AI DATI SENSIBILI E GIUDIZIARI

Il decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, definisce all'articolo 4, comma 1, lettera d) dati sensibili come "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale". Definisce, inoltre, alla lettera e) i dati giudiziari quali dati personali idonei a rivelare provvedimenti iscrivibili nel Casellario giudiziale indicati dall'articolo 3, comma 1, lettere da a) ad o) e da r) ad u) del DPR 14 novembre 2002, n. 313, o la qualità di imputato o di indagato ai sensi degli articolo 60 e 61 del codice di procedura civile.

Gli articoli 20 e 21 affermano che il trattamento dei dati sensibili e giudiziari da parte dei soggetti pubblici è consentito solo se autorizzato da una espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e le operazioni eseguibili quando l'ordinamento riconosca che l'acquisizione ed il trattamento dei dati avvengono in relazione ad una rilevante finalità di interesse pubblico.

Qualora una disposizione di legge riconosca le finalità di rilevante interesse pubblico ma non i tipi di dati sensibili e giudiziari che sia consentito acquisire e le operazioni eseguibili, le singole amministrazioni dovranno predisporre un atto di natura regolamentare nel quale sono individuate le finalità perseguite, in relazione alle quali sia necessario acquisire e trattare i dati sensibili e giudiziari, specificando i tipi di dati e le operazioni eseguibili.

Presupposto necessario alla redazione dei regolamenti è una ricognizione delle attività materiali che il soggetto pubblico persegue in relazione alle finalità attribuite dall'ordinamento. Dovranno, pertanto, essere individua-

te le macrotipologie di dati ed una descrizione della loro utilizzazione riferite alla normativa che la sorregge. La pubblicità che deve essere data al trattamento che viene operato ed al tipo di informazioni che le amministrazioni detengono deve porre il cittadino nelle condizioni di conoscere per quali finalità e con quali modalità questi trattamenti sono effettuati e questi dati sono detenuti.

L'Autorità garante per la protezione dei dati personali, già a sistema normativo previgente, aveva fornito alcune indicazioni per la redazione di tali regolamenti con un'apposita scheda tipo. Sulla base delle indicazioni contenute in quella scheda l'Ufficio per il personale delle pubbliche amministrazioni ha predisposto una prima scheda a contenuto generale per quanto concerne la gestione del rapporto di lavoro dei dipendenti delle pubbliche amministrazioni. Tale scheda costituisce una prima base di partenza per effettuare la ricognizione dei trattamenti in vista dell'adozione dei regolamenti ed è evidentemente suscettibile di ulteriori approfondimenti e delle integrazioni che saranno necessarie anche in relazione alle diversità degli ordinamenti delle pubbliche amministrazioni.

Nella scheda sono poste in evidenza le rilevanti finalità di interesse pubblico individuate dal legislatore, le disposizioni di legge che attribuiscono le singole funzioni alle amministrazioni, i tipi di dati (personali, sensibili e giudiziari) ed il relativo trattamento. Sono inoltre evidenziati i casi in cui i dati sono trasmessi ad altra amministrazione, sempre per fini istituzionali, per espressa disposizione normativa.

Termine per l'adozione dei regolamenti in questione è il 31 dicembre 2005, secondo quanto disposto dall'articolo 3 del decreto legge 24 giugno 2004, n. 158, che ha modificato la lettera a) del comma 1 dell'articolo 181 del decreto legislativo n. 196 del 2003.

Scheda tipo per la ricognizione dei dati sensibili e giudiziari

ATTIVITÀ RECLUTAMENTO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Acquisizione domande	Art. 112, comma 1 e comma 2, lett. c) Dlgs 196/03	Art. 35, comma 1, lett. a), Dlgs 165/01; art. 26 (dirigenza SSN) art. 28 (dirigenti), art 29 (dirigenti scolastici) Dlgs 165/01	Personali, sensibili e giudiziari	Raccolta
Espletamento prove	Art. 112, comma 1 e comma 2, lett. c) Dlgs 196/03	Art. 35, comma 1, lett. a), Dlgs 165/01; art. 26 (dirigenza SSN) art. 28 (dirigenti), art 29 (dirigenti scolastici), Dlgs 165/01 L. 104/92 art. 20	Personali e sensibili	Raccolta, raffronto
Formazione graduatoria	Art. 112, comma 1 e comma 2, lett. c) Dlgs 196/03	Art. 35, comma 1, lett. a), Dlgs 165/01; art. 26 (dirigenza SSN) art. 28 (dirigenti), art 29 (dirigenti scolastici), Dlgs 165/01	Personali, sensibili e giudiziari	Raccolta, raffronto
Selezione	Art. 112, comma 1, comma 2, lettere a) e c) Dlgs 196/03	Art. 35, comma 1, lett. b) e art. 39, Dlgs 165/01 (categorie protette)	Personali, sensibili e giudiziari	Raccolta, raffronto
ATTIVITÀ COSTITUZIONE RAPPORTO DI LAVORO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Stipula contratto individuale di lavoro	Art. 112, comma 1 Dlgs 196/03	Art. 2, comma 2, 7, comma 6, 36, comma 1, Dlgs 165/01 CCNL comparto	Personali e sensibili	raccolta

segue

ATTIVITÀ RAPPORTO DI LAVORO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Inquadramento	Art. 112, comma 2, lett. d), Dlgs 196/03	Art. 52 Dlgs 165/01 – CCNL di Comparto	Personali	
Attribuzione trattamento economico	Art. 112, comma 2, lett. d), Dlgs 196/03	Artt. 2, comma 3, 24 e 45 Dlgs 165/01 – CCNL di comparto Dlgs 151/2001	Personali e sensibili	
Cessione del quinto	Art. 68, comma 1, Dlgs 196/03	DPR 3/1957, ART. 33	Personali sensibili	
Obblighi contributivi Invalidità, vecchiaia, superstiti	Art. 112, comma 2, lett. f) Dlgs 196/03	L. 335/95, DPR 1092/73, Dlgs 503/92 Dlgs 151/2001	Personali e sensibili	Raccolta trasmissione Inpdap
Obblighi assicurativi	Art. 112, comma 2, lett. f) Dlgs 196/03	DPR 1124/65 artt. 1. 4 e 9	Personali e sensibili	Raccolta trasmissione all'Inail
Obblighi fiscali	Art. 112, comma 2,lett. d) Dlgs 196/03	Art. 1 DPR 600/1973	Personali e sensibili	Trasmissione dati al MEF
Pari opportunità	Art. 112, comma 2, lett. b), Dlgs 196/03	Art. 7, comma 1 e 57 Dlgs 165/01 – CCNL di comparto	Personali e sensibili	
Formazione	Art. 112, comma 1, Dlgs 196/03	Art. 7, comma 4, 7-bis Dlgs 165/01	Personali e sensibili	
Valutazione	Art. 112, comma 1, DLgs 196/03	Artt. 20 e 21 Dlgs 165/01	Personali e sensibili	
Assenze per malattie	Art. 112, comma 1, DLgs 196/03	Art. 2, comma 2, Dlgs 165/01 – CCNL di Comparto	Personali e sensibili	
Mutamento mansioni per inidoneità psicofisica	Art. 112, comma 1, DLgs 196/03	CCNL di comparto	Personali e sensibili	
Permessi per motivi familiari e congedi parentali	Art. 112, comma 1, DLgs 196/03	Art. 23 Dlgs 151/2001	Personali e sensibili	
Congedo per maternità	Art. 112, comma 1, DLgs 196/03	L. 1204/1971, Dlgs 151/2001 – CCNL di Comparto	Personali e sensibili	Raccolta
Diritto allo studio	Art. 112, comma 1, DLgs 196/03	L. 300/70 art.10, L. 53/2000 art. 5	Personali e sensibili	

segue

ATTIVITÀ RAPPORTO DI LAVORO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Aspettative: sindacali motivi personali o famiglia assumere altro rapporto cariche pubbliche elettive dottorato di ricerca coniuge all'estero cooperazione paesi in via di sviluppo; assunzione impiego presso O.I. e stati esteri		Dlgs 165/01, art. 42, L.300/70 CCNL di comparto Art. 68 Dlgs 165/01 Art. 2 L. 476/1984 L. 26/1980 L.114/62 Art. 23 bis Dlgs 165/01		
Scambio di funzionari appartenenti a paesi diversi e temporaneo servizio all'estero		Art. 32 Dlgs 165/01		
Infortuni sul lavoro	Art. 112, comma 2, lett. f), Dlgs 196/03	DPR 1124/65, art. 9	Personali e sensibili	Raccolta. Comunicazione entro 48 ore dall'evento all'Inail e PS, artt. 53 e 54 DPR 1124/65
Malattie dovute a causa di servizio	Art. 112, comma 2, lett. d), Dlgs 196/03	Dlgs 165/01 art. 51, comma 2 – l. 300/70 – CCNL di comparto	Personali e sensibili Personali e sensibili	
Igiene e sicurezza del lavoro	Art. 112, comma 2, lett. i), DLgs 196/03	Dlgs 626/94, Dlgs 151/2001		
Esercizio diritti sindacali	Art. 112, comma 2, lett. e), Dlgs 196/03	Art. 9 e 50 Dlgs 165/01 – CCNL di comparto –Legge 300/70	Personali e sensibili	
Procedimenti disciplinari	Art. 112, comma 2, lett. c), Dlgs 196/03	Art. 2, comma 2, 55 Dlgs 165/01 – CCNL di Comparto	Personali, sensibili e giudiziari	

segue

ATTIVITÀ RAPPORTO DI LAVORO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Incompatibilità	Art. 112, comma 2, lett. l) e m), Dlgs 196/03	Art. 53 Dlgs 165/01	Personali e sensibili	
Trasferimenti	Art. 112, comma 2, lett. c), Dlgs 196/03	Art. 2, comma 2, Dlgs 165/01 – CCNL di Comparto		
ATTIVITÀ MOBILITÀ	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Passaggio diretto di personale tra amministrazioni diverse	Art.112, comma 1, d.lgs. n.196/2003	Art. 30 Dlgs 165/01	Personali e sensibili	Raccolta e raffronto
Passaggio per trasferimento attività	Art.112, comma 1, d.lgs. n.196/2003	Art. 31 Dlgs 165/01	Personali e sensibili	Raccolta e raffronto
Eccedenze di personale e mobilità collettiva	Art.112, comma 1, d.lgs. n.196/2003	Art. 33 Dlgs 165/01	Personali e sensibili	Raccolta e raffronto
ATTIVITÀ ESTINZIONE DEL RAPPORTO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Dimissioni con e senza preavviso	Art. 112, comma 1, lett. c), Dlgs 196/03	Art. 2, comma 2, Dlgs 165/01-CCNL comparto	Personali	
Cessazione dall'impiego per raggiunti limiti di età	Art. 112, comma 1, lett. c), Dlgs 196/03		Personali	
Recesso dell'amministrazione	Art. 112, comma 1, lett. c), Dlgs 196/03	Dlgs 165/01 art. 2, comma 2 Art. 2119 c.c. CCNL di comparto	Personali	
ATTIVITÀ TRATTAMENTO FINE LAVORO	FINALITÀ DI RILEVANTE INTERESSE PUBBLICO	FONTE LEGISLATIVA LEGITTIMANTE	TIPI DI DATI	TIPO DI TRATTAMENTO
Buonuscita	Art. 112, comma 2, lett. f), Dlgs 196/03	DPR 1032/1973	Personali e sensibili	Raccolta trasmissione all'INPDAP
Trattamento di fine rapporto	Art. 112, comma 2, lett. f), Dlgs 196/03	L. 335/1995, art. 2	Personali e sensibili	Raccolta trasmissione all'INPDAP

LE RELAZIONI AL PARLAMENTO 2003 E 2004 DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI SUL RAPPORTO DI LAVORO IN AMBITO PUBBLICO

Relazione 2003 - Rapporto di lavoro

Comunicazione o diffusione di dati sulla salute dei dipendenti

L'Autorità si è pronunciata più volte sul tema della protezione dei dati personali nel settore del lavoro e della previdenza sociale, oggetto ora della specifica disciplina dettata dal Titolo VIII del Codice. Nel settore del pubblico impiego sono stati anzitutto esaminati alcuni casi in cui, nelle comunicazioni concernenti l'adozione di provvedimenti di gestione interna del personale (trasferimenti o avvicendamenti) sono riportati dati di carattere sensibile riguardanti, in particolare, la salute di dipendenti. Il trattamento di queste informazioni per perseguire una rilevante finalità d'interesse pubblico di gestione di rapporti di lavoro può in generale ritenersi lecito. Occorre, tuttavia, che sia rispettato anche il principio di necessità, in virtù del quale possono essere oggetto di trattamento soltanto i dati indispensabili al raggiungimento di tale finalità. Non è stata ad esempio ritenuta rispondente al principio di necessità l'indicazione, in questo tipo di comunicazione, del luogo del ricovero di un dipendente e della gravità dei motivi di salute su cui era fondata la sua sostituzione, tenuto oltretutto conto dell'invio della comunicazione anche alle rappresentanze sindacali (Nota 4 settembre 2003).

Trattamento di dati del personale delle forze armate e di polizia

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

consentire l'elaborazione di indicazioni e soluzioni a tutela della riservatezza e degli altri diritti degli interessati.

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

– la richiesta di documentare la diagnosi, oltre alla prognosi, indirizzata ai dipendenti che si assentano dal servizio per motivi di salute, e la successiva conservazione della relativa documentazione nel fascicolo personale;
– il trattamento dei dati sulla salute connesso agli accertamenti dell'idoneità psico-fisica al servizio svolti nei confronti del personale, sia al momento dell'assunzione, sia in costanza del rapporto di lavoro;
– il trattamento dei dati sensibili contenuti in documenti quali il fascicolo personale, il foglio matricolare ed altri atti, con particolare riferimento al principio di necessità dei dati stessi e al periodo della loro conservazione. L'iniziativa ha consentito anche di sollecitare la cessazione di talune prassi adottate da strutture periferiche delle amministrazioni, già portate all'attenzione dell'Autorità.

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

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

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

Questionari di valutazione

In un altro ricorso, il Garante si è invece pronunciato sulla liceità della gestione di questionari di valutazione dell'attività svolta da dipendenti dell'amministrazione. In particolare, sono stati reputati conformi alla normativa sulla protezione dei dati la raccolta e l'esame di schede anonime di valutazione, quando il trattamento coinvolga soltanto uffici interni all'amministrazione interessata.

Si devono peraltro adottare tutte le necessarie misure di sicurezza, anche diverse da quelle minime, al fine di assicurare che i dati contenuti nei questionari siano trattati dal personale specificatamente individuato, per le sole finalità conformi a quelle che rendono lecito il trattamento e con modalità operative rispettose dei principi di pertinenza e di non eccedenza (*Provv*. 22 settembre 2003).

In relazione alla gestione della documentazione matricolare del personale

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

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

Per quanto riguarda la normativa sul diritto al lavoro dei disabili, è pervenuta una segnalazione con la quale si lamentava che la graduatoria del collocamento obbligatorio, contenente i nominativi di circa tredicimila disabili, era stata pubblicata sul sito web del servizio per le politiche del lavoro di una provincia. L'accertamento preliminare ha rilevato che l'elenco era effettivamente accessibile da chiunque attraverso la pagina di apertura di tale sito. La questione risultava rilevante, visto l'ingente numero di soggetti interessati dalla diffusione indiscriminata di dati idonei a rivelare il loro stato di salute.

Il Garante ha pertanto curato ulteriori approfondimenti ai fini del blocco del trattamento, considerando che le disposizioni di settore (art. 8 legge n. 68/1999) non definiscono le modalità per garantire la pubblicità degli elenchi e delle graduatorie degli aventi diritto al collocamento obbligatorio. Anche a tale proposito occorre comunque sottolineare che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge, dai regolamenti o dalla normativa comunitaria (art. 68, comma 3, decreto legislativo n. 196/2003).

Comunicazione all'Inail di dati sulla salute dei pazienti

L'Autorità ha altresì verificato la liceità delle segnalazioni trasmesse da medici all'Inail circa le malattie riscontrate nei pazienti, collegabili allo svolgimento di attività lavorative. Sul punto si è precisato che, secondo il quadro normativo vigente (decreto del Presidente della Repubblica n. 1124/1965; decreto ministeriale del 18 aprile 1973 e decreto legislativo n. 38/2000), il medico può trasmettere all'istituto assicuratore e ad altri organismi preposti le segnalazioni di malattie professionali che potrebbero essere state causate da un'attività lavorativa potenzialmente nociva, indicandone l'anamnesi lavorativa, i rischi e le sostanze cui il lavoratore sia (o sia stato) esposto. Questa comunicazione deve essere però effettuata nel rispetto delle specifiche disposizioni in tema di assicurazioni contro gli infortuni sul lavoro e le malattie professionali, nonché del principio di pertinenza dei dati rispetto alle finalità per cui sono raccolti e successivamente trattati. (*Nota* alla procura della Repubblica di Torino del 27 ottobre 2003).

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

Relazione 2004 - Rapporto di lavoro in ambito pubblico

Dati sensibili

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

Non è stata così ritenuta rispondente al principio di necessità l'indicazione, nelle comunicazioni indirizzate alle sedi interessate, dei gravi motivi di salute su cui era fondato il provvedimento di trasferimento di un dipendente. Il trasferimento, infatti, avrebbe potuto essere comunicato a tali uffici mediante una nota contenente, in sintesi, il testo del provvedimento originario e gli estremi di riferimento del provvedimento. Tale accorgimento, peraltro, non pregiudica l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, l. n. 241/1990), né la facoltà delle persone a ciò legittimate di accedere ad eventuali altri dati, anche di tipo sensibile, contenuti in tali atti, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa. In materia di trattamento di dati sensibili, l'Autorità ha ritenuto che la disciplina sulla protezione dei dati personali non ponesse ostacoli di fondo ad un'iniziativa del Ministero degli affari esteri consistente nell'identificare i dipendenti portatori di handicap ai fini di esercitazione per evacuazioni antincendio in conformità alla disciplina sull'igiene e la sicurezza del lavoro.

Tale attività rientra infatti tra quelle che, sulla base del Codice, possono giustificare il trattamento di dati sensibili (artt. 86, comma 1, lett. c) e 112, comma 2, lett. e) del Codice). Nel ricordare, anche in questo caso, che l'amministrazione può effettuare il trattamento delle informazioni relative allo stato di disabilità dei dipendenti soltanto se esse sono realmente "*indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa*" (art. 22, comma 3, del Codice), dovendo altresì rispettare le regole di proporzionalità, indispensabilità, pertinenza e non eccedenza, si è fatto presente al Ministero che, per questa ed altre attività di trattamento di dati sensibili, è necessario provvedere con atto regolamentare ad individuare i tipi di dati che possono essere trattati e le operazioni eseguibili (art. 20, comma 2, del Codice).

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

Test psico-attitudinali

Si è precisato, in primo luogo, che il divieto di trattare informazioni sensibili nell'ambito di test psico-attitudinali previsto dal Codice (art. 22, comma 10) si riferisce anche alla raccolta di questi dati mediante questionari volti a costruire il profilo o la personalità dell'interessato. Va pertanto espunta dai

questionari utilizzati sia per gli esami psico-attitudinali, sia per quelli psichiatrici, ogni domanda idonea a rivelare profili particolarmente delicati della sfera privata dell'interessato, quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere.

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

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

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

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

Visite medico-legali

Non è risultata, invece, contraria alla disciplina sul trattamento dei dati personali la trasmissione alla questura e alla prefettura da parte di un comune (finalizzata all'adozione dei provvedimenti di competenza) dell'esito di alcune visite medico-legali cui era stato sottoposto un dipendente, essendo l'interessato, un agente di pubblica sicurezza, abilitato al porto di pistola, nonché in possesso del porto d'armi per uso di caccia (*Provv*. 22 gennaio 2004).

Il caso va visto in connessione con un altro, esaminato da questa Autorità, oggetto di una valutazione parzialmente difforme dell'autorità giudiziaria presso cui è stato impugnato il provvedimento del Garante, in considerazione dell'ulteriore documentazione prodotta dall'interessato, invece non presentata in sede di ricorso all'Autorità (v. par. 19.4).

Nel ricorso, il dipendente di una questura aveva lamentato che i dati relativi al proprio stato di salute, accertati nel corso di una visita medica cui era stato sottoposto per verificare la sua idoneità al servizio, erano stati comunicati ad altri soggetti al fine del ritiro cautelativo dell'arma in dotazione e del tesserino di servizio. Nella decisione del ricorso, sulla base degli elementi prodotti dalle parti, il Garante aveva ritenuto che tali comunicazioni fossero

avvenute lecitamente, in quanto effettuate in conformità alle norme sulle autorizzazioni di polizia per la detenzione ed il porto d'armi e finalizzate all'adozione dei relativi provvedimenti (*Provv*. 15 gennaio 2004).

L'Ufficio, invece, ha avviato specifici accertamenti per verificare se all'interessato sia stata fornita un'idonea informativa anche in relazione ai flussi di dati necessari ai fini dell'adozione dei provvedimenti sull'arma di servizio. Sempre in materia di trattamento di dati del personale in servizio presso le questure, è stato oggetto di una decisione su ricorso il trattamento di dati sensibili di un funzionario amministrativo.

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

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

L'utilizzo del fax come mezzo di comunicazione tra amministrazioni è consentito dalla legge e, in linea generale, non è in contrasto con i principi in materia di protezione dei dati personali. Il Garante ha tuttavia evidenziato che per talune circostanze occorre rispettare le specifiche modalità eventualmente previste dalla normativa di settore. Ad esempio, è all'attenzione dell'Autorità una questione relativa alle modalità di trasmissione delle comunicazioni nell'ambito del procedimento disciplinare, per alcune delle quali la normativa prevede la consegna personale all'interessato o, qualora questa non sia possibile, l'invio di una raccomandata (artt. 111 e 104, decreto del Presidente della Repubblica n. 3/1957).

Nel caso in esame, il fax era stato utilizzato anche per le convocazioni dei componenti del Consiglio di disciplina che contenevano il nominativo della persona sottoposta al procedimento, anche se, in ossequio ai principi di pertinenza e non eccedenza, sarebbe stato probabilmente sufficiente anticipare soltanto il tipo di intervento per il quale si richiedeva la presenza del consigliere. È di nuovo all'esame dell'Autorità la questione dell'indicazione di dati personali dei lavoratori nei buoni pasto (in particolare, i nominativi dei singoli beneficiari e la loro sede di servizio), accanto alle informazioni sul datore di lavoro, nonché dei presupposti di liceità per comunicare i dati dei dipendenti al soggetto tenuto all'erogazione del servizio.

Diritto al lavoro dei disabili

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

Anche a tale proposito occorre sottolineare che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti. Un'amministrazione provinciale ha poi informato il Garante, nell'ambito di una comunicazione ai sensi dell'art. 39 del Codice, dell'intenzione di trasmettere ad un comune i dati identificativi degli iscritti ad una lista del collocamento obbligatorio per consentire lo svolgimento di un'indagine sui bisogni dei cittadini disabili.

In proposito, l'Autorità ha precisato che, trattandosi di informazioni idonee a rivelare lo stato di disabilità degli interessati, occorre far riferimento alla distinta e più stringente disciplina prevista per il trattamento dei dati sensibili (artt. 20 e 22 del Codice) (*Nota* 21 settembre 2004). Nel corso degli ulteriori approfondimenti, avviati in collaborazione con gli enti pubblici coinvolti, sono state poi fornite indicazioni idonee a realizzare l'iniziativa nel pieno rispetto delle garanzie poste dal Codice a tutela della riservatezza e degli altri diritti dei disabili interessati dall'indagine.

Sciopero nei servizi pubblici essenziali

Con riferimento alla disciplina sullo sciopero nei servizi pubblici essenziali, l'Autorità si è occupata della prassi, seguita da alcune amministrazioni pubbliche, di comunicare al Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e all'apposita Commissione di garanzia gli elenchi nominativi di dipendenti che hanno esercitato, in specifici casi, il diritto di sciopero. In proposito, considerando la chiarezza del dettato normativo della legge n. 146/1990, che pone in capo alle amministrazioni e alle imprese erogatrici di detti servizi l'obbligo di rendere pubblico "il numero dei lavoratori che hanno partecipato allo sciopero, la durata dello stesso e la misura della trattenuta effettuata secondo la disciplina vigente" (art. 5), si è rilevato che talune amministrazioni potevano essere state indotte ad effettuare siffatte comunicazioni da una espressione utilizzata nella circolare del 18 giugno 2002 del Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, con riferimento alle rilevazioni delle adesioni allo sciopero.

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

Concorsi

Il Ministero degli affari esteri ha sottoposto all'attenzione del Garante l'intenzione di consentire ai candidati interessati a partecipare ai concorsi banditi dall'amministrazione di inviare direttamente *on-line* all'ufficio competente la domanda di partecipazione, corredata di dati personali. Poiché la questione attiene alla più generale tematica dell'informatizzazione dell'amministrazione pubblica, il Garante, nel rilevare che l'iniziativa in esame di per sé non era in contrasto con i principi del Codice, ha evidenziato al Ministero che, tuttavia, la disciplina dell'accesso agli impieghi nelle pubbliche amministrazioni e dello svolgimento dei concorsi pubblici (art. 4, decreto del Presidente

della Repubblica n. 487/1994) esclude espressamente l'utilizzo di strumenti diversi dalla diretta presentazione all'ufficio competente delle domande di ammissione al concorso o dal loro invio tramite raccomandata con avviso di ricevimento (*Nota* 25 agosto 2004).

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

Sempre in tema di trattamento di dati personali nell'ambito di concorsi pubblici, si è precisato che non costituisce violazione della disciplina sulla riservatezza la richiesta, rivolta dalle amministrazioni pubbliche agli aspiranti, di una dichiarazione sostitutiva dei carichi pendenti.

Tale procedura tiene conto dell'esigenza dell'amministrazione di verificare l'eventuale presenza di cause ostative all'accesso al pubblico impiego (art. 85, decreto del Presidente della Repubblica del 10 gennaio 1957, n. 3 e art. 2, decreto del Presidente della Repubblica del 9 maggio 1994, n. 487); esigenza quest'ultima espressamente riconosciuta dall'art. 71 del decreto del Presidente della Repubblica n. 445/2000 e dalla recente riforma del casellario giudiziale, che prevede anche una forma di accesso diretto alla banca dati da parte delle amministrazioni (decreto del Presidente della Repubblica del 14 novembre 2002, n. 313).

I PARERI E LE DECISIONI DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI SULLE ATTIVITÀ DELLE PUBBLICHE AMMINISTRAZIONI

In generale

Le norme attuative per la tenuta del ruolo unico dei dirigenti, gestito dalla funzione pubblica, devono anche tener conto del principio di pertinenza e non eccedenza dei dati previsto all'art. 9 delle legge n. 675. (comma 1, lett. d)).

Roma, lì 24 novembre 1998

Cons. Angelo Piazza
Ministro della funzione pubblica
Corso Vittorio Emanuele II, 116
00186 Roma

OGGETTO: Schema di regolamento recante la disciplina delle modalità di costituzione e tenuta del ruolo unico della dirigenza delle amministrazioni statali, anche ad ordinamento autonomo, e della banca dati informatica della dirigenza, nonché delle modalità di elezione del componente del Comitato di garanti.

Lo schema di regolamento in oggetto, previsto dall'art. 23 del d.lg. n. 29/1993 (come modificato, da ultimo, dall'art. 15 del d.lg. n. 80/1998), detta le norme attuative per la tenuta del ruolo unico dei dirigenti (gestito da un apposito ufficio del Dipartimento per la funzione pubblica) e per la costituzione di una banca dati informatica, al fine di consentire la mobilità e l'interscambio professionale dei dirigenti tra le amministrazioni pubbliche.

Al riguardo, questa Autorità ritiene di formulare le seguenti osservazioni.

Si suggerisce in primo luogo di precisare nell'articolo 3 (o eventualmente in un futuro atto scritto di codesto Dipartimento, il quale deve essere considerato come il «titolare del trattamento» dei dati personali ai sensi della

legge n. 675/1996) se l'incarico di responsabile della tenuta del ruolo unico dei dirigenti sia comprensivo, come sembra, di quello di «responsabile del trattamento» (v. l'art. 8 della stessa legge). Inoltre, al comma 2, lettera e), è opportuno aggiungere alla fine del periodo le seguenti parole: «*e successive modificazioni ed integrazioni*», e coordinare la parte finale della lettera h) con i successivi artt. 4 e 7, specificando se le amministrazioni interessate possono conoscere, in tutto o solo in parte, «*le informazioni risultanti dalla banca dati informatica*».

Appare inoltre opportuno inserire nell'art. 4, comma 1, un riferimento esplicito al principio di pertinenza e non eccedenza dei dati (cfr. l'art. 9, comma 1, lett. d), legge n. 675/1996).

In secondo luogo, si osserva che l'art. 4, commi 2 e 3, sembra distinguere il «*ruolo unico*» dalla «*banca dati informatica*», almeno ai fini della conoscibilità dei dati.

Nel ruolo unico, infatti, sarebbero contenuti soltanto i dati «*essenziali da inserire nel ruolo a fianco del nominativo di ciascun dirigente*», indicati in una tabella allegata al regolamento (che per un disguido non è stata trasmessa a questa Autorità), i quali sarebbero sottoposti ad un regime di piena pubblicità.

Nella banca dati verrebbero inserite «*ulteriori informazioni relative alla carriera, alle esperienze professionali, agli incarichi ricoperti, alle pubblicazioni ed ogni altro elemento conoscitivo utile ad attuare la disciplina contenuta nell'art. 19 del d.lg. n. 29/1993*», le quali sarebbero invece consultabili solo «*dalle amministrazioni pubbliche interessate al conferimento di incarichi dirigenziali*», oltre che dai soggetti «*che abbiano un interesse giuridicamente rilevante*».

Qualora tale interpretazione risulti corretta, si suggerisce di coordinare le disposizioni contenute nei predetti commi dell'art. 4 con la formulazione utilizzata al successivo art. 7, in modo da evidenziare meglio se:

a) con il ruolo unico si istituirebbe una sorta di albo dei dirigenti, i cui dati sarebbero «accessibili a chiunque»;

b) la banca dati informatizzata, contenente gli specifici dati curricolari e professionali di ciascun dirigente ed utilizzata al fine di promuovere la mobilità e l'interscambio dei dirigenti (art. 7 dello schema), sarebbe consultabile e per questi soli motivi, dalle pubbliche amministrazioni interessate al conferimento di incarichi dirigenziali, nonché da coloro che vi abbiano interesse per la tutela di situazioni giuridicamente rilevanti (sotto quest'ultimo profilo, potrebbe essere sufficiente citare la legge n. 241/1990).

A tale ultimo fine, potrebbe essere utile modificare la seconda parte del comma 3 dello stesso articolo, eliminando il riferimento alle «*regole stabilite dal Garante per la protezione dei dati personali*» e aggiungendo invece una frase per specificare che le informazioni inserite nella banca dati informatica potranno essere utilizzate, anche dai soggetti richiedenti, per le sole finalità previste dalla specifica normativa di riferimento o dalla legge n. 241/1990.

Si segnala infine la possibilità di coordinare le attività in esame con quelle concernenti l'anagrafe delle prestazioni dei dipendenti pubblici.

Questa Autorità resta a disposizione per ogni ulteriore chiarimento e collaborazione.

IL PRESIDENTE
Rodotà

Sicurezza dei dati e dei sistemi

In generale

Per i dati la cui inclusione nel cedolino dello stipendio appaia necessaria nell'interesse del dipendente, andrebbero adottate, ai sensi dell'art. 15 della legge n. 675/1996, opportune cautele a tutela della riservatezza che possono consistere, ad esempio, nel piegare e spillare il cedolino, nell'imbustarlo o nell'apporvi una copertura delle parti più significative che non riguardino dati di comune conoscenza (generalità, ufficio di appartenenza, ecc.), ovvero nell'introdurre una cd. «distanza di cortesia» agli sportelli.

Roma li, 31 dicembre 1998

Comune di Roma
Direzione generale

OGGETTO: Contenuto e caratteristiche dei cedolini dello stipendio dei dipendenti comunali.

Si fa riferimento al quesito formulato da codesto Comune e relativo alle misure da adottare a tutela della riservatezza dei dati contenuti nel cd. «cedolino» dello stipendio dei dipendenti comunali.

Si osserva preliminarmente che i dati presenti in tale documento rientrano certamente nella nozione di «dato personale» contenuta nella legge n. 675/1996 in quanto collegati a persone fisiche individuate o individuabili. Alcuni di essi possono avere natura «sensibile» (sussidi di cura, indennità missione handicappati, iscrizione al sindacato, ecc.) o rendono opportune maggiori cautele (multe disciplinari, pignoramenti per alimenti o tasse, ecc.).

Il cedolino è destinato ad essere consegnato, di regola, nelle mani dell'interessato. Ciononostante, si concorda con la necessità di adottare le opportune misure volte a tutelare la riservatezza dei dipendenti per fare in modo che i dati contenuti nel «cedolino» non siano immediatamente accessibili ad altre persone rimanendo conoscibili dai soli incaricati del trattamento che li devono necessariamente utilizzare per la gestione del rapporto di lavoro. Il dipendente ha ovviamente interesse a poter verificare nel modo più semplice possibile le voci relative a ritenute ed emolumenti.

Ciò non preclude al Comune la possibilità di eliminare dai cedolini determinati particolari relativi a situazioni strettamente personali o familiari (es., la causa del pignoramento, la ragione del sussidio, la sigla del sindacato).

Per gli altri dati la cui inclusione nel cedolino appaia necessaria nell'interesse del dipendente, andrebbero invece adottate opportune cautele che possono consistere, ad esempio, nel piegare e spillare il cedolino, nell'imbustarlo o nell'apporvi una copertura delle parti più significative che non riguardino dati di comune conoscenza (generalità, ufficio di appartenenza, ecc.), ovvero nell'introdurre una cd. «distanza di cortesia» agli sportelli.

Nei comuni dotati di un efficiente sistema informativo si potrebbero poi configurare ulteriori modalità basate sulla riduzione al minimo dei dati contenuti nel cedolino e sulla possibilità per il dipendente di accedere facilmente, con l'uso di una password, a tutte le informazioni che riguardano lo stipendio.

Questa Autorità resta a disposizione per ogni ulteriore chiarimento.

IL PRESIDENTE
Rodotà

Dati personali anche di carattere valutativo contenuti in atti del datore di lavoro

È legittima la richiesta del lavoratore di accedere ai dati personali che lo riguardano, ivi compresi i giudizi, le valutazioni ed ogni notizia, informazione o elemento contenuti nella documentazione riferita ad una serie ben individuata di circostanze e di procedimenti. Ciò senza dover motivare la richiesta o dimostrare di dover acquisire i dati per difendere un diritto in giudizio. Il diritto di accesso ai dati personali non è soggetto inoltre a limitazione o differimento secondo i presupposti del diverso diritto di accesso ai documenti amministrativi, ne può essere precluso quando i dati sono contenuti in documenti in passato esibiti all'autorità giudiziaria.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del Mauro Paissan, componente e del dott. Giovanni Buttarelli, segretario generale; esaminato il ricorso presentato dalla Sig.a XY; nei confronti di

INPS, Istituto nazionale della previdenza sociale. Agenzia di produzione di Macerata;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio;

RELATORE il dott. Mauro Paissan;

VISTA la documentazione in atti;

Premesso

La ricorrente, dipendente dell'Istituto indicato in premessa, lamenta di non aver ricevuto un positivo riscontro all'istanza avanzata il 19 giugno 2001 ai sensi dell'ari. 13 della legge n. 675, con la quale aveva chiesto di accedere ai propri dati personali, "ivi compresi i giudizi, le vantazioni ed ogni altra notizia o informazione...contenuti nella documentazione amministrativa relativa a presunte indagini espletate dall'Istituto", in relazione ad una delicata vicenda personale relativa a presunte molestie sessuali che l'aveva coinvolta unitamente ad un dirigente dell'Istituto.

All'invito ad aderire spontaneamente alle richieste della ricorrente, formulato da questa Autorità con nota n. 7221 del 2 luglio 2001, il direttore della sede locale dell'istituto ha risposto con nota anticipata via fax il 5 luglio 2001 nella quale è stato confermato il diniego espresso in precedenza, "trattandosi di una richiesta sulla quale si è pronunciata la direzione generale dell'Istituto" (1a quale aveva già sottolineato in passato come gli atti richiesti dall'interessata rien-trassero fra quelli sottratti all'accesso sulla base delle specifiche norme attuative della legge n. 241). Tale posizione è stata ribadita con successiva nota in data 16 luglio con la quale è stata eccepita anche la presenza all'interno della documentazione richiesta di dati concernenti altre persone.

Con memoria in data 11 luglio 2001 l'interessata ha però ribadito le proprie richieste, evidenziando come l'istanza a suo tempo presentata all'INPS, ed alla quale l'ente si è riferito nel predetto riscontro, fosse in realtà avanzata ai sensi

della legge n. 241 del 1990 in relazione ad uno specifico documento, anziché al complesso di informazioni e dati personali cui fa riferimento il ricorso in questione.

II ricorso è fondato.

Il diritto tutelato dall'art. 13, comma 1, della legge n. 675/1996 permette all'interessato di accedere ai propri dati personali comunque trattati dal titolare del trattamento. Tale diritto presenta caratteri peculiari e non deve essere confuso con il diverso diritto di accedere ad atti e a documenti. Ai sensi del citato art. 13 è infatti possibile proporre un'istanza volta ad avere contezza del complesso (o, come nel caso di specie, di una particolare tipologia) dei propri dati personali dete-nuti da un individuato titolare di trattamento.

A fronte di un'istanza di questo tipo, secondo quanto disposto dal citato art. 13 e dall'ari. 17 del d.P.R. n. 501/1998, il responsabile o gli incaricati del trattamento devono estrarre i dati oggetto di accesso e comunicarli all'interessato senza ritardo. Tali dati possono "essere comunicati al richiedente anche oralmente, ovvero con prospettazione mediante mezzi elettronici o comunque automatizzati...Se vi è richiesta, si provvede in ogni caso alla trasposizione dei dati su supporto cartaceo o informatico...".

Alla luce del citato quadro normativo ogni soggetto interessato può quindi chiedere di avere accesso ai propri dati personali, ma non può chiedere, invocando l'art. 13 della legge n. 675, di avere copia integrale degli atti, delle relazioni o di altri documenti contenenti tali dati. Solo quando l'estrazione dei dati risulti particolarmente difficoltosa, l'adempimento della richiesta di accesso può avvenire anche tramite la modalità dell'esibizione e/o della consegna in copia della documentazione.

Nel concetto di dato personale, attesa l'accezione particolarmente ampia di cui all'art. 1 della Legge n.675/1996, rientrano poi non solo informazioni di tipo anagrafico o comunque oggettivo, ma anche ogni notizia, informazione o elemento che abbia comunque un'efficacia informativa tale da fornire un contributo aggiuntivo di conoscenza rispetto ad un soggetto identificato o identificabile. E ciò in riferimento sia ad informazioni oggettivamente caratterizzate, sia a giudizi, analisi, valutazioni, come quelle presumibilmente contenute anche nella citata documentazione riferita all'interessata.

Nel caso in esame, l'interessata ha espressamente e con evidenza chiesto con istanza del 19 giugno 2001 preliminare al ricorso, ai sensi dell'ari. 13 della legge n. 675, di accedere ai propri dati personali contenuti nella documentazione (detenuta dalla sede locale dell'istituto) riferita ad una serie ben individuata di circostanze e di procedimenti. Pertanto, la risposta da parte dell'istituto titolare del trattamento doveva fare riferimento alla specifica disciplina attinente alla protezione dei dati personali, senza involgere impropri riferimenti ad altre disposizioni normative (come la legge n. 241/1990) poste a tutela di differenti situazioni soggettive.

Va inoltre sottolineato che le richieste di esercizio dei diritti di cui all'ari. 13 della predetta a legge n. 675 non richiedono, da parte del soggetto richiedente, alcuna motivazione, ne tantomeno dimostrazione della necessità di acquisire i dati per difendere un diritto in giudizio. Anche (sotto questo profilo non ha alcuna rilevanza nella vicenda il richiamo a disposizioni regolamentari (attuative della citata legge n. 241) relative a ipotesi di esclusione dall'accesso di determinati tipi B di atti.

Parimenti, l'accesso ai sensi del citato art. 13 non è soggetto a limitazione o differimento secondo i presupposti previsti per il diverso diritto di accesso ai docu-

menti amministrativi, ne può essere precluso in ragione della circostanza che i dati oggetto di richiesta sono contenuti in documenti in passato esibiti all'autorità giudiziaria su sua richiesta.

A seguito della richiesta dell'interessata, si ritiene congrue determinare, ai sensi dell'art. 20, commi 2 e 9, del d.P.R. n. 501/1998, l'ammontare delle spese e dei diritti inerenti al ricorso nella misura forfettaria di lire 300.000, di cui 50.000 per diritti, posti a carico del titolare del trattamento in ragione del mancato riscontro alle richieste della ricorrente.

Per questi motivi il Garante:

– accoglie il ricorso per quanto concerne la richiesta dell'interessata di accedere ai dati personali che la riguardano, ivi compresi gli eventuali dati di carattere valutativo, contenuti negli atti detenuti dall'istituto resistente e indicati nella richiesta di accesso del 19 giugno 2001 e ordina al titolare del trattamento di corrispondere in tal senso alla richiesta dell'interessata entro il 15 settembre 2001, dando conferma di tale adempimento entro la stessa data all'Ufficio del Garante;
– determina ai sensi dell'art. 20, commi 2 e 9, del d.P.R. n. 501/1998, nella misura forfetaria di lire 300.000, di cui 50.000 per diritti, l'ammontare delle spese e dei diritti inerenti al presente ricorso, posti a carico dell'Istituto resistente che dovrà liquidarli direttamente a favore dell'interessata.

Roma, 24 luglio 2001

IL PRESIDENTE Rodotà
IL RELATORE Paissan
IL SEGRETARIO GENERALE Buttarelli

Dati sensibili - Conservazione separata nel fascicolo personale del lavoratore dei dati relativi alla salute - 30 ottobre 2001

Il trattamento dei dati personali idonei a rivelare lo stato di salute dei dipendenti di un soggetto pubblico è sottoposto dalle disposizioni del d.lg. n. 135/1999 a particolari obblighi e cautele che impongono, tra l'altro, la conservazione separata di dette informazioni da ogni altro dato personale dell'interessato; tale principio di tendenziale separazione, che si concreta soprattutto sul piano della custodia dei dati, deve trovare attuazione anche con riferimento ai fascicoli personali cartacei dei dipendenti dell'Inps, con conseguente obbligo dell'Istituto di preporre alla loro custodia apposito personale, specificamente istruito sulle finalità e sulle cautele indicate dal citato decreto.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dottor Mauro Paissan componenti e del dott. Giovanni Buttarelli, segretario generale;

esaminato il ricorso presentato dal Sig. XY nei confronti

dell'INPS, Area territoriale di Casarano;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dottor Mauro Paissan;

Premesso

Il ricorrente, dipendente dell'INPS in servizio presso la sede di Casarano, lamenta di non aver ricevuto riscontro ad una istanza con la quale aveva chiesto all'istituto la cessazione di alcune modalità di trattamento dei dati sulla salute che lo riguardano, raccolti specie in occasione di visite mediche.

I dati sensibili, oltre ad essere raccolti da personale medico non legittimato nel caso di specie a svolgere le visite di controllo, verrebbero inseriti nel fascicolo personale, anziché essere "segretati, come da disposizioni di legge", e sarebbero pertanto conoscibili anche da personale diverso da quello medico.

Pertanto, prendendo spunto da alcuni impropri commenti e "battute" espressi da suoi colleghi nell'ambiente di lavoro circa propri disturbi psichici, il ricorrente ha chiesto di estrapolare i medesimi dati "dal fascicolo personale, in modo da inibirne l'accesso incontrollato a soggetti diversi dal responsabile medico", con specifico riferimento alla conoscenza da parte di altri dipendenti operanti nella medesima sede INPS di dati relativi non solo alla prognosi, ma anche alla diagnosi redatta dai medici.

Nel richiamare, con il ricorso, le proprie richieste, l'interessato ha rappresentato una serie di circostanze riferite alle modalità di custodia e di trattamento dei dati, che evidenzierebbero talune irregolarità da parte dell'ente, riferite in particolare agli anni 1997 e 1998.

Le posizioni dell'interessato sono state ulteriormente precisate nella memoria anticipata via fax in data 18 ottobre 2001 e nell'audizione tenutasi presso gli uffici di questa Autorità il 24 ottobre 2001. In tali atti il ricorrente ha evidenziato che il trattamento dei dati personali sarebbe avvenuto senza il proprio consenso scritto ed ha altresì rilevato che, a causa del rifiuto opposto dal direttore della sede INPS, non avrebbe "potuto prendere visione del proprio fascicolo personale" (questione che si riservava peraltro di prospettare al Garante con ulteriore ricorso).

All'invito a fornire un riscontro alle istanze dell'interessato, inoltrato da questa Autorità in data 8 ottobre 2001, il titolare del trattamento ha risposto con note del 10 e del 23 ottobre 2001 con le quali ha asserito di trattare in piena liceità i dati dell'interessato, sottolineando in particolare che:

- la conoscenza da parte dell'ente di alcuni dati concernenti lo stato di salute dell'interessato conseguirebbe alla prassi adottata spontaneamente da quest'ultimo, il quale, antecedentemente al 6/9/1998, avrebbe giustificato "talune assenze dal servizio facendo spontaneamente pervenire alla segreteria del personale certificati medici comprensivi di prognosi e diagnosi";
- solo successivamente a tale data l'interessato avrebbe inviato "certificazioni contenenti la sola prognosi, inoltrando contemporaneamente al dirigente sanitario di sede le corrispondenti certificazioni contenenti le diagnosi in busta chiusa";
- presso l'ufficio sanitario di sede esisterebbe "un apposito archivio ove vengono custoditi i fascicoli contenenti notizie da proteggere".

Ciò premesso, il Garante osserva

Il ricorso ai sensi dell'art. 29 della legge n. 675 può essere proposto nei confronti di un individuato titolare del trattamento in relazione alle sole posizioni giuridiche elencate nell'art. 13, comma 1, della legge n. 675, trascorsi almeno cinque giorni dalla presentazione di una istanza rivolta al medesimo titolare o al relativo responsabile del trattamento, ai sensi del predetto art. 13.

Nel caso in questione è stata prodotta un'istanza in data 20 marzo 2001 la quale può essere qualificata alla stregua di un'opposizione nei confronti di deter-

minate modalità di trattamento dei dati (sebbene sia stata formulata in modo generico e riguardi anche alcuni aspetti relativi alle modalità di svolgimento delle visite mediche non interamente collegati alla protezione dei dati). L'opposizione riguarda poi alcuni profili relativi alle modalità di raccolta e custodia dei dati sensibili e alla loro conservazione nei fascicoli personali dei dipendenti dell'Istituto resistente.

Il ricorso verte quindi su un trattamento di dati personali comuni e sensibili svolto da un ente pubblico previdenziale relativamente ad un proprio dipendente. A tale trattamento si applicano, in particolare, le disposizioni di cui agli artt. 27 e 22, commi 3 e 3 bis, della legge n. 675, relative al trattamento dei dati personali da parte dei soggetti pubblici, i quali, contrariamente a quanto sostenuto dal ricorrente, non devono acquisire il consenso degli interessati.

Per quanto riguarda più specificamente il trattamento dei dati sensibili, le norme di riferimento sono anzitutto contenute nel già citato art 22, commi 3 e 3 bis, della legge n. 675, modificato dal d.lg. 11 maggio 1999, n. 135.

L'art. 3 del citato decreto n. 135 ha introdotto a carico dei soggetti pubblici una serie di obblighi e cautele da rispettare relativamente alle finalità e alle modalità di trattamento dei dati personali, senza porre peraltro un obbligo di assoluta e integrale "segretazione" dei dati personali sensibili da parte dell'ente pubblico datore di lavoro.

L'ente è però tenuto ad impiegare tecniche, codici o altri sistemi che permettano di identificare gli interessati solo in caso di necessità e unicamente per lo svolgimento delle rilevanti finalità di interesse pubblico per le quali il trattamento è effettuato (art. 3, comma 4 e 5, d.lg. cit.).

Inoltre, i dati idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati "separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo".

Quest'ultimo principio, che mira a realizzare una tendenziale separazione dei dati personali del tipo anzidetto da quelli di altra natura, riguarda in modo particolare la custodia di dati che vertono specificamente sullo stato di salute o sulla vita sessuale, i quali vanno conservati separatamente rispetto ad altri dati personali che siano oggetto di operazioni di trattamento e che non presuppongono l'utilizzazione degli indicati dati sensibili.

Il medesimo principio della conservazione separata rileva in modo parzialmente diverso rispetto ad una specifica raccolta di atti e documenti di vario tipo qual è il fascicolo personale cartaceo del dipendente. Tale fascicolo presenta infatti alcune caratteristiche di unitarietà e, per le varie finalità di cui all'art. 9 del d.lg. n. 135, può richiedere il periodico utilizzo anche di dati riguardanti lo stato di salute o relativi a varie vicende del dipendente medesimo.

Questa particolarità non elimina la necessità di dare congrua applicazione al principio della conservazione separata anche in riferimento ai fascicoli personali cartacei, i quali, pur dovendo mantenere la loro unitarietà in relazione ai singoli dipendenti interessati, richiedono l'adozione di cautele per assicurare, con opportuni accorgimenti, l'osservanza del richiamato principio di separazione (ad esempio, utilizzando sezioni o sottofascicoli dedicati alla custodia di eventuali dati sensibili, da conservare chiusi o comunque con modalità che circoscrivano la possibilità di una indistinta consultazione nel corso di ordinarie attività amministrative).

Contrariamente a quanto ipotizzato dal ricorrente, il d.lg. n. 135/1999 e il d.P.R. n. 318/1999 non hanno poi introdotto un divieto assoluto e generalizzato, per il personale non medico, di trattare dati sullo stato di salute.

Ad identiche conclusioni è dato altresì pervenire, con riferimento alla tenuta

dei fascicoli personali, in virtù dell'art. 40, comma 2, dell'Accordo 14 febbraio 2001 [Contratto collettivo nazionale di lavoro ad integrazione del Contratto collettivo nazionale di lavoro per il personale non dirigente degli Enti pubblici economici (16 febbraio 1999)], secondo il quale "agli atti e ai documenti conservati nel fascicolo personale è assicurata la riservatezza dei dati personali secondo le disposizioni vigenti in materia"; obbligo questo, che viene fatto gravare dall'art. 40, comma 1, del medesimo Accordo sulla "struttura organizzativa cui compete la gestione delle risorse umane".

Il titolare del trattamento non ha però fornito indicazioni idonee a ritenere che i principi sopra richiamati siano compiutamente osservati, in particolare per quanto riguarda:

– la preposizione del personale addetto alla custodia dei fascicoli (art. 19 legge n. 675) e le istruzioni impartite per evitare che i dati sulla salute siano utilizzati anche occasionalmente per finalità diverse da quelle di cui al d.lg. n. 135/1999;
– le cautele da adottare ai sensi dell'art. 3, commi 4 e 5, del d.lg. n. 135/1999;
– la disciplina integrativa del trattamento dei dati sensibili, che l'INPS avrebbe dovuto promuovere ai sensi dell'art. 22, comma 3-bis, della legge n. 675/1996 entro il 31 dicembre 1999 e che non risulta né adottata, né richiamata dall'Istituto, con conseguenti effetti sulla complessiva liceità del trattamento effettuato anche in termini più generali.

Alla luce delle considerazioni suesposte e sulla base dei riscontri forniti dal titolare del trattamento il ricorso è parzialmente fondato, nella parte riguardante i profili di segretazione del fascicolo sollevati dal ricorrente con l'istanza ai sensi dell'art. 13, e con esclusione pertanto degli altri aspetti relativi all'acquisizione delle diagnosi e alle modalità di raccolta dei dati in occasione di visite mediche, che questa Autorità ritiene peraltro di dover approfondire –unitamente ai punti a) e c) poc'anzi menzionati- nell'ambito di un autonomo procedimento attivato ai sensi dell'art. 31, comma 1, lettera b), della citata legge n. 675.

Per questi motivi il Garante:

a) dichiara parzialmente fondato il ricorso nei termini di cui in motivazione, nella parte riguardante la richiesta di diversa custodia del fascicolo personale del ricorrente;
b) instaura un autonomo procedimento ai sensi dell'art. 31, comma 1, lettera b), della legge n. 675 nei confronti dell'Istituto, per la verifica di quanto indicato in motivazione.

Roma, 30 ottobre 2001

IL PRESIDENTE Rodotà
IL RELATORE Paissan
IL SEGRETARIO GENERALE Buttarelli

Illecita divulgazione di dati sensibili mediante affissione in una bacheca

Costituisce diffusione indiscriminata di dati idonei a rivelare lo stato di salute, e risulta quindi in contrasto con la disciplina posta dalla legge n. 675/1996 e dal d.lg. n. 135/1999 in materia di trattamento dei dati sensibili da parte di soggetti pubblici, l'inserimento della dicitura "portatore di handicap", riferita ad un'insegnante, nella graduatoria dei trasferimenti affissa nella bacheca di un provveditorato agli studi. Le esigenze di pubblicità dell'amministrazione possono essere soddisfatte attraverso l'apposizione di diciture generiche o codici numerici.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dottor Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale; esaminato il ricorso presentato dalla Sig.a XY rappresentata e difesa dall'avv. Maria Grazia Longo presso il cui studio ha eletto domicilio nei confronti di

Ministero dell'istruzione, dell'università e della ricerca, Ufficio scolastico regionale per la Puglia – Direzione generale – Centro servizi amministrativi per la provincia di Lecce;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Giuseppe Santaniello;

Premesso:

La ricorrente, insegnante elementare già in servizio presso un istituto scolastico di Lecce, ha chiesto ed ottenuto il trasferimento ad altra sede fruendo di un beneficio previsto in base alla legge 5 febbraio 1992, n. 104 (legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate).

In occasione dell'affissione in bacheca, presso gli uffici del Provveditorato agli studi di Lecce, "della graduatoria delle domande di mobilità", avvenuta nell'estate scorsa, l'interessata ha rilevato che a fianco del proprio nominativo, in luogo di un sintetico riferimento all'art. 21 della citata legge n. 104/1992 (che disciplina le precedenze nelle assegnazioni di sede), "veniva espressamente indicato lo status di portatore di handicap".

Con il ricorso proposto ai sensi dell'art. 29 della legge n. 675, la medesima interessata lamenta di non avere ricevuto positivo riscontro ad una istanza avanzata ai sensi dell'art. 13 della medesima legge, con la quale si era opposta alla diffusione del dato sensibile in questione, chiedendo al Provveditore di cancellare il dato stesso o di trasformarlo in forma anonima.

Con lo stesso ricorso proposto ai sensi dell'art. 29 della legge n. 675, l'interessata ha ribadito le proprie richieste rilevando come il trattamento del dato sensibile sia avvenuto in contrasto con tale legge, determinando una situazione di grave disagio a livello personale e relazionale, anche per effetto del mancata richiesta del consenso e al non rispetto della prevista autorizzazione del Garante. Il Provveditore non avrebbe dato inoltre seguito ad un intervento del proprio ufficio che era stato preannunciato il 13 agosto 2001 in relazione al programma stabilito in materia dal Ministero, per una eventuale sostituzione della dizione "portatrice di handicap".

All'invito ad aderire spontaneamente alle richieste della ricorrente, formulato da questa Autorità in data 11 febbraio 2002, il Ministero dell'istruzione, dell'università e della ricerca – Ufficio scolastico regionale per la Puglia – Direzione generale – Centro servizi amministrativi per la provincia di Lecce, ha risposto con nota anticipata via fax il 14 febbraio 2002 con la quale, nel confermare quanto esposto dal Provveditore agli studi di Lecce in data 13 agosto 2001, ha affermato che:

- l'elenco dei trasferimenti, affisso all'albo in data 19 giugno 2001, sarebbe stato "ritirato 60 giorni dopo";
- il predetto ufficio sarebbe tenuto, per esigenze di pubblicità degli atti e di

trasparenza dell'azione amministrativa, a indicare nell'elenco dei trasferimenti affisso la specifica causale che li determina e che ciò giustificherebbe l'accostamento al nominativo dell'interessata della dizione "portatore di handicap";

– l'intervento preannunciato il 13 agosto 2001 era stato equivocato dall'interessata, avendo l'ufficio assicurato unicamente un "intervento rappresentativo della situazione" al Ministero il quale impartito precise disposizioni ministeriali al riguardo, uniformi a livello nazionali e non modificabili dagli uffici locali.

Ciò premesso, il Garante osserva:

Il ricorso verte sul trattamento di un dato personale di natura sensibile relativo ad un'insegnante, effettuato nel caso di specie presso un ufficio periferico del Ministero dell'istruzione, dell'università e della ricerca, in ordine ad una procedura di trasferimento.

Il ricorso risulta fondato stante l'accertata illiceità dell'avvenuta divulgazione – tramite affissione in bacheca – di un dato sensibile relativo all'interessata, il cui nominativo è stato affiancato dalla dizione "portatrice di handicap".

La modalità di trattamento in questione ha comportato la "diffusione" di un dato idoneo a rivelare lo stato di salute della ricorrente (cfr. art. 1, comma 2, lett. h), della legge n. 675).

Tale specifica ipotesi di diffusione è espressamente vietata dall'art. 23, comma 4, della legge n. 675. Non possono pertanto ritenersi fondati i riferimenti dell'amministrazione scolastica alla generiche esigenze di diffusione e pubblicità di tali dati, asseritamente giustificate in base ad accordi sindacali o a ordinanze ministeriali che invero si limitano a prevedere l'affissione all'albo dell'ufficio scolastico provinciale del "punteggio complessivo" riportato dal personale scolastico "e delle eventuali precedenze", senza imporre alcuna indicazione più specifica delle condizioni di salute che, nella varia casistica esistente, giustificano una precedenza (art. 6 ordinanza ministeriale prodotta in atti).

La prassi adottata – ed eventuali istruzioni ministeriali al riguardo- non possono in alcun caso derogare alla specifica disciplina di rango primario del trattamento dei dati sensibili da parte di organi pubblici (artt. 2, 3, 4, 9 e 13 del d.lg. 11 maggio 1999, n. 135), che ribadisce il divieto di diffusione di dati idonei a rivelare lo stato di salute (art. 4, comma 4, d.lg. cit.).

Applicata ai portatori di handicap, tale cautela rafforza il principio del rispetto della dignità delle persone interessate, garantito dall'art. 1 della legge n. 675 e dall'art. 1 della citata legge-quadro n. 104/1992.

L'affissione in bacheca in essere all'atto dell'opposizione al trattamento dei dati formulata ai sensi del menzionato art. 13 risulta nel frattempo terminata.

La fondata opposizione ribadita con il ricorso è peraltro espressamente riferita ad ogni altro futuro, eventuale trattamento del dato in questione da parte del Ministero, anche presso altre sedi o dipendenze eventualmente preposte al trattamento.

Ai sensi dell'art. 29, comma 4, della legge n. 675/1996, l'amministrazione scolastica, a livello centrale e periferico dovrà pertanto astenersi dal diffondere ulteriormente presso albi di uffici scolastici provinciali la dizione "portatore di handicap" riferita alla ricorrente. Ai sensi della medesima disposizione l'amministrazione potrà unicamente utilizzare diciture generiche o codici numerici che impediscano la diffusione indiscriminata di dati idonei a rivelare lo stato di salute.

L'apposizione di tali accorgimenti (che potranno permettere semmai alle sole persone legittimate di accedere presso gli uffici scolastici ad eventuali altre notizie

in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa) permette di assicurare il doveroso rispetto della riservatezza rispetto a delicate situazioni relative allo stato di salute, nel rispetto della citata disposizione di cui all'art. 23, comma 4, della legge n. 675.

Non risulta invece adeguata a conseguire tale finalità l'ulteriore soluzione, pur avanzata dalla ricorrente, volta ad indicare a fianco del nominativo dell'interessata il puntuale riferimento alla legge n. 104 del 1992.

Trattandosi di provvedimento normativo specificamente volto alla tutela delle persone handicappate, tale indicazione risulterebbe comunque idonea a rivelare (seppure in via mediata) il predetto dato sensibile.

In relazione al citato art. 29, comma 4, i predetti accorgimenti dovranno essere seguiti anche nella compilazione delle graduatorie a fini di comunicazione interna o nella redazione di altri atti amministrativi, in applicazione delle citate disposizioni del d.lg. n. 135/1999.

A tali cautele il Ministero dell'istruzione dovrà quindi conformarsi fornendo idonee indicazioni a tutti gli uffici periferici ed adeguando a tali principi il proprio sistema informativo.

In caso di eventuali difficoltà di esecuzione della presente decisione, il Garante si riserva peraltro di disporre modalità di attuazione della decisione medesima, sentite le parti che potranno in tale sede produrre completi elementi di valutazione, con l'eventuale collaborazione di personale dell'Ufficio del Garante o di altri organi dello Stato (art. 20, comma 11, del d.P.R. n. 501/1998).

L'illiceità del trattamento è riscontrata con la presente decisione in relazione ai soli principi richiamati, non risultano al contrario fondati i rilievi della ricorrente per quanto concerne l'asserita assenza del consenso dell'interessata e dell'autorizzazione del Garante.

Il trattamento del dato sensibile in questione è infatti effettuato nel caso di specie da un soggetto pubblico cui non si applicano le disposizioni in tema di consenso al trattamento dei dati personali "comuni" di cui all'art. 11 della legge n. 675, né le disposizioni relative al consenso ed all'autorizzazione del Garante di cui all'art. 22, comma 1, della medesima legge in materia di dati sensibili. Ai soggetti pubblici si applicano piuttosto le diverse disposizioni di cui agli artt. 27 e 22, commi 3 e 3 *bis*, della citata legge n. 675, nonché le specifiche disposizioni in tema di dati sensibili di cui al citato d.lg. n. 135 del 1999, in base alle quali le amministrazioni pubbliche non devono operare raccogliendo il consenso al trattamento da parte degli interessati.

Per questi motivi il garante:

– accoglie il ricorso e ordina al Ministero dell'istruzione, dell'università e della ricerca di:
– astenersi con effetto immediato da eventuale altra diffusione del dato sensibile relativo all'handicap della ricorrente, nei termini indicati in motivazione, presso l'Ufficio scolastico regionale per la Puglia e ogni altro ufficio centrale o periferico;
– conformarsi alle misure necessarie indicate in motivazione a tutela dei diritti dell'interessata, entro il 30 giugno 2002, dando conferma di tale adempimento all'interessata ed a questa Autorità entro la stesa data.

Roma, 27 febbraio 2002

IL PRESIDENTE Rodotà
IL RELATORE Santaniello
IL SEGRETARIO GENERALE Buttarelli

IL CODICE DELLA PRIVACY (ARTICOLI RICHIAMATI DALLA DIRETTIVA DEL MINISTRO PER LA FUNZIONE PUBBLICA DELL'11 FEBBRAIO 2005)

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali

Art. 1. Diritto alla protezione dei dati personali

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art. 2. Finalità

1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonchè della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonchè per l'adempimento degli obblighi da parte dei titolari del trattamento.

Art. 3. Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:
   a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
   b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
   c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
   d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
   e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del decreto del Presidente della Repubblica del 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
   f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
   g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
   h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
   i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
   l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
   m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
   n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
   o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:
a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
b) "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
c) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
d) "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
f) "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura ditali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei

dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:
   a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
   b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
   c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
   d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
   e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
   f) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonchè i trattamenti ad essa consentiti;
   g) "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
4. Ai fini del presente codice si intende per:
   a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
   b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
   c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qua-

lità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Art. 8. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.
2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
   a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge luglio 1991, n. 197,e successive modificazioni, in materia di riciclaggio;
   b) in base alle disposizioni del decreto-legge 31 dicembre 1991,n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992,n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
   c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
   d) da un soggetto pubblico, diverso dagli enti pubblici economici,in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonchè alla tutela della loro stabilità;
   e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
   f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.
4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonchè l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Art. 9. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
   a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;

b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.
4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.
5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.
7. Quando, a seguito della richiesta di cui all'articolo 7, commi1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.
8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.
9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed uti-

lizzati in altre operazioni del trattamento intermini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verificala conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.
2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.
3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.
4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
   a) le finalità e le modalità del trattamento cui sono destinati i dati;
   b) la natura obbligatoria o facoltativa del conferimento dei dati;
   c) le conseguenze di un eventuale rifiuto di rispondere;
   d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
   e) i diritti di cui all'articolo 7;
   f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.
2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico,

di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
5. La disposizione di cui al comma 4 non si applica quando:
   a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
   b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
   c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

Art. 14. Definizione di profili e della personalità dell'interessato

1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.
2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17.

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 16. Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:
   a) distrutti;
   b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente personali e non destinati aduna comunicazione sistematica o alla diffusione;
   d) conservati o ceduti ad altro titolare, per scopi storici, statistici o

scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonchè per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.
2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.
3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonchè dalla legge e dai regolamenti.
4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.
5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.
2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.
3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20. Principi applicabili al trattamento di dati sensibili

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.
3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.
4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente

Art. 21. Principi applicabili al trattamento di dati giudiziari

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.
2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. Nel fornire l'informativa di cui all'articolo 13 soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.
3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.
4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.
5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonchè la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria inizia-

tiva. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.
8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.
9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonchè i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.
11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonchè la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.
12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

Art. 26. Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonchè dalla legge e dai regolamenti.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

3. Il comma 1 non si applica al trattamento:
   a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;
   b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.
4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:
   a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
   b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
   c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n.397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
   d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.
5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

Art. 28. Titolare del trattamento

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente,associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.
2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.
5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
   a) autenticazione informatica;
   b) adozione di procedure di gestione delle credenziali di autenticazione;
   c) utilizzazione di un sistema di autorizzazione;
   d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
   e) protezione degli strumenti elettronici e dei dati rispetto a tratta-

menti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonchè dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

1-bis. La notificazione relativa al trattamento dei dati di cui al comma 1 non è dovuta se relativa all'attività dei medici di famiglia e dei pediatri di libera scelta, in quanto tale funzione è tipica del loro rapporto professionale con il Servizio sanitario nazionale.

2. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.
3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.
4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

Art. 38. Modalità di notificazione

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare,e può anche riguardare uno o più trattamenti con finalità correlate.
2. La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.
3. Il Garante favorisce la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.
4. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.
5. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.
6. Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'articolo 37 fornisce le notizie contenute nel modello di cui al comma 2 a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Art. 39. Obblighi di comunicazione

1. Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:
   a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;
   b) trattamento di dati idonei a rivelare lo stato di salute previsto dal

programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.

2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.
3. La comunicazione di cui al comma 1 è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

Art. 46. Titolari dei trattamenti

1. Gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento.
2. Con decreto del Ministro della giustizia sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, relativamente a banche di dati centrali od oggetto di interconnessione tra più uffici o titolari. I provvedimenti con cui il Consiglio superiore della magistratura e gli altri organi di autogoverno di cui al comma 1 individuano i medesimi trattamenti da essi effettuati sono riportati nell'allegato C) con decreto del Ministro della giustizia.

Art. 47. Trattamenti per ragioni di giustizia

1. In caso di trattamento di dati personali effettuato presso uffici giudiziari di ogni ordine e grado, presso il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia, non si applicano, se il trattamento è effettuato per ragioni di giustizia, le seguenti disposizioni del codice:
   a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;
   b) articoli da 145 a 151.
2. Agli effetti del presente codice si intendono effettuati per ragioni di giustizia i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonchè le attività ispettive su uffici giudiziari. Le medesime ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla predetta trattazione.

Art. 48 Banche di dati di uffici giudiziari

1. Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire in conformità alle vigenti disposizioni processuali dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con

soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11 del presente codice.

Art. 49. Disposizioni di attuazione

1. Con decreto del Ministro della giustizia sono adottate, anche ad integrazione del decreto del Ministro di grazia e giustizia 30 settembre 1989, n. 334, le disposizioni regolamentari necessarie per l'attuazione dei principi del presente codice nella materia penale e civile.

Art. 50. Notizie o immagini relative a minori

1. Il divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale.

Art. 51. Principi generali

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.
2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo.

Art. 52. Dati identificativi degli interessati

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado,l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.
2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.
3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con

timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: "In caso di diffusione omettere le generalità e gli altri dati identificativi di ...".

4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.
5. Fermo restando quanto previsto dall'articolo 734 bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.
6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 32 della legge 11 febbraio 1994, n. 109, provvede in modo analogo in caso di richiesta di una parte.
7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

Art. 53. Ambito applicativo e titolari dei trattamenti

1. Al trattamento di dati personali effettuato dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento, non si applicano le seguenti disposizioni del codice:
   a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;
   b) articoli da 145 a 151.
2. Con decreto del Ministro dell'interno sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, e i relativi titolari.

Art. 54. Modalità di trattamento e flussi di dati

1. Nei casi in cui le autorità di pubblica sicurezza o le forze di polizia possono acquisire in conformità alle vigenti disposizioni di legge o di regolamento dati, informazioni, atti e documenti da altri soggetti, l'acquisizione può essere effettuata anche per via telematica. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e

banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11. Le convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'articolo 53.

2. I dati trattati per le finalità di cui al medesimo articolo 53 sono conservati separatamente da quelli registrati per finalità amministrative che non richiedono il loro utilizzo.
3. Fermo restando quanto previsto dall'articolo 11, il Centro elaborazioni dati di cui all'articolo 53 assicura l'aggiornamento periodico e la pertinenza e non eccedenza dei dati personali trattati anche attraverso interrogazioni autorizzate del casellario giudiziale e del casellario dei carichi pendenti del Ministero della giustizia di cui al decreto del Presidente della Repubblica 14 novembre 2002, n. 313, o di altre banche di dati di forze di polizia, necessarie perle finalità di cui all'articolo 53.
4. Gli organi, uffici e comandi di polizia verificano periodicamente i requisiti di cui all'articolo 11 in riferimento ai dati trattati anche senza l'ausilio di strumenti elettronici, e provvedono al loro aggiornamento anche sulla base delle procedure adottate dal Centro elaborazioni dati ai sensi del comma 3, o, per i trattamenti effettuati senza l'ausilio di strumenti elettronici, mediante annotazioni o integrazioni dei documenti che li contengono.

Art. 55. Particolari tecnologie

1. Il trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche di dati genetici o biometrici, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie, è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17 sulla base di preventiva comunicazione ai sensi dell'articolo 39.

Art. 56. Tutela dell'interessato

1. Le disposizioni di cui all'articolo 10, commi 3, 4 e 5, della legge 1 aprile 1981, n. 121, e successive modificazioni, si applicano anche, oltre che ai dati destinati a confluire nel Centro elaborazione dati di cui all'articolo 53, a dati trattati con l'ausilio di strumenti elettronici da organi, uffici o comandi di polizia.

Art. 57. Disposizioni di attuazione

1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, sono individuate le modalità di attuazione dei principi del presente codice relativamente al trattamento dei dati effettuato per le finalità di cui all'articolo 53 dal Centro elaborazioni dati e da organi, uffici o comandi di polizia, anche ad integrazione e modifica del decreto del Presidente della Repubblica 3 maggio 1982, n. 378, e in attuazione della Raccomandazione R (87) 15 del Consiglio d'Europa del 17 settembre 1987, e successive modificazioni. Le modalità sono individuate con particolare riguardo:

a) al principio secondo cui la raccolta dei dati è correlata alla specifica finalità perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati, in particolare per quanto riguarda i trattamenti effettuati per finalità di analisi;
b) all'aggiornamento periodico dei dati, anche relativi a valutazioni effettuate in base alla legge, alle diverse modalità relative ai dati trattati senza l'ausilio di strumenti elettronici e alle modalità per rendere conoscibili gli aggiornamenti da parte di altri organi e uffici cui i dati sono stati in precedenza comunicati;
c) ai presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari, anche ai fini della verifica dei requisiti dei dati ai sensi dell'articolo 11, dell'individuazione delle categorie di interessati e della conservazione separata da altri dati che non richiedono il loro utilizzo;
d) all'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, nonchè alla tipologia dei procedimenti nell'ambito dei quali essi sono trattati o i provvedimenti sono adottati;
e) alla comunicazione ad altri soggetti, anche all'estero o per l'esercizio di un diritto o di un interesse legittimo, e alla loro diffusione, ove necessaria in conformità alla legge;
f) all'uso di particolari tecniche di elaborazione e di ricerca delle informazioni, anche mediante il ricorso a sistemi di indice.

Art. 58. Disposizioni applicabili

1. Ai trattamenti effettuati dagli organismi di cui agli articoli3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge, le disposizioni del presente codice si applicano limitatamente a quelle previste negli articoli da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169.
2. Ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, le disposizioni del presente codice si applicano limitatamente a quelle indicate nel comma 1, nonchè alle disposizioni di cui agli articoli 37, 38 e 163.
3. Le misure di sicurezza relative ai dati trattati dagli organismi di cui al comma 1 sono stabilite e periodicamente aggiornate con decreto del Presidente del Consiglio dei ministri, con l'osservanza delle norme che regolano la materia.
4. Con decreto del Presidente del Consiglio dei ministri sono individuate le modalità di applicazione delle disposizioni applicabili del presente codice in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di incaricati, anche in relazione all'aggiornamento e alla conservazione.

Art. 59. Accesso a documenti amministrativi

1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonchè dai relativi regola-

menti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione ditale disciplina si considerano di rilevante interesse pubblico.

Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale

1. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 68. Benefici economici ed abilitazioni

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.
2. Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione:
   a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia;
   b) alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive;
   c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti;
   d) al riconoscimento di benefici connessi all'invalidità civile;
   e) alla concessione di contributi in materia di formazione professionale;
   f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;
   g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.
3. Il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la trasparenza delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 73. Altre finalità in ambito amministrativo e sociale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali, con particolare riferimento a:
   a) interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
   b) interventi anche di rilievo sanitario in favore di soggetti bisognosi o

non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
c) assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;
d) indagini psico-sociali relative a provvedimenti di adozione anche internazionale;
e) compiti di vigilanza per affidamenti temporanei;
f) iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;
g) interventi in tema di barriere architettoniche.

2. Si considerano, altresì, di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità:
a) di gestione di asili nido;
b) concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico;
c) ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;
d) di assegnazione di alloggi di edilizia residenziale pubblica;
e) relative alla leva militare;
f) di polizia amministrativa anche locale, salvo quanto previsto dall'articolo 53, con particolare riferimento ai servizi di igiene,di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo;
g) degli uffici per le relazioni con il pubblico;
h) in materia di protezione civile;
i) di supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;
l) dei difensori civici regionali e locali.

Art. 110. Ricerca medica, biomedica ed epidemiologica

1. Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12 bis del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40.
2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 7 nei riguardi dei trattamenti di cui al comma 1, l'aggiornamento, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

Art. 111. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione degli annunci per finalità di occupazione di cui all'articolo 113, comma 3 e alla ricezione di curricula contenenti dati personali anche sensibili.

Art. 112. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.
2. Tra i trattamenti effettuati per le finalità di cui al comma1, si intendono ricompresi, in particolare, quelli effettuati al fine di:
   a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;
   b) garantire le pari opportunità;
   c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;
   d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonchè ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;
   e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonchè in materia sindacale;
   f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente;
   g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;
   h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;
   i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;

l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;
m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;
n) svolgere l'attività di indagine e ispezione presso soggetti pubblici;
o) valutare la qualità dei servizi resi e dei risultati conseguiti.

3. La diffusione dei dati di cui alle lettere m), n) ed o) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

Art. 146. Interpello preventivo

1. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile ai sensi dell'articolo 8, comma 1, e sono decorsi i termini previsti dal presente articolo, ovvero è stato opposto alla richiesta un diniego anche parziale.
2. Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro quindici giorni dal suo ricevimento.
3. Entro il termine di cui al comma 2, se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso,il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Art. 152. Autorità giudiziaria ordinaria

1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.
2. Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.
3. Il tribunale decide in ogni caso in composizione monocratica.
4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.
5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice,sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.
6. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.
7. Il giudice fissa l'udienza di comparizione delle parti con decreto con il

quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.
9. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli.
10. Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.
11. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza.
12. Con la sentenza il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.
13. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.
14. Le disposizioni di cui al presente articolo si applicano anche nei casi previsti dall'articolo 10, comma 5, della legge 1 aprile 1981, n. 121, e successive modificazioni.

Art. 154. Compiti (del Garante)

1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:
   a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione;
   b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
   c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;
   d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;
   e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139;

f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore;
g) esprimere pareri nei casi previsti;
h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonchè delle misure di sicurezza dei dati;
i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
l) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37;
m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:
   a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione;
   b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol);
   c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo1997, e dalla legge 30 luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;
   d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l"Eurodac" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;
   e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.
3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine,il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.
4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice.
5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può proce-

dere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.

Art. 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Art. 176. Soggetti pubblici

1. Nell'articolo 24, comma 3, della legge 7 agosto 1990, n. 241, dopo le parole: "mediante strumenti informatici" sono inserite le seguenti: ", fuori dei casi di accesso a dati personali da parte della persona cui i dati si riferiscono,".
2. Nell'articolo 2 del decreto legislativo 30 marzo 2001, n. 165, in materia di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, dopo il comma 1 è inserito il seguente: "1-bis. I criteri di organizzazione di cui al presente articolo sono attuati nel rispetto della disciplina in materia di trattamento dei dati personali.".
3. L'articolo 4, comma 1, del decreto legislativo 12 febbraio1993, n. 39, e successive modificazioni, è sostituito dal seguente: "1. È istituito il Centro nazionale per l'informatica nella pubblica amministrazione, che opera presso la Presidenza del Consiglio dei ministri per l'attuazione delle politiche del Ministro per l'innovazione e le tecnologie, con autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e con indipendenza di giudizio.".
4. Al Centro nazionale per l'informatica nella pubblica amministrazione continuano ad applicarsi l'articolo 6 del decreto legislativo 12 febbraio 1993, n. 39, nonchè le vigenti modalità di finanziamento nell'ambito dello stato di previsione del Ministero dell'economia e delle finanze.
5. L'articolo 5, comma 1, del decreto legislativo n. 39 del 1993, e successive modificazioni, è sostituito dal seguente: "1. Il Centro nazionale propone al Presidente del Consiglio dei ministri l'adozione di regolamenti con-

cernenti la sua organizzazione, il suo funzionamento, l'amministrazione del personale, l'ordinamento delle carriere, nonchè la gestione delle spese nei limiti previsti dal presente decreto.".

6. La denominazione: "Autorità per l'informatica nella pubblica amministrazione" contenuta nella vigente normativa è sostituita dalla seguente: "Centro nazionale per l'informatica nella pubblica amministrazione".

LA RELAZIONE DEL PRESIDENTE DELL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI SULLE ATTIVITÀ DEL 2004

Discorso del Presidente, Stefano Rodotà

Signor Presidente della Repubblica, nella natura di queste relazioni al Parlamento ed al Governo è il loro presentarsi, insieme, come bilancio e come programma. Quest'anno il bilancio assume un significato particolare. Poiché si conclude il mandato del Collegio, lo sguardo dev'essere rivolto non solo all'ultimo anno, ma a tutto il passato quadriennio: e, oltre questo, all'intera vita di questa giovane istituzione, per l'evidente legame tra le due prime fasi della sua esistenza.

Una rivoluzione pacifica

La pacifica rivoluzione della *privacy* è cominciata l'8 maggio del 1997, con l'entrata in vigore della legge n. 675 del 1996 che ha finalmente attribuito a ciascuno il potere di governo delle informazioni che lo riguardano. Da allora è proseguita senza soluzioni di continuità, con una complessa costruzione che sappiamo destinata a non essere mai interamente compiuta, immersi come siamo in una ininterrotta dinamica tecnologica e sociale che ci mostra un avvenire sempre mutevole. Siamo entrati in un nuovo mondo, di cui non è possibile definire una volta per tutte i contorni, ma le cui caratteristiche via via emergenti il Garante ha sempre segnalato, con una capacità di anticipazione confermata dai fatti. Il nostro è davvero un cantiere sempre aperto, al quale ogni giorno si aggiungono nuovi materiali. Basta ricordare, tra i nostri ultimi interventi, quelli riguardanti la legge della Regione Toscana sulle elezioni primarie e la possibilità di sottrarsi a quella moderna gogna elettronica rappresentata da una perenne presenza in rete di un numero crescente di dati personali.

Tutto questo non è avvenuto all'insegna della mutevolezza, del caso, di

un inseguimento senza criterio della realtà. Mentre cresceva la consapevolezza di vivere in una situazione in perenne movimento, si faceva netta la coscienza che era necessario riferirsi a principi forti che, già indicati fin dall'articolo 1 della legge, dovevano poi vivere nel nostro lavoro e, tramite questo, venir trasmessi alla società italiana.

È stata un'impresa agevole e ardua. Agevole, perché il riconoscimento del nuovo diritto alla protezione dei dati personali ha subito destato attenzione diffusa, testimoniata dall'ininterrotto flusso di richieste rivolte al Garante. Ardua, perché più d'uno ha cercato, e cerca tuttora, di ridurre la portata della nuova disciplina, di presentarla in opposizione ad altri diritti.

Nell'attenzione della società italiana abbiamo colto un profondo bisogno di "rispetto", ed abbiamo adoperato proprio questa parola prima ancora che venisse proposta come generale criterio interpretativo da importanti ricerche sociologiche. E, partendo da questo bisogno profondo, abbiamo valorizzato il riferimento legislativo al principio di dignità, prima ancora che questo venisse collocato in apertura della Carta dei diritti fondamentali dell'Unione europea.

Non abbiamo "inventato la *privacy*", come si è detto. Abbiamo reagito ad ogni forma di riduzionismo, ispirato da interessi settoriali o da miopia culturale. Abbiamo proiettato la protezione dei dati personali in una dimensione più ricca, senza arbìtri, ma interpretando correttamente una disciplina che vuole collocata tale protezione nel quadro dei diritti e delle libertà fondamentali, legata alla tutela della dignità. Abbiamo così potuto accompagnare una progressiva presa di coscienza della società italiana e pure, possiamo dirlo con un certo orgoglio, dell'opinione pubblica europea. In Europa, infatti, siamo stati i più fermi assertori del rispetto di un diritto fondamentale che si presenta come uno dei più importanti di quest'avvio di millennio, ed abbiamo curato una informazione all'estero con una presenza diretta in diversi istituti italiani di cultura. Abbiamo dialogato con istituzioni di altri Paesi, collaborando allo sviluppo della legislazione e degli strumenti di garanzia.

Pensavamo di discutere soltanto di protezione dei dati. In realtà, ci stavamo occupando di temi che riguardano il destino delle nostre società, il loro presente e soprattutto il loro futuro. Abbiamo affrontato questioni di sicurezza interna e internazionale, di genetica e di salute, del credito e delle telecomunicazioni, del funzionamento del mercato e dell'organizzazione dell'impresa, del sistema dei *media* e del rapporto tra tecnologie e politica, della nuova dimensione della libertà personale, della libertà d'espressione e di circolazione. L'intero orizzonte dei temi di questi tempi difficili è davanti ai nostri occhi. Emerge un legame profondo tra libertà, eguaglianza, democrazia, dignità e *privacy*, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo.

Senza una forte tutela delle loro informazioni, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la *privacy* si presenta così come un elemento fondamentale della società del- l'eguaglianza. Senza una forte tutela dei dati riguardanti i loro rapporti con le istituzioni o l'appartenenza a partiti, sindacati, associazioni, movimenti, i cittadini rischiano d'essere esclusi dai processi democratici: così la *privacy* diventa una condizione

essenziale per essere inclusi nella società della partecipazione. Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale: diventa così evidente che la *privacy* è uno strumento necessario per salvaguardare la società della libertà. Senza una resistenza continua alle microviolazioni, ai controlli continui, capillari, oppressivi o invisibili che invadono la stessa vita quotidiana, ci ritroviamo nudi e deboli di fronte a poteri pubblici e privati: la *privacy* si specifica così come una componente ineliminabile della società della dignità.

La privacy è di tutti

Proprio sulla lunga frontiera della società il Garante si è fortemente impegnato anche nell'anno appena trascorso. Nel momento in cui cresceva il ricorso al credito da parte delle famiglie e dei singoli, il Garante ha risposto con un codice deontologico che rende più sicuro il trattamento dei dati raccolti in questo delicatissimo settore. Nel momento in cui il telefono fisso e mobile non è più soltanto uno strumento per la comunicazione interpersonale, ma fa di ciascuno di noi il terminale di un flusso continuo di comunicazioni sociali, il Garante è intervenuto per restituire agli utenti il pieno diritto di decidere se e quali comunicazioni ricevere, per evitare abusi delle nostre immagini attraverso i videotelefoni, per escludere usi impropri degli *sms* anche da parte di pubblici poteri. Nel momento in cui parole come *Dna* sono ormai parte del vocabolario quotidiano, il Garante ha messo a punto una autorizzazione generale per il trattamento dei dati genetici che mantiene elevato il livello di tutela di queste informazioni che, più di tutte le altre, sono rivelatrici della nostra identità, dei nostri legami biologici, persino del nostro futuro. Nel momento in cui lo stesso corpo fisico conosce un declino della sua inviolabilità, e diviene sempre più manipolabile attraverso l'impianto di elementi elettronici, il Garante ha indicato i criteri per impedire la degradazione dell'uomo a macchina, ad oggetto regolabile e controllabile a distanza. Nel momento in cui l'attenzione per un corretto trattamento dei dati personali diviene un elemento ineliminabile dell'attività economica, il Garante si è impegnato per chiarire come la *privacy*, se impone dei costi (peraltro in Italia assai più contenuti che nel resto dell'Unione europea), rappresenti pure una "risorsa" che, intelligentemente impiegata, può rendere più efficiente l'attività d'impresa.

Siamo, dunque, ben lontani da un'immagine della *privacy* come strumento a disposizione solo di gruppi ristretti. Mai come in questo momento gli interventi Garante rendono evidente che la protezione dei dati personali è davvero affare di tutti. Il codice deontologico sull'attività dei sistemi privati di informazione creditizia, appena entrato in vigore, interessa milioni di persone, così messe al riparo da forme improprie di classificazione, come "cattivo pagatore". In un incontro da noi promosso nei giorni scorsi, vari operatori sanitari, pubblici e privati, hanno potuto mettere in evidenza soluzioni innovative e a basso costo per la tutela della dignità e della riservatezza dei pazienti e, insieme, della loro salute, bene primario d'ogni persona. È ormai avviata la definizione del codice deontologico per *Internet*. Decine di milioni di persone, cioè tutti i titolari di

utenze telefoniche fisse e mobili, stanno ricevendo dalle società che gestiscono i servizi un modulo che le metterà nella condizione di stabilire se figurare o no nei nuovi elenchi, se ricevere o no pubblicità per posta o per telefono, se comparire con il nome per esteso o soltanto puntato, e via dicendo. Mai s'era svolta nel nostro Paese una consultazione di massa di queste dimensioni, dalla quale sarà possibile trarre indicazioni importanti sul modo in cui ciascuno tende a percepire se stesso nella società della comunicazione totale.

Questo bisogno di conoscenza e di consultazione ha ispirato la stessa azione del Garante che, attraverso il proprio sito, ha potuto raccogliere le opinioni dei cittadini sulle bozze di una serie di provvedimenti. Sono consultazioni ancora ristrette. Ma si tratta di un metodo che potrebbe diventare regola nelle occasioni più importanti. Continua, infatti, con intensità l'attività del Garante volta a decidere ricorsi, a trattare segnalazioni e reclami, a rispondere a quesiti, in una dimensione che fa emergere il profilo "giustiziale" della tutela. Ma diviene sempre più significativa l'attività di regolazione. Un compito, questo di particolare delicatezza perché il Garante, a differenza di altre, potrebbe essere definito autorità a "vocazione generale" per la molteplicità degli oggetti di cui si occupa, la platea dei soggetti ai quali si rivolge, la promozione di codici deontologici e l'attenzione per il loro rispetto.

Persona e informazione totale

Nella discussione pubblica su temi di tanto rilievo s'insinua un dubbio legato al rapporto che si stabilisce tra le persone e il sistema dei *media*. In una società dell'apparire, della corsa senza freni ad una qualsiasi presenza pubblica, ha ancora senso preoccuparsi di una difesa della *privacy* che pare rifiutata dai comportamenti sociali? E, allo stesso tempo, l'invadenza dei *media* non sta provocando pure una "implosione nella *privacy*", un rifugiarsi nel privato con effetti di rifiuto della comunicazione con gli altri?

Non è questa la sede per analizzare nel dettaglio questi problemi. Ma poiché toccano aspetti significativi del lavoro del Garante, o la sua stessa ragion d'essere, è opportuno mettere in evidenza almeno quegli elementi che, tratti dalla nostra esperienza, possono contribuire ad un chiarimento della questione più generale. La corsa all'apparire non cancella il bisogno di *privacy*, ma convive con esso: variando i contesti, pure persone che si esibiscono spudoratamente scoprono, di colpo, un'esigenza di riservatezza, d'intimità. Più che di fronte ad una schizofrenia sociale, siamo in presenza della rivelazione di un io diviso, che vuole godere, insieme, dei benefici della pubblicità e delle garanzie della riservatezza.

Su questo terreno impervio il Garante si è sempre avventurato, poiché gli spettava il compito non solo di arbitrare conflitti tra il sistema dell'informazione e le persone oggetto delle notizie, ma pure di cercar di ricomporre quell'io diviso, definendo soprattutto quale sia la sfera d'intimità alla quale tutti, persone "pubbliche" e gente "comune", hanno diritto. Ci siamo mossi cercando di evitare ogni tentazione censoria e la pretesa d'essere guida morale o giudici del buon gusto. Nostro riferimento è stato, anzitutto, il principio di dignità, dal quale discende l'esigenza, già ricordata, di rispetto delle persone. Possiamo dire che questa cultura sta penetrando nel sistema dell'informazione. Uno sguardo ai titoli di otto

anni fa, sulla diffusione senza remore di nomi e di immagini di protagonisti veri o supposti di vicende di cronaca, ci consente di misurare una distanza, poiché oggi molte immagini sono oscurate, molti nomi sono di fantasia, molte informazioni sono fornite in modo più sobrio.

Siamo consapevoli dei limiti della nostra azione. Non mancano le ricadute nelle abitudini del passato, soprattutto in occasione di clamorosi fatti di cronaca. Ma proprio il diffondersi della cultura della *privacy* le rende meno tollerabili da un'opinione pubblica più attenta ed esigente. Riceviamo molte richieste d'intervento, soprattutto quando le notizie riguardano i minori, quando si insiste su particolari inutili o puramente scandalistici. In molti casi siamo di fronte a violazioni che non riguardano soltanto il Codice sulla protezione dei dati personali o il codice deontologico dell'attività giornalistica, ma altre norme sulle intercettazioni o sui minori coinvolti in vicende giudiziarie, sul diritto d'autore o sul diritto al nome o all'immagine. Interveniamo sia bloccando l'ulteriore diffusione di dati illegittimamente raccolti o diffusi, sia cercando la collaborazione dei giornalisti. E, proprio grazie al buon rapporto con l'Ordine dei giornalisti, abbiamo potuto dare una serie di chiarimenti che dovrebbero rendere più agevole ed efficace l'applicazione del codice deontologico.

Un diritto di "uscita"

Ma non è solo nella società della spettacolarizzazione continua che emerge con forza il bisogno di ritirarsi dietro le quinte per riflettere, per rifiatare. Più cresce la nostra immersione nella società dell'informazione totale, più si diffondono le tecnologie dell'informazione e della comunicazione, più si amplia l'area in cui si forniscono beni e servizi in cambio di dati personali, maggiore diventa l'esigenza di precisare la posizione in cui si trova ciascuno di noi. Questo esige uno sguardo nuovo sugli strumenti giuridici disponibili, sull'utilizzazione delle stesse tecnologie come fattori di tutela della *privacy* e, in conclusione, sulla nuova dimensione costituzionale che sta emergendo.

Pensiamo all'uso delle carte di pagamento scalari, che consentono di non lasciar traccia quando si percorre un'autostrada o si telefona o si acquista un programma televisivo, così evitando sia la classificazione da parte delle società che gestiscono il servizio, sia il rischio di ulteriori controlli attraverso la conservazione dei dati raccolti. Pensiamo al diritto del cittadino di poter stabilire, almeno in parte, i contenuti delle carte elettroniche che gli vengono rilasciate, selezionando, ad esempio, quali dati sulla salute debbano comparirvi. Pensiamo alla possibilità tecnologica di disattivare completamente tutti gli apparati elettronici che già portiamo con noi, come i telefoni mobili, o che stanno entrando nella nostra vita, come le "etichette intelligenti", in modo da sottrarsi alla schiavitù della localizzazione permanente.

Si tratta, in sostanza, di poter esercitare un potere di controllo sul flusso dei nostri dati, regolandone direttamente le modalità di raccolta e di circolazione, interrompendolo quando lo riteniamo necessario e riattivandolo quando ci sembra opportuno. Questo esige una forte consapevolezza da parte degli attori di questo processo: i cittadini, messi davvero in condizione di esercitare i poteri loro attribuiti; i soggetti pubblici e privati che raccolgono informazioni, i quali devono rendersi conto del fatto che la legittimazione sociale della loro attività è destinata ad essere tanto

maggiore quanto più sarà percepita come rispettosa di questo valore fondamentale.

Alcuni dei nostri provvedimenti generali vanno proprio in questa direzione. Affrontano le ultime novità tecnologiche, come i videotelefoni e la televisione interattiva. Disciplinano una delle più diffuse forme di raccolta di dati ad opera del settore privato, quella delle "carte di fidelizzazione". In tutti questi casi, le regole hanno come fine quello di evitare forme improprie di "schedatura" degli utenti, utilizzazioni e diffusioni dei loro dati in modi non conformi alla loro volontà.

Ma non basta disciplinare più puntualmente l'attività dei raccoglitori di informazioni e insistere sul momento del consenso. Spesso, infatti, le persone scoprono che, per effetto di un consenso manifestato riempiendo un questionario o acquistando un bene o un servizio, cominciano ad arrivare sollecitazioni o messaggi non graditi. Diviene così essenziale poter revocare nel modo più semplice quel consenso dato con una certa leggerezza, per uscire dalla gabbia che si è contribuito a costruire attorno a noi stessi.

Il "diritto di uscita" si presenta così come una componente essenziale della protezione dei dati personali, come il mezzo che permette di riprendere pienamente il controllo sulla propria sfera privata. E questo esige anche una attenzione più forte per le "*privacy enhancing technologies*", per tutti quegli accorgimenti che permettono di ridurre già a livello tecnico i rischi per la *privacy*.

Il Garante ha dato più di una indicazione in questo senso. Ha stabilito, ad esempio, che le banche possano trattare impronte digitali solo in casi eccezionali e con un *software* che ne garantisca la distruzione entro pochissimi giorni, a meno che non vi siano documentate ragioni di polizia o di giustizia. Riflettiamo sul fatto che non è possibile mettere in commercio un ciclomotore o taluni giocattoli senza una certificazione che ne attesti la sicurezza. La stessa logica deve essere adottata per l'insieme delle tecnologie dell'informazione e della comunicazione, come hanno appena fatto il Garante italiano e il Gruppo dei Garanti europei segnalando ai produttori la necessità di progettare i videotelefoni e le "etichette intelligenti" in modo tale da escludere fin dall'origine alcuni rischi per la *privacy*.

Non dimentichiamo che la rivoluzione elettronica è una rivoluzione giovane e, come tutti i grandi cambiamenti tecnologici del passato, è entrata nella società con una certa prepotenza, con possibili effetti di inquinamento. Da anni si lavora per liberare l'ambiente dalle emissioni nocive, dai rumori insopportabili, dalle aggressioni alla natura, che sono stati conseguenze pesanti della prima rivoluzione industriale. È tempo che strategie analoghe vengano intraprese per cancellare le diverse forme di inquinamento dell'ambiente informativo e delle libertà civili. Diventa così evidente che non v'è contraddizione tra tecnologia e *privacy*, ma che, al contrario, vi sono forme benefiche di alleanza da incentivare in ogni modo.

Opponendosi ad ingiustificate derive tecnologiche, all'idea semplicistica e rischiosa che qualsiasi strumento nuovo possa e debba essere adottato per il solo fatto che esiste, il Garante vuol dare un contributo proprio all'uso razionale della tecnologia. Le regole sulla videosorveglianza, ad esempio, non servono soltanto ad evitarne usi che interferiscono indeb-

itamente sulle libertà delle persone. Sono anche un contributo per evitare sprechi. Agganciando la legittimità dei sistemi di videosorveglianza a serie esigenze, infatti, si può evitare quel che le cronache ci dicono, parlando di comuni che giustificano il ricorso a sistemi costosi con l'unico argomento dell'"entrata nella modernità", e che poi si trovano nella condizione di non disporre dei fondi necessari per la manutenzione e il funzionamento adeguato dei sistemi acquistati.

Accanto al diritto di uscita individuale si delinea così anche un diritto di uscita collettivo dalle strettoie e dai condizionamenti che possono essere imposti attraverso le tecnologie. La vita non deve mai divenire prigioniera della tecnica.

La costruzione elettronica della persona

Le maglie dei sistemi di controllo basati sulla continua raccolta di informazioni personali sembrano farsi sempre più strette. Si tratta di una vicenda che il Garante ha sempre analizzato e seguito nelle sue manifestazioni più significative. Possiamo ben dire d'essere stati i primi in Italia a richiamare l'attenzione su temi come la videosorveglianza, la conservazione dei dati del traffico telefonico, i dati genetici, l'inserimento nel corpo di *chip* elettronici. Allarmi ingiustificati, forzature catastrofistiche?

Quando, nella *Relazione* dell'anno scorso, richiamavamo l'attenzione proprio sui *microchip* introdotti sotto la pelle delle persone e sulle etichettature di persone e prodotti controllabili a distanza con le tecnologie delle radiofrequenze (*Rfid*), a qualcuno sembrò che il Garante si fosse avventurato sul terreno scivoloso della fantascienza. Ora, a pochi mesi di distanza, possiamo dire che la nostra previsione era approssimata per difetto. Conosciamo molte situazioni nelle quali il ricorso a quegli strumenti si avvia ad essere di uso corrente, ad esempio nel settore della salute con l'inserimento sotto la pelle di un *microchip* per l'identificazione di pazienti affetti da particolari patologie, e soprattutto con il ricorso alle "etichette intelligenti" nella distribuzione e nel commercio. E stiamo indicando i criteri generali da seguire.

Vi sono usi delle *Rfid* per sole finalità di gestione aziendale che, non implicando trattamenti di dati personali, sono esclusi dall'applicazione delle relative norme. Vi sono etichettature di prodotti che, potendo determinare un controllo sui movimenti e le utilizzazioni degli acquirenti, esigono valutazioni di proporzionalità, informative adeguate, consenso, esercizio di un "diritto di uscita" grazie alla disattivazione dell'etichetta. Vi sono impianti di *microchip* sottopelle che, potendo portare ad una modifica del corpo contrastante con la dignità della persona, devono essere in via di principio esclusi, salvo casi eccezionali di uso proporzionato a tutela della salute.

Siamo alla vigilia di un cambiamento delle natura stessa del corpo che, modificato tecnologicamente, diverrebbe per ciò post-umano? I casi appena ricordati, infatti, sono solo l'avanguardia più visibile di una larghissima serie di sperimentazioni volte ad inserire nel corpo umano strumenti elettronici e a collegarli con un *computer*.

L'"etichettatura" delle persone viene giustificata anche con l'argomento che, grazie ai controlli a distanza, alcune categorie di persone, come gli anziani, avranno migliori opportunità di essere aiutate in situazioni di emergenza. Ma possiamo affidare un numero crescente di persone solo ad

un "Angelo Custode Digitale"? Il rispetto della dignità delle persone esige che siano interrotte derive che propongono cura elettronica e determinano abbandono sociale.

Il rischio dell'impropria deriva tecnologica si manifesta anche in alcune proposte di costituzione di banche dati del *Dna*. Appare giustificata una normativa che, seguendo le indicazioni della Corte costituzionale, disciplini il prelievo di campioni genetici per finalità di giustizia in forme rispettose delle garanzie della libertà personale e della dignità. Per quanto riguarda la costituzione di banche dati del *Dna* di persone condannate, imputate o indagate, vanno però rispettati i principi di necessità, finalità e proporzionalità che, in primo luogo, richiedono un rigoroso controllo della rilevanza dei dati genetici per ciascun tipo di reato. Che senso ha il prelievo di un campione del *Dna* di un imputato o un condannato per corruzione o diffamazione?

La capacità di intercettare il futuro, inoltre, è stata mostrata dal Garante anche intervenendo sulla conservazione dei dati di traffico telefonico e sulle proposte di estendere tale conservazione a quelli riguardanti la posta elettronica e l'accesso ad *Internet*. Non sempre, però, l'importanza capitale di questo problema è adeguatamente percepita. Un esempio viene dal ricorrente dibattito sul numero eccessivo delle intercettazioni telefoniche, pur avendo queste intercettazioni alla loro origine un provvedimento del magistrato, riguardando persone indagate, essendo accompagnate da specifiche garanzie. Invece, la conservazione massiccia dei dati del traffico telefonico, ormai superiore a seicento miliardi di informazioni per le chiamate in uscita (e si conservano anche i dati riguardanti i trecento milioni di *sms* scambiati ogni giorno), viene considerata senza particolari preoccupazioni, probabilmente perché non riguarda i contenuti delle conversazioni e dei messaggi.

Ma questo è un modo ormai del tutto inadeguato di affrontare il problema, poiché quelle raccolte consentono controlli capillari di tutti i cittadini, non solo una minoranza sia pur cospicua di sospettati. E si pone comunque l'ulteriore questione di rendere più rigorose le regole di sicurezza, soprattutto quando alla gestione dei dati riguardanti le intercettazioni o il traffico telefonico contribuiscono soggetti privati.

Un nuovo quadro costituzionale

Nasce da qui la necessità di riconsiderare alcune fondamentali categorie costituzionali.

Il costante riferimento alla necessità di "rispetto dei diritti e delle libertà fondamentali" (art. 2.1 del Codice) non implica soltanto un confronto continuo tra le specifiche forme di trattamento dei dati personali ed i singoli diritti e libertà. Impone ormai una ricostruzione di libertà e diritti aderente all'ambiente tecnologico nel quale vengono esercitati. Non si può sfuggire ad alcune domande: le "formazioni sociali" (art. 2 della Costituzione) possono essere anche le comunità virtuali create nel ciberspazio? Le garanzie della libertà personale (art. 13) devono essere estese anche al corpo "elettronico", seguendo la traiettoria della rilettura dell'*habeas corpus* come *habeas data*? Qual è la portata della libertà di circolazione (art. 16) in presenza della videosorveglianza e del diffondersi delle tecniche di localizzazione? Regge la distinzione tra dati "esterni" e "interni" delle comunicazioni quando queste si svolgono su *Internet*,

modificando i termini in cui deve parlarsi della loro libertà e segretezza (art. 15)? Come si atteggiano in rete la libertà di associazione (art. 18), la stessa libertà religiosa (art. 19)? Il diritto di manifestare liberamente il proprio pensiero (art. 21) deve essere messo in rapporto con il diritto all'anonimato nelle comunicazioni elettroniche, con il diritto a respingere i controlli sulle proprie relazioni elettroniche (lo abbiamo segnalato in una lettera al Presidente del Senato)? L'accessibilità alla proprietà (art. 42.2), quando si traduce nella libera appropriabilità di determinati beni per via elettronica, secondo una logica dei *commons*, dei beni comuni, deve anche escludere l'identificazione personale dei soggetti che accedono?

Se non si procede a questa reinterpretazione e ricostruzione del quadro costituzionale, la sua capacità di garanzia ne risulterebbe gravemente menomata. Verrebbe esclusa, infatti, la tutela della persona proprio nelle situazioni che, oggi, mettono più a rischio la sua libertà e dignità.

Il Garante e l'interesse generale

Questo non è compito dei soli studiosi, di una dottrina costituzionalistica consapevole. È obbligo, in primo luogo, del legislatore e di tutti coloro che sono chiamati ad applicare norme nelle materie toccate dall'innovazione scientifica e tecnologica, dunque in primo luogo della nostra Autorità. Ma l'osservazione della realtà mostra quante siano la difficoltà di muoversi in questa direzione.

Registriamo violazioni dell'art. 154.4 del Codice per la mancata consultazione del Garante in occasione del varo di norme regolamentari e di atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice stesso. Mentre vi è buona collaborazione con la Presidenza del Consiglio, molti sono i casi di "disattenzione" ministeriale. Ed è nostro dovere segnalarli per diverse ragioni.

L'omessa consultazione del Garante produce un vizio dell'atto, che può essere impugnato e dichiarato invalido. La consultazione è stata prevista per rendere possibile la coerenza tra l'attività di governo ed il sistema della protezione dei dati personali, nel quale – è bene ricordarlo sempre – si manifesta la rilevanza di un diritto fondamentale della persona, ora esplicitamente riconosciuto in ben due articoli del Trattato per la Costituzione europea. Come abbiamo appena scritto al Presidente del Consiglio, "*nelle varie occasioni nelle quali è stata tempestivamente avviata, la consultazione ha permesso di prevenire delicati problemi applicativi nell'interesse pubblico e dei cittadini, e in un quadro di proficua collaborazione istituzionale che diversi ministeri hanno riconosciuto più volte*".

L'omessa consultazione non può essere in nessun caso giustificata con l'argomento che la richiesta di parere avrebbe ritardato l'emanazione dell'atto ministeriale. Quando è stata prospettata l'urgenza dell'intervento, il Garante è intervenuto con assoluta tempestività, addirittura esprimendo il suo parere nel giro di un paio d'ore, com'è avvenuto in occasione della ricerca telefonica dei dispersi nel Sud-est asiatico.

Abbiamo segnalato al Presidente del Consiglio "*la sequenza degli svariati decreti attuativi del sistema di monitoraggio della spesa sanitaria e di introduzione della tessera sanitaria: per diversi provvedimenti*

adottati nel 2004, i Ministeri dell'economia e delle finanze e della salute non hanno consultato il Garante", pur trattandosi di un diritto fondamentale riconosciuto dal Trattato che istituisce la Costituzione europea. Peraltro, il Garante aveva formulato critiche precise al sistema previsto dall'art. 50 della legge finanziaria 2004, perché la raccolta centralizzata dei dati ricavati dalle ricette mediche e da altre prescrizioni specialistiche rischia di compromettere la tutela dei delicatissimi dati sulla salute, oltre a comportare notevoli costi. Quelle critiche, inascoltate, sono ora confermate dai fatti e condivise da diversi ambienti.

Il tema della consultazione del Garante riveste una crescente rilevanza istituzionale in presenza di una situazione in cui si diffonde il ricorso alla tecnica delle norme attuative di provvedimenti legislativi generali. È il caso dell'ultima legge finanziaria, che prevede un centinaio di decreti attuativi, dei quali almeno un terzo incide sulla materia della protezione dei dati. Omissioni della consultazione del Garante rischierebbero di produrre un ridimensionamento della protezione dei dati in forme contrarie ai principi di legalità.

Dobbiamo poi tornare sul tema delle carte elettroniche. È giunto il momento di una ulteriore riflessione per armonizzare le iniziative in corso (carta d'identità, carta dei servizi, tessera sanitaria), per evitare che strumenti volti a migliorare i rapporti con i cittadini possano creare inutili duplicazioni e grandi banche dati centralizzate non necessarie, con una possibile diminuzione delle garanzie.

Indipendenza ed efficienza

Questo progressivo allargamento degli orizzonti non riflette una sorta di volontà di potenza del Garante, che vorrebbe signoreggiare tutte le possibili materie. Nel larghissimo spettro dei temi appena indicati si riflette l'attività quotidiana alla quale ci chiamano i cittadini, le istituzioni nazionali ed internazionali.

Il Garante non può sottrarsi a questo continuo confronto con la società. E non lo ha fatto. Il lavoro comune con il Vice Presidente Giuseppe Santaniello, con Gaetano Rasi e Mauro Paissan, e con il Segretario generale Giovanni Buttarelli, ha avuto una caratteristica meritevole d'essere sempre sottolineata: la discussione serrata, ma una vera unanimità nelle decisioni. Non è un fatto formale. Nessuno dei risultati raggiunti sarebbe stato possibile senza l'assunzione comune di responsabilità, il rispetto reciproco, l'intensità dell'impegno. Chi ha presieduto questo collegio sa che qui è la ragione vera degli esiti positivi del nostro lavoro. E vuole darne testimonianza, e dire un pubblico ringraziamento.

Lasciamo parlare i dati. Nel 2004 abbiamo deciso 731 ricorsi (609 nel 2003, 390, nel 2002), abbiamo risposto a 7.770 segnalazioni e reclami (3.796 nel 2003, 2.532 nel 2002) ed a 1.692 quesiti (786 nel 2003, 824 nel 2002). Anche le ispezioni sono cresciute, del 45%. Le questioni risolte superano le pratiche sopravvenute. L'incremento del lavoro e della produttività dell'Ufficio con picchi superiori al 100% è evidente, anche se i problemi davanti a noi chiedono che si faccia di più, e meglio.

Le valutazioni qualitative confermano l'andamento positivo. Le decisioni sui ricorsi mostrano una elevata capacità del Garante di ottenere una soddisfazione totale (50% dei casi) o parziale (19%) delle richieste già nel corso del procedimento: lavoro enorme, non traducibile in dati statis-

tici. Questa adesione all'iniziativa del Garante è confermata dal fatto che, su centinaia di decisioni, ne sono state impugnate davanti al giudice ordinario soltanto 12. Di queste, 7 sono poi state ritirate, 2 sono state respinte, 2 accolte (ma una sulla base della produzione di nuovi documenti e, per la seconda, dovrà pronunciarsi la Corte di cassazione), 1 risulta ancora in decisione. A questi dati statistici va aggiunta almeno la sottolineatura della nuova procedura per le notificazioni con impiego della firma digitale, primo caso di uso di massa di una tecnologia per produrre effetti giuridici vincolanti, che mostra quanto il Garante sia attento ad ogni uso positivo delle novità tecnologiche.

L'accettazione sociale dell'attività del Garante ci appare significativa, come la sua sintonia con le altre istituzioni. Nei quattro casi finora sottoposti alla Corte di cassazione, le decisioni sono state tutte favorevoli al Garante. Il Consiglio di Stato ha sempre dato rilievo ai nostri pareri e, nei casi di omessa richiesta, ha invitato il Governo a provvedere. Nella dimensione europea, oltre la decisione della Corte europea dei diritti dell'uomo di cui parlerò, riconoscimenti sono venuti dal Parlamento, e la Commissione europea ha appena accolto una sollecitazione da noi avanzata fin dal 1999 per nuovi criteri volti alla protezione dei dati personali anche nelle materie della cooperazione giudiziaria e di polizia.

Fiducia dei cittadini, pieno inserimento nei circuiti istituzionali nazionale e sopranazionale. Ma quali le prospettive per il futuro?

I risultati indicati sono il frutto del lavoro di un organico di appena ottantasette persone, peraltro non tutte a pieno tempo, che vogliamo qui pubblicamente e sinceramente ringraziare. Ma questa limitatezza dell'organico pesa, e rischia di pregiudicare la qualità del lavoro del Garante, la sua capacità di analizzare le tendenze e anticipare i problemi, la tenuta complessiva del suo rapporto con la società. Così come pesa l'inesorabile erosione delle sue risorse, che si sono ridotte del 20% negli ultimi quattro anni.

Non è nostro costume abbandonarsi al pessimismo. Ci conforta, anzi, il riscontrare che questa diagnosi, già prospettata l'anno scorso, sia divenuta patrimonio comune ad altre autorità e segnali un problema che né Governo, né Parlamento possono ormai eludere. Torniamo a dire che la nostra funzione di garanzia, volta ad assicurare buona qualità della vita, rappresenta un limite preciso alla possibilità di finanziarci con risorse proprie. Le garanzie non si pagano con balzelli, esigono l'attenzione della fiscalità generale.

Non chiediamo soltanto risorse. Crediamo che sia necessario salvaguardare la natura delle autorità di garanzia, consentire che possa consolidarsi e rafforzarsi un nuovo circuito istituzionale che sta disegnando nuovi equilibri tra i poteri. Il progetto di riforma costituzionale approvato dalla Camera dei deputati attribuisce rango costituzionale alle autorità indipendenti, come già aveva fatto, proprio per l'autorità per la protezione dei dati personali, il Trattato per la Costituzione europea. È troppo chiedere che le affermazioni di principio siano accompagnate dalla coerenza dei comportamenti? L'autonomia e l'indipendenza delle autorità non devono essere garantite esclusivamente nel momento della scelta dei loro componenti. Esigono il mantenimento costante delle condizioni materiali che consentono di far vivere quei valori nel lavoro d'ogni giorno.

Questo, per noi, è tanto più vero perché l'esperienza di questi anni ci

ha resi consapevoli dei limiti dell'azione passata e dei problemi per quella futura. Sappiamo che dev'essere accentuata la capacità di regolazione attraverso un dialogo sociale che coinvolga tutti gli interessati: ma questa è attività costosa e intellettualmente impegnativa. È necessario allargare l'attività di ispezione, non per una volontà repressiva, ma perché sono i cittadini ad esigere un rigoroso rispetto delle norme da parte dei soggetti che utilizzano i loro dati. Dobbiamo mantenere una forte e qualificata presenza internazionale, non solo per rimanere in una posizione di avanguardia faticosamente costruita, ma per non escluderci da un circuito di conoscenze e di riflessioni essenziali anche per la qualità del lavoro interno.

Un valore fondamentale

Proprio dall'Europa ci giungono significative conferme della giustezza del cammino da noi intrapreso. L'11 gennaio di quest'anno la Corte europea dei diritti dell'uomo, nel caso *Sciacca* v. *Italia*, ha condannato il nostro paese per l'illegittima diffusione delle foto segnaletiche di una persona ad opera delle forse di polizia. Si tratta di una decisione che conferma un orientamento da noi sempre sostenuto, ritenuto di particolare importanza perché contribuisce a definire le modalità dei rapporti tra lo Stato e i cittadini, ai quali è dovuto rispetto in qualsiasi situazione. Non esistono posizioni di supremazia o di privilegio che possano giustificare la mortificazione della dignità. La vicenda in sé può apparire minore, ma il valore di principio della decisione è grandissimo.

Il 27 luglio 2004, con la sentenza del caso *Sidabras* v. *Lithuania*, la stessa Corte ha dato una interpretazione assai estensiva del diritto alla *privacy*, previsto dall'art. 8 della Convenzione europea dei diritti dell'uomo. Ha ritenuto, infatti, che la tutela prevista da questo articolo si estenda fino a comprendere il diritto di ciascuno a sviluppare relazioni sociali al riparo da ogni forma di discriminazione o stigmatizzazione sociale, così consentendogli anche il pieno godimento della sua vita privata. È la complessiva collocazione della persona nella società che viene presa in considerazione, intendendosi il pieno rispetto della *privacy* come condizione per l'eguaglianza e il godimento di diritti fondamentali, come quello al lavoro.

Né letture anguste della disciplina della protezione dei dati, dunque, né sue interpretazioni riduttive sono ormai ammissibili. Essa si presenta come il tramite necessario perché possa trovare concretizzazione un insieme di valori fondamentali che, riconosciuti in via di principio, debbono poi accompagnare la persona in ogni momento della sua vita. In questo senso, la protezione dei dati personali diviene un valore in sé, sintetizza le prerogative della persona, contribuisce a costruire la nuova cittadinanza e a definire le caratteristiche di un sistema politico-istituzionale. Le decisioni appena citate, infatti, individuano nella *privacy* un ineludibile criterio di valutazione dell'esercizio del potere pubblico e privato, in piena sintonia con la logica della Carta dei diritti fondamentali dell'Unione europea, che ha appunto costruito la protezione dei dati personali come un autonomo diritto fondamentale.

È soltanto un uomo trasparente, flessibile, controllato, mitridatizzato, quello che incontriamo alla fine, provvisoria, di questo cammino? O pure una persona munita di nuovi poteri, sempre più consapevole, un soggetto

sociale rafforzato anche dalla presenza di una autorità che lo affianca?

Sappiamo che libertà e diritti sono, insieme, forti e fragilissimi. Vivono non nelle forme giuridiche alle quali sono affidati, ma nella capacità di uomini e istituzioni di dare ad essi attuazione, di difenderli contro insidie e attacchi ai quali sono incessantemente esposti. Abbiamo costruito la nostra autorità con questo spirito e questi intenti. Speriamo che possano durare nel tempo.

Impaginazione e stampa a cura della
Archimedia Comunicazione soc. coop a r.l.
via Tuscolana 680, 00181 roma
archi.media@flashnet.it
aprile 2005