Ministero della
Funzione Pubblica

Direttiva del 9 Febbraio 2005

Decreto legislativo 30 giugno 2003
n. 196 – Tutela della Privacy

Soft.Com

Indice generale

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 istituzionali. 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 presupposti 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 d.P.R. 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, d.l. 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, d.l. 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 d.l. 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 ed 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 5).

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[1], 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 divieto 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[2] 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

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 amministrativa, 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 d.P.R. 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 contenenti 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 Dlgs. 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 Dlgs. n. 135/1999 ed in linea con l'orientamento interpretativo espresso al riguardo dalla giurisprudenza amministrativa (C.d.S., 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" (C.d.S. Sez. VI, 30 marzo 2001, n. 1882 e 9 maggio 2002, n. 2542; cfr. anche C.d.S. Sez. V, 31 dicembre 2003, n. 9276).[3]

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 pertinenza, 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