Commento D.lgs. 196/2003
(articolo per articolo)

di
Michele Iaselli

ART. 1

Il codice si apre con questa chiara enunciazione di principio la cui portata generale e' inequivocabile. La definizione di dato personale e' poi successivamente riportata all'art. 4 (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) mutuata da quella contenuta nell'art. 2 della legge 675/96. La finalita' di tale disposizione appare evidente: i dati personali vanno tutelati sempre indipendentemente dalla loro comunicazione e diffusione, dalla possibilita' stessa della lesione del valore sociale dell'individuo. Bisogna, quindi, fare riferimento a qualsiasi attivita' che abbia per oggetto i dati personali posta in essere nel territorio dello Stato con o senza l'ausilio di mezzi elettronici o automatizzati.

ART. 2

Il primo comma di tale disposizione riproduce quasi fedelmente l'art. 1 comma 1 della legge 675/96 in quanto si preferisce non distinguere piu' fra persone fisiche e persone giuridiche ma parlare genericamente di "interessato". In questo modo, per la verita', il comma in esame si discosta leggermente sia dall'art. 1 della Convenzione del Consiglio d'Europa n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale adottata a Strasburgo il 28 gennaio 1981 che dall'art. 1 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio datata 24 ottobre 1995. Difatti entrambi i documenti fanno riferimento alla tutela dei diritti e delle liberta' fondamentali delle "persone fisiche" utilizzando quindi un'espressione sicuramente piu' restrittiva rispetto al codice italiano.

Del tutto nuovo e' il 2° comma di quest'art. 2 che introduce anche in un settore cosi' delicato come la privacy quei concetti di semplificazione, armonizzazione ed efficacia propri della legge sulla trasparenza (legge 241/90) con particolare riguardo all'esercizio dei diritti da parte degli interessati ed all'adempimento degli obblighi da parte dei titolari del trattamento.

ART. 3

Anche quest'art. 3 del codice non ha precedenti ed avuto riferimento al trattamento informatico dei dati personali sancisce il principio della necessita' di identificare l'interessato solo in casi eccezionali laddove non sia possibile perseguire determinate finalita' in altri modi meno invasivi.

Sin da quando sono stati affrontati i primi problemi di privacy gli studiosi si sono posti il problema della necessita' o meno di una specifica tutela avuto riguardo al rapporto tra "riservatezza-computer"; l'impiego dell'elaboratore elettronico, infatti, consente di impadronirsi ed archiviare informazioni che riguardano l'individuo, comprese quelle della sua vita privata sottoponendolo, cosi', ad una nuova forma di dominio, che si potrebbe chiamare "*il potere informatico*". Il "*right to privacy*" ha quindi acquistato un nuovo significato ed una nuova ampiezza, che non poteva avere un secolo fa: questo ora consiste nel diritto, riconosciuto al cittadino, *di esercitare anche un controllo sull'uso dei propri dati personali inseriti in un archivio elettronico* (FROSINI).

Anch'esso fa parte del "*diritto all'informazione*", in quanto espressione del diritto di informarsi sul proprio conto e di poter disporre dei dati informatizzati, di cui e' in possesso il gestore di un elaboratore

elettronico; piu' correttamente puo' parlarsi di "*liberta' informatica*" intesa come una nuova manifestazione del tradizionale diritto alla liberta' personale; che si aggiunge a quelle del diritto di disporre liberamente del proprio corpo, di esprimere liberamente il proprio pensiero.

Il diritto alla riservatezza, per effetto della nuova dimensione acquisita, non viene, infatti, piu' inteso in un senso puramente negativo, come facolta' di ripulsa delle intromissioni di estranei nella vita privata, o di rifiutare il consenso alla diffusione di informazioni sul proprio conto, di rinuncia alla partecipazione nella vita sociale; ma in senso positivo, come affermazione della liberta' e dignita' della persona, e come potere di limitare il potere informatico, controllandone i mezzi ed i fini di quel potere (FROSINI).

ART. 4

L'art. 4 comprende una vasta serie di definizioni dei termini chiave del codice. Le definizioni di cui al 1° comma sono in larga parte quelle contenute nell'art. 1, comma 2, della legge 675/96 tranne quella di "dati identificativi" contenuta nell'art. 10, comma 5, d.lgs. 30 luglio 1999, n. 281; quella di "dati sensibili" contenuta nell'art. 22, comma 1, della legge

675/96; quella di “dati giudiziari” contenuta nell’art. 24, comma 1, della legge 675/96; quella di “incaricati” contenuta nell’art. 19 della legge 675/96.

Il 2° comma dell’art. 4 riporta, invece, definizioni legate alla importante realta’ delle reti telematiche o di comunicazione elettronica compresa Internet, che sono state mutuate da importanti provvedimenti di carattere comunitario quali la direttiva n. 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) e la direttiva n. 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

Le definizioni di cui al comma 3 sono invece legate alla problematica della sicurezza informatica e si ritrovano in larga parte nell’art. 1 del D.P.R. n. 318 del 28 luglio 1999.

Le definizioni contenute nel comma 4 hanno riferimento, invece, alle finalita’ di studio o di indagine che potrebbero comportare un trattamento di dati personali e si ritrovano nell’ art. 1, comma 2, del d.lgs. n. 281/1999.

Tale tecnica legislativa contraddistinta dalla rappresentazione di una nutrita serie di

definizioni (caratteristica dell'ordinamento angloamericano, ripresa successivamente in ambito comunitario e importata solo in un secondo momento nell'ordinamento interno) e' ormai frequentemente adottata, specie nel caso in cui la legge disciplina settori nel cui ambito viene utilizzato un linguaggio tecnicizzato ovvero nel caso in cui la legge intervenga a disciplinare materie nuove, in relazione alle quali non esista una terminologia univocamente accettata, e consente di superare numerosi problemi ermeneutici.

ART. 5

Tale disposizione assume particolare rilevanza in considerazione del fatto che la materia del trattamento dei dati personali pone spesso problemi di concorso di normative e, conseguentemente, evidenzia la necessita' della determinazione della legge applicabile a tale trattamento, in quanto molteplici possono essere i collegamenti territoriali di tale attivita'. E' opportuno, quindi, adottare dei criteri di determinazione dell'ambito di applicazione spaziale delle leggi sul trattamento dei dati personali.

Il 1° comma dell'art. in esame unisce le disposizioni degli artt. 2 comma 1 e 6 comma 1 della legge 675/96 e sostiene una prospettiva del

tutto territoriale prevedendo che debba rimanere assoggettato ala legge italiana chiunque compia nel territorio dello Stato attivita' che concretino un "trattamento" di dati personali.

Il 2° comma di quest'art. 5 riprendendo le disposizioni di cui agli artt. 2, commi 1 bis, e 1 ter, della l. n. 675/1996 prevede (estendendola) l'applicazione della normativa anche a quei soggetti che hanno sede fuori dall'Unione Europea, ma che utilizzano mezzi localizzati sul territorio italiano per il trattamento dei dati personali come ad esempio le multinazionali americane presenti in Italia. Si ricorda che tali disposizioni furono introdotte dal d.lgs. n. 467/2001 (in particolare l'art. 1 che ando' ad integrare l'art. 2 della legge 675/96).

Il 3° comma della disposizione in esame riprende quanto determinato dall'art. 3 della legge 675/96 e secondo la dottrina (FRANCESCHELLI) questo comma puo' essere interpretato in due diversi modi: o come un'eccezione di fronte a un sistema articolato di protezione della riservatezza informatica e dell'identita' personale o come espressione di un principio generale del nostro ordinamento di protezione delle liberta' fondamentali, della dignita' delle persone fisiche, della riservatezza e dell'identita' personale.

ART. 6

La disposizione in esame e' stata resa necessaria dalla particolare organizzazione sistematica del codice che e' diviso in tre parti: la prima dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato; la seconda e' la parte speciale dedicata a specifici settori: questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori; la terza affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

ART. 7

L'art. 7 del T.U. introduce il Titolo II che disciplina i diritti dell'interessato. In particolare si fa riferimento al diritto di accesso ai dati personali ed agli altri diritti connessi, riprendendo le prescrizioni dell'art. 13 comma 1 della legge 675/96. La dottrina

(RISTUCCIA) ha sottolineato gia' da tempo come l'espressione "diritti dell'interessato" enfatizzi particolarmente la natura di diritto soggettivo delle pretese che l'interessato vanta nei confronti di chi tratta dati che lo riguardano. Il primo diritto che si legge nella disposizione e' quello di avere *conferma dell'esistenza o meno di dati personali anche se non ancora registrati e la loro comunicazione in forma intellegibile*, distinguendosi in cio' da quanto prescritto dalla legge 675/96 che sebbene conteneva disposizione analoga all'art. 13, 1° co., lett. c) punto 1 (prima parte), essa era collocata sistematicamente in ordine successivo, mentre l'art. 13 si apriva riconoscendo il diritto dell'interessato ad accedere al registro dei trattamenti, diritto questo che non viene menzionato nel nuovo art. 7 del T.U.

Particolari problemi di comprensione si sono posti in dottrina sulla natura del diritto di opposizione di cui all'art. 4 lett. a) della disposizione in esame in quanto non risulta prima facie la portata dei risultati che attraverso la previsione normativa l'interessato e' in grado di raggiungere, ne' e' chiaro quale sia la posizione giuridica del titolare rispetto all'opposizione. Appare, innanzitutto evidente che ci si trova di fronte ad un trattamento pienamente legittimo dei dati (la stessa direttiva comunitaria n. 95/46CE

affronta l’argomento in modo analogo riconoscendo l’esistenza di un interesse legittimo/pubblico di chi tratta i dati ed un interesse della persona a cui i dati si riferiscono). Probabilmente secondo la dottrina dominante l’opposizione di cui all’art. 7 lett. a) rappresenta lo strumento nel diritto interno per effettuare la ponderazione degli interessi prevista dalla disciplina comunitaria nei casi di trattamento senza preventivo consenso.

ART. 8

La disposizione in esame si apre con una enunciazione di principio circa la concreta modalita’ di esercizio dei diritti di cui all’art. 7 che non ritroviamo nella legge 675/96, bensi’ nell’art. 13 della direttiva 95/46CE e nell’art. 17, 1° comma, del D.P.R. n. 501/98 (specifico regolamento recante norme per l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali).

Il 2° comma dell’art. 8 riproduce fedelmente (con qualche integrazione) l’art. 14, comma 1, della legge 675/96 fissando alcuni limiti all’esercizio dei diritti dell’interessato cosi’ come previsti dal precedente art. 7, in relazione a determinate specie di trattamenti di dati. Detti limiti, il cui fondamento va rintracciato nella previsione

dell'art. 9, par. 3 della Convenzione di Strasburgo n. 108/81 sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale, si giustificano in relazione alle particolari caratteristiche dei dati presi in considerazione e delle relative finalita' di utilizzazione.

Rispetto al precedente art. 14 della legge 675/96 sono stati aggiunti in questa nuova disposizione altri due limiti, tra l'altro piuttosto prevedibili, relativi a ragioni di giustizia e per le finalita' connesse al trattamento dei dati da parte di forze di polizia.

La disposizione in esame dopo aver enumerato le ipotesi di limitazione dei diritti degli interessati si preoccupa al 3° comma di assicurare che, nelle stesse ipotesi, sia comunque garantito il rispetto delle disposizioni in materia di trattamento di dati personali. A tal fine si attribuisce al Garante, a seconda dei vari casi, il compito di effettuare gli accertamenti e controlli previsti dagli artt. 157-158-159-160 del T.U.

L'art. 8 si chiude con una precisazione che non trova precedenti e che appare pero' particolarmente opportuna in quanto, qualora ci si trovi di fronte a particolari valutazioni di carattere soggettivo che si concretino comunque in dati personali, l'esercizio dei diritti di

rettificazione ed integrazione dati di cui all'art. 7 appare piuttosto difficile se non proibitivo. In tal senso basti vedere il parere del Garante datato 11 settembre 2001 avente per oggetto una richiesta di rettifica di dati personali che costituiscono espressione del livello d'inquadramento mansionistico e retributivo del dipendente in azienda.

ART. 9

Il primo comma di questa disposizione si ispira al 3° comma dell'art. 17 del D.P.R. 501/98 ma ha una portata molto piu' ampia in quanto non si limita a sostenere che la richiesta relativa all'esercizio di un diritto dell'interessato puo' essere trasmessa mediante lettera raccomandata o telefax, ma fa esplicito riferimento alla posta elettronica, non dimenticando di ricomprendere anche ulteriori e non definite soluzioni tecnologiche.

Il 2° comma non e' altro che la fusione di due disposizioni quella di cui all'art. 13, comma 4 della legge 675/96 e quella dell'art. 17, comma 4 del D.P.R. 501/98. Secondo tale prescrizione l'interessato puo' delegare altri all'esercizio dei propri diritti, ma viene imposta la forma scritta a pena di difetto di legittimazione attiva. Il richiamo alle associazioni lascia intendere che parte significativa del disposto

normativo dipendera' dal ruolo che potranno assumere enti esponenziali degli interessi di chi subisce trattamenti di dati personali (RISTUCCIA).

Il 3° comma di quest'art. 9 trae ispirazione dal 3° comma dell'art. 13 della legge 675/96 ma ne corregge un'imprecisione molto criticata in dottrina. Difatti il vecchio art. 13 parlava di esercizio di diritti concernenti dati personali di una persona defunta da parte di *chiunque ne abbia interesse*, e giustamente molti autori (CONTE, GUERRA, BUTTARELLI) hanno sempre sostenuto che in tal modo il dettato normativo non risolveva i dubbi in merito all'individuazione dei soggetti legittimati all'esercizio della tutela postuma, all'ampiezza dei diritti oggetto della tutela stessa ed al delicato problema della c.d. successione nei diritti della personalita'. Il nuovo art. 9, quindi, ha corretto il tiro riconoscendo la legittimazione ad esercitare i diritti di un defunto a chi abbia un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari degne di protezione.

Il 4° ed il 5° comma della disposizione in esame, invece, riprendono rispettivamente l'art. 17, comma 2 del D.P.R. 501/98 e l'art. 13, comma 1, lettera c) punto 1 (secondo periodo) della legge 675/96.

ART. 10

L'articolo in esame disciplina il riscontro all'interessato e riprende molte prescrizioni contenute nell'art. 17 del D.P.R. 501/98.

Il primo comma, ad esempio, riproduce piuttosto fedelmente il comma 9 dell'art. 17 del D.P.R. 501/98, mentre il 2° comma riproduce il 6° comma dello stesso art. 17 con espliciti riferimenti ai nuovi strumenti elettronici e telematici che consentono un'agevole visione o trasmissione dei dati di interesse.

Anche il 3° comma di quest' art. 10 riprende una disposizione dell'art. 17 del D.P.R. 501/98 e per la precisione il 5° comma avendo cura di sottolineare che il riscontro all'interessato sia comprensivo di tutti i dati personali comunque trattati, facendo salva l'applicazione dell'art. 84 del T.U. nel caso la richiesta sia rivolta ad un esercente la professione sanitaria.

I commi 4, 5 e 6 della disposizione in esame, invece, non hanno riferimenti normativi e si preoccupano principalmente di assicurare una comunicazione intelligibile e quindi comprensiva dei dati mediante l'utilizzo di una grafia comprensibile e anche attraverso l'esibizione e la consegna in copia di atti e documenti di interesse.

Il 7° comma affronta un argomento gia' disciplinato sia dall'art. 13, comma 2, della

legge 675/96 che dall'art. 17, comma 7, del D.P.R. 501/98 e cioe' la previsione di un contributo spese di entita' limitata qualora non risulti confermata l'esistenza di dati che riguardino l'interessato. In effetti il problema che si e' sempre posto la dottrina e' un altro, anche se strettamente collegato all'argomento in questione, e cioe' se l'esercizio dei diritti dell'interessato debba essere gratuito o oneroso. La dottrina dominante (IMPERALI RIC. E ROS.) propende per la gratuita', ma esiste qualche perplessita' specie avuto riferimento all'integrazione od opposizione ad un trattamento in se' legittimo.

Anche l'8° ed il 9° comma disciplinano il contributo spese in questione traendo spunto rispettivamente dai commi 7 ed 8 dell'art. 17 del D.P.R. 501/98. In particolare si fa riferimento alle modalita' di corresponsione del contributo (comma 9) ed alla determinazione dell'entita' del contributo da parte del Garante con un provvedimento di carattere generale, specie avuto riferimento ai casi in cui i dati personali figurino su uno speciale supporto di cui si richiede la riproduzione o comunque quando le relative richieste siano particolarmente complesse (comma 8).

ART. 11

Il 1° comma della disposizione in esame nello specificare le modalita' del trattamento ed i requisiti dei dati personali riproduce integralmente il 1° comma dell'art. 9 della legge 675/96. L'art. 5 della Convenzione di Strasburgo del 28/1/81 costituisce un sicuro precedente del comma in argomento. Sin da allora, difatti, si delineano chiaramente le regole cui e' soggetto il trattamento, nonche' gli specifici requisiti che i dati personali devono possedere. La disposizione si ispira anche all'art. 6 della Direttiva 95/46/CE il quale, riprendendo il ventottesimo *Considerando*, dispone tutta una serie di regole relative al trattamento e alla qualita' dei dati personali.

Il 2° comma, invece, rappresenta un'innovazione e tende a puntualizzare (ma per la verita' la precisazione appare inopportuna, in quanto piuttosto ovvia e ridondante) l'impossibilita' di utilizzare quei dati personali trattati in violazione della normativa vigente.

ART. 12

Il primo comma di quest'art. 12 riprende quanto disposto dall'art. 31, comma 1, lett. h) della legge 675/96. Ma naturalmente in questa nuova sede la previsione dei codici di deontologia e buona condotta assume tutt'altra rilevanza ed e' oggetto di una disposizione autonoma, mentre

nella precedente legge rientrava semplicemente nell'elencazione dei compiti del Garante.

Indubbiamente la maggiore rilevanza di tali codici e' dovuta al d.lgs. n. 467/2001 che all'art. 20 li ha introdotti allo scopo di disciplinare il trattamento dei dati personali in determinati settori quali Internet, il marketing, il campo previdenziale, i sistemi informativi adottando un modello gia' sperimentato per il passato in altri campi, come quello giornalistico. L'intento e' quello di pubblicare questi codici di autodisciplina sulla Gazzetta Ufficiale al fine di dotare gli stessi di una specifica forza prescrittiva e poter garantire: la trasparenza, la riservatezza, il corretto uso dei dati che viaggiano nella rete ricorrendo a degli strumenti elastici, in grado di adeguarsi rapidamente alle nuove esigenze dell'epoca attuale. Difatti questi codici saranno elaborati direttamente dalle parti interessate e quindi dagli utenti, dai consumatori, che potranno cosi' difendersi dal pericolo derivante dall'uso improprio delle informazioni, dalle frodi, dalle violazioni di legge.

Il 2° ed il 3° comma della disposizione in esame si ispirano, quindi, all'art. 20 del d.lgs. n. 467/2001 rispettivamente al 4° e 3° comma, mentre l'ultimo comma prevede solo l'estensione della disciplina generale al codice di deontologia per

i trattamenti di dati per finalita' giornalistiche.

ART. 13

Quest'articolo disciplina l'obbligo dei responsabili del trattamento di informare preventivamente l'interessato o la persona della quale sono raccolti i dati personali circa: le finalita' e le modalita' del trattamento dei dati, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto di rispondere, i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, il diritto di accesso dell'interessato ed i diritti connessi, le generalita' del titolare ed eventualmente del responsabile. L'intera disposizione riproduce, anche se con qualche modifica, l'art. 10 della legge 675/96 ad eccezione del 3° comma che prevede la facolta' per il Garante di individuare delle modalita' semplificate per l'informativa fornita dai servizi telefonici di assistenza o di informazione. Altro precedente della disposizione in esame e' rappresentato dall'art. 10 della Direttiva 95/46/CE che fissa le informazioni minime che devono essere fornite all'interessato al momento della raccolta. La Direttiva, inoltre, prevede una tipica clausola di proporzionalita' che rapporta le eventuali ulteriori informazioni

all’esigenza di assicurare un “trattamento leale”.

Il principio generale enunciato in quest’articolo 13 rientra nella tendenza a legificare gli obblighi di informazione. Esso e’ posto nell’evidente intento di consentire all’interessato l’espressione di un “consenso informato” al trattamento. Infatti solo disponendo preventivamente delle informazioni elencate nell’articolo e’ possibile valutare se prestare il consenso (ZENO-ZENCOVICH). Tale principio e’ oggetto di una delle prime decisioni del Garante datata 28/05/97 in merito al contenzioso Adusbef/BNL dove viene sancito che l’informativa deve essere completa e analitica al fine di consentire all’interessato di conoscere i vari aspetti del trattamento e prestare un consenso informato. Ma il Garante e’ tornato sull’argomento diverse volte, basti pensare alla decisione del 16 maggio 2002 dove nell’esaminare l’ipotesi dell'avvenuta inserzione in un sito web, da parte di una societa’ di sviluppo fotografico, di alcune fotografie originariamente ricevute da alcuni fotonegozianti, ha ribadito l'applicabilita’ della legge n. 675/1996 anche alle immagini fotografiche, affrontando le connesse problematiche in tema d’informativa sul trattamento dei dati oppure alla decisione del 19 febbraio 2002 dove il Garante chiarisce che se

nel corso di un’investigazione privata alcuni dati personali vengano acquisiti direttamente dall'interessato (mediante ascolto, registrazione e intercettazione), l’agenzia investigativa che procede all'indagine deve fornire all'interessato medesimo l’informativa prevista dalla legge.

ART. 14

La disposizione in esame non e’ altro che una fedele riproduzione dell’art. 17 della legge 675/96. Essa non ha un testuale precedente nella Convenzione di Strasburgo del 1981, sebbene sia sostenibile che un principio simile possa essere ricavato dall’art. 5 della medesima Convenzione, il quale impone che i dati personali vadano elaborati “lealmente e legalmente” (BELLAVISTA).
Un immediato ed esplicito riferimento a tale disposizione va invece rintracciato nell’art. 15 della Direttiva 95/46/CE. La norma comunitaria parte dal riconoscimento del diritto della persona “di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalita’, quali il rendimento professionale, il credito, l’affidabilita’, il comportamento, ecc.” Poi al par. 2 concede agli Stati membri la facolta’ di disporre che una

persona possa essere sottoposta ad una tale decisione, ma solo in casi eccezionali.

Il primo comma di quest'art. 14 assume un'importanza ed un significato particolare tenuto conto delle potenzialita' notevoli delle tecnologie informatiche che possono consentire la costruzione automatica di profili individuali e collettivi nonche' l'affidamento a procedure automatizzate di determinate decisioni sul conto dei soggetti interessati. Difatti, nell'attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalita'. Su tale presupposto puo' essere facilmente ricostruita la c.d. *persona elettronica* attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto.

Allo stato attuale sono evidenti, quindi, sia il timore che la semplificazione delle procedure e la dimensione globale delle reti informatiche possano tradursi in un appiattimento e svuotamento dei diritti delle persone fisiche e giuridiche, sia la consapevolezza della oggettiva utilita' di tali strumenti che trascendono l'ambito nazionale sia la necessita' di armonizzare quei diritti con la realizzazione di interessi pubblici e collettivi, dando

attuazione, anche nel nostro ordinamento, alle applicazioni comunitarie in materia.

Il 2° comma della disposizione in esame considera il caso in cui una decisione, implicante la "valutazione del comportamento umano", sia "unicamente" fondata su un "trattamento automatizzato di dati personali volto a definire il profilo o la personalita' dell'interessato". Essa, quindi, riguarda l'ipotesi della presa di decisioni sulla base di profili automatizzati. Non e' detto che la stessa decisione debba essere anch'essa automatizzata, e' sufficiente che la base di essa sia costituita da un trattamento automatizzato. Pertanto, il campo di azione dell'enunciato e' estremamente ampio (BELLAVISTA).

ART. 15

Il 1° comma di quest'articolo riproduce in maniera fedele l'art. 18 della legge 675/96.

Il tema della responsabilita' civile per i danni procurati dal trattamento di dati personali non e' esplicitamente affrontato nella Convenzione di Strasburgo. Mentre la Direttiva 95/46/CE dedica all'argomento della responsabilita' l'art. 23 il quale sancisce che "*Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il*

diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento". Inoltre specifica al 2° comma che "*il responsabile del trattamento puo' essere esonerato in tutto o in parte da tale responsabilita' se prova che l'evento dannoso non gli e' imputabile*".

Secondo la dottrina dominante (SICA) la regola risarcitoria contenuta in quest'art. 15 e' da considerare applicabile anche ai danni conseguenti al trattamento dei *manual data*.

Tanto in sede comunitaria quanto in quella nazionale, e' stato ben chiaro che i rischi maggiori sono connessi all'uso "tecnologico" dei dati, ma, valutato che l'angolo visuale e', in ultima analisi, il valore della riservatezza e dei diritti della personalita', e' prevalsa la posizione che la tutela della privacy debba estendersi a tutte le specie di dati personali. Certo, non puo' negarsi che la prevalente portata dell'art. 18 e' da ricondurre al trattamento automatizzato dei dati (SICA).

Anche il 2° comma di quest'art. 15 riprende una disposizione della legge 675/96 e per la precisione l'art. 29, comma 9.

La formulazione di questo comma implicitamente rimanda all'annosa questione relativa alla categoria del danno non patrimoniale. E' noto, difatti, che le frequenti dispute dottrinali

hanno riguardato la nozione in se' di "danno non patrimoniale". Secondo taluni essa viene a coincidere con la sofferenza psico-fisica del soggetto e meglio vi si attaglia la definizione di danno morale (SCOGNAMIGLIO), ma non manca chi tende a circoscrivere nell'area del danno morale i pregiudizi non suscettibili di valutazione economica mediante criteri obiettivi (BUSNELLI). Non bisogna dimenticare, inoltre, un altro indirizzo dottrinale che determina, in negativo, la figura del danno non patrimoniale, facendola coincidere con una serie di fenomeni eterogenei accomunati dalla non patrimonialita' dell'interesse leso o dalla non valutabilita' in denaro della lesione (DE CUPIS).

E' plausibile, comunque, affermare che tale disposizione finisce per contenere una sorta di principio di "*indemnisation* integrale del danno non patrimoniale da trattamento dei dati personali" (SICA). Invero, e' difficile scorgere una fattispecie che resti fuori dalla previsione dell'art. 11 e, dunque, non rilevi, ai fini riparatori, come violazione di detto articolo.

ART. 16

La disposizione in esame riproduce nei suoi due commi il 2° ed il 3° comma dell'art. 16 della legge 675/96. Non trova precedenti nella Convenzione di Strasburgo ed anche la Direttiva comunitaria 95/46/CE non prevede specificamente

l'ipotesi di cessazione del trattamento di dati ma sancisce all'art. 6 lett. b) ed al 28° *Considerando* il principio di "finalita'", che rappresenta una delle regole fondamentali in materia di trattamento dei dati personali, e rispetto al quale il disposto dell'art. 16 rappresenta un corollario (TASSONI).

Benche' la rubrica dell'articolo in esame sia limitata alla cessazione del trattamento dei dati il 2° comma prescrive una sanzione generale per i casi di cessione illecita dei dati, indipendentemente dal fatto che essa violi le norme in tema di cessazione o, invece, altre disposizioni di legge in materia di trattamento dei dati.

Lascia perplessi il fatto che l'articolo in esame non abbia riprodotto ne' fatto riferimento all'obbligo di notifica preventiva al Garante (in caso di cessazione dell'attivita' di trattamento) contenuto invece nel 1° comma dell'art. 16 della legge 675/96. Forse tale omissione si giustifica in quanto il suddetto obbligo puo' essere considerato implicito nella previsione del compito del Garante di cui all'art. 154 del T.U. lett. a) laddove parla di controllo sul fatto che *i trattamenti siano effettuati nel rispetto della disciplina applicabile ed in conformita' alla notificazione, anche in caso di loro cessazione*.

Ritengo, pero', che una previsione esplicita

sarebbe stata sicuramente piu' chiara senza pericolo di inutili ridondanze.

ART. 17

La disposizione in esame nel disciplinare il trattamento di dati diversi da quelli sensibili e giudiziari che presenta rischi specifici, riprende l'art. 24-bis della legge 675/96 riproducendo sostanzialmente entrambi i commi. L'art. 24-bis venne introdotto dall'art. 9 del d.lgs. n. 467/2001 e la relativa previsione si ispira (devo dire molto liberamente) all'art. 20 della Direttiva 95/46/CE il quale prevede che "*gli Stati membri precisano i trattamenti che potenzialmente presentano rischi specifici per i diritti e le liberta' delle persone e provvedono a che tali trattamenti siano esaminati prima della loro messa in opera*". Al 2° comma la disposizione sancisce che tali esami preliminari "*sono effettuati dall'autorita' di controllo una volta ricevuta la notificazione del responsabile del trattamento, oppure dalla persona incaricata della protezione dei dati che, nei casi dubbi, deve consultare l'autorita' di controllo medesima*".

ART. 18

La disposizione in esame al 2° ed al 3° comma riprende i principi contenuti nel 1° comma dell'art. 27 della legge 675/96, mentre riguardo la comunicazione e diffusione dei dati personali

da e a soggetti pubblici fa rinvio all'art. 25 del T.U. (5° comma). Il 4° comma di quest'art. 18 si limita a precisare che al di fuori di quanto stabilito nella parte II in ambito sanitario, i soggetti pubblici non devono richiedere il consenso dell'interessato.

L'analisi delle disposizioni normative di carattere sovranazionale e comunitario relative al trattamento dei dati personali da parte di soggetti pubblici deve necessariamente prendere le mosse dall'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle liberta' fondamentali firmata a Roma il 4 novembre 1950 e ratificata con legge 4 agosto 1955, n. 848. Tale norma prevede espressamente al comma 2 che non possa aversi interferenza di una autorita' pubblica nell'esercizio del diritto di ogni persona al rispetto della propria vita privata, a meno che questa ingerenza sia prevista dalla legge e costituisca una misura necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle liberta' degli altri (TRAVAGLINI). Questi principi sono stati integralmente recepiti dalla Convenzione di Strasburgo che pero' non prevede alcun regime particolare in relazione alla

elaborazione dei dati personali da parte della pubblica autorita'. Anche la Direttiva n. 95/46/CE non prevede un generale regime "ad hoc" in relazione al trattamento dei dati da parte della pubblica autorita'. In realta' le disposizioni della Direttiva risultano integralmente e direttamente applicabili al trattamento dei dati effettuato dalle autorita' pubbliche, con le sole eccezioni espressamente stabilite nella stessa Direttiva, prima fra tutte quella costituita dalla facolta' per gli Stati membri di escludere l'applicazione delle disposizioni della Direttiva ai soli trattamenti in ambito pubblico necessari alla salvaguardia di particolari interessi qualificati quali le attivita' attinenti alla pubblica sicurezza, alla difesa, alla sicurezza dello Stato o alle attivita' dello Stato in materia penale (art. 13).

La norma in esame specie nella parte in cui consente il trattamento dei dati personali da parte dei soggetti pubblici soltanto per lo svolgimento di funzioni istituzionali (2° comma) e nei presupposti e limiti stabiliti dal codice, dalla legge e dai regolamenti (3° comma), invita ad alcune riflessioni.

Difatti, tenuto conto di cio' che si intende per "trattamento" ne consegue che, avendo l'art. 15, comma 2, della legge n. 59/1997 attribuito

validita' e rilevanza giuridica agli "atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici...", lo svolgimento di attivita' giuridicamente rilevanti, da parte della P.A., comporta l'applicazione della disposizione di cui sopra anche in tema di formazione, conservazione e trasmissione dei documenti informatici e, quindi, di trattamento dei dati personali in essi contenuti (COCCO).

Ne dovrebbe discendere, come corollario, che le modalita' di trattamento dei dati, ovverosia con, o senza, l'ausilio di mezzi elettronici, da parte della P.A., sono indifferenti ai fini dell'individuazione degli obblighi imposti e delle facolta' riconosciute dal legislatore alla medesima P.A. qualora il trattamento in parola sia finalizzato allo svolgimento delle funzioni istituzionali e questo avvenga, ovviamente, nei limiti stabiliti dalla legge e dai regolamenti.

E' indubbio comunque che nella disposizione in esame il legislatore ha finalizzato il trattamento dei dati al principio di competenza, operando una scelta che sottolinea il carattere strumentale ed autonomo del trattamento dei dati rispetto allo svolgimento di funzioni di interesse pubblico.

L'ambito di applicazione di quest'art. 18 e la sua reale portata sono stati chiariti dal Garante

(ovviamente con riferimento all'allora art. 27 della legge 675/96) con taluni provvedimenti come il parere reso il 13 febbraio 1998 su richiesta del Consiglio Nazionale dell'Economia e del Lavoro dove ha precisato che la prima condizione per l'applicabilita' del regime speciale previsto dalla norma e' che il trattamento sia svolto da un soggetto pubblico, oppure il parere del 13 novembre 1997 (reso su richiesta dell'Azienda di Stato per gli interventi nel mercato agricolo) dove il Garante ha individuato con esattezza il contenuto della disciplina di cui all'art. in esame (TRAVAGLINI).

ART. 19

La disposizione in esame si ispira anch'essa all'art. 27 della legge 675/96 ma a differenza di quest'ultimo articolo parla esplicitamente di "dati diversi da quelli sensibili e giudiziari". Al 1° comma, quindi, riprendendo il principio gia' enunciato all'art. 18 2° comma, aggiunge che il trattamento di tali dati e' consentito anche in mancanza di una norma di legge o regolamento che lo preveda espressamente, spingendosi piu' in la' di quanto prevedeva la legislazione precedente.

Il 2° ed il 3° comma di quest'art. 19, invece, disciplinano le fattispecie di comunicazioni di dati da parte di un soggetto pubblico ad altro soggetto pubblico e da parte di un soggetto

pubblico a privati o enti pubblici economici riproducendo rispettivamente il 2° ed il 3° comma dell'art. 27 della legge 675/96.

Queste disposizioni hanno fatto sollevare in dottrina (ma si sono verificati anche casi concreti) il problema dell'interconnessione delle banche di dati pubblici con anche il rischio di perdita e distruzione dei dati stessi.

Difatti questo problema assume una specifica connotazione per quanto concerne la comunicazione e la diffusione dei dati fra soggetti pubblici e fra questi e i soggetti privati, tenuto conto che la Rete Unitaria della P.A. (la cui piena funzionalita' e' ancora lontana) ha per suo precipuo scopo e obiettivo finale proprio la condivisione, attraverso lo scambio, dei dati posseduti dalla P.A..

Per quanto concerne il primo profilo, rientrante nel secondo comma dell'art. 19, per lo scambio di dati fra soggetti pubblici, che dovra' essere enormemente facilitato dall'entrata a regime della Rete Unitaria, non si dovrebbero verificare problemi di particolare criticita', in quanto la Rete si configura come una rete interna virtuale, che collega tra loro le reti delle singole Amministrazioni e che sara' rigorosamente preclusa - almeno per quanto concerne lo stato attuale delle conoscenze tecnologiche - all'accesso indesiderato dei terzi estranei alla

P.A. Il problema e' che la RUPA stenta a decollare ed allo stato attuale sono solo 35 le amministrazioni pubbliche e gli enti attualmente collegati. Per non parlare, poi, delle effettive funzionalita', difatti, la percentuale di servizi offerti on line e' solo del 5%.

Ancora piu' delicato si presenta il secondo profilo, quello, cioe', della comunicazione e della diffusione dei dati da parte di soggetti pubblici a privati (comma 3 dell'articolo 19): ulteriore obiettivo, questo, ormai, non solo della RUPA, ma dell'intero progetto di e-government o per meglio dire del piano di azione varato dal Consiglio dei Ministri il 22 giugno 2000 su iniziativa del Ministro della Funzione Pubblica, Franco Bassanini.

Tale piano, difatti, ha come suo obiettivo fondamentale quello di garantire ai cittadini l'accesso on-line a tutti i servizi erogati dalle pubbliche amministrazioni nell'ottica di quella che dovrebbe essere la nuova frontiera di Internet.

E' evidente che l'apertura degli apparati nei confronti di soggetti privati che, per definizione, non operano per lo svolgimento di una funzione istituzionale, anche se, talora, vi cooperano come condizione necessaria di svolgimento da parte delle Pubbliche Amministrazioni aumenta, di certo, il rischio di

distruzione, perdita o, comunque, di trattamento dei dati che costituiscono oggetto di comunicazione o diffusione.

Cio' nondimeno, deve ritenersi che l'esercizio di un diritto, costituzionalmente garantito (art.3, comma 2, della Costituzione), da parte del cittadino, da attuarsi anche mediante l'accesso controllato a determinate informazioni circolanti su e attraverso la Rete Unitaria o qualsiasi altra Rete pubblica, non puo' essere vanificato dall'esigenza che venga assicurata la riservatezza dei suoi dati; ne' cio' puo' impedire, o pregiudicare, il diritto, prima ancora del dovere, all'efficienza, efficacia dell'attivita' svolta dalla Pubblica Amministrazione, fatta salva l'adozione, da parte di quest'ultima, di piu' rigorose misure di sicurezza, da attuarsi anche con il ricorso a meticolose verifiche periodiche sia delle procedure informatiche che della completezza e dell'esattezza dei dati trattati, nonche' con il rigoroso contenimento dei trattamenti nei limiti normativamente previsti, in modo, cioe', non eccedente rispetto agli obblighi e ai compiti attribuiti alla Pubblica Amministrazione medesima (COCCO).

Si tratta, per come e' evidente, di un contesto normativo alquanto rigido, la cui attuazione, se realizzata con una interpretazione ancorata al

dato letterale, puo' procurare serio intralcio al complesso dei servizi che potranno essere resi dalla P.A. e dai privati mediante l'uso massiccio delle nuove tecnologie dell'informazione: e' questa una sfida di civilta' che viene lanciata all'attuale ordinamento dall'uso diffuso delle moderne tecnologie, che del resto costituisce il presupposto fondamentale per avviare quel grande processo di innovazione tecnologica che sta coinvolgendo tutto il sistema pubblico italiano al fine di metterlo cosi' sullo stesso piano rispetto a quello di altri paesi piu' progrediti nelle nuove tecnologie della comunicazione, (si pensi, ad esempio, al nuovo sistema pubblico di connettivita', inteso dal Ministro per l'Innovazione e le tecnologie come la naturale evoluzione della Rete Unitaria, che collega le Pubbliche Amministrazioni Centrali alle quali potranno ricongiungersi le P.A. Locali).

In questa ottica l'interconnessione delle banche di dati pubblici puo' addirittura favorire la tutela del cittadino poiche' assicura meglio il cd. principio della pertinenza in quanto e' possibile raccogliere all'occorrenza il dato che serve e non creare inutilmente basi di dati in piu' Amministrazioni.

ART. 20

La disposizione in esame, nel dettare i principi applicabili al trattamento dei dati sensibili da

parte dei soggetti pubblici riprende i principi gia' enunciati al comma 3 e comma 3-bis dell'art. 22 della legge 675/96.

Il primo comma di quest'articolo 20 riproduce (anche se non vengono esclusi gli enti pubblici economici) il 3° comma, 1° periodo dell'art. 22 della legge 675/96, mentre il 3° comma dell'art. 20 riproduce il 2° periodo del 3° comma dell'art. 22, legge 675/96.

Il 2° comma dell'art. in esame, invece, si ispira al comma 3-bis dell'art. 22, legge 675/96 come il 4° comma.

La necessita' di tutelare il "nocciolo duro" della riservatezza e' stata costante fin dalle prime normative nazionali ed e' stata recepita dalla Convenzione del Consiglio d'Europa all'art. 6. La Direttiva 95/46/CE all'art. 8 disciplina in dettaglio i "trattamenti riguardanti categorie particolari di dati". Esso affronta tre aspetti: i dati che rivelano origini razziali ed etniche, opinioni politiche, religiose e filosofiche, l'appartenenza sindacale, lo stato di salute e la vita sessuale; i dati che riguardano, piu' specificamente, lo stato di salute; i dati sulle infrazioni e condanne penali.

Uno dei problemi di maggiore rilevanza legati all'applicazione della normativa sulla privacy nel campo della Pubblica Amministrazione e' sicuramente rappresentato dalla gestione

illegittima della grande maggioranza dei dati sensibili da parte degli Uffici Pubblici. In realta' tutte le Amministrazioni avrebbero dovuto gia' da tempo emanare dei provvedimenti dai quali risultassero la tipologia dei dati sensibili trattati e l'uso specifico.

Il problema sta diventando particolarmente delicato, anche per le evidenti conseguenze in campo telematico, specialmente adesso che con l'emanazione della direttiva per la conoscenza e l'uso del dominio internet ".gov.it" e l'efficace interazione del portale nazionale "italia.gov.it" con le pubbliche amministrazioni e le loro diramazioni territoriali, la presenza della P.A. in Rete, nella prospettiva di una revisione di tutti i siti Internet degli organi pubblici allo scopo di renderli piu' vicini ai cittadini, principalmente avuto riferimento all'interattivita', sta diventando una realta' tangibile. E le recenti notizie non sono confortanti, visto che il Garante per la protezione dei dati personali, nell'effettuare un'indagine a campione su determinati siti web, al fine di elaborare il codice di deontologia e di buona condotta riguardante il trattamento dei dati personali effettuato nell'ambito dei servizi di comunicazione e informazione offerti per via telematica e in particolare nella rete *web*, ha accertato che piu' del 90% dei siti esaminati non

rispettano le prescrizioni della legge sulla privacy.

Nonostante, quindi, le ripetute raccomandazioni del Garante (l'ultima risale al 17 gennaio 2002, ai sensi dell'art. 31, comma 1, lett. *m*), della legge n. 675/1996), come era logico prevedere, gli Uffici pubblici sono in difficolta', specie avuto riferimento ai dati sensibili. Il problema e' divenuto particolarmente serio, anche perche' la complessita' della normativa, continuamente integrata e modificata nel corso degli anni, ha creato difficolta' interpretative anche al Garante ed alla Presidenza del Consiglio, che, riguardo la natura giuridica dei provvedimenti da porre in essere per la corretta applicazione della legge sulla privacy, hanno discusso sull'opportunita' di emanare un regolamento (secondo l'Autorita') o un atto amministrativo (secondo la Presidenza del Consiglio), ed alla fine ha prevalso la linea del Garante come risulta dal 2° comma della disposizione in esame.

I dati sensibili come e' noto sono quei dati che hanno una particolare capacita' di incidere sulla riservatezza dei singoli individui e di determinare discriminazioni sociali particolarmente odiose (si tratta, in particolare, di quei dati che sono 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, lo stato di salute e la vita sessuale di una persona).

Il Garante per i dati personali, ha sempre dedicato particolare attenzione ai dati sensibili, e sin dall'inizio ha adottato, in merito agli stessi, sei "Autorizzazioni generali" emanate in prima applicazione nel novembre e nel dicembre 1997 e reiterate alla scadenza sempre con scadenza annuale.

Le autorizzazioni toccano i seguenti settori:

1. trattamento di dati sensibili nei rapporti di lavoro;
2. trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale;
3. trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni;
4. trattamento dei dati sensibili da parte dei liberi professionisti;
5. trattamento dei dati sensibili da parte di "diverse categorie di titolari";
6. trattamento di alcuni dati sensibili da parte degli investigatori privati.

ART. 21

La disposizione in esame ripete al 1° comma con esplicito riferimento ai dati giudiziari lo stesso

principio contenuto nell'art. 20, 1° comma (relativo ai dati sensibili). Lo stesso 2° comma rinvia all'art. 20 commi 2 e 4. Appare, quindi, evidente la volonta' del legislatore di dedicare un articolo specifico ai dati giudiziari seppur molti principi siano analoghi ai dati sensibili.
Del resto anche la Convenzione europea n. 108/81, all'art. 6, individuava tra le categorie speciali di dati quella riguardante i dati personali relativi a condanne penali, stabilendo che gli stessi non potessero essere elaborati automaticamente, a meno che il diritto interno prevedesse delle garanzie appropriate. La suddetta indicazione è stata riproposta nella Direttiva 95/46/CE all'art. 8, comma 5 la quale dispone che "*i trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza possono essere effettuati solo sotto controllo dell'autorita' pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che possono essere fissate dallo Stato membro in base ad una disposizione nazionale che preveda garanzie appropriate e specifiche. Tuttavia un registro completo delle condanne penali puo' essere tenuto solo sotto il controllo dell'autorita' pubblica. Gli Stati membri possono prevedere che i trattamenti di dati riguardanti sanzioni amministrative o procedimenti civili*

siano ugualmente effettuati sotto controllo dell'autorita' pubblica".

La stessa legge 675/96 all'art. 24 dedicava una norma specifica anche se con riferimento esplicito ai dati personali idonei a rivelare provvedimenti di cui all'art. 686, commi 1, lettere a) e d), 2 e 3 del cod. proc. pen.

ART. 22

La disposizione in esame detta in maniera piu' particolareggiata la disciplina applicabile al trattamento dei dati sensibili e giudiziari (questa volta considerati insieme). La norma trae ispirazione in tutti i suoi 12 commi dal d.lgs. n. 135/99 (ad eccezione del comma 8 che vietando la diffusione dei dati idonei a rivelare lo stato di salute, riprende l'art. 23, comma 4 della legge 675/96), in particolare dagli artt. 2, 3 e 4.

In effetti considerato che l'operativita' del "vecchio" art. 22 della legge 675/96 nella sua versione originaria era subordinata alla presenza di una normativa specifica che in realta' all'epoca non esisteva, e' stato, in seguito, emanato il d.lgs. n. 135 del 1999, che oltre a concedere piu' tempo agli uffici pubblici, si e' assunto anche il compito di indicare in quali settori ed a quali condizioni potevano essere trattati i dati sensibili sempre a condizione di specificare i tipi di dati oggetto di trattamento, le operazioni eseguibili, e le

rilevanti finalita' di interesse pubblico perseguite. Obiettivo, questo, rispettato con gli articoli da 6 a 23 del decreto citato. Con una prima ricognizione, che dovra' essere completata con successivi decreti (in parte gia' emanati come il d.lgs. n. 281 del 30/07/99, il d.lgs. n. 282 del 30/07/99 e il d.lgs. n. 467 del 28/12/2001), il Governo, in realta', ha concesso il via libera agli uffici pubblici per i dati sensibili utilizzati, per esempio, a fini statistici o di rapporti di lavoro o ancora elettorali, fiscali, di immigrazione. Fermo restando la possibilita' per i soggetti pubblici di richiedere al Garante, in attesa di piu' specifici provvedimenti normativi, l'individuazione di attivita', tra quelle demandate agli stessi soggetti pubblici dalla legge, che perseguono rilevanti finalita' di interesse pubblico e per le quali e' conseguentemente autorizzato, il trattamento dei dati sensibili.

Il problema e' che secondo quanto sottolineato dal Garante nella relazione del 2001, "*anche nell'anno 2001, gli atti adottati in tal senso dalle amministrazioni sono risultati, purtroppo, in numero assolutamente esiguo e non privi di gravi difetti, lacune ed errori, tanto da giustificare la considerazione che varie disposizioni del d.lgs. n. 135/1999 sono rimaste*

sostanzialmente inapplicate e che diversi trattamenti di dati personali effettuati in ambito pubblico sono proseguiti in modo illecito, dal punto di vista formale e sostanziale" e purtroppo la situazione non e' cambiata affatto per il 2002.

Nell'ultima raccomandazione del 17 gennaio 2002 il Garante ha cercato di sgomberare il campo da possibili equivoci segnalando al Governo la necessita' di conformare alle disposizioni vigenti il trattamento di tali dati da parte dei soggetti pubblici e fornendo alle amministrazioni interessate specifiche indicazioni sulle attivita' che debbono essere prontamente intraprese a tale scopo.

In particolare, secondo il Garante, l'individuazione dei tipi di dati sensibili e giudiziari e delle operazioni di trattamento, che diversi soggetti pubblici non hanno definito nelle forme previste dai rispettivi ordinamenti, non rappresenta un mero adempimento formale di ricognizione di prassi esistenti. Trattasi, invece, di un provvedimento che deve attuare con effetti innovativi i principi vincolanti affermati in proposito dal d.lgs. n. 135/1999 (artt. 2-4), al fine di ridefinire su basi piu' rispettose dei diritti della personalita' una serie di trattamenti legati alle finalita' di

rilevante interesse pubblico enumerate dal decreto legislativo.

Lo stesso Garante nella raccomandazione in esame suggerisce la struttura del provvedimento, avuto riferimento alle operazioni di trattamento dei dati sensibili. Si potrebbe, quindi, operare la seguente suddivisione:

a) indicando un primo gruppo di operazioni *standard*, che puo' essere comune a piu' tipologie di dati, ma che deve comunque rispondere al principio di stretta necessita' (raccolta, conservazione, cancellazione, ecc.);
b) ponendo altresi' in maggiore evidenza le operazioni che possono spiegare effetti piu' significativi per l'interessato (es., elaborazione, selezione, raffronto);
c) aggiungendo una descrizione sintetica dei flussi di dati (specificando ad es. dove sono raccolti di regola i dati, le eventuali interconnessioni o consultazioni da parte di altre amministrazioni, ecc.).

Un altro grande settore dove assume una particolare rilevanza la tutela dei diritti della personalita' rispetto alla P.A. e' senz'altro rappresentato dalle banche dati. In effetti, la materia della costituzione di grandi banche dati pubbliche ha registrato di recente un forte sviluppo. Il ricorso ad archivi di grandi dimensioni continua a presentare vantaggi sul

piano dell'efficienza dell'attivita' amministrativa, per l'elevato numero di informazioni che vi sono detenute e per le piu' agevoli interconnessioni che possono operarsi. Per altro verso, tale tendenza alimenta elementi di preoccupazione per i cittadini e induce l'Autorita' Garante a rivolgere una particolare attenzione al fenomeno, per valutare l'incidenza degli effetti delle nuove tecnologie sui diritti fondamentali della personalita'.

Tale problematica si pone in maniera evidente riguardo alle banche dati che possono essere disponibili anche in rete (e con l'avvento di Internet questa e' ormai una realta' concreta). La loro esistenza, infatti, sottintende l'accesso ai dati personali ed il loro trattamento per varie finalita', il che puo' comportare, senza una disciplina ad hoc dell'intera materia, gravi lesioni del diritto alla privacy.

La odierna qualificazione della societa' contemporanea come societa' dell'informazione individua, con assoluta precisione, la tendenza ad identificare ciascun individuo in quell'insieme di informazioni (quindi di dati personali) che lo distinguono rispetto a tutti gli altri consociati. Se queste sono le prospettive future della vita sociale, e' indispensabile che il mondo giuridico fornisca ad ogni soggetto gli strumenti sufficientemente

raffinati e flessibili per consentirgli un'adeguata tutela ed una completa garanzia.

Proprio per questo motivo la privacy, come categoria giuridica, si caratterizza, nella futuribile societa' tecnologica, come quello strumento fondamentale che garantisce una protezione della persona veloce e sicura.

Oggi le potenziali aggressioni del diritto all'identita' personale non provengono esclusivamente da atti, fisici o immateriali, che comportano un'invasione della propria sfera privata. L'evoluzione tecnologica, infatti, se da un lato ha reso sempre piu' semplici ed accessibili i meccanismi attraverso i quali la pretesa di solitudine dell'individuo tende ad essere compressa, dall'altro ha offerto forme di protezione e di prevenzione dalle intrusioni indesiderate che consentono di risolvere o quanto meno di attenuare in radice questo fenomeno. Cosicche' diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo rispetto alle tante informazioni di carattere personale che altri possano aver assunto (MAGLIO).

ART. 23

L'art. in esame riproduce ai primi tre commi l'art. 11 della legge 675/96, mentre il 4° comma

relativo ai dati sensibili si ispira all'art. 22, comma 3 della legge 675/96. Tale ultimo comma precisando che il consenso al trattamento dei dati sensibili e giudiziari e' manifestato in forma scritta, come gia' previsto nella norma generale sul trattamento dei dati sensibili (art. 26, comma 1) e' dettato da quella esigenza propria del T.U. di razionalizzare e coordinare al meglio la materia.

In generale, a prescindere da specifiche normative, la tutela accordata dall'ordinamento giuridico alla propria immagine, al proprio nome, alla propria identita', al segreto epistolare e telefonico impone di ritenere, per analogia, vietata la diffusione senza consenso di notizie della vita privata la cui pubblica conoscenza non sia di alcuna utilita' sociale.

Con l'avvento della normativa sulla privacy e' stato sancito che il trattamento di dati personali da parte di privati o di enti pubblici economici e' ammesso solo con il consenso espresso dell'interessato.

Il consenso e' validamente prestato solo se e' espresso liberamente e in forma specifica. E' necessario inoltre che l'interessato o la persona della quale sono raccolti i dati personali sia stata previamente informata per iscritto circa: le finalita' e le modalita' del trattamento dei dati, la natura obbligatoria o facoltativa del

conferimento dei dati, le conseguenze di un eventuale rifiuto di rispondere, i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, il diritto di accesso dell'interessato ed i diritti connessi, le generalita' del titolare ed eventualmente del responsabile.

L'obbligo di informazione non comprende il trattamento di dati personali effettuato da soggetti pubblici per finalita' di difesa o di sicurezza dello Stato, o di prevenzione, accertamento o repressione dei reati in base ad espresse disposizioni di legge che prevedono specificamente il trattamento ovvero da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge per esclusive finalita' inerenti la politica monetaria e valutaria, il sistema dei pagamenti, il controllo degli intermediari e dei mercati creditizi e finanziari nonche' la tutela della loro stabilita'.

In quest'ottica bisogna riconoscere che la disposizione in esame chiarisce meglio, anche in accoglimento di quanto espressamente richiesto in sede di parere dalla Commissione giustizia del Senato, che il consenso al trattamento dei dati personali deve essere "*espresso liberamente e specificamente in riferimento al trattamento chiaramente individuato,*" e non solo reso "in

forma specifica", in linea con quanto richiesto dalla direttiva europea (art. 2, par. 1, lett. h, dir. n. 95/46/CE).

In effetti a livello europeo la Convenzione di Strasburgo del 1981 non prende posizione sul tema del consenso, mentre la Direttiva comunitaria di riferimento n. 95/46/CE inserisce il requisito del consenso tra le ipotesi di legittimita' del trattamento dei dati tassativamente elencate (art. 7).

Sicuramente negli ultimi tempi il requisito del consenso ha assunto un significato particolare in quanto, come gia' si e' avuto modo di sottolineare, con l'avvento delle tecnologie informatiche il "*right to privacy*" ha acquistato un nuovo significato ed una nuova ampiezza, che non poteva avere un secolo fa: questo ora consiste nel diritto, riconosciuto al cittadino, *di esercitare anche un controllo sull'uso dei propri dati personali inseriti in un archivio elettronico* (FROSINI).

Anch'esso fa parte del "*diritto all'informazione*", in quanto espressione del *diritto di informarsi sul proprio conto e di poter disporre dei dati informatizzati, di cui e' in possesso il gestore di un elaboratore elettronico*; piu' correttamente puo' parlarsi di "*liberta' informatica*" intesa come *una nuova manifestazione del tradizionale diritto alla*

liberta' personale; che si aggiunge a quelle del diritto di disporre liberamente del proprio corpo, di esprimere liberamente il proprio pensiero.

Il diritto alla riservatezza, per effetto della nuova dimensione acquisita, non viene, infatti, piu' inteso in un senso puramente negativo, come facolta' di ripulsa delle intromissioni di estranei nella vita privata, o di rifiutare il consenso alla diffusione di informazioni sul proprio conto, di rinuncia alla partecipazione nella vita sociale; ma in senso positivo, come affermazione della liberta' e dignita' della persona, e come potere di limitare il potere informatico, controllandone i mezzi ed i fini di quel potere (FROSINI).

Il consenso apparentemente rappresenta l'espressione piu' compiuta di quella liberta' positiva di controllare i dati riferiti alla propria persona ed usciti dalla propria sfera di riservatezza in cui si sostanzia la liberta' informatica intesa come diritto di autotutela della propria identita' informatica (COMANDE').

Numerosi sono stati gli interventi del Garante in materia di consenso che hanno principalmente cercato di evitare che l'applicazione concreta della normativa trasformi il consenso in un costoso principio decorativo e di facciata. Si pensi ad esempio alla decisione del 13 febbraio

1998 riferita ad una dubbia circolare della Banca Popolare dell'Alto Adige dove il Garante ha ribadito che il consenso si intende validamente prestato quando e' espresso liberamente. Diverse decisioni hanno poi sottolineato anche la genericita' delle informative riguardo sia i soggetti destinatari che le finalita' (decisione del 8 settembre 1997 relativa al caso Autogerma S.p.A. o decisione Calyx Italia S.r.l. del 15 luglio 1997).

ART. 24

La disposizione in esame nell'elencare i casi nei quali puo' essere effettuato il trattamento senza alcun consenso unifica le previsioni dell'art. 12 e dell'art. 20 della legge 675/96.

L'art. 24 fa salve le specificita' riconosciute, in alcuni casi, per la comunicazione e, soprattutto, per la diffusione dei dati (lett. c), f) e g)). La disciplina risulta ora piu' chiara, essendo state eliminate alcune duplicazioni ed apportate talune opportune precisazioni.

In particolare in relazione alle lettere a) e b), e' stato meglio specificato, in conformita' a quanto previsto dalla direttiva europea (art. 7, par. 1, lett. c), dir. 95/46/CE), il presupposto di liceita' del trattamento relativo alla sussistenza di un obbligo legale, riferita ora correttamente alla necessita' di adempiere

comunque ad un obbligo previsto dalla legge, e non piu' solo al caso di "dati raccolti e detenuti" in base al medesimo obbligo. Inoltre, in sintonia con il diritto vivente, si e' chiarito che il trattamento e' consentito quando e' comunque necessario per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato e non solo per eseguire "misure" precontrattuali su richiesta del medesimo interessato. Quest'ultimo intervento, ripetuto in maniera speculare nell'articolo 43 (gia' 28 della legge n. 675/1996), in relazione al trasferimento di dati all'estero, completa l'allineamento alla direttiva europea delle disposizioni concernenti trattamenti effettuati in relazione a rapporti precontrattuali, gia' avviato con il decreto legislativo n. 467/2001 (art. 7, par. 1, lett. b), dir. 95/46/CE).

Alla lettera e), si e' chiarito che il presupposto di liceita' del trattamento riferito all'esigenza di salvaguardare la vita o l'incolumita' di un terzo e' comunque applicabile anche fuori dei precedenti casi in cui veniva specificato che l'interessato non puo', per incapacita' o altri motivi, prestare il proprio consenso. Inoltre, in relazione al caso in cui la medesima finalita' riguardi la vita o l'incolumita' dell'interessato, la disciplina e' stata allineata a quella vigente in ambito

sanitario in relazione al trattamento di dati idonei a rivelare lo stato di salute per finalita' di cura della persona, che in base alle disposizioni previgenti risultava piu' rigorosa rispetto a quella del trattamento di dati comuni o sensibili effettuato da soggetti diversi da quelli sanitari. La disciplina prevede, ora, che anche in questi ultimi casi, se manca il consenso della persona incapace o altrimenti impossibilitata a prestarlo e' necessario acquisire il consenso dei prossimi congiunti o familiari, e si puo' procedere al trattamento dei dati personali dell'interessato solo se sia impossibile acquisire anche il consenso di tali soggetti o vi e' rischio grave ed imminente per la salute della persona, purche' il consenso sia acquisito successivamente (art. 82, comma 2).

La disposizione in esame ha anche soppresso l'ormai inutile riferimento specifico alla comunicazione effettuata nell'ambito di gruppi bancari o fra societa' controllate o collegate, in quanto la disposizione era legata al generalizzato sistema delle notificazioni di trattamenti correlati che il codice ha sostanzialmente eliminato (cfr. art. 37 – *Notificazione del trattamento*). La medesima esigenza, peraltro, puo' essere comunque efficacemente soddisfatta in applicazione dell'istituto del bilanciamento degli interessi

del titolare con i diritti dell'interessato (art. 24, comma 1, lett. g).

Inoltre e' stato esteso l'esonero dall'obbligo di acquisire il consenso ai trattamenti in ambito "interno" effettuati da organismi "no-profit" anche in relazione a dati comuni, in conformita' a quanto gia' previsto per i dati sensibili, a condizione che le modalita' di utilizzo dei dati siano esplicitate in un'apposita determinazione resa nota agli associati con l'informativa (analoga condizione e' stata inserita per i trattamenti di dati sensibili all'art. 26, comma 4, lett. a)).

La lettera i) reca un miglior coordinamento con la disciplina in materia di trattamenti per scopi storici, statistici o scientifici.

Per gli interventi del Garante si rimanda all'art. 23.

ART. 25

L'art. 25 riprende quei divieti di comunicazione e diffusione di dati personali gia' previsti nell'art. 21, 1° e 2° comma della legge 675/96. Il 2° comma della disposizione in esame riproduce la stessa eccezione contenuta nel 4° comma dell'art. 21 della legge 675/96 anche se non fa piu' riferimento alle finalita' di ricerca scientifica e statistica ed ai codici di deontologia e buona condotta.

La Convenzione di Strasburgo non tratta la questione della comunicazione e diffusione dei dati personali ed anche la Direttiva 95/46/CE non dedica all'argomento un'espressa disciplina. L'attivita' della comunicazione e diffusione viene comunque ricompresa (art. 2, lett. b) nel piu' generale concetto di "trattamento" e dunque soggiace alle medesime regole (ZENO-ZENCOVICH).

Il Garante e' intervenuto a piu' riprese su talune questioni connesse alla comunicazione e/o diffusione dei dati. Tra le varie decisioni vi e' quella del 16/09/97 dove ha stabilito che i dati personali concernenti le classi stipendiali, le indennita' e gli altri emolumenti corrisposti a dipendenti di concessionari di servizi pubblici sono conoscibili da chiunque vi abbia interesse. Altra decisione rilevante e' quella del 08/01/98 dove il Garante ha rilevato che la normativa sulla privacy non ha innovato la legge 441/82 sulla pubblicita' della situazione patrimoniale di titolari di cariche elettive o direttive. Interessante anche la decisione del Garante del 3 aprile 2002 dove ha ritenuto infondata l'opposizione al trattamento dei dati da parte di un interessato che lamenti la violazione delle norme che regolano la comunicazione e la diffusione dei dati personali da un soggetto pubblico ad un soggetto privato senza che risulti comprovata l'inosservanza stessa (fattispecie

concernente la pretesa erronea applicazione, da parte dell'Ufficio delle entrate, delle norme della legge 241/1990). Anche la decisione del Garante datata 20 marzo 2002 si inserisce nel ricco "filone" di decisioni relative ai rapporti tra normativa sulla privacy e legge 241/90. In questo caso l'Autorita' rileva che la semplice manifestazione, da parte del titolare del trattamento, dell'intenzione di aderire alla richiesta di accesso, ove non seguita dall'effettiva comunicazione dei dati all'interessato, comporta l'accoglimento del ricorso proposto al Garante.

ART. 26

L'art. 26 del T.U. riprende molte disposizioni contenute nel precedente art. 22 della legge 675/96. In merito si rinvia a quanto gia' sostenuto, a proposito dei dati sensibili, nel commento dell'art. 20 del T.U.

Per quanto riguarda, piu' in particolare, il trattamento dei dati sensibili, si segnalano alcuni interventi di razionalizzazione del sistema e per il pieno adeguamento della normativa alla direttiva 95/46/CE.

Anzitutto, conformemente a quanto previsto per i soggetti pubblici, si e' nuovamente ricordato che anche i soggetti privati nel trattare dati sensibili devono altresi' rispettare i

presupposti ed i limiti stabiliti dal codice, da disposizioni di legge o di regolamento.

Un importante intervento di razionalizzazione della disciplina, riguarda il trattamento di dati sensibili effettuati da confessioni religiose.

L'art. 8, par. 2, lett. d), della dir. 95/46/CE prevede che i trattamenti effettuati da associazioni o altri organismi senza scopo di lucro operanti in ambito religioso, filosofico, politico o sindacale sono consentiti anche senza il consenso degli interessati, se effettuati in base a *"garanzie adeguate"* e purche' siano utilizzati - all'"interno" degli organismi - i soli dati degli aderenti o delle persone che hanno contatti abituali con gli organismi stessi nell'ambito delle loro finalita' lecite. Il particolare regime si giustifica in ragione del fine perseguito dagli organismi (in ogni caso non di lucro) e del "limite" rappresentato dalla circolazione dei dati solo all'interno degli organismi.

Per quanto riguarda l'ambito religioso, il decreto legislativo n. 135/1999, in materia di trattamento di dati sensibili da parte di soggetti pubblici, ha dato una prima attuazione a tale disciplina in riferimento alle confessioni religiose i cui rapporti con lo Stato sono regolati da accordi o intese (art. 22, comma 1-*bis*, l. n. 675/1996, introdotto dal d. lg. n.

135/1999), "autorizzando" le stesse a trattare i dati in questione anche senza il consenso degli interessati e senza l'obbligo di rispettare l'autorizzazione del Garante, nel rispetto, tuttavia, di idonee garanzie da adottare in relazione ai trattamenti effettuati. Successivamente il decreto legislativo n. 467/2001 ha integrato il medesimo articolo 22 della legge n. 675/1996 prevedendo che tutti gli organismi senza scopo di lucro, anche a carattere religioso, possono trattare i dati sensibili senza il consenso dell'interessato, ma nel rispetto dell'autorizzazione del Garante. L'art. 26, comma 3, lett. a) del codice completa, ora, l'intervento normativo, armonizzando meglio la disciplina normativa delle confessioni religiose, anche in riferimento alla giurisprudenza costituzionale e alle garanzie di cui le medesime confessioni si dotano nel rispetto dei principi contenuti in un'autorizzazione del Garante. Un'apposita disposizione transitoria (art. 181, comma 6) consente, in ogni caso, alle confessioni religiose che, prima dell'entrata in vigore del codice, abbiano gia' determinato e adottato le garanzie richieste nell'ambito del rispettivo ordinamento, di proseguire le attivita' di trattamento nel rispetto delle medesime.

Per quanto riguarda, invece, i casi in cui il trattamento e' consentito anche senza il consenso

dell'interessato, previa autorizzazione del Garante, si evidenzia innanzitutto che la disciplina dei trattamenti effettuati da organismi senza scopo di lucro - analogamente a quanto sopra descritto in relazione al trattamento di dati comuni – e' stata adeguata ad un criterio di maggiore garanzia e trasparenza prevedendo che tali organismi individuino con espressa determinazione le modalita' di utilizzo dei dati, rendendola nota agli interessati all'atto dell'informativa (art. 26, comma 4, lett. a)). Inoltre e' stato apportato un intervento analogo a quello gia' descritto per il trattamento di dati comuni necessario per salvaguardare la vita o l'incolumita' di un terzo o dell'interessato (art, 26, comma 4, lett. b)).
In relazione al diritto di "rango pari" a quello dell'interessato - presupposto di liceita' del trattamento di dati idonei a rivelare lo stato di salute per finalita' di esercizio di un diritto – e' stato precisato, in conformita' alla giurisprudenza e al diritto vivente, che tale diritto e' relativo ad un diritto della personalita' o ad un altro diritto o liberta' fondamentale e inviolabile; tale precisazione normativa ricorre, ovviamente, in ogni altro caso in cui nel codice si fa riferimento ad un diritto di rango pari (artt. 60, 71 e 92) (art. 26, comma 4, lett. c)).

Infine, in attuazione di una specifica disposizione della direttiva europea (art. 8, par. 2, lett. b), dir. 95/46/CE), e' stato introdotto un ulteriore presupposto di liceita' del trattamento in relazione a cio' che e' necessario per adempiere a specifici obblighi previsti dalla normativa, anche comunitaria, in materia di gestione del rapporto di lavoro, nei limiti previsti dall'autorizzazione del Garante e ferme restando le disposizioni del codice di deontologia e di buona condotta (art. 26, comma 4, lett. d).

ART. 27

La disposizione in esame non fa altro che ripetere con riferimento ai privati ed agli enti pubblici economici lo stesso principio gia' enunciato all'art. 21 del T.U. a proposto dei soggetti pubblici. Anch'essa trae ispirazione dall'art. 24 della legge 675/96 ed a tal proposito si rinvia a quanto gia' sostenuto nel commento dell'art. 21 del T.U.

ART. 28

La disposizione in esame, che non trova precedenti nel nostro ordinamento, contiene una precisazione molto importante in merito ai soggetti che effettuano il trattamento dei dati personali. Infatti, rispetto alla normativa previgente, l'art. 28 chiarisce (sebbene cio' sia pacifico sul piano giuridico e dell'applicazione

pratica) che nel caso in cui il trattamento e' effettuato da una persona giuridica, da una pubblica amministrazione o da altro ente, "titolare" e' l'entita' nel suo complesso, oppure l'unita' periferica che esercita un potere decisionale autonomo sulle finalita' del trattamento, anziche' la persona fisica incardinata nell'organo o preposta all'ufficio.
Tale disposizione ha tenuto conto di alcune importanti decisioni del Garante quale quella del 9 dicembre 1997 dove a seguito di un quesito posto dalle F.S. S.p.A. sulla concreta individuazione della figura del titolare del trattamento, il Garante ha chiarito che se il trattamento e' effettuato nell'ambito di una persona giuridica di una pubblica amministrazione o di un altro organismo, il titolare e' l'entita' nel suo complesso anziche' una o piu' persone fisiche. In pari data il Garante ha affrontato un'analoga questione posta dal Ministero delle Finanze ed anche in questo caso ha concluso che non e' possibile individuare la titolarita' del trattamento nelle persone fisiche preposte ad una direzione generale o ad un'area, dovendo tale qualita' essere configurata in capo al Ministero (oppure alle complesse unita' organizzative - direzione generale o aree anche geografiche - qualora sia possibile riconoscere a queste ultime potesta' decisorie effettive e del tutto autonome

in ordine al trattamento dei dati). Resta, pero', ferma la facolta' del Ministero di designare alcuni soggetti (persone fisiche o giuridiche, enti od organismi) quali "responsabili" del trattamento, delineandone analiticamente e per iscritto i compiti attribuiti, e individuando al loro interno, se del caso, ulteriori livelli di responsabilita' in base all'organizzazione delle divisioni e degli uffici o alle tipologie di trattamenti, di archivi e di dati.

ART. 29

La disposizione in esame riproduce quasi integralmente (con qualche modifica che vedremo) l'art. 8 della legge 675/96 avuto riferimento al 1°, 2°, 3° e 4° comma.

La Convenzione di Strasburgo prevedeva un "responsabile dello schedario", ma in realta' tale figura si identifica nel soggetto che poi nella previsione della normativa sulla privacy viene individuato con l'espressione "titolare".

La Direttiva 95/46/CE individua con le espressioni "responsabile del trattamento" ed "incaricato del trattamento" le figure identificate nella normativa interna rispettivamente con i termini "titolare" e "responsabile". In realta', pero', v'e' da sottolineare che la normativa comunitaria attribuisce rilevanza ad una circostanza di mero fatto, sancendo che e' "incaricato" colui che

“elabora dati personali per conto del responsabile del trattamento”.

E’ importante sottolineare che nella disposizione in esame, per fugare ogni possibile dubbio interpretativo emerso in qualche caso, si chiarisce ancor piu’ che la nomina del responsabile e’ meramente facoltativa e compete al solo titolare. Per la verita’ gia’ in un comunicato stampa del 7 maggio 1997 il Garante aveva precisato che “la nomina di un responsabile e’ facoltativa e compete al titolare”. Inoltre con un provvedimento del 22 ottobre 1997 relativo ad un quesito posto dalla American Express, il Garante ha precisato che l’indicazione del responsabile nell’informativa all’interessato puo’ essere effettuata “con riferimento alla qualita’ rivestita pro-tempore, il che eviterebbe, in caso di avvicendamento in tale qualita’, di ripetere l’informativa”.

Nella disposizione in esame viene anche espunto il riferimento agli incaricati, ora opportunamente inserito nella disposizione che riguarda questi ultimi (art. 30).

ART. 30

L’articolo in esame disciplina in maniera specifica la figura *dell’incaricato del trattamento* traendo spunto dall’art. 8 comma 5 e dall’art. 19 della legge 675/96. La disposizione chiarisce, confermando una sperimentata prassi

applicativa considerata corretta anche dal Garante, che alla designazione espressa e specifica degli incaricati - da effettuarsi in ogni caso per iscritto e con riguardo a specifiche mansioni - e' "parificata" la preposizione della persona fisica ad una unita' organizzativa per la quale sia individuato per iscritto l'ambito del trattamento consentito agli addetti ivi preposti. Tale previsione rappresenta un'indubbia forma di semplificazione dell'adempimento per i titolari o responsabili, che tuttavia non va a detrimento della sua efficacia.

In effetti la legge 675/96 non ha mai definito il termine "incaricato" e dalle disposizioni di cui all'art. 8 e 19 e' stata sempre evidenziata l'assoluta dipendenza dell'incaricato dalle istruzioni impartite dal titolare o dal responsabile.

La Direttiva Comunitaria prevede esplicitamente la figura dell'incaricato del trattamento all'art. 17, par. 3 dove dispone che "l'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente:

- che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento;
- che gli obblighi di cui al paragrafo 1, quali sono definiti dalla legislazione dello Stato membro nel quale e' stabilito l'incaricato del trattamento, vincolino anche quest'ultimo".

ART. 31

La disposizione in esame riproduce integralmente il 1° comma dell'art. 15 della legge 675/96 e stabilisce, quindi, un principio di carattere generale inerente gli obblighi di sicurezza. In particolare viene previsto un obbligo di custodia e controllo dei dati personali oggetto di trattamento, da effettuarsi "in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento", in modo da ridurre al minimo i rischi. Se per difetto di custodia o di controllo dovesse derivare danno a terzi, chiunque abbia tenuto tale condotta, avendo realizzato un trattamento illecito, e' tenuto al risarcimento del danno cagionato in base a quanto previsto dall'art. 2050 del cod. civ. che prevede una presunzione di responsabilita' per l'evento, a meno che non venga dimostrato di avere fatto tutto il possibile per evitare l'evento dannoso stesso.

La disposizione in esame sembra essere una diretta conseguenza di quell'altro principio generale che traspare dalla normativa sulla privacy e cioe' l'interesse all'integrita' ed alla completezza dei dati. Si tratta di finalita' che dovra' essere perseguita attraverso misure tecniche ed organizzative di sicurezza che riguardano tutti gli aspetti del trattamento dei dati ed alle quali si fa rinvio al commento delle norme successive sulle misure minime di sicurezza.

La Direttiva 95/46/CE parla di sicurezza all'art. 17 dove impone agli Stati membri di disporre che "il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere".

ART. 32

L’art. in esame riguarda le particolari modalita’ di applicazione delle misure di sicurezza da parte di fornitori di servizi di comunicazione elettronica e ripropone pressoche’ integralmente, salvo per la terminologia che e’ adeguata alla direttiva 2002/58/CE, l’art. 2 del d.lgs. n. 171/1998. Per quanto riguarda il rapporto fra l’adozione delle misure di sicurezza e i relativi costi, e’ confermata la scelta effettuata con il d.lgs. n. 171/1998. La norma, infine, in attuazione di una specifica previsione della predetta direttiva 2002/58 (art. 5), prevede che le misure debbano essere adottate anche per salvaguardare l’integrita’ dei dati trattati e delle comunicazioni elettroniche contro il rischio di intercettazione o altra abusiva cognizione ed utilizzazione.

ART. 33

La disposizione in esame prende spunto dall’art. 15 comma 2 della legge 675/96 sancendo l’obbligo per i titolari del trattamento di adottare le misure minime di sicurezza previste dalla normativa. Rispetto al precedente art. 15, la disposizione in argomento individua con precisione il titolare del trattamento come destinatario fondamentale della disciplina della sicurezza. In effetti il responsabile e’ solo una figura eventuale, che ripete i propri poteri dal

titolare del trattamento, anche se la nomina e' effettuata tra soggetti che forniscano idonea garanzia del pieno rispetto delle disposizioni, ivi compreso il profilo relativo alla sicurezza.

ART. 34

La disposizione in esame che non trova specifici precedenti nella precedente normativa sulla privacy disciplina ed elenca principalmente le misure minime di sicurezza da adottare nel caso di trattamenti di dati personali effettuati con strumenti elettronici, demandando la determinazione delle modalita' di applicazione alle disposizioni contenute nel Disciplinare tecnico allegato al codice (allegato B).

Rispetto alle disposizioni contenute nel D.P.R. 28 luglio 1999, n. 318, emanato in attuazione dell'art. 15 della legge n. 675/1996, il sistema delle misure minime di sicurezza viene semplificato e aggiornato sulla base dell'esperienza applicativa degli ultimi tre anni e dell'evoluzione tecnologica.

Ai fini dell'applicazione delle misure minime richieste, si conferma la distinzione fra trattamenti effettuati con strumenti elettronici e trattamenti "cartacei".

Riguardo i primi disciplinati da tale disposizione, si evidenzia la diversa configurazione della distinzione, presente a determinati effetti nel D.P.R. 318/1999, tra

trattamenti effettuati con elaboratori non accessibili da altri elaboratori o terminali e trattamenti con elaboratori "accessibili" in rete, e, tra questi ultimi, dell'ulteriore distinzione tra l'accessibilita' attraverso reti disponibili o non disponibili al pubblico.

Non ha piu' una sua espressa rilevanza formale la figura dell'*amministratore di sistema*, mentre viene confermato l'obbligo di provvedere alla custodia di copie delle parole chiave per l'autenticazione, qualora sia tecnicamente indispensabile per garantire l'accesso ai dati in caso di impedimento di un incaricato.

Per il trattamento con strumenti elettronici si prevede l'obbligo di adottare l'autenticazione informatica dell'utente, anche mediante l'utilizzo di eventuali sistemi biometrici, e adeguate procedure di gestione delle relative credenziali di autenticazione.

Il titolare deve curare l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, la tenuta di un aggiornato documento programmatico sulla sicurezza e l'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.

A tal proposito si sottolinea che la *sicurezza* nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonche' eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

Si include, quindi, la sicurezza del cuore del sistema informativo, cioe' il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi.

Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessita' crescenti in relazione alla diffusione e agli sviluppi tecnici piu' recenti dell'elaborazione dati; in particolare per quanto riguarda i *data base, la trasmissione dati e la elaborazione a distanza (informatica distribuita).*

La sicurezza puo' essere garantita in diversi modi:

- *tramite mezzi di accesso fisici.* Questi sono consegnati all'utente legittimo ed egli esclusivamente ne viene in possesso e ne e' responsabile. Tali mezzi sono costituiti da documenti di riconoscimento tradizionali, da

chiavi meccaniche di varia forma e complessita', da *chiavi elettroniche* (c.d. tesserini magnetici di riconoscimento, carte di credito). Ciascuno di questi strumenti puo' essere considerato come una forma di legittimazione e di accesso controllato. Detti mezzi non sono, in genere, usati da soli, salvo che in ambienti poco attenti ai problemi della sicurezza. Infatti contraffazione e duplicazione sono abbastanza praticabili con tecnologie di medio livello, e quel che e' piu' pericoloso, i predetti mezzi di identificazione possono essere sottratti o ceduti a soggetti non autorizzati. Pertanto, il livello di sicurezza viene accresciuto, in alcuni casi, con la combinazione di tali strumenti con quelli di seguito indicati.

- *Tramite mezzi di accesso memorizzati dall'utente legittimo*. Essi consistono in una sequenza di elementi (numerici, alfabetici o simbolici) che vengono forniti segretamente e memorizzati dall'utente legittimo e da questo forniti al sistema al momento in cui si vuole accedere allo stesso.

  Tra i principali mezzi di accesso rientranti in questa categoria si ricordano:

  1. *Il P.I.N.* (Personal Identification Number): si tratta di un numero di identificazione personale che viene attribuito in maniera

segreta esclusivamente all'utente legittimo. Molto noto e' quello utilizzato con la carta Bancomat. Tale numero va scritto su un'apposita tastiera numerica al momento in cui si accede al computer.

2. *La Password*, ossia la c.d. "parola chiave": si tratta di una parola, o di una sequenza di lettere e numeri, anche complessa, memorizzata dall'utente legittimo e che deve essere scritta, in genere su una tastiera. Detta combinazione alfanumerica va opportunamente scritta con rapidita' per evitare che malintenzionati riescano a seguire la sequenza dei tasti premuti e a ricavare cosi', la parola chiave.
3. *La combinazione numerica-logica variabile*: in alcuni casi la parola chiave non e' fissa, ma varia dinamicamente con riferimento ad una parte di elementi fissi ed altri variabili. Per esempio, una combinazione dinamica puo' essere rappresentata dalla sommatoria di un certo numero conosciuto dall'utente, addizionato, sottratto, diviso o moltiplicato ad un altro numero che potrebbe variare con riferimento al giorno della settimana, alla data completa, ovvero ad un dato variabile.

- *Tramite mezzi di accesso che confrontano caratteristiche fisiche dell'utente con quelle memorizzate dal sistema* (i cd. sistemi biometrici). Si tratta della ricerca piu' avanzata in tema di sicurezza degli accessi informatici. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

  Tra i sistemi biometrici si ricordano:

  1. *le impronte digitali e le impronte palmari*;
  2. *il riconoscimento della voce* (difettoso in caso di malattie da raffredamento);
  3. *il reticolo venoso della retina dell'occhio*;
  4. *il controllo dinamico della firma* (con riferimento anche alla sua velocita' di esecuzione).

ART. 35

La disposizione in argomento non trova, anch'essa, specifici precedenti nella precedente normativa sulla privacy. Disciplina ed elenca principalmente le misure minime di sicurezza da adottare nel caso di trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici, demandando la determinazione delle modalita' di applicazione alle disposizioni contenute nel Disciplinare tecnico allegato al codice (allegato B).

Si tratta naturalmente di casi residuali, considerato che nell'attuale era informatica, nella maggior parte dei casi, esistono dei trattamenti automatizzati. Comunque, i trattamenti cartacei continuano ad essere in uso in molte amministrazioni pubbliche e ad essi vengono dedicate misure molto semplificate, anche al fine di evitare rilevanti aumenti di complessita' del lavoro in contesti in cui sono gia' presenti, di solito, prescrizioni o consuetudini volte ad assicurare la conservazione e la custodia dei documenti.

Particolarmente importante e' l'obbligo della conservazione degli atti in archivi ad accesso selezionato. L'allontanamento degli atti dall'archivio puo' avere luogo solo per le necessita' del trattamento. In tal caso i documenti sono affidati alla custodia dell'addetto al trattamento, che ha l'obbligo di restituirli all'archivio al termine delle operazioni affidategli.

Ad ogni modo e' opportuno precisare che laddove la limitatezza tecnologica degli strumenti in uso o la loro obsolescenza non consentano di attuare completamente il dettato normativo, si prevede l'obbligo da parte del titolare di descrivere in un documento a data certa, da custodire presso la propria struttura, gli impedimenti tecnici che hanno reso impossibile o parziale l'immediata

applicazione delle misure minime di sicurezza. Viene inoltre introdotto, in relazione alla possibile inadeguatezza di alcuni elaboratori a consentire l'applicazione delle misure minime, un termine di un anno per dare tempo ai titolari di adeguare la propria dotazione tecnologica in modo da consentire l'applicazione delle misure minime di sicurezza (art. 180).

ART. 36

L'articolo in esame prende spunto dall'art. 15, 3° comma della legge 675/96 con la fondamentale differenza rappresentata dall'esistenza di un disciplinare tecnico da aggiornare periodicamente.

Per quanto riguarda le modalita' di applicazione delle misure minime di sicurezza da adottare, sono stati apportati gli adeguamenti richiesti dalla Commissione giustizia della Camera.

In particolare, nel Disciplinare tecnico che reca tali modalita', sono state stabilite due scadenze periodiche (semestrale e annuale) per gli adempimenti a carico del titolare del trattamento e uniformate le scadenze rispondenti a finalita' omogenee (punti 14 e 15 del Disciplinare). E' stato infine determinato il termine di aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito agli incaricati (punto 27 del Disciplinare).

ART. 37

Questa disposizione disciplina la notificazione del trattamento e rivede in maniera piuttosto ampia la precedente normativa che trova il suo punto di riferimento nell'art. 7 della legge 675/96.

In effetti la disposizione in esame ed anche il successivo art. 38 completano l'intervento di semplificazione e razionalizzazione del sistema delle notificazioni gia' avviato dal decreto legislativo n. 467/2001, rivelatosi, sulla base dell'esperienza, per alcuni aspetti non indispensabile rispetto alle reali finalita' di trasparenza perseguite dalla direttiva comunitaria. Con le modifiche apportate, si snelliscono gli adempimenti in favore sia di soggetti privati, sia della pubblica amministrazione. Si prevede, infatti, l'individuazione di un elenco "in positivo" di un numero piu' ristretto di categorie di trattamenti soggetti a notificazione, modificando il precedente impianto della normativa che, com'e' noto, prevedeva un obbligo piu' ampio di effettuare la notificazione e individuava, poi, alcuni casi di esonero dall'obbligo o forme semplificate di notificazione.

Il codice, completando, come si e' detto, l'intervento normativo avviato dal d.lgs. n. 467/2001, che aveva individuato le linee generali

del nuovo sistema e demandato ad un regolamento governativo la determinazione dei casi e della modalita' della notificazione, individua in positivo le tipologie dei trattamenti oggetto di notificazione al Garante in quanto suscettibili di recare pregiudizio ai diritti e alle liberta' dell'interessato.

Si tratta, in sintesi, dei seguenti trattamenti, tutti relativi ad ambiti di particolare delicatezza:

a) dati genetici, biometrici o dati sull'ubicazione di persone od oggetti, da chiunque effettuati;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati per particolari finalita' sanitarie (a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, ecc.);
c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da organismi senza scopo di lucro;
d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalita' dell'interessato, o ad analizzare abitudini o scelte di consumo ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica, con esclusione,

pero', dei trattamenti tecnicamente indispensabili per fornire i medesimi servizi agli utenti;

e) dati sensibili registrati in banche di dati a fini di selezione del personale, ma solo nei casi in cui cio' avvenga per conto terzi, nonche' dati sensibili utilizzati per sondaggi di opinione e simili;

f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilita' economica e simili (c.d "centrali rischi").

A completamento del sistema si prevede che il Garante possa disporre con proprio provvedimento adottato in sede di controllo preliminare (art. 17), che siano soggetti a notificazione anche altri trattamenti in ragione del rischio derivante per i diritti dell'interessato.

Vari sono, inoltre, gli interventi di ulteriore semplificazione del sistema.

La disposizione in esame prevede, anzitutto, che l'Autorita' possa individuare, nell'ambito dei trattamenti individuati dalla norma e appena descritti, eventuali trattamenti non suscettibili, in concreto, di recare pregiudizio agli interessati e quindi sottratti all'obbligo di notificazione.

La notificazione potra' essere, poi, effettuata su un modello piu' snello di quello attuale,

mentre un altro significativo elemento di semplificazione e' riscontrabile nella soppressione dell'obbligo di effettuare una specifica notifica dei dati destinati all'estero (cfr. art. 43, rispetto al previgente art. 28, l. n. 675/1996).

Il titolare del trattamento, pertanto, deve provvedere alla notifica nei soli casi previsti dall'articolo in esame, con un adempimento richiesto *una tantum* (salvo, ovviamente, l'obbligo di notificare le eventuali modifiche del trattamento o la sua cessazione) e sempre con un unico atto anche quando il trattamento comporta un trasferimento di dati all'estero (comma 3).

Le notificazioni sono inserite nel registro dei trattamenti tenuto dal Garante, ove sono consultabili da chiunque con modalita' agevoli.

Infine, una norma di chiusura conferma la piena attuazione del principio di massima trasparenza dei trattamenti previsto, oltre che dalla normativa comunitaria, dalla Convenzione del Consiglio d'Europa n. 108 del 1981, prevedendo che, in ogni caso, il titolare del trattamento il quale non e' tenuto all'obbligo di notificazione ai sensi dell'art. 37, deve fornire all'interessato, ad eventuale richiesta, le notizie contenute nel modello predisposto per le

notificazioni, salvo che il trattamento riguardi registri o elenchi pubblici.

Lo stesso art. 18 della Direttiva 95/46/CE prevede al 1° comma l'obbligo della notificazione a carico del responsabile del trattamento, od eventualmente del suo rappresentante, presso l'autorita' di controllo di cui all'articolo 28, prima di procedere alla realizzazione di un trattamento, o di un insieme di trattamenti, interamente o parzialmente automatizzato, destinato al conseguimento di una o piu' finalita' correlate. Mentre al 2° comma prevede una semplificazione o l'esonero dall'obbligo di notificazione: qualora si tratti di categorie di trattamento che, in considerazione dei dati oggetto di trattamento, non siano tali da recare pregiudizio ai diritti e alle liberta' della persona interessata; qualora il responsabile del trattamento designi, conformemente alla legislazione nazionale applicabile, un incaricato della protezione dei dati, a cui e' demandato in particolare: di assicurare in maniera indipendente l'applicazione interna delle disposizioni nazionali di attuazione della direttiva e di tenere un registro dei trattamenti effettuati dal responsabile del trattamento in cui figurino le informazioni di cui all'articolo 21, paragrafo 2, della direttiva, garantendo in tal modo che il trattamento non sia tale da

recare pregiudizio ai diritti e alle liberta' della persona interessata.

ART. 38

L'articolo in esame disciplina le modalita' di notificazione e partendo dal presupposto che la notificazione e' una dichiarazione prevede per essa una determinata forma e specifiche modalita' di trasmissione:

a) deve essere rilasciata secondo il modello messo a disposizione dal Garante e contenere le informazioni in esso richieste;
b) deve essere trasmessa per via telematica, previa apposizione della firma digitale da parte del dichiarante;
c) deve rispettare le prescrizioni impartite dall'Autorita'.

E' altresi' specificato nella disposizione in esame (1° comma), sulla scorta di quanto stabilito dall'art. 7 comma 2° della precedente legge 675/96, che la notificazione deve essere effettuata in via preventiva una sola volta, indipendentemente dalla durata del trattamento, dal numero delle operazioni da svolgere e puo' riguardare non soltanto un trattamento, ma anche molteplici trattamenti, sia pure con finalita' "correlate".

Quest'art. 38 trova un suo punto di riferimento nell'art. 19 della Direttiva 95/46/CE che disciplina l'oggetto della notificazione.

ART. 39

La disposizione in argomento (che si ricollega a quanto previsto dall'art. 7 lett. e della Direttiva 95/46/CE) specifica le modalita' e gli effetti della comunicazione al Garante dei flussi di dati in ambito pubblico. La norma prevede la possibilita' di effettuare la comunicazione dei dati decorsi 45 giorni dalla comunicazione al Garante, ferma restando la possibilita' di una determinazione dell'Autorita' anche successiva all'avvio del flusso dei dati e si applica anche al trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica e sanitaria di cui all'art. 110.

ART. 40

La disposizione in esame disciplina le c.d. autorizzazioni generali (gia' previste all'art. 41, comma 7 della legge 675/96) tramite le quali l'Autorita' acconsente ad operazioni di trattamento di dati sensibili o giudiziari a determinate condizioni e per determinati fini. Nel caso in cui, invece, lo specifico trattamento che il titolare intende porre in essere non e' contemplato e autorizzato nelle menzionate autorizzazioni generali sussistera' in capo al titolare l'obbligo di sottoporre, in via preventiva rispetto all'inizio del trattamento dei dati, una dettagliata richiesta di autorizzazione al Garante tramite la compilazione

di uno specifico modulo rilasciato dall'Autorita' stessa (IMPERIALI Riccardo e Rosario).

Per consentire la rapida circolazione delle informazioni, il Garante ha rilasciato delle autorizzazioni generali per tipologie di trattamenti, con le quali sono state legittimati alcuni trattamenti di dati sensibili o giudiziari analiticamente specificati.

Si pensi ad esempio, per i dati sensibili, alle sei "Autorizzazioni generali" emanate in prima applicazione nel novembre e nel dicembre 1997 e reiterate alla scadenza sempre con scadenza annuale (le ultime produrranno i loro effetti giuridici fino al giugno del 2004).

Le autorizzazioni toccano, in particolare, i seguenti settori:

7. trattamento di dati sensibili nei rapporti di lavoro;
8. trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale;
9. trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni;
10. trattamento dei dati sensibili da parte dei liberi professionisti;
11. trattamento dei dati sensibili da parte di "diverse categorie di titolari";
12. trattamento di alcuni dati sensibili da parte degli investigatori privati.

Le Autorizzazioni generali vengono pubblicate sulla Gazzetta Ufficiale al fine di darvi massima diffusione e conoscibilita'.

ART. 41

La disposizione in esame nel disciplinare le richieste di autorizzazione riprende quanto previsto dall'art. 14 del D.P.R. n. 501/98. In effetti nessuna modifica e' intervenuta riguardo il procedimento per il rilascio delle autorizzazioni del Garante, salvo la previsione di un termine ritenuto piu' congruo per un'efficace valutazione dei trattamenti sottoposti all'esame dell'Autorita' (45 giorni). Quindi nel caso ci si trovi in una delle situazioni gia' previste ed acconsentite nelle autorizzazioni generali, il "titolare" non sara' tenuto a presentare specifica richiesta di autorizzazione al Garante (1° comma). Qualora, invece, il caso non sia stato gia' regolamentato, oppure le modalita' di trattamento siano diverse da quelle prospettate nell'Autorizzazione generale, il titolare deve sottoporre all'Autorita' una specifica richiesta di autorizzazione (comma 3). La richiesta deve essere preventiva al trattamento che si intende effettuare. Il Garante comunica la sua decisione entro 45 giorni dal ricevimento della richiesta ed in caso di mancata pronuncia entro tale termine la richiesta si intende rigettata (art. 26 comma 2° del T.U.), non essendo possibile, nel caso di

specie, applicare il principio del silenzio assenso della Pubblica Amministrazione (IMPERIALI Riccardo e Rosario).

ART. 42

La disposizione in esame non trova precedenti nella legge 675/96. Essa disciplina il trasferimento dei dati personali all'interno dell'Unione Europea e stabilisce che le disposizioni del codice non possono essere applicate in modo da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione Europea, fatta salva l'adozione, in conformita' allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati per eludere le stesse disposizioni. Una prima dottrina (ATELLI) ha interpretato la norma come una sorta di abilitazione per eventuali iniziative comunque devolute alla competenza di organismi non titolari della potesta' legislativa.

La direttiva 95/46/CE non esamina nello specifico la fattispecie in esame in quanto parte dal presupposto esplicitato al Considerando 9 che data la protezione equivalente derivante dal ravvicinamento delle legislazioni nazionali, gli Stati membri non potranno piu' ostacolare la libera circolazione tra loro di dati personali per ragioni inerenti alla tutela dei diritti e

delle liberta' delle persone fisiche, segnatamente del diritto alla vita privata.

ART. 43

La disposizione in esame disciplina i trasferimenti di dati personali consentiti in paesi terzi e riprende quanto previsto dall'art. 28, 1° comma e 4° comma della legge 675/96 (con esclusione per quest'ultimo comma della lett. g) e dall'art. 26, comma 2, della legge 675/96.

Un'importante novita' rispetto alla precedente disposizione normativa di riferimento e' comunque rappresentata da un ulteriore semplificazione del sistema del trasferimento dei dati verso paesi non appartenenti all'Unione europea, con l'esclusione dell'obbligo di notificare specificamente al Garante il trasferimento dei dati (l'obbligo e' adempiuto, *una tantum*, con l'unica notifica eventualmente dovuta ai sensi dell'art. 37) e dalla conseguente soppressione dell'obbligo di attendere il decorso del termine originariamente prima di poter procedere al trasferimento dei dati (art. 28, comma 2, l. n. 675/1996).

La disposizione in esame cerca, inoltre, di assicurare la piena simmetria della disciplina del trattamento dei dati personali effettuato a fini di trasferimento dei dati all'estero con quella relativa al trattamento sul territorio nazionale (1° comma, lett. b) e d)).

Queste novita' introdotte dal codice appaiono piu' coerenti con la stessa disciplina dettata dalla direttiva 95/46/CE che all'art. 25 sancisce il principio secondo il quale il trasferimento di dati personali da uno Stato membro verso un paese terzo puo' aver luogo "soltanto a condizione che quest'ultimo garantisca un livello di protezione adeguato". Il paragrafo 2 precisa quali sono gli elementi da prendere in considerazione per la valutazione dell'adeguatezza: si tratta di tutte le circostanze che influiscono su un trasferimento o su una categoria di trasferimenti, come la natura dei dati, le finalita' del o dei trattamenti previsti, le misure di sicurezza e le disposizioni del paese in questione; a tale proposito e' necessario esaminare le disposizioni legislative generali e settoriali del paese, unitamente alle discipline deontologiche. Nei successivi paragrafi dell'art. 25 si prevede la possibilita' per la Commissione di constatare se un paese terzo prevede o meno un livello di protezione adeguato; gli Stati membri devono adottare di conseguenza tutte le misure necessarie per conformarsi alla decisione della Commissione e, se del caso, per impedire ogni trasferimento di dati verso il paese terzo in questione. Ma in deroga a quanto disposto dall'articolo 25 il successivo art. 26 della direttiva prevede che gli Stati membri possono

disporre un trasferimento di dati personali verso un paese terzo, che non garantisce una tutela adeguata ai sensi dell'articolo 25, solo a determinate condizioni quali ad esempio quando la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure quando il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento oppure quando il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, ecc. In ogni caso il paragrafo 2 dell'art. 26 precisa che uno Stato membro puo' autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle liberta' fondamentali delle persone, nonche' per l'esercizio dei diritti connessi.

ART. 44

La disposizione in esame riproduce piuttosto fedelmente quanto previsto dall'art. 28, comma 4, lett. g) della legge 675/96 prevedendo ulteriori

trasferimenti di dati personali verso paesi non appartenenti all'Unione Europea consentiti in quanto autorizzati dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: individuate dal Garante stesso anche in relazione a garanzie prestate con un contratto oppure individuate con le decisioni previste dagli artt. 25, paragrafo 6 e 26, paragrafo 4 della direttiva 95/46/CE (gia' esaminate nel commento all'art. 43) con le quali la Commissione europea constata che un paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Appare quindi evidente che nella materia della tutela dei dati personali vi e' da sempre la preoccupazione che, proprio al fine di eludere le protezioni offerte dalle legislazioni degli Stati, i dati personali vengono trasferiti all'estero, verso paesi con una minore, o con nessuna, legislazione sul punto della protezione degli individui rispetto al trattamento dei dati personali (CERINA).

ART. 45

La disposizione in esame riprende quanto previsto dall'art. 28, comma 3, della legge 675/96 ed e' se vogliamo anche una logica conseguenza di quanto disciplinato dalle disposizioni precedenti

del codice e di quanto previsto dalla direttiva 95/46/CE.

E' quindi la norma di chiusura in materia di trasferimento all'estero dei dati secondo la quale fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, e' vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalita' del trasferimento e dei trattamenti previsti, le relative finalita', la natura dei dati e le misure di sicurezza. Si tratta di una valutazione delicata, anche se eventuali condotte persino colpose, in proposito, non sembrerebbero comunque esporre l'autore al rischio di applicazione delle pesanti sanzioni penali previste dall'art. 167, comma 2, del codice (ATELLI).

ART. 46

La disposizione in esame non trova precedenti nella legge 675/96 ed ha lo scopo di individuare i titolari dei trattamenti effettuati in tale ambito negli uffici giudiziari, nel CSM e negli altri organi di autogoverno e nel Ministero della giustizia, in relazione alle rispettive

attribuzioni, prevedendo l'individuazione dei trattamenti, limitatamente a quelli effettuati con strumenti elettronici, in banche dati centrali o interconnesse.

ART. 47

Questa disposizione richiama quanto previsto all'art. 4, comma 1, lett. c) e d) e comma 2 della legge 675/96. L'articolo in commento individua le disposizioni del codice applicabili a tali trattamenti, dalle quali rimangono escluse quelle non agevolmente compatibili con un efficace perseguimento dell'interesse pubblico perseguito, e individua l'ambito di applicabilita' della particolare disciplina in commento in relazione alle "*ragioni di giustizia*" di cui e' fornita una specificazione sulla base dell'esperienza applicativa. L'art. 47 chiarisce che si devono intendere 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.

Le medesime ragioni di giustizia non ricorrono, ad esempio, per l'ordinaria attivita' amministrativo-gestionale di personale e mezzi. Rispetto a questi ultimi trattamenti, pertanto, trova applicazione *in toto* la pertinente

disciplina del codice. Si ricorda in questa sede che in relazione a tali trattamenti il Garante effettua, ove necessario, i necessari accertamenti, anche su segnalazione dell'interessato, con le particolari modalita' di cui all'art. 160, secondo opportuni moduli piu' proficuamente sperimentati, che tengono conto della particolare collocazione istituzionale degli organi interessati.

La direttiva 95/46/CE fa riferimento ai trattamenti effettuati per ragioni di giustizia all'art. 3, par. 2 laddove sancisce che le proprie disposizioni non si applicano ai trattamenti di dati personali qualora effettuati per l'esercizio di attivita' che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attivita' dello Stato in materia di diritto penale.

ART. 48

Tale disposizione che non trova precedenti nella normativa pregressa sulla privacy favorisce le modalita' di collegamento dell'autorita'

giudiziaria con altre banche di dati della pubblica amministrazione. In tal senso si prevede che ferma restando la necessita' del rispetto delle eventuali previsioni normative sull'acquisizione dei dati, questa puo' avvenire anche per via telematica sulla base di convenzioni che agevolino la consultazione degli archivi, nel rispetto delle regole di correttezza nel trattamento di dati personali (art. 11) e del principio di necessita' del trattamento (art. 3) in base al quale i sistemi informatici e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, dovendosi, invece, di norma trattare dati anonimi o dati che non consentano di identificare l'interessato.

ART. 49

La disposizione in esame prevede l'adozione di norme regolamentari per l'attuazione dei principi del codice sia nella materia penale sia in quella civile.

ART. 50

Tale disposizione, anch'essa inedita, estende ai procedimenti giudiziari in materie diverse da quella penale il divieto di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore (art. 13 D.P.R. 22 settembre 1988, n. 448). A tal riguardo si precisa che il Garante

gia' con pareri del 28 maggio 2001 e del 15 novembre 2001 ricordava che il diritto di cronaca deve essere esercitato nel rispetto del principio dell'essenzialita' dell'informazione sottolineando la necessita' che il giornalista valuti, sotto la propria responsabilita', l'oggettivo interesse del minore alla diffusione dell'informazione che lo riguarda, al fine di salvaguardarne la personalita' e l'armonico processo di maturazione.

ART. 51

La disposizione in esame tende ad agevolare lo sviluppo dell'informatica giuridica nel rispetto dei principi in materia di protezione dei dati personali. Con tale articolo, in termini analoghi a quelli previsti dal recente d.d.l. relativo alla legge di semplificazione, si favorisce la conoscibilita' dei dati identificativi dei giudizi pendenti e delle decisioni giudiziarie adottate mediante reti di comunicazione elettronica anche attraverso il sito *internet* dell'autorita' giudiziaria, senza innovare sulle esistenti disposizioni processuali sulla conoscibilita' di atti giudiziari. Per favorire un'efficace applicazione di tale disposizione, una norma di attuazione consente di adeguare i sistemi informativi entro un anno dall'entrata in vigore del codice (art. 181, comma 5).

ART. 52

Con tale disposizione si definiscono le modalita' con cui garantire le parti in giudizio nel caso di riproduzione di una decisione giudiziaria (ivi compreso il lodo arbitrale rituale) in qualunque forma (su riviste giuridiche, mediante *compact disk*, o mediante la rete *internet*), ferma restando, ovviamente, la pubblicazione della sentenza nelle forme previste dai codici di rito.

L'ambito applicativo della disposizione e' stato precisato in accoglimento di una specifica osservazione della Commissione giustizia del Senato, chiarendo che essa riguarda la "riproduzione" di sentenze o altri provvedimenti giurisdizionali e per "finalita' d'informazione giuridica". Il sistema si articola in una semplice procedura che sfocia nell'apposizione, sull'originale della decisione, di un timbro che attesti la volonta' dell'interessato di precludere l'indicazione delle proprie generalita' o altri dati identificativi in caso di diffusione dell'atto o della relativa massima giuridica, con il conseguente divieto di diffusione di tali dati da parte di qualunque soggetto. Tale annotazione puo' anche essere apposta d'ufficio dal giudice, a tutela della dignita' dell'interessato.

Un divieto specifico e' previsto in caso di decisioni giudiziarie concernenti minori in

ordine ai quali non e' consentito, anche in assenza della predetta annotazione, la diffusione delle generalita', di altri dati identificativi o di altri dati anche relativi a terze persone dai quali possa ricavarsi l'identita' del minore (comma 5).

Un'apposita disposizione transitoria prevede precisi limiti di applicabilita' del divieto di diffusione dei dati relativi a persone non minori, contenuti in decisioni adottate prima dell'entrata in vigore del codice, in relazione a riviste gia' pubblicate (art. 181, comma 5).

Si ricorda che gia' per il passato, il Garante in un parere inviato al Ministero della giustizia riguardo alla predisposizione di un regolamento integrativo della disciplina e dell'accesso al servizio di informatica giuridica del CED, aveva suggerito maggiori garanzie rispetto agli usi ulteriori dei dati personali contenuti negli archivi informatici del Centro elettronico di documentazione (CED) della Corte Suprema di Cassazione ma anche maggiori tutele per gli utenti che per motivi professionali o di studio li consultano in via telematica.

In merito al primo aspetto l'Autorita' aveva sottolineato al Ministero innanzitutto l'esigenza di assicurare un uso legittimo dei dati personali consultati nelle banche dati da parte degli utenti del Ced. Difatti, spesso, i provvedimenti

giudiziari riportano generalita' delle parti e dati riferiti a particolari condizioni o status, anche di natura sensibile e secondo il Garante anche se i dati consultabili attraverso l'accesso al Ced possono essere utilizzati dagli utenti per scopi di documentazione e ricerca in ambito giudiziario o professionale, di studio o per eventuali statistiche, gli stessi non possono essere utilizzati in mancanza di una specifica previsione e di una previa informativa agli interessati, per altre finalita' indebite, quali potrebbero essere, ad esempio, il monitoraggio della giurisprudenza di alcuni uffici giudiziari che miri alla "profilazione" del comportamento del singolo imputato o magistrato o la valutazione a fini disciplinari della produttivita' dell'organo decidente.

Per quanto riguarda poi la tutela degli utenti, il Garante, riconoscendo legittimo il "tracciamento" delle operazioni di accesso e consultazione degli archivi informatici da parte del Centro per esigenze di sicurezza del sistema, aveva escluso la possibilita' che esso potesse essere usato, per quanto in via ipotetica, per monitorare l'accesso di utenti identificabili e il contenuto delle singole operazioni di consultazione.

ART. 53

La disposizione in esame trova un precedente nell'art. 4. comma 1, lett. a) ed e) e comma 2 della legge 675/96. Con essa vengono definiti l'ambito applicativo ed i titolari dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza, ovvero dalle forze di polizia, organi di pubblica sicurezza e altri soggetti pubblici per finalita' di tutela dell'ordine o della sicurezza pubblica e di prevenzione, accertamento o repressione dei reati. La norma specifica che a tali trattamenti si applicano le medesime esclusioni gia' menzionate per i trattamenti effettuati per ragioni di giustizia, cioe' le disposizioni concernenti le modalita' di esercizio dei diritti riconosciuti all'interessato, l'informativa, i codici deontologici, la cessazione del trattamento, la notificazione, le disposizioni concernenti gli obblighi di comunicazione al Garante, le norme sul trattamento dei dati da parte dei soggetti pubblici e la tutela davanti al Garante. La norma prevede, anche, l'individuazione, con decreto ministeriale, dei trattamenti effettuati con l'ausilio di strumenti elettronici e dei relativi titolari.

Si ricorda che gia' la Convenzione di Strasburgo n. 108 ammetteva la possibilita' di derogare ad alcuni dei principi fissati quando tale deroga

costituisse una misura necessaria in una societa' democratica per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati. Stesso tenore per l'art. 3, par. 2 della Direttiva 95/46/CE che esclude dalla propria applicazione i trattamenti di dati personali effettuati per l'esercizio di attivita' che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attivita' dello Stato in materia di diritto penale.

Sempre nella stessa direttiva (art. 13) si concede agli Stati membri la facolta' di adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti, sempre che tale restrizione costituisse una misura necessaria alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, dell'accertamento e del perseguimento di infrazioni penali.

ART. 54

La norma in esame non trova precedenti nelle disposizioni legislative dettate in materia. Analogamente a quanto previsto per l'autorita' giudiziaria (art. 48) la disposizione favorisce le modalita' di collegamento dell'autorita' di pubblica sicurezza e delle forze di polizia con altre banche di dati di altri soggetti. In tal senso si prevede che, nei casi in cui una previsione normativa autorizza l'acquisizione dei dati, questa puo' avvenire anche per via telematica sulla base di convenzioni che agevolino la consultazione degli archivi, nel rispetto delle regole di correttezza nel trattamento di dati personali (art. 11) e del principio di necessita' del trattamento (art. 3). Tali convenzioni devono conformarsi ad una convenzione-tipo adottata dal Ministero dell'Interno, su conforme parere del Garante.

I dati trattati per finalita' di prevenzione, accertamento e repressione dei reati devono essere conservati separatamente da quelli registrati per finalita' amministrative.

La norma, inoltre, prevede per il Centro elaborazione dati l'obbligo di assicurare l'aggiornamento dei dati ivi registrati anche mediante opportuni collegamenti con il casellario giudiziale e dei carichi pendenti del Ministero

della Giustizia. Analoga previsione e' stabilita per gli organi e uffici di polizia.

ART. 55

La disposizione in esame, anch'essa inedita, stabilisce che i trattamenti che implicano maggiori rischi di danno per l'interessato (in relazione, ad esempio, a banche di dati contenenti dati genetici o biometrici) devono essere comunicati previamente al Garante (art. 39) e devono essere effettuati nel rispetto delle misure stabilite dal Garante per tutti i trattamenti che presentano rischi per i diritti dell'interessato (art. 17).

A tal proposito e' opportuno sottolineare il recente interessamento del Garante (anche nella Relazione sull'attivita' 2002) in alcuni settori particolarmente delicati collegati sempre alle nuove tecnologie quali le manipolazioni genetiche e l'utilizzo dei sistemi biometrici nel campo della sicurezza.

Come e' noto le tecnologie biometriche, consentono, mediante l'uso di specifici software e apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare. In particolare queste tecnologie sofisticate, riconosciute anche dal legislatore italiano, utilizzano delle chiavi c.d. biometriche intese

come la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identita' personale basati su specifiche caratteristiche fisiche dell'utente. In tema di accessi informatici i sistemi biometrici rappresentano la ricerca piu' avanzata nel campo della sicurezza. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

Di fronte alla rapida ascesa di tali metodologie il Garante sta assumendo un atteggiamento particolarmente rigido in quanto spesso le finalita' di identificazione, sorveglianza, sicurezza delle transazioni non possono giustificare qualsiasi utilizzazione del corpo umano resa possibile dall'innovazione tecnologica. Vanno garantiti sempre il rispetto della dignita' della persona, il rispetto dell'identita' personale, il rispetto dei principi di finalita' e di proporzionalita' ed infine la necessaria attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Ma cio' che piu' preoccupa il Garante e' che il problema della protezione dell'identita' dai suoi

possibili “furti”, gia’ imponente nel settore del commercio elettronico e che esige cautele particolari per le impronte digitali, puo’ divenire drammatico se il furto riguarda materiale che consente di ottenere informazioni genetiche. Se, infatti, grandi sono le opportunita’ offerte dalla genetica, altrettanto grandi sono i rischi di utilizzazioni dei dati genetici che possono determinare discriminazioni nell’accesso al lavoro o al credito, nella conclusione di contratti di assicurazione vita o malattia, o attraverso forme di schedatura genetica di massa. Insomma come giustamente sottolineato dall’Autorita’ possono nascere nuove disuguaglianze ed in campo internazionale si fa molta attenzione a questo aspetto. E’ necessario, quindi, controllare la legittimita’ di ogni forma di trattamento dei dati genetici ed approntare un sistema di tutela dei dati necessario anche per consentire a tutti di godere al massimo dei benefici della ricerca genetica. Anche in questo settore l’avvento di Internet ha complicato ulteriormente le cose e la diffusione dell’offerta di tests genetici tramite la Rete costituisce un drammatico esempio.

ART. 56

L’articolo in esame estende le disposizioni sull’accesso ai dati destinati a confluire nel Centro elaborazioni di cui alla legge 1 aprile

1981, n. 121, anche agli altri trattamenti effettuati dagli organi e uffici di polizia con strumenti elettronici, assicurando, cosi', piena tutela ai diritti dell'interessato.

ART. 57

La disposizione in argomento prevede l'attuazione dei principi del codice in relazione al trattamento di dati effettuato da forze di polizia o dagli altri soggetti cui si applica il presente titolo, anche mediante l'integrazione e la modifica della normativa vigente in materia (d.P.R. n. 378/1982, di attuazione della predetta legge n. 121/1981). La norma prevede specifici "criteri" per l'individuazione delle modalita' del trattamento, anche in attuazione della Raccomandazione del Consiglio d'Europa n. R(87)15 del 17 settembre 1987 sui trattamenti di dati personali effettuati per finalita' di polizia e di prevenzione e repressione di reati.

Si prevede, quindi, con apposito futuro D.P.R. l'individuazione delle modalita' di attuazione del codice sulla privacy, con particolare riferimento al principio secondo cui la raccolta dei dati e' correlata alla prevenzione di un pericolo concreto o alla repressione di reati, e all'aggiornamento, all'individuazione di termini di conservazione dei dati, alla loro comunicazione ad altri soggetti, anche

all’estero, e alla loro diffusione, ove necessaria in conformita’ della legge.

ART. 58

La disposizione in esame disciplina il trattamento dei dati personali nel campo della difesa e sicurezza dello Stato. Essa trova un suo precedente logico negli artt. 4, commi 1, lett. b) e lett. e) e 2 nonche’ nell’art. 15, comma 4, della legge 675/96.

In particolare la norma riguarda i trattamenti effettuati dai servizi di informazione e di sicurezza previsti dalla legge n. 801/1977 (in merito ad informazioni la cui diffusione sia idonea a recar danno all’integrita’ dello Stato democratico, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, al libero esercizio delle funzioni degli organi costituzionali, alla indipendenza dello Stato rispetto agli altri Stati ed alle relazioni con essi, alla preparazione ed alla difesa militare dello Stato) e da altri soggetti pubblici per finalita’ di difesa o di sicurezza dello Stato, ovvero su dati coperti dal segreto di Stato. La norma specifica quali sono le sole disposizioni del codice applicabili a tali trattamenti.

In ragione della specificita’ di tali trattamenti e della loro particolare delicatezza, l'articolo stabilisce che con Decreto del Presidente del

Consiglio si provveda, non solo all'individuazione delle misure minime di sicurezza (come gia' previsto dalla legge n. 675/1996), ma anche alla determinazione delle modalita' di applicazione a tali trattamenti della normativa del codice. La disposizione assume particolare importanza al fine di assicurare, anche in sintonia con orientamenti giurisprudenziali internazionali in materia di diritti dell'uomo, la necessaria trasparenza alle tipologie di trattamenti effettuati per tali finalita', in relazione ai tipi di operazioni e di dati oggetto di trattamento e alle esigenze di aggiornamento e conservazione dei dati medesimi.

ART. 59

L'articolo in esame, richiamando implicitamente l'art. 43, comma 2, della legge 675/96, ribadisce la compatibilita' delle disposizioni in materia di accesso ai documenti amministrativi (legge 241/90) con quelle che regolano il diritto di accesso ai dati personali. La norma deve essere letta anche in combinato con la modifica apportata all'articolo 24, comma 3, della legge n. 241/1990, che fa salva l'applicabilita' della disciplina prevista dal presente codice nei casi in cui la richiesta di accesso ai dati raccolti mediante strumenti informatici riguarda dati personali del richiedente. La norma riproduce inoltre la previsione gia' contenuta nell'art. 16

del d.lgs. n. 135/1999, in materia di trattamenti di dati sensibili da parte di soggetti pubblici, prevedendo che le attivita' finalizzate all'applicazione della disciplina in materia di accesso ai documenti amministrativi sono di rilevante interesse pubblico.

ART. 60

La disposizione in esame, va vista in stretto collegamento con la precedente e prevede che il trattamento dei dati personali e' consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso e' di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalita' o in un altro diritto o liberta' fondamentale e inviolabile. La disposizione chiarisce in modo inequivoco i presupposti per il trattamento di tali dati sensibili oggetto di una richiesta di accesso ai documenti, in linea con l'orientamento interpretativo espresso dalla giurisprudenza amministrativa sul predetto art. 16 del d. lgs. n. 135/1999.

In questo contesto, la nuova disciplina dei conflitti tra privacy ed accesso eventualmente innescati da istanze di ostensione implicanti un trattamento, ai fini del riscontro dell'istanza medesima, di dati idonei a rivelare lo stato di salute e la vita sessuale, risulta per vero largamente innovativa, occupandosi in un certo

modo di delimitare e profilare piu' specificamente i termini di bilanciamento (ATELLI).

In merito e' opportuno segnalare alcune decisioni del Garante perfettamente in linea con quanto sostenuto in precedenza; si pensi alla decisione del 27 giugno 2001 con la quale l'Autorita' ha precisato che il diritto di accesso ai documenti amministrativi, esercitabile nei casi e nei limiti previsti dalla legge n. 241/1990, e' distinto - e basato su altri presupposti - dal diritto di accesso ai propri dati personali, riconosciuto solo alla persona alla quale i dati si riferiscono e tutelato anche dinanzi al Garante, oppure alla decisione del 3 marzo 2001 con la quale il Garante ha chiarito che non preclude il ricorso all'Autorita' una precedente azione giudiziaria relativa all'accesso ai documenti amministrativi ai sensi della legge n. 241/1990.

ART. 61

La disposizione in esame prevede innanzitutto la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento di tutti quei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici richiamando alla memoria quanto previsto dall'art. 20 del d.lgs. 467/2001 che ha introdotto nel nostro ordinamento i c.d. codici

di condotta o di autoregolamentazione previsti per disciplinare il trattamento dei dati personali in determinati settori quali Internet, il marketing, il campo previdenziale, i sistemi informativi sulla scorta di un modello gia' sperimentato per il passato in altri campi, come quello giornalistico.

L'articolo in esame disciplina, fra l'altro, il trattamento dei dati personali contenuti in albi professionali, in applicazione dei principi in materia di comunicazione e diffusione di dati da parte di soggetti pubblici (art. 19, commi 2 e 3), consentendone il trattamento anche mediante reti di comunicazione elettronica. La disposizione, inoltre, ad integrazione di tali principi (specifica "copertura" normativa o perseguimento di finalita' istituzionali), fa salva la possibilita' che, a richiesta dell'interessato, siano inseriti nell'albo anche altri dati, purche' pertinenti rispetto all'attivita' professionale, o siano comunicate a terzi altre informazioni.

ART. 62

La norma in esame si limita sostanzialmente a riprodurre la disposizione che individua quali finalita' di rilevante interesse pubblico, la tenuta degli atti e dei registri dello stato civile, delle anagrafi e delle liste elettorali (gia' art. 7, d.lgs. n. 135/1999), con la

precisazione che vi sono ricomprese anche le finalita' relative al rilascio di documenti di riconoscimento e al cambiamento delle generalita'.

In relazione a tali materie, inoltre, si segnalano, in questa sede, nelle disposizioni transitorie alcuni interventi che adeguano la normativa vigente ai principi in materia di protezione dei dati personali (art. 177).

ART. 63

La disposizione in esame precisa che gli atti dello stato civile conservati negli Archivi di Stato sono consultabili nei limiti previsti dall'art. 107 del d.lgs. n. 490/99. Tale norma, difatti prevede la libera consultazione di tutti i documenti ad eccezione di quelli dichiarati di carattere riservato, a norma dell'articolo 110 del d.lgs. stesso, relativi alla politica estera o interna dello Stato, che diventano consultabili cinquanta anni dopo la loro data, e di quelli riservati relativi a situazioni puramente private di persone, che lo diventano dopo settanta anni. I documenti dei processi penali sono consultabili settanta anni dopo la data della conclusione del procedimento. E' previsto inoltre, nella stessa disposizione che il Ministero dell'Interno, d'intesa con il Ministero dei Beni Culturali, possa permettere, per motivi di studio, la consultazione di documenti di carattere riservato

anche prima della scadenza dei termini previsti dalla legge. Ai fini di tale autorizzazione, il Ministero dell'Interno ha facolta' di avvalersi del parere del competente comitato di settore del Consiglio nazionale per i beni culturali e ambientali, in relazione al valore storico-culturale dei documenti riservati dei quali sia stata richiesta la consultazione.

ART. 64

La disposizione in esame riproduce in modo fedele l'art. 7 del d.lgs. n. 135/99 che ha per oggetto il trattamento dei dati sensibili e giudiziari avuto riferimento alla cittadinanza, immigrazione e condizione dello straniero.

La disposizione non si applica a quei trattamenti di dati sensibili e giudiziari effettuati in esecuzione degli accordi e convenzioni di carattere internazionale (come quelli previsti 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; o dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia) o comunque effettuati per finalita' di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad

espressa disposizione di legge che prevede specificamente il trattamento.

L'articolo in esame deve essere applicato in coordinamento con le recenti disposizioni introdotte dalla legge n. 189/2002, in relazione alle quali resta consentita la raccolta dei dati biometrici ivi previsti nel rispetto, ovviamente, dei principi in materia di protezione dei dati personali.

ART. 65

La disposizione in esame riproduce l'art. 8 del d.lgs. n. 135/99 e disciplina il trattamento dei dati sensibili e giudiziari (consentendolo in determinati casi) in materia di elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonche' di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari (quest'ultima previsione e' stata aggiunta in sede di redazione del codice) ed in materia di documentazione dell'attivita' istituzionale di organi pubblici.

ART. 66

La disposizione in esame riproduce sostanzialmente l'art. 10 del d.lgs. n. 135/99 prevedendo, in primo luogo, tra le finalita' di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice le attivita' dei soggetti pubblici dirette all' applicazione,

anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonche' in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione e' affidata alle dogane. In secondo luogo le attivita' dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi e alla adozione dei provvedimenti previsti da leggi, regolamenti o dalla normativa comunitaria, nonche' al controllo e alla esecuzione forzata dell'esatto adempimento di tali obblighi, alla effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari.

ART. 67

La disposizione in esame riproduce l'art. 11 del d.lgs. n. 135/99 prevedendo tra le finalita' di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice la verifica della legittimita', del buon andamento, dell'imparzialita' dell'attivita' amministrativa, nonche' della rispondenza di detta attivita' a requisiti di razionalita', economicita', efficienza ed efficacia per le quali sono,

comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti; nonche' l'attivita' di accertamento, nei limiti delle finalita' istituzionali, con riferimento a dati sensibili e giudiziari relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'articolo 65, comma 4 del codice.

ART. 68

La disposizione riproduce l'art. 13 del d.lgs. n. 135/99 prevedendo tra le finalita' di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice quelle di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.

Viene inoltre precisato che tra i trattamenti disciplinati dall'articolo in esame rientrano le comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia; le elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive; la corresponsione delle pensioni di guerra o il riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti; il riconoscimento di benefici connessi

all'invalidita' civile; la concessione di contributi in materia di formazione professionale; la 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; il riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o il rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.

ART. 69

La disposizione riproduce l'art. 14 del d.lgs. n. 135/99 prevedendo tra le finalita' di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice quelle di applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di

patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali.

ART. 70

La disposizione riproduce l’art. 15 del d.lgs. n. 135/99 prevedendo tra le finalita’ di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice quelle di applicazione della disciplina in materia di rapporti tra i soggetti pubblici e le organizzazioni di volontariato, in particolare per quanto riguarda l’elargizione di contributi finalizzati al loro sostegno, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale. Si considerano, inoltre, di rilevante interesse pubblico le finalita’ di applicazione della legge 8 luglio 1998, n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza.

ART. 71

La disposizione riproduce l’art. 16 del d.lgs. n. 135/99 prevedendo tra le finalita’ di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice quelle di applicazione delle norme in materia di sanzioni amministrative e ricorsi nonche’ quelle volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo, anche ai sensi dell’articolo 391-quater del codice di procedura penale (quest’ultimo inciso e’ stato aggiunto

allo scopo di chiarire alcuni dubbi applicativi, in accoglimento delle osservazioni formulate dalla Commissione Giustizia della Camera dei Deputati) o direttamente connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo (anche questa previsione e' stata introdotta ex novo in sede di redazione del codice) o di un'ingiusta restrizione della liberta' personale.

ART. 72

La disposizione in esame riproduce l'art. 21 del d.lgs. n. 135/99 prevedendo tra le finalita' di rilevante interesse pubblico disciplinate dagli artt. 20 e 21 del codice quelle relative allo svolgimento dei rapporti istituzionali con enti di culto, confessioni religiose e comunita' religiose.

ART. 73

Tale disposizione riporta le altre finalita' di rilevante interesse pubblico individuate, in materia amministrativa e sociale, dal Garante, ai sensi dell'art. 22, comma 3, della legge n. 675/1996, con il provvedimento n. 1/P/2000 del 30 dicembre 1999-13 gennaio 2000, pubblicato nella G.U. n. 26 del 2 febbraio 2000.

In particolare si fa riferimento 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; 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; assistenza nei confronti di minori, anche in relazione a vicende giudiziarie; indagini psico-sociali relative a provvedimenti di adozione anche internazionale; compiti di vigilanza per affidamenti temporanei; iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi; interventi in tema di barriere architettoniche; attivita' di gestione di asili nido; attivita' concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico; attivita' 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; attivita' di assegnazione di alloggi di edilizia residenziale pubblica; attivita' relative alla leva militare; attivita' 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; attivita' degli uffici per le

relazioni con il pubblico; attivita' in materia di protezione civile; attivita' 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; attivita' dei difensori civici regionali e locali.

ART. 74

La disposizione in esame che non trova precedenti nella preesistente normativa sulla privacy individua alcune cautele a garanzia della riservatezza delle persone in relazione al trattamento di dati personali contenuti in contrassegni di circolazione, destinati all'esposizione all'interno di veicoli, anche relativi a persone handicappate. La disposizione prende in esame i principi a suo tempo richiamati dal Garante con un provvedimento generale (adottato il 19 gennaio 1999), gia' in larga parte applicati in ambito locale.

ART. 75

La disposizione in esame individua l'ambito di applicazione del Titolo V e riproduce sostanzialmente l'art. 1 del d.lgs. n. 282/1999. In ambito comunitario la particolare materia è stata trattata dall'art. 8 della direttiva 95/46/CE che fa riferimento, al par. 3, al trattamento dei dati necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure

o alla gestione di centri di cura e quando il trattamento dei medesimi dati viene effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale, comprese le norme stabilite dagli organi nazionali competenti, o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente.

ART. 76

La disposizione in esame definisce i presupposti di liceita' del trattamento dei dati idonei a rivelare lo stato di salute da parte degli esercenti le professioni sanitarie e degli organismi sanitari pubblici. L'articolo riproduce pedissequamente il previgente art. 23 della legge n. 675/1996 chiarendo che tale trattamento e' effettuato con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se riguarda dati e operazioni indispensabili per perseguire una finalita' di tutela della salute o dell'incolumita' fisica dell'interessato, ovvero anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalita' riguarda un terzo o la collettivita'.

L'art. 76 inoltre, anticipa, che nei casi in cui e' richiesto, il consenso puo' essere prestato con forme semplificate e secondo le modalita' contenute nel capo II.

ART. 77

La disposizione introduce il capo II che prevede modalita' semplificate per il rilascio dell'informativa e per la prestazione del consenso dell'interessato in relazione al trattamento di dati in ambito sanitario, recependo integralmente e ulteriormente semplificando (con particolare riguardo a quello a fini amministrativi), le proposte formulate da una apposita commissione istituita presso il Ministero della Salute per la redazione dello schema di regolamento ministeriale gia' previsto dalla normativa previgente (art. 23, comma 1-bis, l. n. 675/1996).

L'articolo in esame individua, in particolare, l'ambito oggettivo e soggettivo di tali forme di semplificazione chiarendo che esse riguardano sia il rilascio dell'informativa, sia la prestazione del consenso dell'interessato (e, piu' in generale, le modalita' del trattamento dei dati) e si applicano a tutti i soggetti operanti in ambito sanitario, pubblici o privati.

A tal riguardo occorre ricordare come gia' il d.lgs. n. 135/99 avesse definito i principi generali in base ai quali i soggetti pubblici, con criteri piu' rigidi a maggior tutela del cittadino, sono autorizzati a trattare i dati sensibili o attinenti particolari provvedimenti giudiziari e avesse individuato alcune rilevanti

attivita' di interesse pubblico, per il cui perseguimento e' consentito tale trattamento, nonche' le operazioni eseguibili e i tipi di dati che possono essere trattati. L'argomento e' stato ripreso dall'art. 20 del presente codice al quale si rinvia.

ART. 78

La disposizione individua le modalita' di semplificazione per l'informativa all'interessato da parte del medico "di famiglia" (o del pediatra), sotto tre profili:

a) per quanto riguarda l'ambito "oggettivo" di applicazione, l'informativa puo' essere fornita, con un unico atto, per il complessivo trattamento di dati relativo al paziente (diagnosi, cura, riabilitazione, ecc.) e puo' riguardare anche dati raccolti presso terzi;

b) sotto il profilo "soggettivo", essa puo' riguardare anche il trattamento di dati *"correlato"* a quello del medico "di famiglia", effettuato da altro professionista che con quello venga, in vario modo, in contatto professionale nell'interesse del paziente;

c) infine, circa le modalita', l'informativa e' resa preferibilmente per iscritto, ma anche con modalita' alternative come le piu' recenti carte tascabili o altri simili strumenti, integrandola oralmente, se necessario.

L’elemento innovativo di tale disposizione e’ che l’informativa e’ valida per il complessivo trattamento dei dati personali necessario per l’attivita’ sanitaria svolta dal medico, nonche’ per ogni trattamento correlato, effettuato dal medico che sostituisce temporaneamente il medico o il pediatra, da chi fornisce la richiesta prestazione specialistica, da chi puo’ trattare lecitamente i dati nell’ambito di un’attivita’ professionale prestata in forma associata, da chi fornisce i farmaci prescritti (ZANETTA).

Il comma 5 contiene un’importante previsione sul contenuto dell’informativa, in base alla quale essa deve evidenziare analiticamente eventuali trattamenti potenzialmente rischiosi per i diritti e le liberta’ fondamentali dell’interessato, come quelli effettuati a fini di ricerca scientifica o di sperimentazione clinica, oppure effettuati mediante il ricorso alle piu’ moderne tecnologie, in particolare in forma di teleassistenza o telemedicina.

ART. 79

L’articolo in esame estende le previste modalita’ semplificate in ambiti piu’ ampi rispetto a quello dei singoli professionisti con cui il paziente puo’ venire in contatto piu’ direttamente, in relazione, cioe’, agli organismi sanitari pubblici e privati nel loro complesso, anche in riferimento ad una pluralita’ di

prestazioni erogate da distinti reparti dello stesso organismo o di piu' strutture ospedaliere o aziende sanitarie. E' evidente l'intento della norma di semplificare il piu' possibile il rilascio dell'informativa assicurando al contempo l'effettivita' dell'adempimento. Infatti si precisa che i vari organismi o strutture devono annotare l'avvenuta informativa con modalita' uniformi, tali da consentire ogni verifica al riguardo da parte di altri reparti ed unita' o di altre strutture.

ART. 80

L'articolo prevede la possibilita' di un'unica informativa anche a fini amministrativi e per una pluralita' di trattamenti di dati, quando i trattamenti siano effettuati dai competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro. In tal caso la norma precisa che, a ulteriore garanzia dell'interessato, l'informativa e' integrata con appositi avvisi, agevolmente visibili al pubblico o diffusi anche con strumenti telematici al fine di far conoscere meglio le finalita' della legge sulla privacy e soprattutto i diritti del cittadino.

ART. 81

La disposizione in esame disciplina le modalita' semplificate per la prestazione del consenso,

applicabili, ove necessario, in tutti i casi descritti in relazione agli articoli 78 e 79. Il consenso al trattamento dei dati, nei casi in cui e' necessario ai sensi del presente codice o di altra disposizione di legge, puo' essere manifestato con un'unica dichiarazione. Non si richiede che sia necessariamente prestato in forma scritta dall'interessato, ma e' sufficiente che il medico o l'organismo annoti il consenso medesimo. L'articolo, poi, "raccorda" il rilascio dell'informativa con la prestazione del consenso nel caso di informativa resa dal medico "di famiglia" per conto di piu' professionisti, prevedendo che, in tal caso, gli altri professionisti siano messi in condizione di conoscere l'avvenuta prestazione del consenso mediante l'apposizione di un bollino o altro segno sulla tessera sanitaria, anche con riferimento a eventuali "specificita'" dell'informativa resa.

ART. 82

La disposizione disciplina i casi in cui, in relazione a situazioni di emergenza, anche connesse allo stato di salute del paziente, l'informativa e il consenso possono intervenire in un momento successivo alla prestazione medica resa dal sanitario.

A parte i casi in cui sussistono emergenze di carattere pubblico, sanitarie o di igiene, il

trattamento dei dati idonei a rivelare lo stato di salute del paziente e' consentito anche in assenza del suo consenso – purche' questo e la relativa informativa intervengano successivamente - quando:

a) l'interessato non e' in grado di prestare il proprio consenso per incapacita' o impossibilita' e non puo' acquisirsi neanche il consenso delle persone che, gia' in base alla normativa previgente, possono esprimere il consenso per conto dell'interessato (chi esercita legalmente la potesta', un prossimo congiunto, ecc.);
b) nel caso di rischio grave per la salute o l'incolumita' dell'interessato;
c) quando la prestazione medica potrebbe essere altrimenti pregiudicata dall'acquisizione preventiva del consenso.

ART. 83

La disposizione in esame prevede la possibilita' per i soggetti cui si riferisce il presente capo di adottare, nell'ambito dell'organizzazione dei servizi, altre misure a garanzie dei diritti dell'interessato. Si tratta, in particolare, di interventi organizzativi, cautele comportamentali, aggiornamenti di procedure che possono agevolare l'applicazione della legge e che sono stati individuati anche grazie alle indicazioni e suggerimenti del Garante a tutela

delle liberta' fondamentali e della dignita' degli interessati, nonche' del segreto professionale (distanze di cortesia, riservatezza nei colloqui, regole di condotta analoghe al segreto professionale per gli incaricati che non vi sono gia' sottoposti, ecc.).

ART. 84

L'articolo in esame riproduce l'art. 23, comma 2, della legge n. 675/1996 in base al quale i dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato. Poiche' la norma ha il chiaro intento di evitare al paziente di venire a conoscenza di notizie sul suo stato di salute da soggetti professionalmente non preposti a tale compito, che spesso e' alquanto delicato, la norma e' stata integrata prevedendo la sua inapplicabilita' in riferimento ai dati personali gia' conosciuti dal medesimo interessato in quanto da lui forniti in precedenza. In ogni caso si prevede ulteriormente che possa essere espressamente incaricato a tale scopo anche altro personale sanitario che abbia rapporti diretti con il paziente.

ART. 85

La disposizione in esame riproduce l'art. 17 commi 1 e 2 del d.lgs. n. 135/99 specificando le

finalita' di rilevante interesse pubblico rientranti nei compiti del Servizio Sanitario Nazionale. Si tratta di tutte quelle attivita' amministrative correlate alla prevenzione, cura, riabilitazione, nonche' ai trapianti di organo e di tessuto, alle trasfusioni, alla programmazione e vigilanza dell'assistenza sanitaria, alle attivita' certificatorie, all'applicazione della normativa in materia di igiene e sicurezza sul posto di lavoro, ai rapporti fra i soggetti del Servizio Sanitario Nazionale.

ART. 86

Tale disposizione riproduce gli artt. 18, 19 e 20 del d.lgs. n. 135/99 specificando tutte quelle finalita' di rilevante interesse pubblico che pur non direttamente attribuibili al Servizio Sanitario Nazionale sono sempre di carattere sanitario.

In tale categoria rientrano le attivita' amministrative correlate all'applicazione della disciplina in materia di tutela della maternita' e interruzione volontaria della gravidanza, stupefacenti e sostanze psicotrope, assistenza, integrazione sociale e diritti delle persone handicappate.

Trattandosi ovviamente di finalita' relative ad attivita' a carattere amministrativo, i soggetti che operano nell'ambito del SSN o gli altri organismi sanitari pubblici, se ricorrono tali

finalita', possono trattare dati idonei a rivelare lo stato di salute dell'interessato anche in assenza del suo consenso, previa identificazione delle operazioni eseguibili e dei tipi di dati idonei a rivelare lo stato di salute, ai sensi dell'articolo 20 del codice, alla quale deve essere assicurata ampia pubblicita'. Particolari cautele sono previste, in ogni caso, per il trattamento dei dati identificativi dell'interessato.

ART. 87

La disposizione in esame apre il capo IV che reca la disciplina delle modalita' di rilascio delle prescrizioni mediche, riproducendo la normativa vigente (d.lgs. n. 282/99) opportunamente razionalizzata al fine di garantire la riservatezza dell'interessato e tenendo conto, anche in questo caso, delle indicazioni formulate dall'apposita commissione istituita presso il Ministero della Salute. Si distinguono diverse modalita' di rilascio delle prescrizioni a secondo che le "ricette" siano a carico o meno del SSN.

L'articolo in esame prevede che i medicinali siano a carico del SSN. In tal caso l'esigenza, gia' contenuta nel d.lgs. n. 282/1999, e' di permettere di risalire all'identita' dell'interessato solo in caso di necessita' connesse al controllo della correttezza della

prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca. In tal senso il modello di "ricetta" gia' in uso e' integrato da un tagliando predisposto su carta o con tecnica di tipo copiativo e unito ai bordi della prescrizione, posizionato in modo da "coprire" le generalita' dell'interessato, e separabile temporaneamente, ove necessario.

ART. 88

Questa disposizione prevede invece il caso in cui i medicinali non siano a carico del Servizio Sanitario Nazionale. Sulle relative prescrizioni, quindi, non sono riportate le generalita' dell'interessato, salvo che il medico lo ritenga necessario per consentirne l'individuazione quando particolari situazioni lo richiedano.

ART. 89

La disposizione in esame prevede e fa salvi quei casi particolari dove possono essere rilasciate ricette non identificative dell'interessato come il famoso decreto "Di Bella" oppure quei casi collegati agli stati di tossicodipendenza nei quali deve essere accertata l'identita' dell'interessato a cui vengono somministrate specifiche sostanze e le ricette sono conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.

ART. 90

L’articolo in esame, ai commi 1 e 2, riproduce la disposizione previgente in materia di dati genetici (art. 17 d.lgs. n. 135/99) chiarendo piu’ in dettaglio il contenuto della necessaria autorizzazione del Garante al trattamento di tali dati, con riferimento, in particolare, all’informativa all’interessato.

Al comma 3, l’art. 90 inserisce nel codice per omogeneita’ di materia una disposizione in materia di riservatezza nel caso di trapianto di midollo osseo (art. 4, comma 3, l. 6 marzo 2001, n. 52), abrogando l’originaria disposizione (art. 183, comma 3, lett. c)). Alla luce di tale disposizione il donatore di midollo osseo ha il diritto e il dovere di mantenere l’anonimato, sia nei confronti del ricevente sia nei confronti di terzi.

ART. 91

Questa disposizione riguarda i trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale dell’interessato eventualmente registrati su carte anche non elettroniche o trattati mediante le medesime carte, come, ad esempio, la carta nazionale dei servizi.

Ferma restando l’esigenza di una "copertura" normativa di tali trattamenti, la delicatezza di essi, per la natura dei dati e le particolari tecnologie adoperate, richiede che siano effettuati solo se necessari, nel rispetto del

principio di necessita' piu' volte richiamato (art. 3), e nell'osservanza delle misure eventualmente prescritte dal Garante nei modi di cui all'articolo 17, trattandosi di trattamenti che possono presentare specifici rischi per i diritti e le liberta' fondamentali.

ART. 92

L'articolo in esame introduce alcune importanti disposizioni in materia di trattamento di dati contenuti nelle cartelle cliniche e nelle accluse schede di dimissione ospedaliera.

Da un lato, si favorisce l'intelligibilita' dei dati ivi contenuti da parte del medesimo interessato (art. 10), tutelando al contempo dati di terzi eventualmente presenti, come nel caso in cui, ad esempio, dal particolare stato di salute della madre possano ricavarsi dati relativi al nascituro.

Dall'altro, si assicura l'accesso alle informazioni ivi contenute anche a terzi, nei limiti dei principi del presente codice. In tal senso, si prevede, infatti, che a tali dati si possa avere accesso per far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), o per tutelare, in conformita' alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante, purche' in entrambi i casi la situazione soggettiva da far

valere sia di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalita' o in un altro diritto o liberta' fondamentale e inviolabile.

ART. 93

Tale disposizione fa parte di un piu' complessivo intervento tendente a inserire nel codice alcune disposizioni che riguardano la riservatezza dei dati contenuti nel certificato di assistenza al parto, gia' previste dall'art. 16 del D.P.R. 28 dicembre 2000, n. 445, recante il testo unico in materia di documentazione amministrativa, che viene, pertanto, abrogato *in parte qua* (art. 183, comma 3, lett. d)). La disciplina e' completata dall'art. 109 che riguarda gli aspetti della rilevazione di tali dati a fini statistici.

L'art. 93, inoltre, raccorda tale disciplina con il diritto all'anonimato della madre, di cui all'art. 30 del D.P.R. 3 novembre 2000, n. 396, in materia di stato civile, prevedendo che il certificato di assistenza al parto (ed anche la cartella clinica), ove comprensivi dei dati personali che rendono identificabile la madre, possono essere rilasciati in copia integrale a chi vi abbia interesse solo decorsi cento anni dalla formazione del documento. Prima di tale termine, la richiesta di accesso al certificato o alla cartella non e', ovviamente, preclusa, ma devono essere adottate le opportune cautele per

scongiurare l'identificabilita' della madre che voglia rimanere anonima.

ART. 94

Tale disposizione prevede la specifica applicazione del principio di necessita' nel trattamento dei dati al trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati o altri archivi o registri tenuti in ambito sanitario.

Diventa ora fondamentale la diffusione e la informazione piu' capillare sulle innovazioni e semplificazioni introdotte dal T.U. al fine di ottimizzare il rapporto operatore sanitario-cittadino, nella consapevolezza dell'interesse generale all'applicazione di norme che garantiscano il rispetto della persona (ZANETTA).

ART. 95

La disposizione in esame riproduce l'art. 12 del d.lgs. n. 135/99 individuando le finalita' di rilevante interesse pubblico in materia di istruzione e di formazione.

ART. 96

Questa disposizione riproduce l'art. 330-bis del d.lgs. 16 aprile 1994, n. 297, introdotto dal d.lgs. n. 281/1999, concernente il trattamento di dati relativi a studenti e la pubblicazione dell'esito degli esami, e conferma la vigenza di altre disposizioni in materia di tutela del diritto dello studente alla riservatezza.

ART. 97

La disposizione in esame definisce l'ambito applicativo relativo al trattamento di dati personali effettuato per scopi storici, statistici o scientifici, gia' disciplinato, oltre che da specifiche disposizioni della legge n. 675/1996, dal d. lgs. 30 luglio 1999, n. 281. Inoltre il 14 marzo del 2001 e' stato varato il codice per il trattamento di dati per scopi storici (allegato al presente codice a scopo conoscitivo).

Si ricorda che la materia e' stata disciplinata in ambito comunitario all'art. 6 comma 1 lett. b) della direttiva 95/46/CE dove viene specificato che il trattamento successivo dei dati personali per scopi storici, statistici o scientifici non e' ritenuto incompatibile, purche' gli Stati membri forniscano garanzie appropriate. Inoltre alla lett. e) viene precisato che gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.

ART. 98

La disposizione in esame per evidente esigenze di armonizzazione normativa considera come finalita' di rilevante interesse pubblico anche quelle concernenti i trattamenti effettuati per scopi scientifici, che cosi' si aggiungono agli scopi

storici e alle finalita' di statistica gia' previste dagli artt. 22 e 23 del d.lgs. n. 135/99.

ART. 99

La disposizione, riprendendo l'art. 9, comma 1 bis, della legge 675/96, sottolinea la compatibilita' del trattamento di dati personali effettuato per scopi storici, statistici o scientifici con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

Inoltre precisa che lo stesso trattamento puo' essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

ART. 100

La disposizione in esame riproduce il disposto dell'art. 6, comma 4, del decreto legislativo 5 giugno 1998, n. 204, in materia di diffusione di dati a fini di ricerca e collaborazione in campo scientifico e tecnologico, riportato nell'ambito del codice per omogeneita' di materia.

ART. 101

La disposizione in esame sancisce che i dati personali raccolti per scopi storici non possono essere utilizzati per adottare provvedimenti amministrativi sfavorevoli all'interessato. I documenti contenenti dati personali trattati per

scopi storici possono essere utilizzati solo se pertinenti ed indispensabili al perseguimento degli scopi prefissi. Inoltre per scopi storici, statistici e scientifici possono essere conservati o ceduti ad altro titolare anche dati personali per i quali e' cessato il trattamento. Per promuovere e sostenere la ricerca la disposizione autorizza i soggetti pubblici, compresi universita' ed enti di ricerca, a comunicare e diffondere, anche ai privati e per via telematica dati legati ad attivita' di studio e ricerca, a laureati, a dottori di ricerca, tecnici e tecnologi, docenti, esperti e studiosi. Restano pero' esclusi i dati sensibili e quelli giudiziari.

ART. 102

La disposizione in esame in conformita' all'orientamento del Garante, fatto proprio dal codice in materia di protezione dei dati personali, prevede la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici. Ma l'articolo non si limita ad una semplice previsione in quanto al 2° comma individua anche gli aspetti che vanno maggiormente approfonditi tra i quali: le regole di correttezza e di non discriminazione nei

confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del codice applicabili ai trattamenti di dati per finalita' giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica; le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse e' informato dall'utente della prevista diffusione di dati; le modalita' di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a scopi storici, anche in riferimento all'uniformita' dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

ART. 103

L'articolo in esame dispone che per la consultazione dei documenti conservati negli archivi di Stato o in quelli storici degli enti pubblici ovvero in archivi privati si applicano le pertinenti disposizioni del testo unico in materia di beni culturali e ambientali, approvato con il d.lgs. n. 490 del 1999, nel quale sono confluite le disposizioni del D.P.R. 30 settembre

1963, n. 1049, gia' modificato dal citato d.lgs. n. 281/1999.

ART. 104

La disposizione in esame introduce il Capo III che contiene le disposizioni riguardanti il trattamento di dati personali effettuato per scopi statistici o scientifici.

Il 2° comma, in considerazione del fatto che il complesso delle informazioni telematiche e delle memorie elettroniche rischia di invadere la sfera privata dell'individuo turbandone la vita personale, familiare e sociale e di creare deformazioni sulla identita' della persona umana, costituisce un valido esempio di quei meccanismi di adeguamento previsti dal Codice che lo renderanno meno soggetto all'obsolescenza di fronte all'avanzare delle tecnologie, restando peraltro immune da tecnicismi e mantenendo invece una sufficiente generalita' e indipendenza da specifiche tecnologie.

In questo senso, il Codice ha fatto proprio l'obiettivo di ripristino del principio giuridico della norma a carattere generale ed astratto che sia applicabile anche alle fattispecie future che l'evoluzione tecnologica puo' presentare.

ART. 105

La disposizione in esame contiene un importante intervento di semplificazione in relazione all'obbligo di fornire all'interessato

l'informativa di cui all'art. 13. Difatti stabilisce che quando specifiche circostanze individuate dai rispettivi codici di deontologia sono tali da consentire ad un soggetto di rispondere in nome e per conto di un altro, in quanto familiare o convivente, l'informativa all'interessato di cui all'art. 13 e' validamente prestata anche per il tramite del soggetto legittimato alla risposta (comma 4). La semplificazione puo' trovare applicazione nell'ambito delle procedure di rilevamento di dati statistici in occasione del censimento della popolazione.

Inoltre l'informativa non e' dovuta in relazione al trattamento effettuato per scopi statistici o scientifici rispetto a dati originariamente raccolti per altri scopi, quando richiederebbe uno sforzo sproporzionato rispetto al diritto tutelato, purche' siano, pero', adottate idonee forme di pubblicita' alternative, individuate dai medesimi codici deontologici (comma 4). Dati personali raccolti per scopi statistici o scientifici non possono essere usati per prendere decisioni o adottare provvedimenti in merito all'interessato.

ART. 106

La disposizione in esame sottolinea il compito del Garante di promuovere la sottoscrizione di uno o piu' codici che regolino la condotta di

soggetti pubblici e privati, comprese le societa' scientifiche e le associazioni professionali interessate a trattare dati per scopi statistici e scientifici. E' necessario tener conto delle raccomandazioni del Consiglio d'Europa per individuare gli ulteriori presupposti del trattamento e le connesse garanzie legate alla durata della conservazione dei dati, alle informazioni da rendere agli interessati sui dati raccolti anche presso terzi, alla comunicazione e diffusione dei dati, alle misure di sicurezza e alle modalita' per modificare i dati su richiesta dell'interessato (GIULIANTE).

Devono essere indicati i mezzi che possono essere usati dal titolare del trattamento o da altri per individuare il soggetto interessato tenendo conto delle nuove tecnologie; le garanzie che permettono di prescindere dal consenso dell'interessato; le modalita' semplificate per prestare il consenso al trattamento dei dati sensibili; le regole di correttezza da seguire nella raccolta dei dati e le indicazioni necessarie per il personale incaricato; le misure utili a favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e le misure di sicurezza per impedire l'accesso di persone non incaricate; misure da adottare nell'interconnessione dei sistemi informativi e nell'interscambio di dati per scopi statistici e

scientifici da effettuarsi verso l'estero. Gli incaricati che non sono tenuti in base alla legge, al segreto d'ufficio o professionale, devono impegnarsi a rispettare le regole di condotta per assicurare il livello di sicurezza e riservatezza nella protezione dei dati.

ART. 107

La disposizione in esame disciplina in particolare il trattamento dei dati sensibili ed il relativo consenso dell'interessato che puo' essere prestato, quando e' richiesto, con modalita' semplificate, individuate dal codice di cui all'articolo 106 e l'autorizzazione del Garante puo' essere rilasciata anche ai sensi dell'articolo 40.

ART. 108

L'articolo in esame chiarisce che il trattamento dei dati personali da parte di soggetti che fanno parte del Sistan (Sistema statistico nazionale) e' disciplinato altresi' dal decreto legislativo 6 settembre 1989, n. 322, gia' modificato dal decreto legislativo n. 281/1999, in particolare sul fronte dei trattamenti sensibili, dell'informativa all'interessato, dell'esercizio dei diritti di accesso, modifica e cancellazione dei dati e per i dati non tutelati dal segreto statistico.

ART. 109

La disposizione in esame riproduce, in parte, il disposto dell'art. 16, comma 3, del D.P.R. 28 dicembre 2000, n. 445, recante il testo unico in materia di documentazione amministrativa, concernente i dati statistici relativi all'evento della nascita, aggiornato in base al D.M. n. 349/2001. La norma completa, sotto il profilo degli adempimenti a fini statistici (il che giustifica la sua collocazione in questo capo) la disposizione dell'articolo 93 *(Certificato di assistenza al parto).*

ART. 110

La disposizione in esame riguarda il trattamento di dati idonei a rivelare lo stato di salute per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico (gia' art. 5, d. lg. n. 282/1999), che puo' essere effettuato anche senza il consenso dell'interessato quando il medesimo trattamento e' previsto da una disposizione di legge o rientra in un programma di ricerca biomedica o sanitaria (art. 12-bis del d.lgs. 502/1992). La disposizione e' stata integrata, come gia' anticipato nel commento all'art. 39, prevedendo la previa comunicazione del trattamento al Garante e l'avvio del medesimo solo dopo il decorso dei 45 giorni ivi previsti. Inoltre la possibilita' di trattare i dati dell'interessato senza il suo consenso e' stata estesa all'ipotesi in cui non sia possibile, a

causa di particolari ragioni, informarlo e il programma di ricerca sia oggetto di parere favorevole del competente comitato etico e sia, altresi', autorizzato dal Garante.

Eventuali aggiornamenti, rettifiche o integrazioni dei dati sono annotati senza modifiche quando l'operazione non produce effetti significativi sul risultato della ricerca.

ART. 111

La disposizione in esame riproduce l'art. 20, comma 2, lett. b) del d. lgs. n. 467/2001 in tema di codice di deontologia e di buona condotta relativo al trattamento di dati in materia di gestione del rapporto di lavoro, in osservanza dei pareri espressi dalle Commissioni giustizia della Camera e del Senato.

In particolare viene demandato al codice di deontologia e buona condotta la regolamentazione dell'informativa all'interessato e le modalita' di acquisizione del consenso relativamente alla pubblicazione degli annunci per finalita' di occupazione e alla ricezione di curricula contenenti dati personali anche sensibili.

La materia del trattamento dei dati, degli annunci e dei curricula e', peraltro, trattata anche nel d.lgs. di attuazione della legge n. 30/2003 di riforma del mercato del lavoro, che all'art. 9 dispone il divieto di comunicazioni relative a ricerca e selezione del personale

effettuate, con qualsiasi mezzo, da soggetti diversi da quelli accreditati o autorizzati (GHEIDO).

ART. 112

La disposizione in esame riproduce l'articolo 9, del d. lgs. n. 135/1999 che individua le finalita' di rilevante interesse pubblico in materia di lavoro, in osservanza dei pareri espressi dalle Commissioni giustizia della Camera e del Senato.

Poiche' l'art. 20 del codice in materia di protezione dei dati personali stabilisce che il trattamento dei dati sensibili da parte degli enti pubblici e' possibile solo se autorizzato da una espressa previsione normativa che specifichi la tipologia dei dati da trattare e le finalita' di rilevante interesse pubblico perseguito, l'articolo in esame dispone che si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalita' 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.

La stessa disposizione elenca i trattamenti che rientrano nelle suddette finalita', fra cui in particolare quelli effettuati ai fini di:

applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette; garantire le pari opportunita'; accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi; adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonche' ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali; 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, nonche' in materia sindacale; applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa; svolgere attivita' dirette all'accertamento della responsabilita' civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformita' alle norme che regolano le rispettive materie; 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; salvaguardare la

vita o l'incolumita' fisica dell'interessato o di terzi; gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti; applicare la normativa in materia di incompatibilita' e rapporti di lavoro a tempo parziale; svolgere l'attivita' di indagine e ispezione presso soggetti pubblici; valutare la qualita' dei servizi resi e dei risultati conseguiti.

ART. 113

L'articolo in esame precisa che restano ferme le disposizioni dell'art. 8 della legge 25 maggio 1970 n. 300, ("statuto dei lavoratori") sul divieto di indagini sulle opinioni dei lavoratori, che riguarda il trattamento di dati sensibili. Tale disposizione, a differenza del testo originariamente proposto nel Consiglio dei Ministri, non stabilisce criteri autonomi.

Come e' noto l'art. 8 della legge n. 300/70 fissa il divieto di indagine sulle opinioni e vieta al datore di lavoro di effettuare ai fini dell'assunzione o nel corso del rapporto di lavoro, indagini sulle opinioni politiche, religiose o sindacali del lavoratore nonche' su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

ART. 114

Anche tale disposizione, analogamente a quanto gia' descritto in relazione all'art. 113, precisa che restano ferme le disposizioni dell'art. 4 della legge 25 maggio 1970 n. 300, sul divieto di controllo a distanza dei lavoratori. Viene, quindi, mantenuto il divieto di usare impianti audiovisivi e altre apparecchiature per il controllo a distanza dell'attivita' dei lavoratori. Qualora tali impianti fossero necessari per finalita' produttive ed organizzative l'installazione potra' essere effettuata solo previo accordo sindacale o, in difetto, su provvedimento della Direzione Provinciale del lavoro – Servizio Ispettivo (GHEIDO).

ART. 115

L'articolo in esame, riproduce alcune disposizioni extravaganti in materia di riservatezza nell'ambito del lavoro domestico (art. 6, l. 2 aprile 1958, n. 339), che sono, conseguentemente, abrogate (art. 179, comma 1).

In tale disposizione si fa esplicita menzione del telelavoro che e' una modalita' di prestazione di lavoro svolta da un dipendente in un qualsiasi luogo ritenuto idoneo (esterno alla sede di lavoro) dove la prestazione sia tecnicamente possibile. E' caratterizzato dal supporto di tecnologie dell' informazione e della

comunicazione, che consentono il collegamento con l'Ente per il quale viene svolta la prestazione.
Le modalita' di svolgimento della prestazione nel telelavoro possono essere le piu' varie: "domiciliare" in cui il dipendente lavora presso il proprio domicilio. E' possibile dove e' presente lavoro di tipo ripetitivo oppure in autonomia. Un esempio del primo caso e' l'immissione in massa di informazioni provenienti dal cartaceo in una banca dati elettronica (es. recupero vecchie delibere, scansione di documenti da avere sempre "in linea", ecc.). Esempi del secondo caso sono la realizzazione di programmi per computer oppure lavoro di ricerca che richieda la connessione all'ufficio per l'accesso a banche dati o altre informazioni. Deve essere utilizzato quando l'obiettivo del lavoro e' ben definito e soprattutto verificabile a posteriori. Richiede capacita' di autogestione e di mantenimento di rapporti interpersonali in forma scritta. Presenta evidenti vantaggi se applicato a persone con handicap fisici. Nelle esperienze gia' realizzate il dipendente effettua alcune giornate di lavoro a casa (2 o 3 a settimana) mentre nelle altre rientra in ufficio per svolgere attivita' diverse per consentire un controllo del lavoro effettuato. "Delocalizzato dalla sede principale" consistente nella delocalizzazione di parte dell'attivita' svolta

in un centro satellite o telecentro collegato alla sede per via telematica. Si puo' trattare anche di un centro di lavoro in cui vengono istituite una serie di postazioni utilizzate da piu' amministrazioni che lavorano in rete. Cio' e' possibile ove siano presenti strutture distaccate di una struttura centralizzata realizzate in collaborazione con altri enti. Puo' essere sfruttato per delocalizzare i servizi ai cittadini (si pensi all'Ufficio Relazioni col Pubblico che potrebbe essere realizzato in collaborazione tra i vari Enti negli stessi locali consentendo al cittadino di andare in un unico posto per avere diversi servizi e/o informazioni) e contemporaneamente avvicinare i dipendenti alle proprie abitazioni. Le caratteristiche di tale forma di telelavoro sono quindi piu' elastiche della precedente in quanto possono riguardare quelle figure dell'ente preposte ad avere contatti con il pubblico da dislocare sul territorio, ed inoltre, per la loro tipologia, non hanno quei problemi di controllo delle prestazioni normalmente associati alle forme di telelavoro domiciliare.

"Telelavoro mobile" in cui il dipendente svolge il proprio lavoro utilizzando posti di lavoro mobile. Questo tipo di lavoro si caratterizza per non avere una sede di lavoro fissa come nei casi precedenti. Va preso in considerazione,

soprattutto, per migliorare la prestazione dei dipendenti che per la tipologia dell'incarico devono viaggiare molto e trasmettere informazioni o dati alla sede centrale (ad esempio le guardie forestali che potrebbero trasmettere informazioni all'ufficio per via telematica oppure i cantonieri che potrebbero stendere dei rapporti sui lavori realizzati durante il giorno spedendoli poi alla sede centrale per la rendicontazione).

In Italia la normativa di riferimento del telelavoro nella P.A. e' costituita dal d.lgs. n. 165 del 2001 art. 36; dalla legge 16 giugno 1998, n. 191; dal D.P.R 8 marzo 1999, n.70 (regolamento); dall'Atto di indirizzo all'ARAN e l'Accordo quadro nazionale sul telelavoro nella Pubblica Amministrazione siglato il 23 marzo 2000; dalla deliberazione AIPA del 31 maggio 2001 (regole tecniche).

ART.116

La disposizione in esame in osservanza dei pareri espressi dalle Commissioni giustizia della Camera e del Senato, riproduce l'art. 12 della legge 30 marzo 2001, n. 152, che viene conseguentemente abrogato (art. 183, comma 3, lett. b). In particolare, per lo svolgimento delle proprie attivita', gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle

banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato ai sensi dell'articolo 23 del codice.

ART. 117

La disposizione in esame riproduce l'art. 20, comma 2, lett. e) del d. lgs. n. 467/2001 recante il codice di deontologia e di buona condotta relativo al trattamento di dati in materia di affidabilita' e puntualita' nei pagamenti. In osservanza del parere espresso dalla Commissione giustizia del Senato, la parola "favorire" e' stata sostituita dalla parola "garantire".

ART. 118

La disposizione in esame riproduce l'art. 20, comma 2, lett. d) del d. lgs. n. 467/2001 recante il codice di deontologia e di buona condotta relativo al trattamento di dati in materia di informazioni commerciali. In osservanza del parere espresso dalla Commissione giustizia del Senato, la parola "favorire" e' stata sostituita dalla parola "garantire".

ART. 119

Tale disposizione contiene una norma di "chiusura" relativa ai trattamenti effettuati nell'ambito di banche di dati per finalita' connesse ai comportamenti debitori (es. registro dei protesti), al fine di assicurare modalita' del trattamento e termini di conservazione dei

dati omogenei. A tale scopo la disposizione chiarisce che con il codice di deontologia e di buona condotta di cui all'articolo 118 (relativo al trattamento di dati in materia di informazioni commerciali) sono altresi' individuati termini armonizzati di conservazione dei dati personali contenuti, in particolare, in banche di dati, registri ed elenchi tenuti da soggetti pubblici e privati, riferiti, appunto, al comportamento debitorio dell'interessato, in casi diversi da quelli gia' disciplinati nel codice di cui all'articolo 117, che riguarda i trattamenti effettuati nell'ambito delle c.d. "centrali rischi" private. Al riguardo una specifica disposizione transitoria stabilisce che dalla data di efficacia delle disposizioni del codice deontologico di cui all'art. 118, i termini di conservazione dei dati indicati dal presente articolo, eventualmente previsti da norme di legge o di regolamento, si osserveranno nella misura indicata nel medesimo codice (art. 183, comma 5).

ART. 120

La disposizione in esame si riferisce alla banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli presso l'ISVAP, prevedendo che il medesimo organismo stabilisca le modalita' per

l’accesso alle informazioni ivi raccolte da parte degli organi giudiziari e delle pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti, nonche’ delle imprese di assicurazione. La norma era contenuta nell’art. 2, comma 5 *quater 1,* del d.l. 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge n. 137/2000, che viene conseguentemente abrogato *in parte qua* (art. 183, comma 3, lett. f)).

ART. 121

Con tale disposizione si apre il Titolo X interamente dedicato all’attuazione della direttiva 2002/58 del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, secondo quanto previsto dall’articolo 26 della legge 3 febbraio 2003, n. 14 (legge comunitaria 2002) che ha prorogato il termine per l’adozione del presente codice anche al fine del previo recepimento della predetta direttiva.

Com’e’ noto, la direttiva 2002/58 ha sostituito la precedente direttiva 97/66/CE del 15 dicembre 1997, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni, recepita nel nostro ordinamento con il decreto legislativo 13 maggio

1998, n. 171 e con alcuni mirati interventi di completamento apportati al medesimo d.lgs. n. 171/1998 dal decreto legislativo n. 467/2001 (artt. 21, 22 e 23, in materia di modalita' di pagamento alternative alla fatturazione, di informazione al pubblico sull'identificazione della linea chiamante e collegata, nonche' in materia di chiamate di emergenza).

Il titolo in commento, pertanto nel "riportare" nel codice le disposizioni previgenti contenute nel d. lgs. n. 171/1998, le modifica ed integra al fine di attuare le disposizioni della direttiva n. 2002/58 innovative o specificative della precedente direttiva.

In particolare con quest'art.121 si definisce l'ambito di applicazione del Titolo X rappresentato dal trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, per le cui definizioni, in parte innovative rispetto a quanto previsto dalla direttiva 97/66, in ragione del progresso tecnologico registrato in questi anni, si rimanda all'art. 4 del codice.

ART. 122

La disposizione in esame recepisce una nuova previsione della direttiva 58/2002 (art. 5, par. 3). La disposizione introdotta vieta l'uso di una rete di comunicazione elettronica per accedere a

informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, a fini di archiviazione di informazioni o di monitoraggio delle operazioni effettuate dall'utente medesimo.

Si prevede, tuttavia, che il codice di deontologia da adottare in materia (cfr. art. 133) possa individuare i presupposti in presenza dei quali l'uso della rete nei modi predetti puo' essere consentito, purche' si tratti di scopi legittimi relativi a specifici servizi richiesti dall'abbonato o dall'utente, e quest'ultimo abbia espresso il proprio consenso informato.

Qualche autore (CIACCI) ritiene che questa disposizione tende a risolvere i dubbi inerenti alla regolamentazione dei cosiddetti cookies e comunque di tutte quelle metodologie tecniche che permettono o permetteranno di acquisire informazioni sull'utente in maniera piu' o meno "trasparente".

ART. 123

La disposizione in esame, che riguarda il trattamento dei dati relativi al traffico, individua il periodo di tempo entro il quale il fornitore puo' trattare i dati strettamente necessari per la fatturazione, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento (non superiore a sei mesi, salvo in caso di

contestazione). In aderenza al parere espresso dalla Commissione giustizia del Senato, la disposizione chiarisce meglio l'ambito temporale di conservazione dei dati in caso di contestazione.

Rispetto alla previgente disposizione (art. 4, comma 3, d. lg. 171/1998), il comma 3 e' integrato con la previsione che il consenso espresso dall'abbonato o dall'utente al trattamento dei dati personali a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, puo' essere revocato in ogni momento.

Il comma 4, interamente innovativo, introduce una specifica garanzia di trasparenza per l'abbonato o per l'utente, precisando che nel fornire l'informativa di cui all'articolo 13, il fornitore del servizio, in relazione ai trattamenti appena descritti, deve informare espressamente l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata dei medesimi trattamenti (art. 6, par. 4, dir. 2002/58).

ART. 124

Tale disposizione riguarda le modalita' di documentazione dei dati di traffico ai fini della fatturazione. Com'e' noto, gia' in base alla normativa previgente (art. 5, d. lgs. n.

171/1998), l’abbonato ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura (data e ora di inizio della conversazione, numero selezionato, scatti, ecc.). Il citato art. 21 del d. lgs. n. 467/2001 aveva gia’ integrato tale normativa apportandovi, in linea con quanto previsto dalla precedente direttiva 97/66, alcuni correttivi per assicurare il contemperamento dell’esigenza degli abbonati di visionare il dettaglio del proprio traffico telefonico ai fini del pagamento della fattura con la riservatezza di altri utenti, in relazione, in particolare, alla disponibilita’ di modalita’ di pagamento alternative alla fatturazione. Il codice completa l’intervento di attuazione della corrispondente ed analoga previsione della nuova direttiva 2002/58, stabilendo che il fornitore del servizio e’ tenuto ad abilitare l’utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente e in modo agevole, avvalendosi per il pagamento di modalita’ alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate. L’art. 124, peraltro, conferma la previsione del "mascheramento" sulle fatture delle ultime tre cifre dei numeri chiamati, ma in linea con il progressivo adeguamento dei

fornitori alla previsione comunitaria, a seguito dell'ampia diffusione nel nostro Paese dei mezzi di pagamento alternativi, prevede che il Garante, accertata l'effettiva disponibilita' di tali mezzi, puo' autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

Per i casi in cui si adotti il "mascheramento", la disposizione contiene, inoltre, un'importante integrazione precisando che l'abbonato puo' richiedere la comunicazione "in chiaro" dei numeri chiamati per esclusivi fini di specifica contestazione dell'esattezza di determinati addebiti o di periodi limitati.

ART. 125

La disposizione in esame riproduce pedissequamente l'art. 6 del d. lgs. n. 171/1998, come integrato dall'art. 22 del d. lgs. n. 467/2001.

ART. 126

L'articolo in esame (del tutto nuovo) da' attuazione alla disposizione della direttiva 2002/58 che ha previsto il trattamento di dati relativi all'ubicazione dell'abbonato o dell'utente.

Per "dati relativi all'ubicazione", si intende 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 (art. 4).

La disposizione prevede che se tali dati sono diversi da quelli relativi al traffico e sono effettivamente oggetto di trattamento, nei limiti in cui l'attuale tecnologia lo consenta, essi possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, anche in questo caso revocabile in ogni momento. Gli stessi soggetti conservano, inoltre, il diritto di richiedere l'interruzione temporanea del trattamento di tali dati.

Anche tale norma prevede, a fini di trasparenza, uno specifico onere informativo per il fornitore del servizio in relazione alla natura dei dati, agli scopi e alla durata del trattamento, nonche' sull'eventualita' che i dati siano trasmessi ad un terzo per la prestazione di un servizio a valore aggiunto.

ART. 127

La disposizione in esame riguarda le chiamate di disturbo o di emergenza e ricalca pressoche' pedissequamente quella previgente (art. 7, d. lgs. n. 171/1998, come modificato dall'art. 23, d. lgs. n. 467/2001), salvo due precisazioni relative alle chiamate di disturbo che consentono una piu' agevole applicazione della norma: a) la richiesta di rendere temporaneamente inefficace

la soppressione della presentazione dell'identificazione della linea chiamante e di conservare i dati relativi alla provenienza della chiamata ricevuta, nel caso in cui sia preceduta da una richiesta telefonica deve essere inoltrata comunque in forma scritta entro quarantotto ore e non piu' entro ventiquattro ore, termine apparso, in sede applicativa, troppo stringente per l'abbonato; b) i dati conservati possono essere comunicati all'abbonato che dichiari di utilizzarli per esclusive finalita' di tutela rispetto a chiamate di disturbo.

Per quanto riguarda le chiamate di emergenza, la norma precisa che i servizi abilitati in base alla legge a ricevere chiamate d'emergenza sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorita' per le garanzie nelle comunicazioni.

ART. 128

La disposizione in esame riproduce pressoche' pedissequamente l'art. 8 del d. lgs. n. 171/1998.

ART. 129

La disposizione in esame riguarda gli elenchi degli abbonati. La norma conferma l'assetto secondo cui le modalita' di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico, sono individuate dal Garante con proprio

provvedimento, in cooperazione con l'Autorita' per le Garanzie nelle comunicazioni anche in riferimento ai dati gia' raccolti prima dell'entrata in vigore del presente codice.

ART. 130

La disposizione in esame riguarda le comunicazioni indesiderate (c.d. spamming), gia' oggetto di previsione normativa nell'art. 10 del d. lgs. n. 171/1998, e da' piena attuazione al principio codificato nell'art. 13 della direttiva 2002/58 in base al quale l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore (dispositivi automatici di chiamata), del fax e della posta elettronica "a fini di commercializzazione diretta" e' consentito solo "nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso" (c.d. opt-in).

L'art. 130 chiarisce che la disposizione riguarda l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale e si applica anche alle comunicazioni elettroniche effettuate, per le finalita' appena indicate, mediante messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

Sempre in attuazione del medesimo art. 13 della direttiva, l'art. 130 stabilisce che se il

titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica gia' fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, puo' non richiedere il consenso dell'interessato sempre che l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, inoltre, deve essere informato della possibilita' di opporsi in ogni momento al trattamento.

Si prevede, inoltre, il divieto di inviare comunicazioni per le finalita' in esame o, comunque, a scopo promozionale, camuffando o celando l'identita' del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i propri diritti.

Il problema dello spamming e' stato innanzitutto affrontato in ambito comunitario e si deve riconoscere che le soluzioni adottate dai vari provvedimenti sono state diverse. Difatti la Direttiva sul commercio elettronico 2000/31/CEE, di recente recepita dal nostro ordinamento, nell' affrontare all'art. 7 il tema della comunicazione commerciale non sollecitata esige dal destinatario un comportamento attivo di rifiuto preliminare stabilendo l'onere di inclusione delle persone fisiche all'interno di registri «negativi» che le societa' di

telemarketing sono obbligate a consultare, prima dell'invio della comunicazione commerciale non sollecitata. E' questo il principio dell'opt-out che prevede appunto l'onere di iscriversi in determinati registri c.d. orange-books per non ricevere la posta non sollecitata.

Al contrario la direttiva 2002/58/CE ha recepito, quale sistema di regolamentazione del problema, il principio secondo cui l'invio di messaggi di posta elettronica di carattere pubblicitario e' subordinato all'espresso consenso dell'interessato ("opt-in"). In particolare secondo tale principio esiste un onere a carico del "sollecitatore telematico" in quanto il destinatario deve essere messo in grado di identificare immediatamente, con una dicitura particolare sulla "busta" della posta elettronica, la comunicazione commerciale non sollecitata, senza doverla aprire. In sostanza, la comunicazione commerciale non sollecitata deve potersi distinguere dalle altre comunicazioni che il destinatario riceve al proprio domicilio informatico, con la facolta' di poter cestinare il messaggio senza doverlo leggere. Naturalmente la presenza della accettazione espressa del messaggio non sollecitato non esime il mittente dall'indicare con precisione l'indirizzo a cui inviare eventuali doglianze.

Il nostro Garante ha espresso un positivo avviso in ordine alla predetta opzione (v. Newsletter 12 - 18 febbraio 2001). D'altronde, come chiarito dall'Autorita' nel corso del 2002, le precedenti disposizioni: legge 675/1996 (art. 11), il d.lgs. 171/1998 (art. 10) ed il d.lgs. 185/1999 (art. 10, comma 1) gia' riconducevano la fattispecie in esame alla regola del consenso preventivo ed esplicito che e' stata confermata dal nuovo codice in materia di protezione dei dati personali.

In particolare il fenomeno e' disciplinato dall'art. 10 del d.lgs. n. 171/98 (Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attivita' giornalistica). La norma per la verita' non e' molto chiara, difatti testualmente dispone che "L'uso di un sistema automatizzato di chiamata senza intervento di un operatore o del telefax per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, e' consentito con il consenso espresso dell'abbonato". Comunque, anche se manca un esplicito riferimento ai messaggi di posta elettronica, il collegamento al telefax ed ad un sistema automatizzato di chiamata autorizza

un’agevole interpretazione estensiva della stessa norma, che implicitamente diventa comprensiva sia dei messaggi sms che della posta elettronica. Piu’ nello specifico, con particolare riguardo ai contratti a distanza, e’ applicabile l’art. 10 del d.lgs. n. 185/99 che ha recepito la direttiva n. 97/7/CE e testualmente dispone che “L'impiego da parte di un fornitore del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax, richiede il consenso preventivo del consumatore”.

In senso conforme, il Garante si e’ espresso in occasione di diverse decisioni adottate in merito ai ricorsi presentati da alcuni utenti, ai sensi dell’ art. 29 della legge 675/1996 (Provvedimenti del 25 giugno, 25 luglio e 30 settembre 2002). Accertata la fondatezza delle pretese dei ricorrenti l’Autorita’ ha provveduto a bloccare le banche dati delle relative societa’ che avevano inviato numerose e-mail pubblicitarie e promozionali senza aver acquisito, in via preventiva, il consenso informato degli interessati.

Addirittura in un recente provvedimento datato 29 maggio 2003 che ha per oggetto lo spamming a fini di profitto, il Garante ha puntualizzato che inviare e-mail pubblicitarie senza il consenso del destinatario e’ vietato dalla legge. Se

questa attivita', specie se sistematica, e' effettuata a fini di profitto si viola anche una norma penale e il fatto puo' essere denunciato all'autorita' giudiziaria.

Infine, in caso di reiterata violazione di tali disposizioni e' previsto che il Garante possa prescrivere ai fornitori dei servizi di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

ART. 131

Tale disposizione riproduce pedissequamente l'art. 3 del d. lgs. n. 171/1998.

ART. 132

La disposizione in esame da' attuazione all'art. 15 della direttiva 2002/58 che attribuisce allo Stato membro la facolta' di adottare disposizioni volte a limitare alcuni diritti ed obblighi previsti dalla medesima direttiva quando cio' sia necessario per eccezionali esigenze di tutela di particolari interessi pubblici delimitati, dopo ampio dibattito, dalla stessa direttiva prevedendo, fra l'altro, che i dati siano conservati dai fornitori per un tempo limitato.

In effetti questa disposizione e' stata di recente modificata dal Decreto legge n.354 del 24 dicembre 2003 che all'art. 3 contiene una nuova formulazione di quest'art. 132.

La vecchia formulazione della norma si limitava a stabilire che "fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi, per finalita' di accertamento e repressione di reati, secondo le modalita' individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante". Mentre il nuovo testo (molto piu' articolato) si compone di ben sei commi che, essenzialmente, allungano i tempi di conservazione dei dati di traffico fino a cinque anni, oltre a definire i criteri soggettivi, tecnici e procedurali per la conservazione e l'accesso.

Tra le misure piu' interessanti assume una particolare rilevanza la previsione di nuovi e piu' lunghi tempi di conservazione dei dati di traffico telefonico per favorire indagini su gravi fatti connessi alla criminalita' organizzata ed al terrorismo. Inoltre, per il medesimo fine, e con le adeguate garanzie determinate dal Garante per la privacy, i fornitori di accesso ad Internet sono tenuti a conservare per un periodo di trenta mesi (prorogabili di ulteriori trenta mesi) i dati relativi alle connessioni, con tutti gli elementi

utili ad individuare data, ora e durata del collegamento, esclusi comunque i contenuti.

Sul piano formale, tenendo conto della giurisprudenza costituzionale e di legittimita' in materia, in particolare sulla natura dei dati in questione e sulle modalita' di acquisizione da parte della sola autorita' giudiziaria, la finalita' della conservazione di tali dati viene piu' direttamente collegata all'accertamento e alla repressione dei reati, specificando meglio il contesto per il quale l'esigenza cui fa riferimento l'articolo in commento e' stata prefigurata, vale a dire in relazione ai dati di traffico telefonico.

ART. 133

La disposizione in esame riproduce l'art. 20, comma 2, lett. a) del d. lgs. n. 467/2001 prevedendo la promozione da parte del Garante della sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, con particolare riguardo ai criteri per assicurare ed uniformare una piu' adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalita' del loro

trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una piu' ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualita' delle modalita' prescelte e il livello di sicurezza assicurato.

Come e' noto questi codici di deontologia rappresentano un modello gia' sperimentato per il passato in altri campi, come quello giornalistico. In particolare il Garante ha emanato tre codici di comportamento e cioe' nel 1998 quello per l'attivita' giornalistica e nel 2001 quelli sul trattamento dei dati per obiettivi storici e statistici.

L'intento e' quello di pubblicare questi codici di autodisciplina sulla Gazzetta Ufficiale al fine di dotare gli stessi di una specifica forza prescrittiva e poter garantire: la trasparenza, la riservatezza, il corretto uso dei dati che viaggiano nella rete ricorrendo a degli strumenti elastici, in grado di adeguarsi rapidamente alle nuove esigenze dell'epoca attuale.

Questi codici, difatti, sono elaborati direttamente dalle parti interessate e quindi dagli utenti, dai consumatori e d'altro canto l'Autorita' sta coinvolgendo tutti i soggetti

pubblici e privati maggiormente rappresentativi e interessati a questo tipo di trattamento, che abbiano titolo a partecipare all'elaborazione e all'adozione dei rispettivi codici deontologici.
In questo modo tutti potranno cosi' difendersi dal pericolo derivante dall'uso improprio delle informazioni, dalle frodi, dalle violazioni di legge.
Tale metodologia per quanto innovativa e sicuramente democratica non appare, per la verita', particolarmente efficace in un settore come Internet potenzialmente molto pericoloso e gia' difficile da disciplinare. Si auspica, quindi, che questi stessi codici di autodisciplina possano avere una piu' incisiva forza cogente, allo scopo di evitare inutili dichiarazioni di intenti che puntualmente non vengano rispettate.
La novita' rappresentata dall'introduzione di un simile codice e' comunque estremamente significativa perche' crea i presupposti per una disciplina di autoregolamentazione con forti aperture di semplificazione, ma inquadrata entro precisi parametri di conformita' alle leggi ed ai regolamenti, alle raccomandazioni del Consiglio d'Europa ed ai principi fondanti la disciplina europea della privacy cosi' come interpretati dal Gruppo di lavoro costituito dalla direttiva n. 95/46/CE (COMANDE').

Con tale disposizione e' evidente che il legislatore pensi alle notevoli opportunita' che un quadro di sicurezza per gli utenti puo' offrire per lo sviluppo delle attivita' informative in rete. Il riferimento esplicito sia ai principi dell'art. 11 che alla possibilita' di certificare la qualita' lascia chiaramente intendere che vi saranno spazi per livelli diversi di qualita' della tutela offerta e che i singoli fornitori potranno utilizzare i loro investimenti in protezione a fini di distinzione e fidelizzazione sul mercato (COMANDE'). Inoltre, per quanto rimangano le perplessita' sopra evidenziate, il richiamo alle modalita' del trattamento ed ai requisiti dei dati lascia intuire che a presidiare i contenuti del codice sono poste pure le regole della responsabilita' civile (l'art. 15, comma 2, del codice sanziona la risarcibilita' del danno non patrimoniale per violazione dell'art. 11).

ART. 134

La disposizione in esame riproduce l'art. 20, comma 2, lett. g) del d. lgs. n. 467/2001 prevedendo la promozione da parte del Garante della sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalita' di trattamento e forme semplificate di

informativa all’interessato per garantire la liceita’ e la correttezza anche in riferimento a quanto previsto dall’articolo 11. Chiaramente per quest’articolo valgono le stesse considerazioni fatte per l’articolo precedente, ma sono necessarie ulteriori riflessioni.

La videosorveglianza rimane un tema di grande rilievo e interesse per l' opinione pubblica. Difatti le videocamere ormai sono molto diffuse nelle nostre citta’ e gli utilizzi piu’ comuni dei sistemi di videosorveglianza possono essere classificati in: sistemi di rilevazione e controllo dei flussi di traffico; sistemi di rilevazione delle infrazioni al codice della strada; sistemi di vigilanza nel pubblico trasporto; sistemi di controllo dei perimetri e degli spazi di stabilimenti ed edifici pubblici da sottoporre a particolare tutela; aree a grande presenza di pubblico quali le stazioni, le aree aeroportuali e portuali, i grandi magazzini e centri commerciali, centri direzionali; filiali bancarie, sportelli automatici, farmacie e rivendite di merci di valore; stazioni di rifornimento; parcheggi e aree pubbliche ove si sono riscontrati frequenti episodi malavitosi.

Considerato che la normativa sulla privacy ha sempre considerato dato personale qualsiasi informazione che permette l' identificazione della persona compresi i suoni e le immagini. Di

conseguenza, anche, una semplice installazione di videocamera, o una registrazione sonora per esempio, deve essere conforme alle disposizioni sulla privacy: a quale tipo di funzione o per quale finalita' viene realizzata; la sicurezza e la conservazione delle immagini e delle riproduzioni; l' uso appropriato rispetto alla finalita'; l' informazione agli interessati. Questa e' la posizione del Garante resa nota, non solo, in diverse decisioni e pareri ma anche in una sorta di decalogo elaborato il 29 novembre 2000 che raccoglie le regole da rispettare per non violare la privacy, in caso di attivita' di videosorveglianza. In particolare il Garante ritiene che sia necessario determinare esattamente le finalita' perseguite attraverso la videosorveglianza e verificarne la liceita' in base alle norme vigenti; il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi; qualora sia richiesta la notifica e' necessario indicare fra le modalita' di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza; nell'ambito delle informazioni e' necessario fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza; occorre rispettare scrupolosamente il divieto di controllo a

distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970); occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalita' perseguite; occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorita' giudiziarie o di polizia; occorre designare per iscritto i soggetti - responsabili e incaricati del trattamento dei dati; i dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalita' diverse o ulteriori, salvo alcune eccezioni (finalita' di polizia e giustizia); i particolari impianti per la rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato devono essere conformi anche alle disposizioni contenute nel D.P.R. 250/1999.

Come si puo' rilevare, quindi, il Garante ha prescritto con questo decalogo per gli impianti di videosorveglianza il rispetto di tutte le cautele previste dalla normativa sulla privacy con qualche garanzia in piu'. Ma le difficolta', anche di natura tecnologica, che comportano tali

impianti non sempre sono facilmente risolvibili ed in alcuni casi il Garante ha dovuto affrontare questioni molto complesse. Si pensi, ad esempio, a quando i vari istituti di credito hanno richiesto al Garante per la protezione dei dati personali l'autorizzazione ad utilizzare presso i propri sportelli sistemi di temporanea acquisizione cifrata delle impronte eventualmente associati ad immagini specie in relazione a determinate situazioni di rischio. Il Garante a fronte di una tale richiesta ha dovuto decidere in maniera "salomonica" sottolineando da un lato, che l'utilizzo generalizzato ed indiscriminato di tali sistemi non e' consentito, in quanto viola la normativa sulla privacy mentre dall'altro lato, ha ammesso che le esigenze di sicurezza degli Istituti bancari connesse a particolari circostanze di rischio possono giustificare l'utilizzo di sistemi di rilevazione cifrata di impronte digitali sul presupposto del rispetto di fondamentali garanzie.

Ed e' proprio per affrontare tali difficolta', che il Codice ha previsto la sottoscrizione di un codice deontologico e di buona condotta.

ART. 135

La disposizione in esame riproduce, con gli opportuni adeguamenti, l'art. 20, comma 4, lett. c), della l. n. 675/1996 prevedendo la promozione da parte del Garante della sottoscrizione di un

codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o per far valere o difendere un diritto in sede giudiziaria, in particolare da liberi professionisti o da soggetti che esercitano un'attivita' di investigazione privata autorizzata in conformita' alla legge.

ART. 136

La disposizione in esame apre il Titolo XII relativo al trattamento effettuato nell'esercizio della professione di giornalista o da pubblicisti o per finalita', anche temporanee, di pubblicazione o diffusione occasionale di articoli e altre manifestazioni del pensiero anche nell'espressione artistica.

Il capo si limita, sostanzialmente, a riordinare la materia disciplinata dalla l. n. 675/1996, ove non risultava di agevole leggibilita' anche perche' le pertinenti disposizioni erano collocate in piu' parti della medesima legge, a secondo che riguardassero il trattamento di dati comuni o di dati sensibili, o altri aspetti.

L'articolo in esame contiene anche un importante intervento di attuazione della direttiva 95/46, prevedendo che nell'ambito dei trattamenti effettuati per finalita' di manifestazione del pensiero rientrano anche quelli nel campo

dell'espressione artistica, nel caso in cui, ovviamente, abbiano ad oggetto dati personali (art. 9, dir. 95/46).

ART. 137

La disposizione in esame riprende i principi enunciati negli artt. 25 comma 1 e 28 comma 6 della precedente legge 675/96.

L'esercizio della professione giornalistica o dell'attivita' informativa, proprio in quanto assistito dalla garanzia costituzionale, costituisce eccezione e dunque gode di un regime derogatorio (entro certi limiti) con riferimento specialmente al consenso dell'interessato, all'autorizzazione del Garante, al trasferimento dei dati all'estero ed alle garanzie previste per i dati giudiziari.

ART. 138

La disposizione in esame riprende quanto prescritto dall'art. 13, comma 5, della legge 675/96 sancendo la validita' delle norme sul segreto professionale degli esercenti la professione di giornalista limitatamente alla fonte di notizia.

ART. 139

La disposizione in esame riproduce, con gli opportuni adeguamenti formali, l'art. 25 della l. n. 675/1996, nella parte relativa all'adozione del codice di deontologia.

Un’importante intervento di razionalizzazione consiste nell’aver esteso, per ragioni di omogeneita’, anche al codice di deontologia in materia di giornalismo la particolare "efficacia" delle disposizioni in esso contenute, il cui rispetto costituisce condizione di liceita’ del trattamento, nonche’ la previsione dell’allegazione al presente codice (art. 12, comma 4).

Una delle caratteristiche di maggior rilievo del codice di deontologia dei giornalisti e’ quella di essere applicabile non solo ai giornalisti iscritti all’albo, ma anche a tutti i soggetti che realizzano trattamenti diretti alla pubblicazione occasionale di “articoli, saggi o altre manifestazioni di pensiero). Le disposizioni adottate dal Consiglio dell’Ordine spiegano, dunque, la propria efficacia anche al di fuori della categoria sottoposta a tale organismo, abbandonando cosi’ la valenza di disposizioni deontologiche in senso tradizionale.

ART. 140

La disposizione in esame riproduce l’art. 20, comma 2, lett. g) del d. lgs. n. 467/2001 prevedendo la promozione da parte del Garante della sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il

compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni.

ART. 141

La disposizione in esame indica le forme di tutela dell'interessato dinanzi al Garante, che trovano poi la propria specifica disciplina nelle sezioni successive. L'articolo consente di avere, da subito, il quadro d'insieme delle diverse possibilita' di tutela per l'interessato, agevolando, cosi', la lettura delle norme successive.

L'art. 141 conferma che l'interessato puo' rivolgersi al Garante in tre forme diverse a secondo dei diritti che intende far valere o, comunque, della tutela richiesta:

a) mediante "reclamo" circostanziato (art. 142), quando intende rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;

b) mediante "segnalazione" se, pur non essendo possibile presentare un reclamo circostanziato, intende sollecitare un controllo da parte del Garante sulla disciplina medesima (art. 144);

c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7.

Da segnalare il riferimento alla "disciplina rilevante" in materia di protezione dei dati, con il quale il codice, da un lato, reca un ulteriore riconoscimento delle nuove fonti normative rappresentate dai codici di deontologia, che si aggiungono, quale ulteriore parametro di liceita' del trattamento, alle disposizioni di legge o di regolamento, e, dall'altro, opportunamente rinvia a disposizioni anche di altri settori dell'ordinamento che comunque rilevino ai fini dell'applicazione dei principi in materia di protezione dei dati personali.

ART. 142

La disposizione in esame chiarisce, in linea con quanto l'esperienza di questi primi anni di applicazione della legge n. 675/1996 ha "suggerito", che il reclamo deve contenere un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, oltre che delle disposizioni che si presumono violate e delle misure richieste. Tale aspetto "qualifica" il reclamo rispetto alla segnalazione, alla quale, invece, l'interessato puo' ricorrere per sottoporre al Garante una violazione meno dettagliata e circoscritta della disciplina in materia di protezione dei dati personali, sollecitando un intervento di

controllo del Garante nei modi previsti dai successivi articoli.

L’articolo reca anche indicazioni circa le modalita’ di presentazione del reclamo, specificando che esso e’ inoltrato al Garante senza particolari formalita’, al fine di rendere piu’ agevole possibile il ricorso a questa forma di tutela. A tale scopo, il Garante puo’ anche predisporre un modello per la proposizione del reclamo.

L’istituto del reclamo, quindi, nel codice acquista un’autonomia strutturale, passando da meccanismo idoneo ad attivare la funzione di controllo che fa capo al Garante a una specifica forma di tutela, nella disponibilita’ della parte, a cui corrisponde un dovere di pronuncia da parte del Garante (TRICOMI).

ART. 143

La disposizione in esame, sempre nel quadro di un sistema semplificato e snello, "procedimentalizza" le fasi di proposizione del reclamo e del suo esame da parte del Garante.

Si prevede, infatti, una fase di istruttoria preliminare, all’esito della quale se il reclamo non e’ manifestamente infondato e sussistono i presupposti per un intervento dell’Autorita’, il Garante, anche prima della definizione del procedimento, adotta le prescrizioni e i divieti necessari.

Non si tratta di specifiche decisioni adottabili esclusivamente nell'ambito di tali procedimenti, ma dei provvedimenti che il Garante puo' adottare anche d'ufficio nell'ambito dei poteri di controllo attribuitigli (art. 154, gia' 31 della legge n. 675/1996).

In particolare il Garante puo':

- invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente prima di prescrivere le misure di cui ai punti seguenti;
- prescrivere al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;
- disporre il blocco o vietare, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui al punto precedente, oppure quando, in considerazione della natura dei dati o, comunque, delle modalita' del trattamento o degli effetti che esso puo' determinare, vi e' il concreto rischio del verificarsi di un pregiudizio rilevante per uno o piu' interessati;
- vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettivita'.

L’art. 143 prendendo sicuramente spunto dalla notificazione per pubblici proclami, precisa, altresi’, che i provvedimenti adottati dal Garante sono pubblicati nella Gazzetta Ufficiale se i relativi destinatari non sono facilmente identificabili per il numero o per la complessita’ degli accertamenti.

ART. 144

La disposizione in esame chiarisce che i provvedimenti descritti possono essere adottati dal Garante anche a seguito della proposizione di una segnalazione, nel caso in cui sia stata avviata un’istruttoria.

La segnalazione quindi non e’ altro che una comunicazione informale e non circostanziata al Garante, con cui l’interessato sollecita un controllo da parte di quest’ultimo sulle prospettate violazioni della disciplina in materia di trattamento dei dati personali (TRICOMI).

Da notare che mentre l’art. 31, comma 1, lett. d) non faceva alcuna distinzione tra reclami e segnalazioni, il codice per la protezione dei dati personali disciplina diversamente i due istituti prevedendo procedure particolari.

ART. 145

La disposizione in esame introduce la sezione III che disciplina la proposizione dei ricorsi al Garante, il relativo procedimento, i

provvedimenti adottabili dall'Autorita' e i rimedi esperibili dal titolare o dall'interessato. Il sistema normativo e' stato razionalizzato mediante una piu' ordinata collocazione delle norme - che nel quadro previgente erano "sparse" in piu' parti della legge n. 675/1996 e nel regolamento di attuazione (D.P.R. n. 501 del 1999) - e con alcuni mirati interventi volti a rendere piu' snello il procedimento, ferma restando l'effettivita' della tutela dell'interessato.

Aderendo allo spirito di tutta la normativa in materia di protezione dei dati personali, improntata piu' ad orientare l'applicazione delle disposizioni da parte degli stessi titolari piuttosto che a sanzionare, nelle diverse forme, i trattamenti illeciti, il codice ha proseguito lungo la linea gia' avviata dalla legge n. 675/1996 di favorire la "composizione" delle controversie direttamente fra l'interessato e il titolare del trattamento, assicurando, da un lato, che i diritti di cui all'art. 7 siano esercitati con richieste il piu' possibile mirate e chiare e, dall'altro, che il riscontro del titolare sia tempestivo e pertinente.

L'articolo in esame chiarisce al 1° comma che la tutela amministrativa e' alternativa a quella giurisdizionale, precisando al 2° comma come il ricorso al Garante non possa essere proposto se,

per il medesimo oggetto e tra le stesse parti, e' gia' stata adita l'autorita' giudiziaria. Naturalmente il ricorso al Garante rende improponibile un'ulteriore domanda all'autorita' giudiziaria tra le stesse parti e per il medesimo oggetto.

ART. 146

La disposizione in esame fissa una condizione di procedibilita' (interpello preventivo) per la proposizione del ricorso al Garante, derogabile solo in caso di urgenza, in presenza di un pregiudizio imminente e irreparabile (TRICOMI). L'interessato per poter proporre ricorso al Garante, deve presentare la domanda che costituirebbe oggetto del ricorso al titolare o al responsabile come previsto dall'art. 8, comma 1, del codice.

La disposizione aggiorna il termine entro il quale e' dovuto il riscontro, anche ai fini della proponibilita' del ricorso al Garante, a quindici giorni dal ricevimento della richiesta, termine ritenuto oggettivamente piu' congruo rispetto a quello di cinque giorni previsto dalla normativa previgente. Inoltre se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessita', ovvero ricorre altro giustificato motivo, il titolare o il responsabile, purche' ne diano comunicazione

all’interessato, possono esaudire la richiesta entro trenta giorni dal suo ricevimento.

ART. 147

La disposizione in esame disciplina il contenuto e le modalita’ di presentazione del ricorso, nei confronti del titolare. La struttura complessiva avvicina il ricorso al Garante ad un ricorso giurisdizionale (TRICOMI). Infatti occorre indicare le parti, il domicilio eletto, l’esperimento dell’interpello preventivo, le ragioni della domanda e i provvedimenti richiesti. Il ricorso oltre che dall’interessato puo’ essere proposto dal procuratore speciale, che non deve essere necessariamente un avvocato. La sottoscrizione del ricorso deve essere autenticata, a meno che sia stata apposta presso l’ufficio del Garante, o con firma digitale, o il procuratore speciale sia un avvocato cui e’ stata conferita procura alle liti (TRICOMI). In relazione, quindi, all’evoluzione tecnologica, e’ previsto che il ricorso e’ validamente proposto anche se e’ trasmesso per via telematica osservando le modalita’ relative alla sottoscrizione con firma digitale e alla conferma del ricevimento dell’istanza.

Inoltre a seguito di qualche incertezza applicativa verificatasi, si e’ chiarito che il ricorso e’ proposto nei confronti del titolare ed e’ rivolto al Garante (commi 1 e 4).

ART. 148

La disposizione in esame prevede i casi di inammissibilita' del ricorso, riprendendo le previsioni dell'art. 19, comma 1, del D.P.R. n. 501/98 e dell'art. 18, comma 5, sempre del D.P.R. n. 501/98.

In particolare il ricorso e' inammissibile se proviene da un soggetto non legittimato e in caso di inosservanza delle disposizioni di cui agli artt. 145 e 146 del codice. Inoltre il ricorso che risulti carente di alcuni degli elementi indicati dalla stessa disposizione in esame puo' essere integrato dal ricorrente, a pena di inammissibilita', o di propria iniziativa, entro sette giorni dalla presentazione, o su sollecitazione del Garante entro sette giorni dalla ricezione dell'invito.

ART. 149

La disposizione in esame disciplina il procedimento relativo al ricorso e riprende in parte la disciplina gia' contenuta nell'art. 29 della legge 675/96 e nel D.P.R. n. 501/98.

L'articolo si caratterizza per alcuni interventi di razionalizzazione nell'ambito del procedimento dove alcuni termini sono stati adeguati all'esperienza applicativa degli ultimi anni, ivi compreso quello entro il quale il Garante deve adottare la propria decisione sul ricorso (sessanta giorni).

Le fasi principali del procedimento sono le seguenti:

- verifica ammissibilita' e non manifesta infondatezza del ricorso;
- eventuale invito alla regolarizzazione;
- comunicazione del ricorso al titolare a cura del Garante con invito all'adesione spontanea, che, se accolto, determina il non luogo a provvedere sul ricorso;
- contestuale comunicazione al ricorrente e al titolare del termine per il deposito di memorie e documenti e della data in cui le parti possono essere sentite in contraddittorio;
- espletamento anche d'ufficio di una o piu' perizie.

ART. 150

La disposizione in esame disciplina i provvedimenti che possono essere emanati a seguito del ricorso e li distingue dalle misure cautelari. Anche in questo caso viene ripresa la disciplina gia' contenuta nell'art. 29 della legge 675/96 e nel D.P.R. n. 501/98.

In via cautelare il Garante puo' disporre provvisoriamente il blocco in tutto o in parte di taluno dei dati, o l'immediata sospensione di una o piu' operazioni di trattamento. La misura decade se non viene definito nei termini il

procedimento ed e' impugnabile insieme alla decisione del ricorso. Con la pronuncia finale il Garante in sede di accoglimento del ricorso ordina al titolare la cessazione del comportamento illegittimo indicando le misure necessarie a tutela dei diritti dell'interessato e dando un termine per l'adozione (TRICOMI).

Si segnala, inoltre, un importante intervento in materia di spese del procedimento, in base al quale in caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese, o di suo rigetto, il provvedimento medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile (comma 6).

ART. 151

La disposizione in esame prendendo spunto dall'art. 29, comma 6, della legge 675/96 prevede che contro il provvedimento espresso o il rigetto tacito di cui all'articolo 150, comma 2, il titolare o l'interessato possono proporre opposizione con ricorso ai sensi dell'articolo 152 del codice.

L'opposizione non sospende l'esecuzione del provvedimento.

ART. 152

La disposizione in esame disciplina il procedimento innanzi all'autorita' giudiziaria ordinaria, sostituendo l'attuale previsione del

procedimento in camera di consiglio con un nuovo procedimento instaurabile con ricorso innanzi al tribunale in composizione monocratica. La disposizione introduce un procedimento molto snello, che tuttavia assicura pienamente alle parti le dovute garanzie, strutturato in modo da assicurare in tempi brevi la decisione. La sentenza non e' appellabile.

La tutela dinnanzi al giudice ordinario abbraccia non solo le controversie in ordine all'applicazione delle disposizioni del codice della privacy, ma anche quelle relative ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione.

Il termine per la presentazione del ricorso all'autorita' giudiziaria avente ad oggetto un provvedimento del Garante e' di trenta giorni dalla comunicazione (anche via fax o posta elettronica – articolo 142, comma 2, art. 150, comma 4) del provvedimento o dalla data del rigetto tacito (TRICOMI).

ART. 153

La disposizione in esame riproduce sostanzialmente l'art. 30 della legge 675/96. Nessuna novita', quindi, e' stata introdotta riguardo all'istituzione, alla natura e alla composizione del Garante.

Nella materia della privacy informatica la scelta del modello dell'Authority, indipendente dal Governo quale e' il Garante, era quasi obbligata in quanto gia' la Direttiva Comunitaria 95/46/CEE del 25 ottobre 1995 imponeva espressamente ad ogni Stato membro di disporre "*che una o piu' autorita' pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente Direttiva, adottate dagli Stati membri*". La Direttiva precisa, inoltre, che tali autorita', che dovranno formare una vera e propria rete europea di controllori, "*sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite*". Le funzioni, che sono di tipo investigativo, regolamentare e giurisdizionale tutelano coloro che ritengano di essere stati lesi in un diritto o liberta' riferita al trattamento dei dati personali (CLARICH).

La legge italiana segue fedelmente il modello comunitario. Infatti il Garante "*opera in piena autonomia e con indipendenza di giudizio e di valutazione*" e non attribuisce al Governo alcun potere diretto nei suoi confronti. Vi e' invece un collegamento istituzionale con il Parlamento che elegge i quattro membri che compongono il nuovo organo collegiale e riceve annualmente una relazione del Garante sull'attivita' svolta. Il legame con il Parlamento oltre ad essere

istituzionale e' anche politico visto che i quattro membri sono eletti, due dalla Camera e due dal Senato, con voto limitato in modo tale da garantire alle opposizioni la possibilita' di esprimere un proprio candidato.

ART. 154

L'articolo in esame disciplina i compiti del Garante riprendendo in buona parte le disposizioni dell'art. 31 della legge 675/96. In particolare quest'articolo e' contraddistinto da alcuni interventi non solo formali: a completamento del compito gia' previsto dalla normativa previgente, in linea con la direttiva europea (art. 28, par. 3, secondo trattino) e con la disciplina normativa di altre autorita' indipendenti, e', ora, previsto che il Garante possa segnalare anche al Parlamento e non solo al Governo l'opportunita' di interventi normativi, con l'ulteriore precisazione che tale segnalazione e' effettuata dall'Autorita' per la necessita' di tutelare i diritti fondamentali della persona, anche a seguito dell'evoluzione del settore (comma 1, lett. f); l'articolo e' stato coerentemente aggiornato nella parte relativa ai compiti di controllo o assistenza attribuiti al Garante in materia di trattamento dei dati personali, in relazione alle altre leggi di ratifica di accordi o convenzioni internazionali o ai regolamenti comunitari che

prevedono tale competenza dell'Autorita' (l. 30 settembre 1993, n. 388, di ratifica dell'accordo di Schengen; l. 23 marzo 1998, n. 93, di ratifica della convenzione istitutiva di Europol; regolamento (Ce) n. 515/97 del Consiglio del 13 marzo 1997 e l. 30 luglio 1998, n. 291, di ratifica della convenzione sull'uso dell'informatica nel settore doganale; regolamento (Ce) n. 2725/2000 del Consiglio dell' 11 dicembre 2000 che istituisce l'"Eurodac").

Inoltre si segnala un'importante intervento con il quale si prevede che nei casi in cui il Garante debba esprimere un parere ai sensi di legge, tale parere deve essere adottato, salvi i termini piu' brevi eventualmente previsti, nel termine di quarantacinque giorni dal ricevimento della richiesta, decorso il quale l'amministrazione puo' procedere indipendentemente dall'acquisizione del parere. E' previsto, peraltro, che per esigenze istruttorie il termine puo' essere interrotto per una sola volta e il parere reso entro venti giorni dal ricevimento degli elementi istruttori (comma 5). La scelta del termine di quarantacinque giorni e' omogenea a quella relativa al rilascio delle autorizzazioni da parte del Garante (art. 40) ed e' in linea con quanto previsto per i pareri del Consiglio di

Stato (art. 17, comma 27, l. 15 maggio 1997, n. 127).

ART. 155

La disposizione in esame nel prevedere i principi applicabili all'ufficio del Garante riprende quanto gia' disciplinato dall'art. 33, comma 1-sexies, della legge 675/96. In particolare si continua a fare riferimento alla legge 241/90 sulla trasparenza amministrativa ai fini dell'individuazione e della disciplina delle funzioni del responsabile del procedimento e al d.lgs. n. 165/2001 ai fini della distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice e le funzioni di gestione attribuite ai dirigenti.

ART. 156

L'articolo in esame riproduce sostanzialmente le restanti disposizioni dell'art. 33 della legge 675/96. In merito alla composizione dell'ufficio del Garante si ricorda che allo stesso e' preposto un segretario generale che dispone di un contingente organico di 100 unita' di personale dipendente.

Inoltre, quale intervento di razionalizzazione, si segnala l'allineamento della disposizione sul segreto d'ufficio cui e' tenuto il personale alla pertinente disposizione del codice penale (il personale e' tenuto al segreto in ordine a

notizie che "*devono rimanere segrete*") (art. 326, c.p.).

ART. 157

La disposizione in esame introduce il Capo III relativo agli accertamenti e controlli effettuati dal Garante. Essa riproduce quanto previsto dall'art. 32, comma 1, della legge 675/96 specificando che il Garante per l'espletamento dei propri compiti puo' richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni o esibire documenti.

ART. 158

La disposizione in esame detta una disciplina generale in materia di accertamenti eseguiti dal Garante riprendendo le previsioni dell'art. 32, commi 2 e 3, della legge 675/96. In particolare se gli accertamenti vengono svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, essi debbono essere effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al piu' tardi entro tre giorni dal ricevimento della richiesta del Garante quando e' documentata l'indifferibilita' dell'accertamento.

ART. 159

La disposizione in esame disciplina le modalita' dell'accertamento riprendendo le previsioni dell'art. 15 commi 2, 4, 5, 6 e 7 del D.P.R. 501/98.

ART. 160

La disposizione in esame riprende quanto previsto dall'art. 32, commi 6 e 7 della legge 675/96 e disciplina le modalita' di esecuzione di accertamenti dell'ufficio del Garante relativi a taluni trattamenti disciplinati ai titoli I, II e III della Parte II del codice, e indicati all'articolo 8, comma 3.

In relazione a questi ultimi si registra un intervento integrativo della normativa, necessario per regolare le modalita' e gli effetti degli accertamenti del Garante riguardo ai trattamenti effettuato nei riguardi di uffici giudiziari, al fine di consentire, in ogni caso, il pieno esercizio della funzione giurisdizionale.

La disposizione chiarisce, infatti, che nell'effettuare tali accertamenti il Garante adotta idonee modalita' che tengano conto anche della particolare collocazione istituzionale dell'organo che procede. Inoltre nel caso di indagini coperte dal segreto, gli accertamenti, quando vi sia richiesta dell'organo procedente, sono differiti (comma 5). In ogni caso, la validita', l'efficacia e l'utilizzabilita' di

atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (comma 6).

ART. 161

La disposizione in esame introduce il capo I che riguarda le fattispecie per la cui violazione e' prevista l'applicazione di una sanzione amministrativa.

La violazione prevista dalla presente disposizione e' l'omessa o inidonea informativa all'interessato. Essa viene punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o piu' interessati, da cinquemila euro a trentamila euro. La disposizione prevede altresi' che, in ambedue le ipotesi la somma puo' essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

ART. 162

La disposizione in esame prevede diverse ipotesi sanzionatorie. Nel comma 1 la cessione dei dati

in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), (quando cioe' essendovi un'ipotesi di cessazione del trattamento, i dati vengono ceduti ad altro titolare, purche' destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono stati raccolti) o di altre disposizioni in materia di disciplina del trattamento dei dati personali e' punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro. Mentre al 2° comma si punisce la violazione della disposizione di cui all'articolo 84, comma 1 (quando vengono resi noti all'interessato o agli altri soggetti che, in determinate condizioni, possono riceverli in sua vece, dati idonei a rivelare lo stato di salute, facendo cio' non per il tramite di un medico designato dallo stesso interessato o dal titolare del trattamento) con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro.

ART. 163

La disposizione in esame, riprendendo l'art. 34, comma 1 della legge 675/96, punisce con la sanzione amministrativa del pagamento di una somma da diecimila a sessantamila euro (oltre che con la pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o piu' giornali indicati nel provvedimento che la applica),

chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione di cui agli artt. 37 e 38 del codice, ovvero indica in tali comunicazioni notizie incomplete. Si tratta, in effetti, della violazione dell'obbligo di tempestiva comunicazione al Garante dell'intenzione di procedere al trattamento di dati personali, affinche' il Garante stesso possa inserire tale notificazione nell'apposito registro (OBERDAN FORLENZA).

ART. 164

La disposizione in esame, riprendendo l'art. 39, comma 1, della legge 675/96 prevede la sanzione amministrativa del pagamento di una somma da quattromila a ventiquattromila euro, nei confronti di chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante, ai sensi degli articoli 150, comma 2 e 157. Mentre quest'ultima disposizione prevede espressamente e in via generale che per l'espletamento dei propri compiti il Garante puo' richiedere al titolare, al responsabile all'interessato o anche a terzi di fornire informazioni e di esibire documenti, l'art. 150, comma 2, nel trattare dei provvedimenti del Garante sui ricorsi propostigli, afferma che cio' avviene "assunte le necessarie informazioni", ipotesi che potrebbe comunque ritenersi

ricompresa in quella piu' generale di cui al citato articolo 157 (OBERDAN FORLENZA).

ART. 165

La disposizione in esame registra l'unico intervento integrativo della normativa in merito al capo I. Essa prevede che nelle fattispecie precedenti (art. 161, 162, 164) puo' essere applicata, in ogni caso, a titolo di sanzione accessoria, la pubblicazione dell'ordinanza-ingiunzione del Garante. La previsione non riguarda, ovviamente, la fattispecie dell'omessa o incompleta notificazione ove la sanzione accessoria e' gia' prevista come obbligatoria.

ART. 166

La disposizione in esame, riprendendo quanto previsto dall'art. 39, comma 3, della legge n. 675/96, disciplina il procedimento di applicazione delle sanzioni. Inevitabile il rinvio alle disposizioni della legge n. 689/81 qualora applicabili.

Commento T.U. privacy

ART. 167

La disposizione in esame riproduce pressoche' pedissequamente l'art. 35 della legge 675/1996, con un unico intervento di razionalizzazione in base al quale si rendono punibili le condotte ivi richiamate solo se dal fatto derivi nocumento, mentre in precedenza il nocumento costituiva solo un'aggravante.

Le condotte punibili riproducono, oltre a quelle gia' contenute nel citato art. 35 della legge 675/1996, anche quelle punite ai sensi del medesimo articolo 35 dall'art. 11 del d. lgs. 171/1998.

Ai sensi del comma 1, quindi, e' punibile il trattamento in violazione delle disposizioni contenute negli articoli 18 e 19 (trattamenti effettuati da soggetti pubblici in relazione a dati diversi da quelli sensibili e giudiziari), art. 23 (che disciplina la prestazione del consenso), art. 123 (trattamento di dati relativi al traffico), art. 126 (trattamento di dati relativi all'ubicazione), art. 130 (comunicazioni indesiderate), ovvero in applicazione dell'art. 129 (elenchi di abbonati).

Ai sensi del comma 2, e' punibile il trattamento in violazione delle disposizioni contenute negli articoli 17 (trattamento che presenta rischi specifici), 20, 21 e 22, commi 8 e 11 (trattamento di dati sensibili e giudiziari effettuato da soggetti pubblici), artt. 25 (divieto di comunicazione e diffusione di dati), 26 e 27 (trattamento di dati sensibili o giudiziari da parte di privati) e 45 (divieto di trasferimento di dati all'estero).

Le pene edittali sono state pienamente adeguate a quanto richiesto dalla Commissione giustizia del Senato.

Si ricorda che la giurisprudenza ha avuto modo di affermare che non risponde del reato di trattamento illecito dei dati personali il giornalista che rivela dati relativi allo stato di salute o alla sfera sessuale di un soggetto, se rispetta i limiti della veridicita' della notizia e dell'essenzialita' dell'informazione riguardo a fatti di interesse pubblico (Tribunale di Pescara, sentenza 12 ottobre 2000). Allo stesso modo, e' stata esclusa la sussistenza del reato allorche' la rilevazione dei dati avvenga nell'ambito della ricostruzione di un episodio delittuoso, in esercizio del diritto di cronaca e vi sia notorieta' dei protagonisti e della parte offesa (Pretura di Roma, 10 ottobre 1998). Al contrario, costituisce trattamento illecito di dati l'organizzazione di questi ultimi in un archivio informatico e il successivo uso per inviare lettere promozionali a clienti, senza il loro consenso (Pretura di Palermo, 4 febbraio 1999).

ART. 168

La disposizione in esame disciplina una fattispecie, introdotta dal decreto legislativo n. 467/2001, che e' stata tecnicamente integrata, per omogeneita' di materia, sanzionando anche il mendacio commesso nelle comunicazioni dovute al Garante ai sensi dell'art. 39. Si rammenta, al riguardo, che la legge 675/1996 gia' sanzionava

la mancata comunicazione, per la quale si veda ora l'art. 167, comma 1 del codice.

ART. 169

La disposizione in esame riproduce l'art. 36 della legge 675/96 prevedendo la pena dell'arresto fino a due anni o l'ammenda da diecimila a cinquantamila euro per chiunque, essendovi tenuto, omette di adottare le misure minime di sicurezza nel trattamento dei dati. Tuttavia per tali ipotesi l'articolo prevede un particolare procedimento di oblazione, potendosi estinguere il reato se: 1) l'autore del reato provvede alla regolarizzazione, in ottemperanza ad una prescrizione del Garante ed entro un termine non superiore a sei mesi; 2) versa una somma pari al quarto del massimo dell'ammenda stabilita (12.500 euro).

ART. 170

La disposizione in esame amplia, coerentemente, le ipotesi di inosservanza di provvedimenti del Garante penalmente sanzionate, punendo anche l'inosservanza dell'autorizzazione adottata dall'Autorita' in relazione al trattamento dei dati genetici. L'intervento si giustifica in ragione della particolare delicatezza della materia disciplinata.

In merito e' opportuno segnalare la preoccupata relazione del Garante sull'attivita' del 2002 avuto riferimento al problema della protezione

dell'identita' dai suoi possibili "furti", (gia' imponente nel settore del commercio elettronico e che esige cautele particolari per le impronte digitali), che puo' divenire drammatico se il furto riguarda materiale che consente di ottenere informazioni genetiche. Se, infatti, grandi sono le opportunita' offerte dalla genetica, altrettanto grandi sono i rischi di utilizzazioni dei dati genetici che possono determinare discriminazioni nell'accesso al lavoro o al credito, nella conclusione di contratti di assicurazione vita o malattia, o attraverso forme di schedatura genetica di massa. Insomma come giustamente sottolineato dall'Autorita' posso nascere nuove disuguaglianze ed in campo internazionale si fa molta attenzione a questo aspetto. E' necessario, quindi, secondo il Garante, controllare la legittimita' di ogni forma di trattamento dei dati genetici ed approntare un sistema di tutela dei dati necessario anche per consentire a tutti di godere al massimo dei benefici della ricerca genetica. Anche in questo settore l'avvento di Internet ha complicato ulteriormente le cose e la diffusione dell'offerta di tests genetici tramite la Rete costituisce un drammatico esempio.

ART. 171

La disposizione in esame punisce il trattamento effettuato in violazione delle disposizioni di

cui agli articoli 113, comma 1, e 114 del codice, che riproducono, sostanzialmente, le disposizioni di cui agli articoli 4 e 8 dello "Statuto dei lavoratori".

Coerentemente resta applicabile la sanzione penale prevista dall'articolo 38 della legge n. 300/1970.

ART. 172

La disposizione in esame riproduce l'art. 38 comma 1 della legge 675/96 prevedendo che la condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

ART. 173

La disposizione in esame apporta alcune modifiche alla disciplina in materia di accesso ai dati registrati nel Sistema d'informazione Schengen di cui agli articoli 10 e ss. della legge 30 settembre 1993, n. 388, di ratifica dell'Accordo di Schengen e della relativa convenzione di applicazione.

Il comma 1, lett. a), modificando l'articolo 9, comma 2, della legge 388/1993, stabilisce che le richieste di accesso, rettifica o cancellazione, nonche' di verifica dei dati personali inserite nel S.I.S. sono rivolte direttamente al Ministero dell'Interno. Il Garante per la protezione dei dati personali esercita, in ogni caso, il controllo sul trattamento di tali dati, anche su

segnalazione o reclamo dell'interessato all'esito di un inidoneo riscontro alla richiesta gia' formulata ai competenti organi del citato ministero e in relazione alla risposta eventualmente fornita dai medesimi organi (art. 11, l. 388/1993, come modificato dall'art. 173, lett. c)).

Sono, inoltre, abrogate le disposizioni della legge n. 388/1993 che operavano un rinvio "temporaneo" alla legge 1 aprile 1981, n. 121, sull'ordinamento della pubblica sicurezza, fino all'entrata in vigore della legge istitutiva del Garante, nonche' quelle relative alla responsabilita' per i danni derivanti dalla violazione delle norme che regolano la raccolta, la conservazione e l'utilizzazione dei dati in relazione alla disciplina prevista al codice (artt. 10, comma 2, e 12, l. 388/1993).

ART. 174

La disposizione in esame contiene alcuni mirati interventi su norme, anche processuali, al fine di tutelare la riservatezza delle persone alle quali sono notificati atti giudiziari, verbali di contravvenzione, avvisi o altri atti amministrativi.

L'intervento normativo riproduce sostanzialmente una proposta parlamentare di modifica di alcune norme dei codici di rito e della legge sulle notificazioni a mezzo posta, approvata da un ramo

del Parlamento nella XIII legislatura e all'esame della Commissione giustizia del Senato.

L'intervento sul codice di procedura civile e' articolato. La principale modifica prevede, intervenendo sull'articolo 137 del medesimo codice, che, nel caso in cui la notificazione non possa essere eseguita nelle mani del destinatario – ipotesi che viene comunque riaffermata come prioritaria, ai sensi del successivo articolo 138, come novellato – la copia dell'atto sia consegnata in busta sigillata sulla quale non sono apposte indicazioni dalle quali possa desumersi il contenuto dell'atto. Un rinvio a tale disciplina viene poi inserito anche nella legge n. 689/1981, relativamente alle notificazioni di sanzioni amministrative.

Si aggiunge, poi, una disposizione al D.P.R. n. 445 del 2000, recante il testo unico delle disposizioni legislative e regolamentari in materia amministrativa (art. 15-bis), volta ad estendere l'applicazione di tale disciplina anche alle notificazioni di atti e di documenti da parte di organi delle pubbliche amministrazioni, ove effettuate a soggetti diversi dagli interessati.

Sono inoltre modificate alcune norme del codice di procedura penale (articoli 148 e 157), e delle relative disposizioni di attuazione, sempre al fine di stabilire che la notifica nelle mani di

soggetti diversi dal destinatario e dal suo difensore deve essere effettuata in busta sigillata e precisando che nelle altre comunicazioni sono contenute le sole indicazioni strettamente necessarie.

Infine, sempre con lo stesso obiettivo, si apportano alcune modifiche alla legge 20 novembre 1982, n. 890, recante notificazioni di atti a mezzo posta.

Da ultimo l'articolo modifica due disposizioni del codice di procedura civile concernenti la pubblicazione degli avvisi relativi alle vendite giudiziarie (artt. 490 e 570, c.p.c.).

ART. 175

L'articolo in esame contiene alcune disposizioni di raccordo con la normativa in materia di trattamenti effettuati nell'ambito del Centro elaborazione dati del Dipartimento della pubblica sicurezza del Ministero dell'interno, in relazione alle disposizioni di cui al Titolo II della Parte II.

ART. 176

La disposizione in esame apporta alcune modifiche a testi normativi che disciplinano l'attivita' e l'organizzazione delle pubbliche amministrazioni.

Al comma 1, l'articolo interviene sulla regolamentazione del diritto di accesso agli atti amministrativi contenuta, in particolare, nell'art. 24, comma 3, della legge n. 241/1990,

al fine di chiarire che le eventuali limitazioni al diritto di accesso ai dati raccolti mediante strumenti informatici – che possono essere stabilite con decreto a tutela degli interessi ivi descritti – non si applicano all'accesso ai dati personali da parte della persona cui i dati si riferiscono, che e' disciplinato dal presente testo unico.

Al comma 2, per assicurare l'omogeneita' del relativo testo unico di settore, l'articolo "sposta" nel decreto legislativo 30 marzo 2001, n. 165, in materia di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, la disposizione gia' contenuta nella legge n. 675/1996 (art. 27, comma 4) in base alla quale i criteri di organizzazione dei pubblici uffici sono attuati nel rispetto della disciplina in materia di trattamento dei dati personali.

Ai commi 3 e seguenti, la disposizione reca una disciplina di raccordo con problematiche relative all'Autorita' per l'informatica nella pubblica amministrazione (ora CNIPA), raccordo che deriva dalla presenza di tali tematiche nell'abrogando art. 42 della legge n. 675/1996.

ART. 177

L'articolo in esame reca alcune disposizioni in materia di anagrafe, stato civile e liste elettorali, necessarie per una piena applicazione dei principi in materia di protezione dei dati

personali e per assicurare il rispetto delle disposizioni del codice.

Un primo intervento riguarda le adozioni e si ricollega a quanto disciplinato dal codice in relazione al diritto all'anonimato della madre in occasione del parto (art. 93). Al riguardo la disposizione al comma 2, novellando l'art. 28, comma 7, della legge n. 184 del 1983, precisa, con una formulazione della norma piu' chiara rispetto a quella originaria, che l'adottato non puo' accedere alle informazioni relative alla madre che abbia dichiarato, alla nascita, di non volere essere nominata nella dichiarazione di nascita.

Altre disposizioni riguardano l'uso di elenchi o liste elettorali o il rilascio di atti in base alla normativa in materia di anagrafe, elettorato attivo e passivo e stato civile (rispettivamente D.P.R. n. 223/1989, D.P.R. n. 223/1967 e D.P.R. n. 396/2000) (commi 1, 4 e 5).

In particolare, per effetto del comma 4, che sopprime le lettere d) ed e) dell'articolo 25 del D.P.R. n. 223/1967, le liste elettorali non indicheranno il titolo di studio, ne' la professione o il mestiere dell'elettore. Inoltre in base ad una modifica apportata all'art. 51 del medesimo D.P.R. 223/1967, ai sensi del quale era consentito a chiunque di copiare, stampare o mettere in vendita le liste elettorali del

comune, si prevede, in relazione al principio di finalita', che copia delle liste elettorali puo' essere rilasciata solo in applicazione della disciplina in materia di elettorato attivo o passivo o per finalita' di studio, ricerca scientifica o storico o socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso.

La disposizione al comma 1, contiene un "raccordo" con la disciplina del rilascio degli elenchi anagrafici per uso di pubblica utilita' (art. 34, comma 1, D.P.R. n. 223/1989), in relazione all'uso di tali elenchi in applicazione della disciplina sulla comunicazione istituzionale.

Il comma 3, infine, contiene alcune importanti precisazioni in relazione al rilascio degli estratti degli atti dello stato civile, chiarendo il novero dei soggetti cui tali estratti possono essere rilasciati e prevedendo, in ogni caso, il libero accesso ad essi decorsi settanta anni dalla formazione dell'atto.

ART. 178

La disposizione in esame contiene alcune modifiche che riguardano la disciplina vigente in materia sanitaria. In particolare, l'art. 5 della legge n. 135/1990, in materia di prevenzione dell'AIDS, e' modificato al fine di precisare che nell'assistenza ai malati di AIDS gli operatori

sanitari devono adottare ogni accorgimento occorrente per la tutela dei diritti e delle liberta' fondamentali dell'interessato, nonche' della relativa dignita'.

L'art. 5 del d.lgs. 539/1992, riguardante la classificazione per la fornitura dei medicinali per uso umano, e' modificato al fine di chiarire che, decorsi sei mesi, il farmacista e' tenuto a distruggere le ricette mediche ed a farlo con modalita' idonee ad escludere l'accesso di soggetti terzi ai dati in esse contenute.

All'art. 2 del decreto del Ministro della Sanita' 11 febbraio 1997, in materia di importazione di medicinali registrati all'estero, sono abrogate le lettere f) ed h) che contenevano disposizioni tali da comportare la violazione della riservatezza del paziente, in quanto prevedevano l'indicazione delle sue generalita' e la menzione del consenso informato prestato.

L'articolo 5-bis del decreto legge 23/1998, convertito con modificazioni dalla legge n. 94 del 1998, (c.d. Di Bella) recante disposizioni urgenti in materia di sperimentazioni cliniche in campo oncologico, e' modificato al fine di chiarire la distinzione fra il consenso medico reso dal paziente e il consenso al trattamento dei dati personali, che tuttavia possono comunque essere prestati in un unico atto.

ART. 179

La disposizione in esame reca alcune modifiche normative di raccordo con disposizioni del codice in materia di lavoro (artt. 114, 115 e 171).

Il comma 2, in particolare, sopprime i riferimenti agli articoli 4 (sugli impianti audiovisivi) e 8 (divieto di indagini sulle opinioni dei lavoratori) della legge n. 300 del 1970, sullo "statuto dei lavoratori", presenti nell'articolo 38 della medesima legge, che riconnetteva alla loro violazione l'applicazione della sanzione penale, ora contenuta nell'art. 171 del codice.

Il comma 3, invece, riguarda un'integrazione alla disciplina delle informazioni dovute a tutela del consumatore, in relazione all'obbligo di rilascio dell'informativa di cui all'art. 13 del codice (art. 12, d. lgs. 22 maggio 1999, n. 185).

ART. 180

La disposizione in esame prevede al 1° comma che le misure minime di sicurezza di cui agli articoli da 33 e 35 e all'allegato B del codice, e gia' non previste dal D.P.R. n. 318/1999, devono essere adottate entro il 30 giugno 2004, assicurando cosi' ai titolari del trattamento un congruo periodo di tempo per l'adeguamento.

I commi 2 e 3 consentono ai titolari che non possiedono strumenti elettronici idonei all'applicazione delle misure minime di disporre

di un ulteriore anno dall'entrata in vigore del codice per adeguarvisi. Essi devono comunque descrivere in un documento a data certa, da conservare presso la propria struttura, le obiettive ragioni tecniche che non consentono le dovute applicazioni e devono, in ogni caso, adottare ogni possibile misura compatibile con gli strumenti elettronici posseduti in modo da evitare un incremento dei rischi.

ART. 181

L'articolo in esame prevede specifici e dettagliati termini di applicazione di alcune disposizioni in relazione ai trattamenti iniziati prima dell'entrata in vigore del codice, al fine di consentire un efficace adeguamento alle nuove norme introdotte in taluni settori che richiedono specifici adempimenti per i titolari del trattamento. In particolare la presente disposizione e' stata modificata dal decreto legge n. 254/2003 a sua volta emendato dal Senato in sede di conversione in legge che ha aggiunto il comma 6-bis con il quale si fa riferimento alla reale efficacia delle misure e degli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, del codice, per la conservazione del traffico telefonico. Lascia perplessi, invece, il richiamo al termine di cui all'articolo 4, comma 2, del decreto legislativo n. 171/98, in quanto a seguito della soppressione

dell'art. 5 del decreto-legge lo stesso d.lgs. n. 171 non esiste piu'.

ART. 182

La disposizione in esame fa riferimento ad eventuali atti interni del Garante di adeguamento alle norme relative al funzionamento dell'Ufficio. In particolare e' previsto che il Garante possa individuare i presupposti per l'inquadramento in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilita' di organico, del personale appartenente ad amministrazioni pubbliche o ad enti pubblici in servizio presso l'Ufficio in posizione di fuori ruolo o equiparato alla data di pubblicazione del presente codice; inoltre il Garante puo' prevedere riserve di posti nei concorsi pubblici, unicamente nel limite del trenta per cento delle disponibilita' di organico, per il personale non di ruolo in servizio presso l'Ufficio che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

ART. 183

L'articolo in esame nel quale si esaurisce il capo III sulle abrogazioni, contiene l'elenco delle disposizioni abrogate.

ART. 184

L’articolo in esame al comma 1, specifica che le disposizioni del codice danno attuazione alle piu’ volte ripetute direttive 95/46/CE e 2002/58/CE.

Il comma 3 riproduce la previgente disposizione della legge n. 675/1996 in base alla quale restano ferme le disposizioni di legge o di regolamento che stabiliscono divieti o limiti piu’ restrittivi in materia di trattamento di taluni dati personali.

ART. 185

La disposizione in esame prevede che i codici deontologici siano allegati al codice. Come gia’ chiarito l’allegazione ha finalita’ documentali.

ART. 186

Questa disposizione stabilisce l'entrata in vigore del codice al 1° gennaio 2004, calibrandola in funzione dei congrui tempi necessari, ferme restando alcune disposizioni transitorie.

Si ricorda che in merito al presente decreto legislativo sono stati acquisiti i pareri delle competenti Commissioni parlamentari. In particolare, per la Camera dei deputati, la V Commissione e la XIV Commissione hanno espresso, parere favorevole; la II Commissione ha espresso anch’essa parere favorevole in merito al provvedimento, formulando alcune osservazioni,

che sono state parzialmente recepite nel testo legislativo. In particolare, non e' stato ritenuto opportuno accogliere le osservazioni che riguardavano alcuni aspetti concernenti l'organico ed il trattamento economico del personale dell'ufficio del Garante e la proposta di riferire le disposizioni di cui agli articoli 7, comma 4, lettera b), 130, comma 1, e 140, comma 1, alle comunicazioni commerciali "interattive". In merito e' stato rilevato che il quadro normativo vigente disciplina l'intero spettro delle comunicazioni, riferendosi, in senso lato, alle comunicazioni commerciali, pubblicitarie e promozionali, senza ulteriori distinzioni, peraltro spesso non di facile individuazione. Inoltre, il testo unico recepisce, all'articolo 130 la disposizione di cui all'articolo 13 della direttiva n. 2002/58/CE, che si riferisce a "fini di commercializzazione diretta", senza introdurre ulteriori distinzioni fra comunicazioni interattive e non.

Sono stati altresi' acquisiti, per il Senato, il parere favorevole, con osservazioni, della 1^ Commissione e il parere favorevole della 5^ Commissione, resi alla 2^ Commissione.