ATTI PARLAMENTARI

XV LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **CXXXVI**
n. **1**

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE E SULLO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(Anno 2005)

(Articolo 154, comma 1, lettera m), del decreto legislativo 30 giugno 2003, n. 196)

Presentata dal Garante per la protezione dei dati personali

(PIZZETTI)

Trasmessa alla Presidenza il 9 maggio 2007

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

RELAZIONE PER L'ANNO 2005

Discorso del Presidente
Francesco Pizzetti

Roma, 7 luglio 2006

PAGINA BIANCA

Signor Presidente della Repubblica,

Signori Presidenti delle Camere,

Signore e Signori,

nel presentare per la prima volta la Relazione sull'attività dell'Autorità, i miei colleghi ed io sentiamo profondamente l'importanza dell'appuntamento e dell'eredità ricevuta dai componenti dei Collegi precedenti al nostro, presieduti dalla grande personalità di Stefano Rodotà. Collegi che hanno edificato e diffuso nel Paese la cultura della privacy, intesa come un più avanzato diritto fondamentale, a presidio della libertà e della dignità delle persone nella società dell'informatizzazione e del trattamento sempre più massiccio dei dati personali.

Il Garante ha dato vita in questi anni ad una significativa esperienza umana e professionale. Ha raccolto intorno a sé donne e uomini di valore che, insieme al Segretario Generale, hanno maturato competenze e professionalità e che vanno ringraziati per il grande impegno profuso.

A livello europeo, l'Autorità ha assunto un ruolo trainante e, anche per il contributo personale di Rodotà, la tutela dei dati è oggi un diritto fondamentale dei cittadini europei, sancito nella Carta dei diritti dell'Unione e poi trasfuso nel Trattato costituzionale che prevede espressamente i Garanti della protezione dei dati personali, come le sole "necessarie" Autorità indipendenti.

Abbiamo ricevuto un patrimonio prezioso che intendiamo onorare, persuasi che, in una democrazia matura e rispettosa della dignità della persona, la protezione dei dati rappresenta un crocevia in cui si intersecano interessi, valori e diritti.

La protezione dei dati personali nelle società "a cambiamento velocissimo"

Le tecnologie si sviluppano con una rapidità inaudita; le relazioni fra gli uomini e i popoli hanno una dimensione globale e una latitudine in cui, senza la

mediazione della tecnica, l'orizzonte non è più visibile allo sguardo dell'uomo; il bisogno di comunicare, di raggiungere tutti e ognuno, convive con l'aspirazione ad un'esistenza sicura, posta al riparo da vecchi e nuovi pericoli.

La società della tecnica, già diventata nel secolo scorso una società "a cambiamento veloce", è divenuta oggi una società "a cambiamento velocissimo".

Il nostro bagaglio di cognizioni è sempre più inadeguato a dare risposte convincenti e persuasive agli interrogativi che gli sviluppi della tecnica pongono alla nostra coscienza.

Rispetto a questa incredibile metamorfosi, è naturale interrogarsi sulla possibilità dell'uomo di esercitare un ruolo di guida e di governo del progresso tecnico; sulla sua capacità di indirizzare l'uso della tecnologia, che è un mezzo, verso fini e risultati al servizio dell'uomo e rispettosi della sua dignità.

La tecnologia può essere un formidabile strumento di libertà oppure causa di inedite differenziazioni sociali.

È qui che si colloca il valore fondamentale racchiuso nelle regole e nei comportamenti in cui consiste il diritto alla privacy.

La protezione dei dati personali assolve un ruolo essenziale nella ricerca di un rapporto armonico e bilanciato fra l'uomo e la tecnica; fra la società in continuo divenire e la capacità di adattamento dell'individuo.

È indispensabile l'esistenza di istituzioni capaci di assicurare che i dati accumulati grazie alle tecnologie non siano usati *contro* di noi, ma solo *per* noi.

In una società libera e democratica, la tutela dei valori e dei principi connaturati all'essere cittadino rappresenta la risposta più efficace per contrastare una lettura pessimista del progresso.

La compatibilità democratica e l'accettazione sociale della tecnologia richiedono un sistema di garanzie che a pieno titolo comprende anche la protezione dati.

Più cresce la mobilità esistenziale e sociale che, consapevolmente o inconsapevolmente, ci fa disperdere parti del nostro essere in innumerevoli luoghi, più è

essenziale l'attività di un'Autorità che, proteggendo i dati di ciascuno da trattamenti indebiti, consenta di tenere l'identità di tutti al riparo da una frammentazione e ricomposizione artificiale, che trasformerebbe ciascuno di noi in una "cosa".

Opportunità e timori

La protezione dei dati personali si situa, dunque, sul confine che divide la fiducia dalla paura, l'oppressione e il controllo dalla libertà e dalla democrazia.

Solo se si è certi che vengono richieste le informazioni realmente necessarie, e che queste sono protette e rese inaccessibili a chi non ha diritto di conoscerle, si potranno sfruttare senza timore le opportunità che la tecnica offre.

Perché si deve temere che la carta di credito usata via Internet possa essere clonata o che la rilevazione della targa dell'auto possa essere usata per tracciare gli spostamenti e localizzare le persone?

Perché quando si fa una telefonata, si manda un *sms* o una *e-mail*, si accede a un sito Internet, si deve aver timore di essere ascoltati, letti, spiati?

Perché quando si acquista un prodotto si deve aver paura che vi sia chi analizza le nostre scelte per conoscere e profilare i gusti, le preferenze, la stessa capacità di acquisto?

Perché si deve essere costretti a guardare con timore alla richiesta di avere un dato biometrico e il DNA, anche quando questa richiesta sia fatta per curare o per proteggere?

Perché accettare che il grande villaggio globale debba essere una giungla senza regole, nella quale informazioni, errate o esatte, obsolete o recenti, possano essere catturate e diffuse senza che sia possibile verificare chi e per quali scopi lo fa, e senza che si possa rivendicare che esse siano rettificate o cancellate?

Perché dovremmo accettare di perdere la nostra anima per salvare il nostro corpo o, al contrario, rischiare di perdere il nostro corpo per salvare la nostra anima?

Sono dilemmi di fronte ai quali le nostre società non devono essere costrette a trovarsi. Mai!

La nostra Autorità, anche nell'anno trascorso, si è interrogata su tutto ciò. Abbiamo agito con l'obiettivo di governare, per quanto ci è possibile, il cambiamento in corso.

Nei settori maggiormente esposti, abbiamo intensificato le attività di disciplina, di verifica e di accertamento.

Tra i provvedimenti più innovativi possiamo ricordare quelli che hanno precisato i limiti e i casi in cui l'utilizzo dei dati biometrici può essere applicato ai lavoratori; il provvedimento generale di inizio d'anno sull'uso delle etichette intelligenti (o RFID) e le successive decisioni relative ai limiti della loro applicazione negli istituti bancari e nei luoghi di lavoro; l'iniziativa – la prima da parte di un'Autorità di protezione dati – assunta nei confronti di Google, al fine di ottenere che le regole della *privacy*, dalla rettifica dei dati sino al diritto all'oblìo, siano rispettate dai motori di ricerca in Internet, anche quando il gestore sia stabilito fuori del territorio italiano.

L'attività svolta con Google America, peraltro ancora in corso, assume una ulteriore valenza. Essa è un primo passo concreto per introdurre garanzie per gli utenti adeguate alle attuali forme di utilizzazione di Internet. Un passo che stiamo facendo anche con il sostegno delle altre Autorità europee.

Ci guida la consapevolezza che la mancanza di poteri regolatori sovranazionali e la perdurante assenza della tanto necessaria "Costituzione di Internet", se rappresentano un'espressione della libertà nella rete costituiscono però anche un serio limite ad un'effettiva tutela nel mondo telematico.

È la stessa consapevolezza che ci ha spinto a promuovere sul versante nazionale l'elaborazione di un codice deontologico degli operatori di Internet, che speriamo possa vedere la luce entro l'anno.

Le imprese e il lavoro nella rete dei dati

Anche il sistema economico è coinvolto in questo processo di innovazione, che moltiplica il trattamento dei dati.

Nonostante ciò, la tutela dei dati personali è spesso avvertita dal mondo delle attività produttive come un vincolo e un freno.

É probabile che questa opinione trovi giustificazione nella strumentazione giuridica, che in alcuni casi è generale ed uniforme e, quindi, non coglie a pieno le differenze fra le diverse realtà produttive e le diseguali dimensioni di impresa. Possono, pertanto, essere opportune idonee soluzioni di semplificazione.

Un punto però deve essere tenuto ben fermo.

La protezione dei dati personali non è un "lusso" o un "orpello" a cui possiamo rinunciare. È una necessità in un mondo in cui l'uso di dati è condizione vitale per la crescita economica e spesso per la sopravvivenza delle imprese.

Se il portafoglio ordini, i sistemi di approvvigionamento, i dati relativi ai dipendenti, ai consulenti, ai clienti, non sono protetti, può essere a rischio una parte essenziale del patrimonio aziendale, dell'avviamento commerciale, del valore stesso del marchio.

La protezione dei dati può e deve essere un "valore aggiunto".

Sui giornali campeggiano spesso inserzioni pubblicitarie che propongono l'acquisto di apparecchiature "sicure". Man mano che crescerà la consapevolezza dei valori e dei pericoli in gioco, vedremo sempre più le imprese offrire prodotti che promettono la sicurezza dei dati.

La "compatibilità privacy" sarà sempre più un valore essenziale anche per la qualità dei prodotti.

La privacy non è dunque solo un costo. È anche una importante risorsa.

Abbiamo, pertanto, salutato con soddisfazione la decisione del Governo precedente di non rinviare il termine per l'adozione dei documenti programmatici di

sicurezza. Questo necessario adempimento è stato avvertito da molti come "costoso" e "burocratico".

Non è così.

Esso risponde a una rilevante finalità: garantire al lavoratore, al cittadino, all'utente e al consumatore la tutela dei diritti fondamentali della personalità. Si pensi ai rischi per il lavoratore cagionati dall'uso di tecnologie produttive non regolate, o ai danni a cui può essere esposto l'utente o il consumatore dall'uso non protetto dei dati.

Ma vi è di più: l'adozione del documento programmatico stimola gli operatori ad assimilare la cultura della *privacy*.

È possibile semplificare alcune regole anche in questo campo. Siamo disposti a discuterne e per ciò abbiamo incontrato le associazioni di categoria e promosso una consultazione pubblica con gli operatori.

Abbiamo sempre detto, e qui lo ripetiamo, che vogliamo intensificare il dialogo con le imprese, le categorie economiche, i sindacati, le associazioni di rappresentanza, il mondo degli utenti e dei consumatori.

Vogliamo essere sostegno anche per coloro che svolgono attività professionali, collaborando con gli ordini e le categorie. Con questo intento, abbiamo avviato il tavolo per la redazione del codice deontologico sull'utilizzo dei dati nell'ambito dell'attività forense; abbiamo promosso un'attività di consultazione con i medici di base e con gli amministratori di condominio su provvedimenti che interessano tantissimi cittadini.

È con questo spirito che abbiamo monitorato l'attuazione del codice deontologico nel settore del credito al consumo; un settore che, nel 2005, ha movimentato una cifra pari a 76 miliardi di euro. Abbiamo regolato le attività di *marketing* e di profilazione nella grande distribuzione commerciale e nell'offerta di servizi di vario genere, vietando quelle svolte senza il consenso dei consumatori.

È in questo quadro che si collocano il provvedimento generale sulle cd. "carte di fedeltà", che sono oltre 30 milioni, e un recente provvedimento che ha vietato trattamenti illeciti nel settore alberghiero.

Abbiamo prestato la consueta attenzione alla tematica relativa alla tutela delle informazioni personali dei lavoratori, che presenta sempre nuove dimensioni e sfaccettature: ricordiamo, in particolare, l'utilizzo del sistema RFID che può determinare forme gravemente pervasive di controllo sulla vita del lavoratore.

Con riferimento alle relazioni tra cittadini e attività economiche, segnaliamo i provvedimenti sulle società di recupero crediti; sui rapporti dei cittadini con le compagnie assicurative; sulle corrette modalità di uso del *telepass*; sul rapporto tra utenti e servizi di radio-taxi. Massima cura abbiamo dedicato ad agevolare l'aggiornamento della normativa antiriciclaggio.

Tenendo presente la necessità di garantire la libertà di commercio e di circolazione dei beni, abbiamo rilasciato nuove autorizzazioni generali e dato esecuzione alle decisioni della Commissione europea sul trasferimento dati verso Paesi terzi, in applicazione dell'istituto delle clausole contrattuali tipo.

Intendiamo continuare ad impegnarci, insieme alle Autorità europee, sulla circolazione dei flussi transfrontalieri. Siamo convinti che la protezione dei dati non deve mai trasformarsi in una barriera che divida l'Europa dal resto del mondo.

Per questo, non ci siamo sottratti al confronto con i principali *privacy officer* di importanti multinazionali, alla ricerca di soluzioni che, senza pregiudicare il diritto alla protezione dei dati, consentano di fluidificare gli scambi fra Unione e Paesi terzi.

Un'esortazione alle grandi e medie imprese italiane: è poco diffusa la figura del *privacy officer*, ben conosciuta invece in altri Paesi. È il segno di una certa fatica ad adeguarsi ad una visione della protezione dati attiva e dinamica, essenziale per lo sviluppo del sistema Italia.

La *privacy* entra nell'Amministrazione Pubblica

Il 2005 è stato un anno particolarmente importante per la protezione dati nella Pubblica Amministrazione.

La trasformazione dell'Amministrazione, sotto la spinta dell'innovazione tec-

nologica, moltiplica reti e archivi informatici. È forte la tentazione efficientista ad interconnetterli fra loro, determinando una circolazione incontrollata dei dati e l'accesso indiscriminato da parte degli operatori.

L'Autorità si è misurata con questi fenomeni, affrontando la complessa vicenda nota come "Laziomatica". I provvedimenti prescrittivi e sanzionatori adottati sono un punto di riferimento non solo per i Comuni, ma per tutta l'Amministrazione: abbiamo dimostrato che è possibile far circolare i dati in rete senza duplicare gli archivi o accedere direttamente e indiscriminatamente alle banche dati.

Delicatissimo è, inoltre, il problema della protezione dei dati sensibili da parte della P.A., chiamata istituzionalmente a trattare una quantità enorme di dati riferiti alla salute, all'appartenenza etnica, alle opinioni e attività politiche e sindacali dei cittadini.

Uno dei successi più importanti dell'attività svolta nel 2005, e proseguita nel 2006, è l'aver favorito e ottenuto l'adempimento da parte delle Pubbliche Amministrazioni dell'obbligo di adottare i regolamenti per il trattamento dei dati sensibili.

Siamo grati al Governo precedente e a quello in carica per l'impegno dimostrato in risposta alle nostre sollecitazioni e consideriamo la proroga di recente approvata legata unicamente a ragioni obiettive derivanti dalle modifiche introdotte dal nuovo Governo nella struttura di alcuni Ministeri e Dipartimenti.

Comuni, Province, Regioni, Università, Camere di Commercio hanno risposto bene, così come moltissimi organi di rilevanza costituzionale, tutte le Autorità indipendenti, i grandi Enti nazionali e quasi tutti i Ministeri.

Il numero complessivo degli schemi di regolamento tipo relativi a categorie di enti e soggetti pubblici approvati supera la cinquantina. Ad essi si aggiungono centinaia di regolamenti adottati dai singoli enti sulla base degli schemi tipo.

Possiamo dire che nel 2005 la *privacy* ha fatto passi decisivi nella P.A.

È stata e continuerà ad essere un'occasione preziosa per le Amministrazioni

per ripensare se stesse, per riflettere sulle procedure interne, sulla funzionalità degli assetti organizzativi, sull'effettiva necessità dei dati di volta in volta richiesti.

É iniziata una nuova e più trasparente stagione nel rapporto fra Pubblica Amministrazione e cittadino.

Noi continueremo ad operare con scrupolo e con spirito collaborativo per verificare come il sistema amministrativo riuscirà a convertire le regole adottate in virtuosa prassi amministrativa.

Anche quest'anno, del resto, il rapporto di collaborazione del Garante con l'Amministrazione ha favorito l'adozione di soluzioni positive in settori strategici, come ad esempio in tema di monitoraggio della spesa sanitaria da parte del Ministero dell'Economia e delle finanze e di trattamento dei dati sensibili in materia sanitaria da parte delle Regioni.

Proprio la sanità ci ha impegnato molto e continuerà a impegnarci in futuro. I provvedimenti relativi all'organizzazione delle strutture sanitarie finalizzati a tutelare la riservatezza degli assistiti, quelli relativi all'attuazione della recente disciplina sulla procreazione assistita e all'informativa semplificata per i medici di base e pediatri ne sono esempio.

È prossima l'approvazione della autorizzazione generale in materia di trattamento dei dati genetici. All'orizzonte si affaccia il tema ancora in parte inesplorato della c.d. "sanità elettronica".

Impegnativa è stata l'attività nel settore specifico dell'amministrazione digitale. Abbiamo dato il parere sul nuovo codice dell'Amministrazione digitale, sul riutilizzo di documenti pubblici a fini privati, sul passaporto elettronico. Abbiamo avviato un'attività collaborativa con il CNIPA, che ha formato oggetto anche di un comune documento d'intenti. Essa ci ha consentito ad esempio di dare un importante parere preventivo sul bando di gara predisposto dal Ministero di Giustizia per la sicurezza di basi di dati strategiche nel contrasto alla criminalità organizzata.

L'innovazione tecnologica della P.A. è una linea di azione prioritaria per il Paese. Siamo pronti a fare la nostra parte.

La sicurezza nella società tecnologica

Un settore particolare è quello delle strutture e degli apparati di sicurezza e di prevenzione.

Le nostre società hanno bisogno di sicurezza.

L'Europa ha bisogno di sicurezza.

L'Unione Europea, nata per promuovere il libero mercato e svilupparsi come spazio di democrazia e libertà, ora dedica particolare attenzione alla tutela della sicurezza dei cittadini.

Sono sempre più forti le spinte ad avvalersi di tutte le opportunità informative offerte dalle tecnologie per ottenere un controllo generalizzato, preventivo e spesso pervasivo per finalità di sicurezza.

Le decisioni assunte dopo i fatti di Madrid e Londra hanno ampliato, sia nel nostro Paese che nell'Unione, la quantità e qualità dei dati conservati per ragioni di sicurezza.

L'Unione Europea ha adottato alla fine del 2005 una direttiva sulla c.d. "*data retention*", che comporterà la conservazione di miliardi e miliardi di informazioni, riguardanti aspetti essenziali della vita di relazione di tutti i cittadini europei. Si è calcolato che dovrebbero essere conservati ogni giorno 200 milioni di conversazioni, 300 milioni di "eventi" di telefonia mobile e 2 milioni e 400 mila gigabyte di dati annui solo per la posta elettronica.

Nel nostro Paese, dove già erano previsti tempi lunghissimi di conservazione dei dati di traffico telefonico, lo scorso anno con il c.d. decreto Pisanu si è esteso l'obbligo di conservazione anche ai dati di traffico telematico, sia pure per un tempo più breve.

Non è detto che più dati significhino maggior sicurezza.

Per questo Governo e Parlamento sono chiamati a verificare l'efficacia di tali misure, tanto più quando, come accade in Italia, i tempi di conservazione sono più lunghi di quelli previsti dall'Unione.

In ogni caso, questa massa di informazioni va adeguatamente salvaguardata, per garantire che sia usata soltanto dai soggetti autorizzati e per le finalità stabilite.

A ciò si aggiunge che l'*Europa della sicurezza* sta intensificando l'interconnessione fra le banche dati utilizzate per i controlli sui movimenti delle persone, per il contrasto all'immigrazione clandestina e al crimine. I nuovi sistemi SIS II e VIS II prevedono per la Commissione un ruolo penetrante di coordinamento dell'interoperabilità delle banche dati nazionali.

Alcuni Stati europei (Francia, Germania, Spagna, Belgio, Austria, Paesi Bassi e Lussemburgo) hanno recentemente sottoscritto a Prum, nell'ambito della cooperazione rafforzata, un Trattato che prevede anche la possibilità di scambiarsi informazioni riguardanti dati genetici. Si tratta di una problematica che anche in Italia dobbiamo affrontare con la massima attenzione alle ragioni e valutazioni di tutti.

Su questi temi abbiamo sempre adottato un atteggiamento altamente responsabile, attenti alle ragioni complessive e all'interesse generale.

La *privacy* non può essere un ostacolo alla sicurezza. Sicurezza e *privacy* sono parti coessenziali del sistema democratico.

Riteniamo così necessario che, come proposto dalla Commissione, l'adozione degli strumenti normativi relativi al rafforzamento della cooperazione giudiziaria e investigativa avvenga contestualmente all'approvazione di una robusta normativa sulla "*data protection*" anche nei settori della sicurezza e della giustizia.

Rivolgiamo un appello al Governo, ed in particolare al Ministro dell'interno e al Ministro della giustizia, affinché sostengano la posizione della Commissione, condivisa in modo unanime dal Gruppo europeo delle Autorità.

Ancora sul versante europeo. Dopo la recente decisione della Corte di Giustizia che, su ricorso del Parlamento europeo, ha annullato l'accordo fra UE e USA relativo al cd. PNR, è necessario negoziare un nuovo e più soddisfacente accordo sulla comunicazione dei dati dei cittadini europei in transito o in volo per gli Stati Uniti.

Su questi temi siamo stati sempre presenti sia nell'ambito del Gruppo dei Garanti europei sia nelle Conferenze internazionali delle Autorità di protezione dati: da Montreux a Madrid, da Budapest a Varsavia.

Sul versante delle strutture strumentali all'attività investigativa e di vigilanza, ci stiamo muovendo e intendiamo farlo ancora, sia con misure di tipo prescrittivo che con una adeguata attività di verifica della loro applicazione.

Da un lato, il nostro intervento, rispettoso delle competenze di ciascuno, può aiutare le strutture di sicurezza a rendere più efficaci le modalità di conservazione dei dati. Da un altro lato, la nostra azione può aiutare i cittadini ad avere maggiore fiducia nelle strutture di sicurezza.

È un compito importante anche perché tocca un settore delicatissimo, nel quale il diritto del cittadino di accedere ai dati che lo riguardano è affievolito.

In questa prospettiva, nel 2005 abbiamo avviato un'attività di ispezione sul Centro di elaborazione dati del Dipartimento di pubblica sicurezza del Ministero dell'interno. Si tratta di un'attività di controllo che in una prima fase è stata finalizzata a verificare le misure di protezione delle informazioni registrate e che ha già dato luogo ad un provvedimento contenente misure per il rafforzamento del sistema di sicurezza. Un secondo, più organico, provvedimento sul complesso di attività svolte dal Ced sarà adottato a breve, all'esito dell'attività.

Privacy e pubblicazione delle intercettazioni telefoniche fra mezzi di informazione e autorità giudiziaria

Nel 2005, l'Autorità è intervenuta sulla libertà di informazione e sul tema della pubblicazione dei contenuti delle intercettazioni telefoniche. Fenomeno, questo, che ha conosciuto un continuo crescendo in queste ultime settimane.

Le decisioni del Garante sono sempre state improntate a cautela e prudenza, essendo in gioco tanto la libertà di informazione, sancita dall'art. 21 della Costituzione, quanto il diritto alla riservatezza e alla dignità, che trovano fondamento costituzionale nell'art. 2.

Valori costituzionali che vanno bilanciati e applicati in concreto alle singole fattispecie, tenendo conto di molteplici variabili.

Vengono in gioco la natura dell'informazione, l'oggetto e il soggetto, il contesto in cui viene resa la notizia e il diritto dei cittadini a conoscere tutto quanto è necessario sapere per esercitare un salutare controllo democratico.

È uno dei risvolti più nobili del mestiere di chi fa informazione, valutare se una notizia è essenziale per consentire all'opinione pubblica una conoscenza obiettiva dei fatti, o se invece è, oltre che irrilevante, anche lesiva della dignità personale.

Non è buon giornalismo, e comunque non è mai lecito, ledere la dignità delle persone per mero "*gossip*", utile ad aumentare le vendite o a solleticare forme di "*voyerismo*".

Nelle numerose decisioni adottate, abbiamo sempre cercato di contribuire a far sì che chi esercita un mestiere tanto delicato si ponga alcune domande, adotti filtri, si sforzi di valutare in modo scrupoloso l'impatto di un dettaglio o del riferimento ad una persona. In una parola, sia consapevole del ruolo fondamentale della libera informazione in una società democratica.

Non sono mancati interventi dell'Autorità di divieto e di blocco, anche con

riferimento a fatti riguardanti persone note o che svolgono funzioni pubbliche. Sempre abbiamo ribadito il rispetto del principio di essenzialità della notizia e della tutela della sfera privata, quali limiti invalicabili al corretto esercizio del diritto di cronaca.

Numerosi sono stati i provvedimenti a tutela di singoli cittadini adottati in seguito a ricorso. I più interessanti ci hanno permesso di precisare sia i principi relativi al diritto all'oblìo che quelli legati alla tutela dei minori.

Consentiteci, infine, un supplemento di riflessione sulla pubblicazione dei contenuti delle intercettazioni telefoniche.

Particolare clamore hanno suscitato di recente modalità e forme inedite di pubblicazione integrale dei contenuti delle intercettazioni, talvolta disponibili su Internet o raccolte in *dossier* posti in vendita.

Il fenomeno merita attenzione.

I testi delle intercettazioni finiscono in un brogliaccio contenente il riassunto delle conversazioni registrate, redatto da un operatore di giustizia, finalizzato ad essere conservato, valutato e utilizzato da altri operatori di giustizia (giudici e avvocati).

Pubblicare pressoché integralmente questo materiale in forma grezza, senza alcuna intermediazione e commento, non sempre è un servizio utile alla formazione di un libero e corretto convincimento del lettore.

Offrire all'opinione pubblica, senza adeguata mediazione, il contenuto di testi destinati alla diversa funzione di concorrere, insieme ad altri strumenti probatori, alla formazione del convincimento del pubblico ministero e/o del giudice, significa muoversi su un terreno minato.

Con il provvedimento generale, adottato alcuni giorni fa, abbiamo voluto ribadire con forza l'importanza delle regole che devono presiedere l'esercizio di un diritto-dovere di cronaca e d'informazione rispettoso della riservatezza e della dignità individuale, confermando orientamenti e indirizzi consolidati.

Nessuno, meno che mai il Garante, chiede censure preventive o bavagli all'informazione.

Chiediamo che il giornalista svolga fino in fondo il proprio mestiere, soppesando, anche rispetto a persone che hanno rilievo pubblico, le notizie e distinguendo fra informazioni necessarie per valutare il fatto e informazioni che invece attengono prevalentemente alla sfera privata del soggetto.

La posizione del "terzo incolpevole", dei familiari e dei minori deve essere sempre tutelata, così come particolare attenzione va prestata alle informazioni sensibili.

Siamo consapevoli che l'uso delle intercettazioni telefoniche investe anche la responsabilità di altri soggetti, in primo luogo gli operatori della giustizia.

Ed è per questo che abbiamo rivolto un nuovo caloroso invito al Consiglio Superiore della Magistratura affinché, nell'ambito delle sue competenze, si attivi perché siano migliorate le garanzie e le misure di sicurezza a tutela della riservatezza delle informazioni processuali.

Inoltre, ci siamo impegnati a collaborare su questi temi con Parlamento e Governo anche attivando il diritto-dovere di segnalazione che la legge ci attribuisce.

Quanto al nostro potere di controllo, che, per sua natura, è destinato sempre a svolgersi "a posteriori", riteniamo doveroso chiedere soprattutto al Parlamento una revisione normativa che preveda la possibilità per l'Autorità di comminare sanzioni amministrative di carattere pecuniario, qualora si accerti la violazione dei principi contenuti nel Codice deontologico.

Il Garante e i servizi di comunicazione elettronica

Nel 2005 la materia delle intercettazioni telefoniche è stata affrontata dal Garante anche sotto un altro profilo, parimenti importante.

In Italia, l'autorità giudiziaria fa un ampio ricorso a questo metodo investiga-

tivo, con la conseguenza che il numero delle intercettazioni, così come i relativi costi, sono, come ha ricordato di recente il Ministro di Giustizia, particolarmente alti, specialmente in confronto agli altri Paesi europei.

Va ricordato che, oltre alle intercettazioni telefoniche, l'autorità giudiziaria può chiedere ai fornitori del servizio molto altro, come la localizzazione delle chiamate e la realizzazione di intercettazioni ambientali. Inoltre vi sono le intercettazioni preventive svolte, su autorizzazione del magistrato, dalle forze di polizia.

Siamo di fronte a scelte del legislatore, prima, e dei singoli magistrati inquirenti, dopo. Non spetta a noi esprimere valutazioni al riguardo.

Sappiamo, però, che più si raccolgono dati personali, maggiore è il rischio che le misure di sicurezza non siano sufficienti ad assicurare la loro riservatezza.

È prioritario l'obbligo che i gestori telefonici adottino ferree misure di sicurezza e che l'autorità giudiziaria protegga le informazioni e i dati ottenuti.

Il Garante ha svolto un'attenta attività di accertamento sulle modalità con cui i gestori adempiono alle richieste dell'Autorità giudiziaria, fornendo il servizio indispensabile per l'attività di intercettazione.

Le verifiche hanno evidenziato la urgente necessità di incrementare in modo significativo i livelli di sicurezza dei sistemi e lo scorso dicembre il Garante ha prescritto numerose misure di sicurezza da adottare entro 180 giorni. Il termine fissato è ormai scaduto e ora verificheremo se le nostre prescrizioni sono state rispettate.

Allo stesso tempo, abbiamo sottolineato la necessità che misure analoghe siano adottate dagli uffici giudiziari e fin da marzo abbiamo deciso di promuovere un'attività collaborativa finalizzata a questo, chiedendo il sostegno del Consiglio Superiore della Magistratura e del Ministro della Giustizia.

I recentissimi episodi ci hanno spinto pochi giorni fa a rinnovare il nostro allarme.

L'attenzione e disponibilità manifestata dal Ministro della Giustizia e da auto-

revoli esponenti della magistratura requirente ci confortano.

Consideriamo, dunque, l'indagine conoscitiva decisa dalla Commissione Giustizia del Senato un'occasione preziosa, e, se ci sarà richiesto, assicuriamo il nostro contributo. Così come non mancheremo di darlo ad ogni altra iniziativa che Parlamento o Governo intendessero intraprendere.

Un altro profilo molto delicato riguarda le modalità di protezione dei dati di traffico telefonico, obbligatoriamente conservati dai gestori per 5 anni.

Abbiamo recentemente accertato, allo stato soltanto nei confronti del più importante gestore italiano, l'insufficienza di misure adeguate a protezione proprio di questi dati e dei relativi tabulati. In particolare, è risultato inadeguato il sistema di registrazione degli accessi ai *data-base,* e incompleto il sistema di tracciamento e di identificazione di coloro che possono accedervi. Abbiamo subito adottato un provvedimento dettagliato, indicando le necessarie misure e dato 120 giorni per attuarle.

Contestualmente abbiamo avviato un'attività istruttoria e programmato un'impegnativa attività ispettiva, finalizzate ad adottare un provvedimento generale sulla conservazione dei dati di traffico, così come previsto dall'art. 132 del nostro codice. Si tratta di un provvedimento che dovrà definire in modo organico le misure e gli accorgimenti che ciascun gestore dovrà introdurre per mettere in piena sicurezza le sue banche dati.

Ancora per quanto riguarda il settore dei gestori telefonici vanno ricordate altre due nostre attività in corso.

Negli scorsi mesi abbiamo emanato un provvedimento rivolto a tutti i gestori in ordine all'inquietante fenomeno dei servizi non richiesti quali, ad esempio, l'indebita attivazione di linee adsl. Si tratta di un provvedimento che riguarda da vicino anche i cd. *call center* e rispetto al quale verificheremo ora se le nostre prescrizioni sono state attuate.

Solo qualche settimana fa, abbiamo aperto un'istruttoria per verificare se,

come una recente ordinanza della Corte di Appello di Milano ha ritenuto in sede cautelare, vi siano state da parte di un gestore illecite attività di profilazione di ex abbonati passati ad altro gestore.

In questo settore, il 2005 è stato, dunque, un anno di grande impegno, intensificato in questi ultimi mesi. Esso aumenterà ancora nei prossimi.

Sulla tutela dei dati di comunicazione e sulla loro conservazione bisogna riflettere con attenzione, sforzandosi anche di ricercare soluzioni innovative, idonee ad assicurare maggiori garanzie.

Noi lo sentiamo come un dovere.

Un'ipotesi, che qualcuno invita a esplorare, potrebbe essere la creazione di una struttura pubblica, in cui i gestori, scaduto il periodo per la fatturazione, siano tenuti a far confluire i dati in loro possesso. Si tratta di una idea già avanzata in sede europea e che ha destato perplessità, ma sulla quale si potrebbe provare a ragionare. Tale struttura dovrebbe comunque essere sottoposta alla vigilanza della nostra Autorità e dovrebbe garantire il più rigoroso rispetto delle misure di sicurezza prescritte.

La tutela delle banche dati e il ruolo dell'Autorità

Una tematica più generale attiene alle garanzie da prevedere a tutela della sicurezza e integrità delle grandi banche dati che costituiscono, e sempre più costituiranno, porzione significativa dell'organizzazione sociale.

Sino ad oggi, le Autorità di protezione hanno svolto prevalentemente alcuni fondamentali compiti: garantire il diritto di accesso dei cittadini ai loro dati personali, assicurare la rigorosa applicazione della normativa a tutela dei diritti individuali lesi da trattamenti illeciti, favorire un'applicazione il più possibile "armonizzata" delle direttive europee e assicurare l'implementazione della normativa nazionale.

A questo si aggiunge, specialmente per il Garante italiano, un potere, più o meno legislativamente definito, di prescrizione generale sulle modalità con le quali la

normativa europea e nazionale va applicata nei diversi settori. La stessa attività di promozione dei codici di deontologia e di buona condotta si inscrive in questo contesto.

È ora giunto il momento di accentuare l'attenzione sulla problematica della messa in sicurezza delle informazioni contenute nelle grandi banche dati.

Occorre una svolta.

Tutte le Autorità europee ne avvertono l'esigenza.

Su questo terreno, in parte nuovo, il Garante italiano vuole essere in prima fila.

Se questa prospettiva è condivisa, è necessario individuare con chiarezza le banche dati da sottoporre a una più attenta vigilanza, isolando quelle di interesse nazionale operanti in settori di particolare rilevanza.

Le banche dati di traffico nell'ambito delle telecomunicazioni, così come quelle operanti nei settori della sicurezza e quelle contenenti campioni biometrici e del dna, dovrebbero certamente far parte del novero di queste strutture.

A tal proposito, dobbiamo fare presente che non hanno ancora trovato attuazione le previsioni del Codice che assegnano al Ministro della giustizia e al Ministro dell'interno il compito di individuare le banche dati centrali di cui si avvalgano le loro amministrazioni e la cui elencazione deve essere allegata al codice della *privacy*.

Tale individuazione, peraltro, potrebbe essere il primo passo per dar vita ad un apposito "registro delle banche dati ad alto rischio", che assolverebbe anche una funzione di trasparenza nei confronti dei cittadini.

Ci auguriamo che il legislatore voglia formulare chiari indirizzi sul nostro ruolo futuro in questo difficile settore.

Su un piano più generale, riteniamo peraltro utile invitare il Parlamento a riflettere sull'opportunità di individuare sedi e forme idonee per assicurare un dialogo costante fra il luogo della democrazia rappresentativa e un'Autorità come la nostra che, per la sua natura e per vincolo comunitario, non può che essere ed agire come Autorità indipendente, ma che ha e deve avere nel Parlamento il suo interlocutore privilegiato.

Ed è per questo che riteniamo sia giusto esprimere qui la nostra consapevolezza che, di fronte alla complessità e all'ampiezza degli obiettivi che ci proponiamo, i poteri dell'Autorità sono insufficienti.

Occorrono necessarie modifiche normative in relazione agli strumenti ispettivi e alle misure prescrittive e sanzionatorie. In particolare, è necessario attribuire all'Autorità il potere di irrogare sanzioni pecuniarie di carattere amministrativo in misura maggiore e in un numero di casi più ampio di quelli oggi tipizzati dal Codice. Occorre, inoltre, un ripensamento delle strutture organizzative e della dotazione organica dell'Autorità. Attualmente, essa si avvale di un Ufficio di supporto composto da circa cento unità. Troppo poco per poter operare come Autorità pienamente capace di garantire anche il corretto funzionamento delle grandi banche dati.

Altri settori di intervento dell'Autorità nel corso del 2005

È ora di avviarci alla conclusione.

Come negli anni precedenti, anche nel 2005 siamo intervenuti in molteplici ambiti, sia in seguito a istanze dei singoli cittadini, associazioni, ordini professionali e categorie, sia *ex officio*.

I dati dimostrano che il Garante rappresenta un'Autorità peculiare nel panorama delle c.d. Autorità indipendenti.

L'elemento distintivo di maggiore evidenza attiene al rapporto 'simbiotico' fra l'Autorità e la materia "*privacy*", che ha al suo centro il diritto fondamentale del cittadino alla protezione dei suoi dati personali.

Il Garante non è chiamato a regolare un settore specifico.

A noi spetta promuovere e accompagnare l'assimilazione e il radicamento di un nuovo modo di trattare le informazioni personali da parte di una platea vastissima di soggetti. Il nostro compito ultimo è di concorrere a garantire non solo il

rispetto della libertà e dignità dei singoli, ma anche il rafforzamento del quadro democratico del Paese.

La complessità e la ricchezza del nostro operato deriva dall'ampiezza e trasversalità dei settori su cui siamo chiamati a intervenire.

Di qui l'elevata quantità di pronunce, pareri, provvedimenti emessi in quest'anno e la nutrita serie di decisioni legate alla nostra attività di controllo, di regolazione, di stimolo verso i decisori pubblici e privati.

Alcuni numeri. Nel solo 2005 l'Autorità ha adottato 724 provvedimenti collegiali, che hanno riguardato anche la trattazione di 634 ricorsi. Considerando anche alcuni casi trattati nell'anno e definiti più di recente, ha risposto a 1633 reclami e segnalazioni e a 364 quesiti; ha dato 31 pareri su atti normativi del Governo; ha approvato 61 schemi di regolamento sul trattamento dei dati sensibili nella P.A.. I provvedimenti generali sono stati più di un centinaio, fra cui il rinnovo di sette autorizzazioni generali.

Abbiamo dedicato tempo ed energie all'ascolto delle categorie economiche e produttive, degli ordini professionali, dei consumatori.

Auspichiamo che la *privacy* sia sentita come un aspetto positivo della vita e per questo abbiamo avviato una riflessione sul rapporto fra *privacy* e felicità.

Abbiamo svolto un'intensa attività per dotare l'Autorità dei regolamenti indispensabili per il suo funzionamento, in modo da irrobustirne la struttura e l'organizzazione e da aumentare le garanzie dei cittadini che si rivolgono a noi.

Abbiamo innovato nel metodo di lavoro, introducendo la programmazione semestrale degli affari da trattare e delle attività ispettive.

Duecento ispezioni nel corso del 2005 e centoquarantacinque solo nel primo semestre di quest'anno testimoniano l'importanza che ha per noi quest'attività. Intendiamo continuare su questa via, rafforzando sempre di più la collaborazione con la Guardia di Finanza. Collaborazione fattiva e preziosa, della quale voglio qui ringraziare il Comandante del Corpo, gli alti ufficiali e tutti coloro che lavorano con noi.

Conclusione

Signor Presidente,

Signore e Signori.

Insieme ai miei colleghi, Giuseppe Chiaravalloti, Mauro Paissan e Giuseppe Fortunato, mi auguro di aver dato un riassunto fedele della nostra attività, delle nostre riflessioni, delle prospettive che ci poniamo.

Vogliamo assicurare Lei, Signor Presidente, il Parlamento e il Governo che non verremo mai meno ai doveri e compiti assegnati.

Il Garante si muove sul crinale più sensibile della società a "cambiamento velocissimo": la linea di confine fra democrazia e libertà da un lato, controllo e paura dall'altro.

Il Garante opera perché si continui a vivere in una comunità di donne e di uomini liberi, responsabili, capaci di usare la tecnica senza diventarne prigionieri, impegnati a costruire la propria sicurezza senza rinunciare alla loro dignità di uomini.

Chiediamo al Paese e al Parlamento fiducia e lavoriamo per dare fiducia.

IL CODICE
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

PAGINA BIANCA

PARTE I - DISPOSIZIONI GENERALI

Titolo I - Principi generali

Art. 1. Diritto alla protezione dei dati personali
Art. 2. Finalità
Art. 3. Principio di necessità nel trattamento dei dati
Art. 4. Definizioni
Art. 5. Oggetto ed ambito di applicazione
Art. 6. Disciplina del trattamento

Titolo II - Diritti dell'interessato

Art. 7. Diritto di accesso ai dati personali ed altri diritti
Art. 8. Esercizio dei diritti
Art. 9. Modalità di esercizio
Art. 10. Riscontro all'interessato

Titolo III - Regole generali per il trattamento dei dati

Capo I - Regole per tutti i trattamenti

Art. 11. Modalità del trattamento e requisiti dei dati
Art. 12. Codici di deontologia e di buona condotta
Art. 13. Informativa
Art. 14. Definizione di profili e della personalità dell'interessato
Art. 15. Danni cagionati per effetto del trattamento
Art. 16. Cessazione del trattamento
Art. 17. Trattamento che presenta rischi specifici

Capo II - Regole ulteriori per i soggetti pubblici

Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici
Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari
Art. 20. Principi applicabili al trattamento di dati sensibili
Art. 21. Principi applicabili al trattamento di dati giudiziari
Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari

Capo III - Regole ulteriori per privati ed enti pubblici economici

Art. 23. Consenso
Art. 24. Casi nei quali può essere effettuato il trattamento senza il consenso
Art. 25. Divieti di comunicazione e diffusione
Art. 26. Garanzie per i dati sensibili
Art. 27. Garanzie per i dati giudiziari

Titolo IV - Soggetti che effettuano il trattamento

Art. 28. Titolare del trattamento
Art. 29. Responsabile del trattamento
Art. 30. Incaricati del trattamento

Titolo V - Sicurezza dei dati e dei sistemi

Capo I - Misure di sicurezza

Art. 31. Obblighi di sicurezza
Art. 32. Particolari titolari

Capo II - Misure minime di sicurezza

Art. 33. Misure minime
Art. 34. Trattamenti con strumenti elettronici
Art. 35. Trattamenti senza l'ausilio di strumenti elettronici
Art. 36. Adeguamento

Titolo VI - Adempimenti

Art. 37. Notificazione del trattamento
Art. 38. Modalità di notificazione
Art. 39. Obblighi di comunicazione
Art. 40. Autorizzazioni generali
Art. 41. Richieste di autorizzazione

Titolo VII - Trasferimento dei dati all'estero

Art. 42. Trasferimenti all'interno dell'Unione europea
Art. 43. Trasferimenti consentiti in Paesi terzi
Art. 44. Altri trasferimenti consentiti
Art. 45. Trasferimenti vietati

PARTE II - DISPOSIZIONI RELATIVE A SPECIFICI SETTORI

Titolo I - Trattamenti in ambito giudiziario

Capo I - Profili generali

Art. 46. Titolari dei trattamenti
Art. 47. Trattamenti per ragioni di giustizia
Art. 48. Banche di dati di uffici giudiziari
Art. 49. Disposizioni di attuazione

Capo II - Minori

Art. 50. Notizie o immagini relative a minori

Capo III - Informatica giuridica

Art. 51. Principi generali
Art. 52. Dati identificativi degli interessati

Titolo II - Trattamenti da parte di forze di polizia

Capo I - Profili generali

Art. 53. Ambito applicativo e titolari dei trattamenti
Art. 54. Modalità di trattamento e flussi di dati
Art. 55. Particolari tecnologie
Art. 56. Tutela dell'interessato
Art. 57. Disposizioni di attuazione

Titolo III - Difesa e sicurezza dello Stato

Capo I - Profili generali

Art. 58. Disposizioni applicabili

Titolo IV - Trattamenti in ambito pubblico

Capo I - Accesso a documenti amministrativi

Art. 59. Accesso a documenti amministrativi
Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale

Capo II - Registri pubblici e albi professionali

Art. 61. Utilizzazione di dati pubblici

Capo III - Stato civile, anagrafi e liste elettorali

Art. 62. Dati sensibili e giudiziari

Art. 63. Consultazione di atti

Capo IV - Finalità di rilevante interesse pubblico

Art. 64. Cittadinanza, immigrazione e condizione dello straniero

Art. 65. Diritti politici e pubblicità dell'attività di organi

Art. 66. Materia tributaria e doganale

Art. 67. Attività di controllo e ispettive

Art. 68. Benefici economici ed abilitazioni

Art. 69. Onorificenze, ricompense e riconoscimenti

Art. 70. Volontariato e obiezione di coscienza

Art. 71. Attività sanzionatorie e di tutela

Art. 72. Rapporti con enti di culto

Art. 73. Altre finalità in ambito amministrativo e sociale

Capo V - Particolari contrassegni

Art. 74. Contrassegni su veicoli e accessi a centri storici

Titolo V - Trattamento di dati personali in ambito sanitario

Capo I - Principi generali

Art. 75. Ambito applicativo

Art. 76. Esercenti professioni sanitarie e organismi sanitari pubblici

Capo II - Modalità semplificate per informativa e consenso

Art. 77. Casi di semplificazione

Art. 78. Informativa del medico di medicina generale o del pediatra

Art. 79. Informativa da parte di organismi sanitari

Art. 80. Informativa da parte di altri soggetti pubblici

Art. 81. Prestazione del consenso

Art. 82. Emergenze e tutela della salute e dell'incolumità fisica

Art. 83. Altre misure per il rispetto dei diritti degli interessati

Art. 84. Comunicazione di dati all'interessato

Capo III - Finalità di rilevante interesse pubblico

Art. 85. Compiti del Servizio sanitario nazionale

Art. 86. Altre finalità di rilevante interesse pubblico

Capo IV - Prescrizioni mediche

Art. 87. Medicinali a carico del Servizio sanitario nazionale

Art. 88. Medicinali non a carico del Servizio sanitario nazionale

Art. 89. Casi particolari

Capo V - Dati genetici

Art. 90. Trattamento dei dati genetici e donatori di midollo osseo

Capo VI - Disposizioni varie

Art. 91. Dati trattati mediante carte

Art. 92. Cartelle cliniche

Art. 93. Certificato di assistenza al parto

Art. 94. Banche di dati, registri e schedari in ambito sanitario

Titolo VI - Istruzione

Capo I - Profili generali

Art. 95. Dati sensibili e giudiziari

Art. 96. Trattamento di dati relativi a studenti

Titolo VII - Trattamento per scopi storici, statistici o scientifici

Capo I - Profili generali

Art. 97. Ambito applicativo

Art. 98. Finalità di rilevante interesse pubblico

Art. 99. Compatibilità tra scopi e durata del trattamento

Art. 100. Dati relativi ad attività di studio e ricerca

Capo II - Trattamento per scopi storici

Art. 101. Modalità di trattamento

Art. 102. Codice di deontologia e di buona condotta

Art. 103. Consultazione di documenti conservati in archivi

Capo III - Trattamento per scopi statistici o scientifici

Art. 104. Ambito applicativo e dati identificativi per scopi statistici o scientifici

Art. 105. Modalità di trattamento

Art. 106. Codici di deontologia e di buona condotta

Art. 107. Trattamento di dati sensibili

Art. 108. Sistema statistico nazionale

Art. 109. Dati statistici relativi all'evento della nascita

Art. 110. Ricerca medica, biomedica ed epidemiologica

Titolo VIII - Lavoro e previdenza sociale

Capo I - Profili generali

Art. 111. Codice di deontologia e di buona condotta

Art. 112. Finalità di rilevante interesse pubblico

Capo II - Annunci di lavoro e dati riguardanti prestatori di lavoro

Art. 113. Raccolta di dati e pertinenza

Capo III - Divieto di controllo a distanza e telelavoro

Art. 114. Controllo a distanza

Art. 115. Telelavoro e lavoro a domicilio

Capo IV - Istituti di patronato e di assistenza sociale

Art. 116. Conoscibilità di dati su mandato dell'interessato

Titolo IX - Sistema bancario, finanziario ed assicurativo

Capo I - Sistemi informativi

Art. 117. Affidabilità e puntualità nei pagamenti

Art. 118. Informazioni commerciali

Art. 119. Dati relativi al comportamento debitorio

Art. 120. Sinistri

Titolo X - Comunicazioni elettroniche

Capo I - Servizi di comunicazione elettronica

Art. 121. Servizi interessati

Art. 122. Informazioni raccolte nei riguardi dell'abbonato o dell'utente

Art. 123. Dati relativi al traffico
Art. 124. Fatturazione dettagliata
Art. 125. Identificazione della linea
Art. 126. Dati relativi all'ubicazione
Art. 127. Chiamate di disturbo e di emergenza
Art. 128. Trasferimento automatico della chiamata
Art. 129. Elenchi di abbonati
Art. 130. Comunicazioni indesiderate
Art. 131. Informazioni ad abbonati e utenti
Art. 132. Conservazione di dati di traffico per altre finalità

Capo II - Internet e reti telematiche
Art. 133. Codice di deontologia e di buona condotta

Capo III - Videosorveglianza
Art. 134. Codice di deontologia e di buona condotta

Titolo XI - Libere professioni e investigazione privata

Capo I - Profili generali
Art. 135. Codice di deontologia e di buona condotta

Titolo XII - Giornalismo ed espressione letteraria ed artistica

Capo I - Profili generali
Art. 136. Finalità giornalistiche e altre manifestazioni del pensiero
Art. 137. Disposizioni applicabili
Art. 138. Segreto professionale

Capo II - Codice di deontologia
Art. 139. Codice di deontologia relativo ad attività giornalistiche

Titolo XIII - Marketing diretto

Capo I - Profili generali
Art. 140. Codice di deontologia e di buona condotta

PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

Titolo I - Tutela amministrativa e giurisdizionale

Capo I - Tutela dinanzi al Garante
Sezione I - Principi generali
Art. 141. Forme di tutela

Sezione II - Tutela amministrativa
Art. 142. Proposizione dei reclami
Art. 143. Procedimento per i reclami
Art. 144. Segnalazioni

Sezione III - Tutela alternativa a quella giurisdizionale
Art. 145. Ricorsi
Art. 146. Interpello preventivo
Art. 147. Presentazione del ricorso
Art. 148. Inammissibilità del ricorso
Art. 149. Procedimento relativo al ricorso
Art. 150. Provvedimenti a seguito del ricorso

Art. 151. Opposizione

Capo II - Tutela giurisdizionale

Art. 152. Autorità giudiziaria ordinaria

Titolo II - L'Autorità

Capo I - Il Garante per la protezione dei dati personali

Art. 153. Il Garante

Art. 154. Compiti

Capo II - L'Ufficio del Garante

Art. 155. Principi applicabili

Art. 156. Ruolo organico e personale

Capo III - Accertamenti e controlli

Art. 157. Richiesta di informazioni e di esibizione di documenti

Art. 158. Accertamenti

Art. 159. Modalità

Art. 160. Particolari accertamenti

Titolo III - Sanzioni

Capo I - Violazioni amministrative

Art. 161. Omessa o inidonea informativa all'interessato

Art. 162. Altre fattispecie

Art. 163. Omessa o incompleta notificazione

Art. 164. Omessa informazione o esibizione al Garante

Art. 165. Pubblicazione del provvedimento del Garante

Art. 166. Procedimento di applicazione

Capo II - Illeciti penali

Art. 167. Trattamento illecito di dati

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

Art. 169. Misure di sicurezza

Art. 170. Inosservanza di provvedimenti del Garante

Art. 171. Altre fattispecie

Art. 172. Pene accessorie

Titolo IV - Disposizioni modificative, abrogative, transitorie e finali

Capo I - Disposizioni di modifica

Art. 173. Convenzione di applicazione dell'Accordo di Schengen

Art. 174. Notifiche di atti e vendite giudiziarie

Art. 175. Forze di polizia

Art. 176. Soggetti pubblici

Art. 177. Disciplina anagrafica dello stato civile e delle liste elettorali

Art. 178. Disposizioni in materia sanitaria

Art. 179. Altre modifiche

Capo II - Disposizioni transitorie

Art. 180. Misure di sicurezza

Art. 181. Altre disposizioni transitorie

Art. 182. Ufficio del Garante

Capo III - Abrogazioni

Art. 183. Norme abrogate

Capo IV - Norme finali

Art. 184. Attuazione di direttive europee

Art. 185. Allegazione dei codici di deontologia e di buona condotta

Art. 186. Entrata in vigore

Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali

ALLEGATI

Allegato A

Codici di deontologia

A.1. Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica

A.2. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici

A.3. Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale

A.4. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici

A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti

Allegato B

Disciplinare tecnico in materia di misure minime di sicurezza

Allegato C

Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia

PAGINA BIANCA

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Testo aggiornato a giugno 2006, in base ai seguenti provvedimenti legislativi:

- decreto legge 12 maggio 2006, n. 173 (cfr. nota redazionale p. 63);
- legge 23 febbraio 2006, n. 51 di conversione, con modificazioni, del decreto-legge 30 dicembre 2005, n. 273;
- legge 27 gennaio 2006, n. 21 di conversione, con modificazioni, del decreto legge 30 novembre 2005, n. 245;
- decreto legislativo 7 settembre 2005, n. 209;
- legge 31 luglio 2005, n. 155 di conversione, con modificazioni, del decreto-legge 27 luglio 2005, n. 144;
- legge 1 marzo 2005, n. 26 di conversione, con modificazioni, del decreto-legge 30 dicembre 2004, n. 314;
- legge 27 dicembre 2004, n. 306 di conversione, con modificazioni, del decreto-legge 9 novembre 2004, n. 266;
- legge 27 luglio 2004, n. 188 di conversione, con modificazioni, del decreto-legge 24 giugno 2004, n. 158;
- legge 26 maggio 2004, n. 138 di conversione, con modificazioni, del decreto-legge 29 marzo 2004, n. 81;
- decreto legislativo 22 gennaio 2004, n. 42;
- legge 26 febbraio 2004, n. 45 di conversione, con modificazioni, del decreto-legge 24 dicembre 2003, n. 354.

Il Codice

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

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Visto l'articolo 1 della legge 24 marzo 2001, n. 127, recante delega al Governo per l'emanazione di un testo unico in materia di trattamento dei dati personali;

Visto l'articolo 26 della legge 3 febbraio 2003, n. 14, recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee (legge comunitaria 2002);

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni;

Vista la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Vista la direttiva 95/46/Ce del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;

Vista la direttiva 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;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 9 maggio 2003;

Sentito il Garante per la protezione dei dati personali;

Acquisito il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 27 giugno 2003;

Sulla proposta del Presidente del Consiglio dei ministri, del Ministro per la funzione pubblica e del Ministro per le politiche comunitarie, di concerto con i ministri della giustizia, dell'economia e delle finanze, degli affari esteri e delle comunicazioni;

emana il seguente decreto legislativo:

PARTE I - DISPOSIZIONI GENERALI

TITOLO I - PRINCIPI GENERALI

Art. 1. Diritto alla protezione dei dati personali

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

Art. 2. Finalità

1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Art. 3. Principio di necessità nel trattamento dei dati

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

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

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

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da *a*) a *o*) e da *r*) a *u*), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

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

attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:
   a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
   b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
   c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
   d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
   e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
   f) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
   g) "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:
   a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
   b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
   c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 5. Oggetto ed ambito di applicazione

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

Art. 6. Disciplina del trattamento

1. Le disposizioni contenute nella presente Parte si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II.

TITOLO II - DIRITTI DELL'INTERESSATO

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

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere *a)* e *b)* sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Art. 8. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
   a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
   b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
   c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
   d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
   e) ai sensi dell'articolo 24, comma 1, lettera *f)*, limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere *a*), *b*), *d*), *e*) ed *f*) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere *c*), *g*) ed *h*) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Art. 9. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la

quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere *a*), *b*) e *c*) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

TITOLO III - REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

CAPO I - REGOLE PER TUTTI I TRATTAMENTI

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
   c) esatti e, se necessario, aggiornati;
   d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

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

Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del prin-

cipio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.

3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

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

1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17.

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 16. Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

a) distrutti;

b) ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

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

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

CAPO II - REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

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

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

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

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20. Principi applicabili al trattamento di dati sensibili

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera *g*), anche su schemi tipo.

3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 21. Principi applicabilial trattamento di dati giudiziari

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

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

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere *c*), *d*) ed *e*), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

CAPO III - REGOLE ULTERIORI PER PRIVATI ED ENTI PUBBLICI ECONOMICI

Art. 23. Consenso

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Art. 25. Divieti di comunicazione e diffusione

1. La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:

a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera *e*);

b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

2. È fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 26. Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

3. Il comma 1 non si applica al trattamento:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

Art. 27. Garanzie per i dati giudiziari

1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

TITOLO IV - SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art. 28. Titolare del trattamento

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

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Art. 30. Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

TITOLO V - SICUREZZA DEI DATI E DEI SISTEMI

CAPO I - MISURE DI SICUREZZA

Art. 31. Obblighi di sicurezza

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

Art. 32. Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di

misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

CAPO II - MISURE MINIME DI SICUREZZA

Art. 33. Misure minime

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

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

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

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36. Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

TITOLO VI - ADEMPIMENTI

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;

d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;

f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

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

2. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta Ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.

3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.

4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

Art. 38. Modalità di notificazione

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

2. La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.

3. Il Garante favorisce la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.

4. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.

5. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.

6. Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'articolo 37 fornisce le notizie contenute nel modello di cui al comma 2 a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Art. 39. Obblighi di comunicazione

1. Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;

b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.

2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

3. La comunicazione di cui al comma 1 è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

Art. 40. Autorizzazioni generali

1. Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica italiana.

Art. 41. Richieste di autorizzazione

1. Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'articolo 40 non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.

2. Se una richiesta di autorizzazione riguarda un trattamento autorizzato ai sensi dell'articolo 40 il Garante può provvedere comunque sulla richiesta se le specifiche modalità del trattamento lo giustificano.

3. L'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'articolo 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

4. Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, il termine di quarantacinque giorni di cui all'articolo 26, comma 2, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

5. In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

TITOLO VII - TRASFERIMENTO DEI DATI ALL'ESTERO

Art. 42. Trasferimenti all'interno dell'Unione europea

1. Le disposizioni del presente codice non possono essere applicate in modo tale da

restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Art. 43. Trasferimenti consentiti in Paesi terzi

1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando:

a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;

b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21;

d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

Art. 44. Altri trasferimenti consentiti

1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

a) individuate dal Garante anche in relazione a garanzie prestate con un contratto;

b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/Ce del Parlamento europeo e del Consiglio, del 24 ottobre 1995, 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.

Art. 45. Trasferimenti vietati

1. 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, è 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 modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

PARTE II - DISPOSIZIONI RELATIVE A SPECIFICI SETTORI

TITOLO I - TRATTAMENTI IN AMBITO GIUDIZIARIO

CAPO I - PROFILI GENERALI

Art. 46. Titolari dei trattamenti

1. Gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento.

2. Con decreto del Ministro della giustizia sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, relativamente a banche di dati centrali od oggetto di interconnessione tra più uffici o titolari. I provvedimenti con cui il Consiglio superiore della magistratura e gli altri organi di autogoverno di cui al comma 1 individuano i medesimi trattamenti da essi effettuati sono riportati nell'allegato C) con decreto del Ministro della giustizia.

Art. 47. Trattamenti per ragioni di giustizia

1. In caso di trattamento di dati personali effettuato presso uffici giudiziari di ogni ordine e grado, presso il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia, non si applicano, se il trattamento è effettuato per ragioni di giustizia, le seguenti disposizioni del codice:

a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;

b) articoli da 145 a 151.

2. Agli effetti del presente codice si intendono effettuati per ragioni di giustizia i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché le attività ispettive su uffici giudiziari. Le medesime ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla predetta trattazione.

Art. 48. Banche di dati di uffici giudiziari

1. Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire in conformità alle vigenti disposizioni processuali dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11 del presente codice.

Art. 49. Disposizioni di attuazione

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

CAPO II - MINORI

Art. 50. Notizie o immagini relative a minori

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

CAPO III - INFORMATICA GIURIDICA

Art. 51. Principi generali

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e

il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.

2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo.

Art. 52. Dati identificativi degli interessati

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.

2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.

3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: "In caso di diffusione omettere le generalità e gli altri dati identificativi di ...".

4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.

5. Fermo restando quanto previsto dall'articolo 734-*bis* del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.

6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 32 della legge 11 febbraio 1994, n. 109, provvede in modo analogo in caso di richiesta di una parte.

7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

TITOLO II - TRATTAMENTI DA PARTE DI FORZE DI POLIZIA

CAPO I - PROFILI GENERALI

Art. 53. Ambito applicativo e titolari dei trattamenti

1. Al trattamento di dati personali effettuato dal Centro elaborazione dati del Diparti-

mento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento, non si applicano le seguenti disposizioni del codice:

a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;
b) articoli da 145 a 151.

2. Con decreto del Ministro dell'interno sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, e i relativi titolari.

Art. 54. Modalità di trattamento e flussi di dati

1. Nei casi in cui le autorità di pubblica sicurezza o le forze di polizia possono acquisire in conformità alle vigenti disposizioni di legge o di regolamento dati, informazioni, atti e documenti da altri soggetti, l'acquisizione può essere effettuata anche per via telematica. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11. Le convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'articolo 53.

2. I dati trattati per le finalità di cui al medesimo articolo 53 sono conservati separatamente da quelli registrati per finalità amministrative che non richiedono il loro utilizzo.

3. Fermo restando quanto previsto dall'articolo 11, il Centro elaborazioni dati di cui all'articolo 53 assicura l'aggiornamento periodico e la pertinenza e non eccedenza dei dati personali trattati anche attraverso interrogazioni autorizzate del casellario giudiziale e del casellario dei carichi pendenti del Ministero della giustizia di cui al decreto del Presidente della Repubblica 14 novembre 2002, n. 313, o di altre banche di dati di forze di polizia, necessarie per le finalità di cui all'articolo 53.

4. Gli organi, uffici e comandi di polizia verificano periodicamente i requisiti di cui all'articolo 11 in riferimento ai dati trattati anche senza l'ausilio di strumenti elettronici, e provvedono al loro aggiornamento anche sulla base delle procedure adottate dal Centro elaborazioni dati ai sensi del comma 3, o, per i trattamenti effettuati senza l'ausilio di strumenti elettronici, mediante annotazioni o integrazioni dei documenti che li contengono.

Art. 55. Particolari tecnologie

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

Art. 56. Tutela dell'interessato

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

Art. 57. Disposizioni di attuazione

1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, sono individuate le modalità di attuazione dei principi del presente codice relativamente al trattamento dei dati effettuato per le finalità di cui all'articolo 53 dal Centro elaborazioni dati e da organi, uffici o comandi di polizia, anche ad integrazione e modifica del decreto

del Presidente della Repubblica 3 maggio 1982, n. 378, e in attuazione della Raccomandazione R (87)15 del Consiglio d'Europa del 17 settembre 1987, e successive modificazioni. Le modalità sono individuate con particolare riguardo:

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

TITOLO III - DIFESA E SICUREZZA DELLO STATO

CAPO I - PROFILI GENERALI

Art. 58. Disposizioni applicabili

1. Ai trattamenti effettuati dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge, le disposizioni del presente codice si applicano limitatamente a quelle previste negli articoli da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169.

2. Ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, le disposizioni del presente codice si applicano limitatamente a quelle indicate nel comma 1, nonché alle disposizioni di cui agli articoli 37, 38 e 163.

3. Le misure di sicurezza relative ai dati trattati dagli organismi di cui al comma 1 sono stabilite e periodicamente aggiornate con decreto del Presidente del Consiglio dei ministri, con l'osservanza delle norme che regolano la materia.

4. Con decreto del Presidente del Consiglio dei ministri sono individuate le modalità di applicazione delle disposizioni applicabili del presente codice in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di incaricati, anche in relazione all'aggiornamento e alla conservazione.

TITOLO IV - TRATTAMENTI IN AMBITO PUBBLICO

CAPO I - ACCESSO A DOCUMENTI AMMINISTRATIVI

Art. 59. Accesso a documenti amministrativi

1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

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

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

CAPO II - REGISTRI PUBBLICI E ALBI PROFESSIONALI

Art. 61. Utilizzazione di dati pubblici

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla Raccomandazione R (91)10 del Consiglio d'Europa in relazione all'articolo 11.

2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione.

3. L'ordine o collegio professionale può, a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale.

4. A richiesta dell'interessato l'ordine o collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari.

CAPO III - STATO CIVILE, ANAGRAFI E LISTE ELETTORALI

Art. 62. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative alla tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché al rilascio di documenti di riconoscimento o al cambiamento delle generalità.

Art. 63. Consultazione di atti

1. Gli atti dello stato civile conservati negli Archivi di Stato sono consultabili nei limiti previsti dall'articolo 107 del decreto legislativo 29 ottobre 1999, n. 490.

CAPO IV - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 64. Cittadinanza, immigrazione e condizione dello straniero

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e del profugo e sullo stato di rifugiato.

2. Nell'ambito delle finalità di cui al comma 1 è ammesso, in particolare, il trattamento dei dati sensibili e giudiziari indispensabili:

a) al rilascio e al rinnovo di visti, permessi, attestazioni, autorizzazioni e documenti anche sanitari;
b) al riconoscimento del diritto di asilo o dello stato di rifugiato, o all'applicazione della protezione temporanea e di altri istituti o misure di carattere umanitario, ovvero all'attuazione di obblighi di legge in materia di politiche migratorie;
c) in relazione agli obblighi dei datori di lavoro e dei lavoratori, ai ricongiungimenti,

all'applicazione delle norme vigenti in materia di istruzione e di alloggio, alla partecipazione alla vita pubblica e all'integrazione sociale.

3. Il presente articolo non si applica ai trattamenti di dati sensibili e giudiziari effettuati in esecuzione degli accordi e convenzioni di cui all'articolo 154, comma 2, lettere *a)* e *b)*, o comunque effettuati per finalità 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.

Art. 65. Diritti politici e pubblicità dell'attività di organi

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di:

a) elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari;

b) documentazione dell'attività istituzionale di organi pubblici.

2. I trattamenti dei dati sensibili e giudiziari per le finalità di cui al comma 1 sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti:

a) lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità;

b) le richieste di referendum, le relative consultazioni e la verifica delle relative regolarità;

c) l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi;

d) l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni di inchiesta, il rapporto con gruppi politici;

e) la designazione e la nomina di rappresentanti in commissioni, enti e uffici.

3. Ai fini del presente articolo, è consentita la diffusione dei dati sensibili e giudiziari per le finalità di cui al comma 1, lettera *a)*, in particolare con riguardo alle sottoscrizioni di liste, alla presentazione delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti.

4. Ai fini del presente articolo, in particolare, è consentito il trattamento di dati sensibili e giudiziari indispensabili:

a) per la redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

b) per l'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo.

5. I dati sensibili e giudiziari trattati per le finalità di cui al comma 1 possono essere comunicati e diffusi nelle forme previste dai rispettivi ordinamenti. Non è comunque consentita la divulgazione dei dati sensibili e giudiziari che non risultano indispensabili per assicurare il rispetto del principio di pubblicità dell'attività istituzionale, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 66. Materia tributaria e doganale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività 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, nonché in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane.

2. Si considerano inoltre di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività 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, nonché 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. Attività di controllo e ispettive

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di:

a) verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, 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;

b) accertamento, nei limiti delle finalità 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.

Art. 68. Benefici economici ed abilitazioni

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.

2. Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione:

a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia;

b) alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive;

c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti;

d) al riconoscimento di benefici connessi all'invalidità civile;

e) alla concessione di contributi in materia di formazione professionale;

f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;

g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.

3. Il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la trasparenza delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 69. Onorificenze, ricompense e riconoscimenti

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilità e di professionalità 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, nonché 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. Volontariato e obiezione di coscienza

1. Si considerano di rilevante interesse pubblico, ai sensi dell'articoli 20 e 21, le finalità 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.

2. Si considerano, altresì, di rilevante interesse pubblico le finalità di applicazione della legge 8 luglio 1998, n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza.

Art. 71. Attività sanzionatorie e di tutela

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità:
   a) di applicazione delle norme in materia di sanzioni amministrative e ricorsi;
   b) 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, o direttamente connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo o di un'ingiusta restrizione della libertà personale.

2. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se il diritto da far valere o difendere, di cui alla lettera *b*) del comma 1, è di rango almeno pari a quello dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 72. Rapporti con enti di culto

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative allo svolgimento dei rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose.

Art. 73. Altre finalità in ambito amministrativo e sociale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali, con particolare riferimento a:
   a) interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
   b) interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
   c) assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;
   d) indagini psico-sociali relative a provvedimenti di adozione anche internazionale;
   e) compiti di vigilanza per affidamenti temporanei;
   f) iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;
   g) interventi in tema di barriere architettoniche.

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

CAPO V - PARTICOLARI CONTRASSEGNI

Art. 74. Contrassegni su veicolie accessi a centri storici

1. I contrassegni rilasciati a qualunque titolo per la circolazione e la sosta di veicoli a servizio di persone invalide, ovvero per il transito e la sosta in zone a traffico limitato, e che devono essere esposti su veicoli, contengono i soli dati indispensabili ad individuare l'autorizzazione rilasciata e senza l'apposizione di simboli o diciture dai quali può desumersi la speciale natura dell'autorizzazione per effetto della sola visione del contrassegno.

2. Le generalità e l'indirizzo della persona fisica interessata sono riportati sui contrassegni con modalità che non consentono, parimenti, la loro diretta visibilità se non in caso di richiesta di esibizione o necessità di accertamento.

3. La disposizione di cui al comma 2 si applica anche in caso di fissazione a qualunque titolo di un obbligo di esposizione sui veicoli di copia del libretto di circolazione o di altro documento.

4. Per il trattamento dei dati raccolti mediante impianti per la rilevazione degli accessi di veicoli ai centri storici ed alle zone a traffico limitato continuano, altresì, ad applicarsi le disposizioni del decreto del Presidente della Repubblica 22 giugno 1999, n. 250.

TITOLO V - TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

CAPO I - PRINCIPI GENERALI

Art. 75. Ambito applicativo

1. Il presente titolo disciplina il trattamento dei dati personali in ambito sanitario.

Art. 76. Esercenti professioni sanitariee organismi sanitari pubblici

1. Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute:

a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;
b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera *a*) riguarda un terzo o la collettività.

2. Nei casi di cui al comma 1 il consenso può essere prestato con le modalità semplificate di cui al capo II.

3. Nei casi di cui al comma 1 l'autorizzazione del Garante è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità.

CAPO II - MODALITÀ SEMPLIFICATE PER INFORMATIVA E CONSENSO

Art. 77. Casi di semplificazione

1. Il presente capo individua modalità semplificate utilizzabili dai soggetti di cui al comma 2:

a) per informare l'interessato relativamente ai dati personali raccolti presso il medesimo interessato o presso terzi, ai sensi dell'articolo 13, commi 1 e 4;
b) per manifestare il consenso al trattamento dei dati personali nei casi in cui ciò è richiesto ai sensi dell'articolo 76;
c) per il trattamento dei dati personali.

2. Le modalità semplificate di cui al comma 1 sono applicabili:

a) dagli organismi sanitari pubblici;
b) dagli altri organismi privati e dagli esercenti le professioni sanitarie;
c) dagli altri soggetti pubblici indicati nell'articolo 80.

Art. 78. Informativa del medico di medicina generale o del pediatra

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1.

2. L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

3. L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'articolo 13, comma 3, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.

4. L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;
b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;
c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;
d) fornisce farmaci prescritti;
e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

5. L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;
b) nell'ambito della teleassistenza o telemedicina;
c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

Art. 79. Informativa da parte di organismi sanitari

1. Gli organismi sanitari pubblici e privati possono avvalersi delle modalità semplificate relative all'informativa e al consenso di cui agli articoli 78 e 81 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati.

2. Nei casi di cui al comma 1 l'organismo o le strutture annotano l'avvenuta informativa e il consenso con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

3. Le modalità semplificate di cui agli articoli 78 e 81 possono essere utilizzate in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie.

4. Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalità semplificate possono essere utilizzate per più trattamenti di dati effettuati nei casi di cui al presente articolo ed ai soggetti di cui all'articolo 80.

Art. 80. Informativa da parte di altri soggetti pubblici

1. Oltre a quanto previsto dall'articolo 79, possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti ser-

vizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro.

2. L'informativa di cui al comma 1 è integrata con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative di rilevante interesse pubblico che non richiedono il consenso degli interessati.

Art. 81. Prestazione del consenso

1. Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, nei casi in cui è necessario ai sensi del presente codice o di altra disposizione di legge, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato, nei modi indicati negli articoli 78, 79 e 80.

2. Quando il medico o il pediatra fornisce l'informativa per conto di più professionisti ai sensi dell'articolo 78, comma 4, oltre quanto previsto dal comma 1, il consenso è reso conoscibile ai medesimi professionisti con adeguate modalità, anche attraverso menzione, annotazione o apposizione di un bollino o tagliando su una carta elettronica o sulla tessera sanitaria, contenente un richiamo al medesimo articolo 78, comma 4, e alle eventuali diverse specificazioni apposte all'informativa ai sensi del medesimo comma.

Art. 82. Emergenze e tutela della salute e dell'incolumità fisica

1. L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'articolo 117 del decreto legislativo 31 marzo 1998, n. 112.

2. L'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di:

a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;

b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.

3. L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.

4. Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario.

Art. 83. Altre misure per il rispetto dei diritti degli interessati

1. I soggetti di cui agli articoli 78, 79 e 80 adottano idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.

2. Le misure di cui al comma 1 comprendono, in particolare:

a) soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;

b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;

c) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
d) cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
e) il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;
f) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
g) la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;
h) la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
i) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

2-*bis*. Le misure di cui al comma 2 non si applicano ai soggetti di cui all'articolo 78, che ottemperano alle disposizioni di cui al comma 1 secondo modalità adeguate a garantire un rapporto personale e fiduciario con gli assistiti, nel rispetto del codice di deontologia sottoscritto ai sensi dell'articolo 12.

Art. 84. Comunicazione di dati all'interessato

1. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera *a*), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato.

2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera *a*). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

CAPO III - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 85. Compiti del Servizio sanitario nazionale

1. Fuori dei casi di cui al comma 2, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle seguenti attività:
a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;
b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
d) attività certificatorie;
e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;
f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;

g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.

2. Il comma 1 non si applica ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da esercenti le professioni sanitarie o da organismi sanitari pubblici per finalità di tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, per i quali si osservano le disposizioni relative al consenso dell'interessato o all'autorizzazione del Garante ai sensi dell'articolo 76.

3. All'identificazione dei tipi di dati idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta.

4. Il trattamento di dati identificativi dell'interessato è lecito da parte dei soli soggetti che perseguono direttamente le finalità di cui al comma 1. L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività di cui al medesimo comma, secondo il principio dell'indispensabilità dei dati di volta in volta trattati.

Art. 86. Altre finalità di rilevante interesse pubblico

1. Fuori dei casi di cui agli articoli 76 e 85, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di:

a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza;

b) stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste;

c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di:

1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni;

2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge;

3) realizzare comunità-alloggio e centri socio riabilitativi;

4) curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.

2. Ai trattamenti di cui al presente articolo si applicano le disposizioni di cui all'articolo 85, comma 4.

CAPO IV - PRESCRIZIONI MEDICHE

Art. 87. Medicinali a carico del Servizio sanitario nazionale

1. Le ricette relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale sono redatte secondo il modello di cui al comma 2, conformato in modo da permettere di risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della correttezza della prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca, nel rispetto delle norme deontologiche applicabili.

2. Il modello cartaceo per le ricette di medicinali relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale, di cui agli allegati 1, 3, 5 e 6 del decreto del Ministro della sanità 11 luglio 1988, n. 350, e al capitolo 2, paragrafo 2.2.2. del

relativo disciplinare tecnico, è integrato da un tagliando predisposto su carta o con tecnica di tipo copiativo e unito ai bordi delle zone indicate nel comma 3.

3. Il tagliando di cui al comma 2 è apposto sulle zone del modello predisposte per l'indicazione delle generalità e dell'indirizzo dell'assistito, in modo da consentirne la visione solo per effetto di una momentanea separazione del tagliando medesimo che risulti necessaria ai sensi dei commi 4 e 5.

4. Il tagliando può essere momentaneamente separato dal modello di ricetta, e successivamente riunito allo stesso, quando il farmacista lo ritiene indispensabile, mediante sottoscrizione apposta sul tagliando, per una effettiva necessità connessa al controllo della correttezza della prescrizione, anche per quanto riguarda la corretta fornitura del farmaco.

5. Il tagliando può essere momentaneamente separato nei modi di cui al comma 3 anche presso i competenti organi per fini di verifica amministrativa sulla correttezza della prescrizione, o da parte di soggetti legittimati a svolgere indagini epidemiologiche o di ricerca in conformità alla legge, quando è indispensabile per il perseguimento delle rispettive finalità.

6. Con decreto del Ministro della salute, sentito il Garante, può essere individuata una ulteriore soluzione tecnica diversa da quella indicata nel comma 1, basata sull'uso di una fascetta adesiva o su altra tecnica equipollente relativa anche a modelli non cartacei.

Art. 88. Medicinali non a carico del Servizio sanitario nazionale

1. Nelle prescrizioni cartacee di medicinali soggetti a prescrizione ripetibile non a carico, anche parziale, del Servizio sanitario nazionale, le generalità dell'interessato non sono indicate.

2. Nei casi di cui al comma 1 il medico può indicare le generalità dell'interessato solo se ritiene indispensabile permettere di risalire alla sua identità, per un'effettiva necessità derivante dalle particolari condizioni del medesimo interessato o da una speciale modalità di preparazione o di utilizzazione.

Art. 89. Casi particolari

1. Le disposizioni del presente capo non precludono l'applicazione di disposizioni normative che prevedono il rilascio di ricette che non identificano l'interessato o recanti particolari annotazioni, contenute anche nel decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94.

2. Nei casi in cui deve essere accertata l'identità dell'interessato ai sensi del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni, le ricette sono conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.

2-*bis*. Per i soggetti di cui all'articolo 78, l'attuazione delle disposizioni di cui all'articolo 87, comma 3, e 88, comma 1, è subordinata ad un'esplicita richiesta dell'interessato.

CAPO V - DATI GENETICI

Art. 90. Trattamento dei dati genetici e donatori di midollo osseo

1. Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.

2. L'autorizzazione di cui al comma 1 individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'articolo 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.

3. Il donatore di midollo osseo, ai sensi della legge 6 marzo 2001, n. 52, ha il diritto e il dovere di mantenere l'anonimato sia nei confronti del ricevente sia nei confronti di terzi.

CAPO VI - DISPOSIZIONI VARIE

Art. 91. Dati trattati mediante carte

1. Il trattamento in ogni forma di dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, compresa la carta nazionale dei servizi, o trattati mediante le medesime carte è consentito se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17.

Art. 92. Cartelle cliniche

1. Nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera *c*), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 93. Certificato di assistenza al parto

1. Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Si osservano, altresì, le disposizioni dell'articolo 109.

2. Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.

3. Durante il periodo di cui al comma 2 la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art. 94. Banche di dati, registri e schedari in ambito sanitario

1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:

a) il registro nazionale dei casi di mesotelioma asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;

b) la banca di dati in materia di sorveglianza della malattia di Creutzfeldt-Jakob o delle varianti e sindromi ad essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella Gazzetta Ufficiale n. 8 del 10 gennaio 2002;

c) il registro nazionale delle malattie rare di cui all'articolo 3 del decreto del Ministro della sanità in data 18 maggio 2001, n. 279;

d) i registri dei donatori di midollo osseo istituiti in applicazione della legge 6 marzo 2001, n. 52;
e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella Gazzetta Ufficiale n. 78 del 3 aprile 2001.

TITOLO VI - ISTRUZIONE

CAPO I - PROFILI GENERALI

Art. 95. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata.

Art. 96. Trattamento di dati relativi a studenti

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

TITOLO VII - TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI

CAPO I - PROFILI GENERALI

Art. 97. Ambito applicativo

1. Il presente titolo disciplina il trattamento dei dati personali effettuato per scopi storici, statistici o scientifici.

Art. 98. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative ai trattamenti effettuati da soggetti pubblici:
a) per scopi storici, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato e negli archivi storici degli enti pubblici, secondo quanto disposto dal decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice;
b) che fanno parte del Sistema statistico nazionale (Sistan) ai sensi del decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni;
c) per scopi scientifici.

Art. 99. Compatibilità tra scopi e durata del trattamento

1. Il trattamento di dati personali effettuato per scopi storici, statistici o scientifici è considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. Il trattamento di dati personali per scopi storici, statistici o scientifici può 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.

3. Per scopi storici, statistici o scientifici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento.

Art. 100. Dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli sensibili o giudiziari.

2. Resta fermo il diritto dell'interessato di opporsi per motivi legittimi ai sensi dell'articolo 7, comma 4, lettera *a*).

3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241.

4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

CAPO II - TRATTAMENTO PER SCOPI STORICI

Art. 101. Modalità di trattamento

1. I dati personali raccolti per scopi storici non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 11.

2. I documenti contenenti dati personali, trattati per scopi storici, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.

3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

Art. 102. Codice di deontologia e di buona condotta

1. Il Garante promuove ai sensi dell'articolo 12 la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici.

2. Il codice di deontologia e di buona condotta di cui al comma 1 individua, in particolare:
   a) 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 presente codice applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica;
   b) 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 è informato dall'utente della prevista diffusione di dati;
   c) le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a scopi storici, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 103. Consultazione di documenti conservati in archivi

1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati è disciplinata dal decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice.

CAPO III - TRATTAMENTO PER SCOPI STATISTICI O SCIENTIFICI

Art. 104. Ambito applicativo e dati identificativi per scopi statistici o scientifici

1. Le disposizioni del presente capo si applicano ai trattamenti di dati per scopi statistici o, in quanto compatibili, per scopi scientifici.

2. Agli effetti dell'applicazione del presente capo, in relazione ai dati identificativi si tiene conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare o da altri per identificare l'interessato, anche in base alle conoscenze acquisite in relazione al progresso tecnico.

Art. 105. Modalità di trattamento

1. I dati personali trattati per scopi statistici o scientifici non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura.

2. Gli scopi statistici o scientifici devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui all'articolo 13 anche in relazione a quanto previsto dall'articolo 106, comma 2, lettera *b)*, del presente codice e dall'articolo 6-*bis* del decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni.

3. Quando specifiche circostanze individuate dai codici di cui all'articolo 106 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 può essere data anche per il tramite del soggetto rispondente.

4. Per il trattamento effettuato per scopi statistici o scientifici rispetto a dati raccolti per altri scopi, l'informativa all'interessato non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate dai codici di cui all'articolo 106.

Art. 106. Codici di deontologia e di buona condotta

1. Il Garante promuove ai sensi dell'articolo 12 la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi statistici o scientifici.

2. Con i codici di cui al comma 1 sono individuati, tenendo conto, per i soggetti già compresi nell'ambito del Sistema statistico nazionale, di quanto già previsto dal decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni, e, per altri soggetti, sulla base di analoghe garanzie, in particolare:

a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal medesimo decreto legislativo n. 322 del 1989, siano effettuati per idonei ed effettivi scopi statistici o scientifici;

b) per quanto non previsto dal presente codice, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalità per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle pertinenti raccomandazioni del Consiglio d'Europa;

c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico;

d) le garanzie da osservare ai fini dell'applicazione delle disposizioni di cui all'articolo 24, comma 1, lettera *i)*, e 43, comma 1, lettera *g)*, che permettono di prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle predette raccomandazioni;

e) modalità semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati sensibili;

f) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire al personale incaricato;

g) le misure da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'articolo 31, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche che non sono incaricati e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per scopi statistici o scientifici da effettuarsi con enti ed uffici situati all'estero anche sulla base delle garanzie previste dall'articolo 44, comma 1, lettera *a*);

h) l'impegno al rispetto di regole di condotta degli incaricati che non sono tenuti in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.

Art. 107. Trattamento di dati sensibili

1. Fermo restando quanto previsto dall'articolo 20 e fuori dei casi di particolari indagini statistiche o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati sensibili, quando è richiesto, può essere prestato con modalità semplificate, individuate dal codice di cui all'articolo 106 e l'autorizzazione del Garante può essere rilasciata anche ai sensi dell'articolo 40.

Art. 108. Sistema statistico nazionale

1. Il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, oltre a quanto previsto dal codice di deontologia e di buona condotta sottoscritto ai sensi dell'articolo 106, comma 2, resta inoltre disciplinato dal decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni, in particolare per quanto riguarda il trattamento dei dati sensibili indicati nel programma statistico nazionale, l'informativa all'interessato, l'esercizio dei relativi diritti e i dati non tutelati dal segreto statistico ai sensi dell'articolo 9, comma 4, del medesimo decreto.

Art. 109. Dati statistici relativi all'evento della nascita

1. Per la rilevazione dei dati statistici relativi agli eventi di nascita, compresi quelli relativi ai nati affetti da malformazioni e ai nati morti, nonché per i flussi di dati anche da parte di direttori sanitari, si osservano, oltre alle disposizioni di cui al decreto del Ministro della sanità 16 luglio 2001, n. 349, le modalità tecniche determinate dall'Istituto nazionale della statistica, sentito il Ministro della salute, dell'interno e il Garante.

Art. 110. Ricerca medica, biomedica ed epidemiologica

1. Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 7 nei riguardi dei trattamenti di cui al comma 1, l'aggiornamento, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

TITOLO VIII - LAVORO E PREVIDENZA SOCIALE

CAPO I - PROFILI GENERALI

Art. 111. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deon-

tologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione degli annunci per finalità di occupazione di cui all'articolo 113, comma 3 e alla ricezione di *curricula* contenenti dati personali anche sensibili.

Art. 112. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli effettuati al fine di:

a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;
b) garantire le pari opportunità;
c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;
d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;
e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;
f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente;
g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;
h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;
i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;
l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;
m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;
n) svolgere l'attività di indagine e ispezione presso soggetti pubblici;
o) valutare la qualità dei servizi resi e dei risultati conseguiti.

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

CAPO II - ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO

Art. 113. Raccolta di dati e pertinenza

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300.

CAPO III - DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO

Art. 114. Controllo a distanza

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

Art. 115. Telelavoro e lavoro a domicilio

1. Nell'ambito del rapporto di lavoro domestico e del telelavoro il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

CAPO IV - ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE

Art. 116. Conoscibilità di dati su mandato dell'interessato

1. Per lo svolgimento delle proprie attività 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.

2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee-guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

TITOLO IX - SISTEMA BANCARIO, FINANZIARIO ED ASSICURATIVO

CAPO I - SISTEMI INFORMATIVI

Art. 117. Affidabilità e puntualità nei pagamenti

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati, individuando anche specifiche modalità per garantire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato.

Art. 118. Informazioni commerciali

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale, prevedendo anche, in correlazione con quanto previsto dall' articolo 13, comma 5, modalità semplificate per l'informativa all'interessato e idonei meccanismi per garantire la qualità e l'esattezza dei dati raccolti e comunicati.

Art. 119. Dati relativi al comportamento debitorio

1. Con il codice di deontologia e di buona condotta di cui all'articolo 118 sono altresì 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 al comportamento debitorio dell'interessato nei casi diversi da quelli disciplinati nel codice di cui all'articolo 117, tenendo conto della specificità dei trattamenti nei diversi ambiti.

Art. 120. Sinistri

1. L'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Isvap) definisce con proprio provvedimento le procedure e le modalità di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalità di accesso alle informazioni raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.

2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.

3. Per quanto non previsto dal presente articolo si applicano le disposizioni dell'articolo 135 del Codice delle assicurazioni private.

TITOLO X - COMUNICAZIONI ELETTRONICHE

CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121. Servizi interessati

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.

Art. 122. Informazioni raccolte nei riguardi dell'abbonato o dell'utente

1. Salvo quanto previsto dal comma 2, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.

Art. 123. Dati relativi al traffico

1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento.

4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione.

Art. 124. Fatturazione dettagliata

1. L'abbonato ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla località, alla durata e al numero di scatti addebitati per ciascuna conversazione.

2. Il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto ad abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente ed in modo agevole, avvalendosi per il pagamento di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate.

3. Nella documentazione inviata all'abbonato relativa alle comunicazioni effettuate non sono evidenziati i servizi e le comunicazioni di cui al comma 2, né le comunicazioni necessarie per attivare le modalità alternative alla fatturazione.

4. Nella fatturazione all'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

5. Il Garante, accertata l'effettiva disponibilità delle modalità di cui al comma 2, può autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

Art. 125. Identificazione della linea

1. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'utente chiamante la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.

2. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione delle chiamate entranti.

3. Se è disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avviene prima che la comunicazione sia stabilita, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuita, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.

4. Se è disponibile la presentazione dell'identificazione della linea collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Le disposizioni di cui al comma 1 si applicano anche alle chiamate dirette verso Paesi non appartenenti all'Unione europea. Le disposizioni di cui ai commi 2, 3 e 4 si applicano anche alle chiamate provenienti da tali Paesi.

6. Se è disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilità previste ai commi 1, 2, 3 e 4.

Art. 126. Dati relativi all'ubicazione

1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto.

3. L'utente e l'abbonato che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30, sono la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

Art. 127. Chiamate di disturbo e di emergenza

1. L'abbonato che riceve chiamate di disturbo può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.

2. La richiesta formulata per iscritto dall'abbonato specifica le modalità di ricezione delle chiamate di disturbo e nel caso in cui sia preceduta da una richiesta telefonica è inoltrata entro quarantotto ore.

3. I dati conservati ai sensi del comma 1 possono essere comunicati all'abbonato che dichiari di utilizzarli per esclusive finalità di tutela rispetto a chiamate di disturbo. Per i servizi di cui al comma 1 il fornitore assicura procedure trasparenti nei confronti degli abbonati e può richiedere un contributo spese non superiore ai costi effettivamente sopportati.

4. Il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predispone procedure trasparenti per garantire, linea per linea, l'inefficacia della soppressione dell'identificazione della linea chiamante, nonché, ove necessario, il trattamento dei dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. I servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorità per le garanzie nelle comunicazioni.

Art. 128. Trasferimento automatico della chiamata

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta le misure necessarie per consentire a ciascun abbonato, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle chiamate verso il proprio terminale effettuato da terzi.

Art. 129. Elenchi di abbonati

1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 3, e in conformità alla nor-

mativa comunitaria, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico, anche in riferimento ai dati già raccolti prima della data di entrata in vigore del presente codice.

2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per le finalità di cui all'articolo 7, comma 4, lettera *b*), in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca dell'abbonato per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri.

Art. 130. Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo *Mms* (Multimedia Messaging Service) o *Sms* (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24.

4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. É vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera *b*), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

Art. 131. Informazioni ad abbonati e utenti

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa l'abbonato e, ove possibile, l'utente circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

2. L'abbonato informa l'utente quando il contenuto delle comunicazioni o conversazioni può essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'abbonato medesimo.

3. L'utente informa l'altro utente quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti.

Art. 132. Conservazione di dati di traffico per altre finalità

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore

per ventiquattro mesi, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi.

2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, sono conservati dal fornitore per ulteriori ventiquattro mesi e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori sei mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera *a*) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale, ferme restando le condizioni di cui all'articolo 8, comma 2, lettera *f*), per il traffico entrante.

4. Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera *a*), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

4-*bis*. Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.

5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti anche a:

a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B);
b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;
c) individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al comma 4 e all'articolo 7;
d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.

CAPO II - INTERNET E RETI TELEMATICHE

Art. 133. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per 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 più 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 modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più 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 qualità delle modalità prescelte e il livello di sicurezza assicurato.

CAPO III - VIDEOSORVEGLIANZA

Art. 134. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11.

TITOLO XI - LIBERE PROFESSIONI E INVESTIGAZIONE PRIVATA

CAPO I - PROFILI GENERALI

Art. 135. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per 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'attività di investigazione privata autorizzata in conformità alla legge.

TITOLO XII - GIORNALISMO ED ESPRESSIONE LETTERARIA ED ARTISTICA

CAPO I - PROFILI GENERALI

Art. 136. Finalità giornalistiche e altre manifestazioni del pensiero

1. Le disposizioni del presente titolo si applicano al trattamento:
   a) effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità;
   b) effettuato dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69;
   c) temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica.

Art. 137. Disposizioni applicabili

1. Ai trattamenti indicati nell'articolo 136 non si applicano le disposizioni del presente codice relative:
   a) all'autorizzazione del Garante prevista dall'articolo 26;
   b) alle garanzie previste dall'articolo 27 per i dati giudiziari;
   c) al trasferimento dei dati all'estero, contenute nel Titolo VII della Parte I.

2. Il trattamento dei dati di cui al comma 1 è effettuato anche senza il consenso dell'interessato previsto dagli articoli 23 e 26.

3. In caso di diffusione o di comunicazione dei dati per le finalità di cui all'articolo 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'articolo 2 e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico.

Art. 138. Segreto professionale

1. In caso di richiesta dell'interessato di conoscere l'origine dei dati personali ai sensi dell'articolo 7, comma 2, lettera *a*) restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

CAPO II - CODICE DI DEONTOLOGIA

Art. 139. Codice di deontologia relativo ad attività giornalistiche

1. Il Garante promuove ai sensi dell'articolo 12 l'adozione da parte del Consiglio nazionale dell'ordine dei giornalisti di un codice di deontologia relativo al trattamento dei dati di cui all'articolo 136, che prevede misure ed accorgimenti a garanzia degli interessati rappor-

tate alla natura dei dati, in particolare per quanto riguarda quelli idonei a rivelare lo stato di salute e la vita sessuale. Il codice può anche prevedere forme semplificate per le informative di cui all'articolo 13.

2. Nella fase di formazione del codice, ovvero successivamente, il Garante, in cooperazione con il Consiglio, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire.

3. Il codice o le modificazioni od integrazioni al codice di deontologia che non sono adottati dal Consiglio entro sei mesi dalla proposta del Garante sono adottati in via sostitutiva dal Garante e sono efficaci sino a quando diviene efficace una diversa disciplina secondo la procedura di cooperazione.

4. Il codice e le disposizioni di modificazione ed integrazione divengono efficaci quindici giorni dopo la loro pubblicazione nella Gazzetta Ufficiale ai sensi dell'articolo 12.

5. In caso di violazione delle prescrizioni contenute nel codice di deontologia, il Garante può vietare il trattamento ai sensi dell'articolo 143, comma 1, lettera *c*).

TITOLO XIII - MARKETING DIRETTO

CAPO I - PROFILI GENERALI

Art. 140. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per 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.

PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

TITOLO I - TUTELA AMMINISTRATIVA E GIURISDIZIONALE

CAPO I - TUTELA DINNANZI AL GARANTE

Sezione I - Principi generali

Art. 141. Forme di tutela

1. L'interessato può rivolgersi al Garante:
   a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
   b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera *a*), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
   c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo.

Sezione II - Tutela amministrativa

Art. 142. Proposizione dei reclami

1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante.

2. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai sensi dell'articolo 9, comma 2, ed è presentato al Garante senza particolari formalità. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.

3. Il Garante può predisporre un modello per il reclamo da pubblicare nel Bollettino e di cui favorisce la disponibilità con strumenti elettronici.

Art. 143. Procedimento per i reclami

1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento:

a) prima di prescrivere le misure di cui alla lettera *b*), ovvero il divieto o il blocco ai sensi della lettera *c*), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente;

b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;

c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera *b*), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;

d) può 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 collettività.

2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

Art. 144. Segnalazioni

1. I provvedimenti di cui all'articolo 143 possono essere adottati anche a seguito delle segnalazioni di cui all'articolo 141, comma 1, lettera *b*), se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento.

Sezione III - Tutela alternativa a quella giurisdizionale

Art. 145. Ricorsi

1. I diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante.

2. Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.

3. La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

Art. 146. Interpello preventivo

1. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile ai sensi dell'articolo 8, comma 1, e sono decorsi i termini previsti dal presente articolo, ovvero è stato opposto alla richiesta un diniego anche parziale.

2. Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro quindici giorni dal suo ricevimento.

3. Entro il termine di cui al comma 2, se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il

titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Art. 147. Presentazione del ricorso

1. Il ricorso è proposto nei confronti del titolare e indica:
   a) gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7;
   b) la data della richiesta presentata al titolare o al responsabile ai sensi dell'articolo 8, comma 1, oppure del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima;
   c) gli elementi posti a fondamento della domanda;
   d) il provvedimento richiesto al Garante;
   e) il domicilio eletto ai fini del procedimento.

2. Il ricorso è sottoscritto dal ricorrente o dal procuratore speciale e reca in allegato:
   a) la copia della richiesta rivolta al titolare o al responsabile ai sensi dell'articolo 8, comma 1;
   b) l'eventuale procura;
   c) la prova del versamento dei diritti di segreteria.

3. Al ricorso è unita, altresì, la documentazione utile ai fini della sua valutazione e l'indicazione di un recapito per l'invio di comunicazioni al ricorrente o al procuratore speciale mediante posta elettronica, telefax o telefono.

4. Il ricorso è rivolto al Garante e la relativa sottoscrizione è autenticata. L'autenticazione non è richiesta se la sottoscrizione è apposta presso l'Ufficio del Garante o da un procuratore speciale iscritto all'albo degli avvocati al quale la procura è conferita ai sensi dell'articolo 83 del codice di procedura civile, ovvero con firma digitale in conformità alla normativa vigente.

5. Il ricorso è validamente proposto solo se è trasmesso con plico raccomandato, oppure per via telematica osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento prescritte ai sensi dell'articolo 38, comma 2, ovvero presentato direttamente presso l'Ufficio del Garante.

Art. 148. Inammissibilità del ricorso

1. Il ricorso è inammissibile:
   a) se proviene da un soggetto non legittimato;
   b) in caso di inosservanza delle disposizioni di cui agli articoli 145 e 146;
   c) se difetta di taluno degli elementi indicati nell'articolo 147, commi 1 e 2, salvo che sia regolarizzato dal ricorrente o dal procuratore speciale anche su invito dell'Ufficio del Garante ai sensi del comma 2, entro sette giorni dalla data della sua presentazione o della ricezione dell'invito. In tale caso, il ricorso si considera presentato al momento in cui il ricorso regolarizzato perviene all'Ufficio.

2. Il Garante determina i casi in cui è possibile la regolarizzazione del ricorso.

Art. 149. Procedimento relativo al ricorso

1. Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, il ricorso è comunicato al titolare entro tre giorni a cura dell'Ufficio del Garante, con invito ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea. L'invito è comunicato al titolare per il tramite del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, ove indicato nel ricorso.

2. In caso di adesione spontanea è dichiarato non luogo a provvedere. Se il ricorrente lo richiede, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte o compensati per giusti motivi anche parzialmente.

3. Nel procedimento dinanzi al Garante il titolare, il responsabile di cui al comma 1 e l'in-

teressato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. A tal fine l'invito di cui al comma 1 è trasmesso anche al ricorrente e reca l'indicazione del termine entro il quale il titolare, il medesimo responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio anche mediante idonea tecnica audiovisiva.

4. Nel procedimento il ricorrente può precisare la domanda nei limiti di quanto chiesto con il ricorso o a seguito di eccezioni formulate dal titolare.

5. Il Garante può disporre, anche d'ufficio, l'espletamento di una o più perizie. Il provvedimento che le dispone precisa il contenuto dell'incarico e il termine per la sua esecuzione, ed è comunicato alle parti le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti designati. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia.

6. Nel procedimento, il titolare e il responsabile di cui al comma 1 possono essere assistiti da un procuratore o da altra persona di fiducia.

7. Se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti il termine di sessanta giorni di cui all'articolo 150, comma 2, può essere prorogato per un periodo non superiore ad ulteriori quaranta giorni.

8. Il decorso dei termini previsti dall'articolo 150, comma 2 e dall'articolo 151 è sospeso di diritto dal 1 agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussiste il pregiudizio di cui all'articolo 146, comma 1, e non preclude l'adozione dei provvedimenti di cui all'articolo 150, comma 1 .

Art. 150. Provvedimenti a seguito del ricorso

1. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento può essere adottato anche prima della comunicazione del ricorso ai sensi dell'articolo 149, comma 1, e cessa di avere ogni effetto se non è adottata nei termini la decisione di cui al comma 2. Il medesimo provvedimento è impugnabile unitamente a tale decisione.

2. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto.

3. Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico, anche in parte, del soccombente o compensati anche parzialmente per giusti motivi.

4. Il provvedimento espresso, anche provvisorio, adottato dal Garante è comunicato alle parti entro dieci giorni presso il domicilio eletto o risultante dagli atti. Il provvedimento può essere comunicato alle parti anche mediante posta elettronica o telefax.

5. Se sorgono difficoltà o contestazioni riguardo all'esecuzione del provvedimento di cui ai commi 1 e 2, il Garante, sentite le parti ove richiesto, dispone le modalità di attuazione avvalendosi, se necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato.

6. In caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese e dei diritti, 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.

Art. 151. Opposizione

1. Avverso 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. L'opposizione non sospende l'esecuzione del provvedimento.

2. Il tribunale provvede nei modi di cui all'articolo 152.

CAPO II - TUTELA GIURISDIZIONALE

Art. 152. Autorità giudiziaria ordinaria

1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.

2. Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.

3. Il tribunale decide in ogni caso in composizione monocratica.

4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.

6. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.

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

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

9. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli.

10. Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.

11. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza.

12. Con la sentenza il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale

atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.

13. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.

14. Le disposizioni di cui al presente articolo si applicano anche nei casi previsti dall'articolo 10, comma 5, della legge 1 aprile 1981, n. 121, e successive modificazioni.

TITOLO II - L'AUTORITÀ

CAPO I - IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Art. 153. Il Garante

1. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

2. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

3. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. Il presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai componenti compete un'indennità non eccedente nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate dall'articolo 6 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

7. Alle dipendenze del Garante è posto l'Ufficio di cui all'articolo 156.

Art. 154. Compiti

1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione;

b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;

c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;

d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139;

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

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:
a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione;
b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol);
c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo 1997, e dalla legge 30 luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;
d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;
e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.

4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice.

5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

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

Capo II - L'Ufficio del Garante

Art. 155. Principi applicabili

1. All'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 30

marzo 2001, n. 165, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e le funzioni di gestione attribuite ai dirigenti. Si applicano altresì le disposizioni del medesimo decreto legislativo n. 165 del 2001 espressamente richiamate dal presente codice.

Art. 156. Ruolo organico e personale

1. All'Ufficio del Garante è preposto un segretario generale scelto anche tra magistrati ordinari o amministrativi.

2. Il ruolo organico del personale dipendente è stabilito nel limite di cento unità.

3. Con propri regolamenti pubblicati nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce:

a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti di cui all'articolo 154;

b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo le procedure previste dall'articolo 35 del decreto legislativo n. 165 del 2001;

c) la ripartizione dell'organico tra le diverse aree e qualifiche;

d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e successive modificazioni e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-*bis* del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e organizzative. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni;

e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'articolo 6, comma 2, della legge 31 luglio 1997, n. 249.

4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale di cui al presente comma è corrisposta un'indennità pari all'eventuale differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al personale di ruolo, sulla base di apposita tabella di corrispondenza adottata dal Garante, e comunque non inferiore al cinquanta per cento della retribuzione in godimento, con esclusione dell'indennità integrativa speciale.

5. In aggiunta al personale di ruolo, l'Ufficio può assumere direttamente dipendenti con contratto a tempo determinato, in numero non superiore a venti unità ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma 7.

6. Si applicano le disposizioni di cui all'articolo 30 del decreto legislativo n. 165 del 2001.

7. Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedono, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due volte.

8. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

9. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

10. Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

CAPO III - ACCERTAMENTI E CONTROLLI

Art. 157. Richiesta di informazioni e di esibizione di documenti

1. Per l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

Art. 158. Accertamenti

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1 sono eseguiti da personale dell'Ufficio. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 1, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono 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 più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

Art. 159. Modalità

1. Il personale operante, munito di documento di riconoscimento, può essere assistito ove necessario da consulenti tenuti al segreto ai sensi dell'articolo 156, comma 8. Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti è redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

2. Ai soggetti presso i quali sono eseguiti gli accertamenti è consegnata copia dell'autorizzazione del presidente del tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento, che per questa parte costituisce titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

3. Gli accertamenti, se effettuati presso il titolare o il responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o non è designato, agli incaricati. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile.

4. Se non è disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso quando ciò può facilitarne l'esecuzione.

5. Le informative, le richieste e i provvedimenti di cui al presente articolo e agli articoli 157 e 158 possono essere trasmessi anche mediante posta elettronica e telefax.

6. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

Art. 160. Particolari accertamenti

1. Per i trattamenti di dati personali indicati nei titoli I, II e III della Parte II gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto ai sensi dell'articolo 156, comma 8. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 156, comma 3, lettera *a)*.

4. Per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

5. Nell'effettuare gli accertamenti di cui al presente articolo nei riguardi di uffici giudiziari, il Garante adotta idonee modalità nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo procedente. Gli accertamenti riferiti ad atti di indagine coperti dal segreto sono differiti, se vi è richiesta dell'organo procedente, al momento in cui cessa il segreto.

6. La validità, l'efficacia e l'utilizzabilità 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.

TITOLO III - SANZIONI

CAPO I - VIOLAZIONI AMMINISTRATIVE

Art. 161. Omessa o inidonea informativa all'interessato

1. La violazione delle disposizioni di cui all'articolo 13 è 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 più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

Art. 162. Altre fattispecie

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera *b)*, o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.

2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro.

Art. 163. Omessa o incompleta notificazione

1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

Art. 164. Omessa informazione o esibizione al Garante

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da quattromila euro a ventiquattro mila euro.

Art. 165. Pubblicazione del provvedimento del Garante

1. Nei casi di cui agli articoli 161, 162 e 164 può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

Art. 166. Procedimento di applicazione

1. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente capo e all'articolo 179, comma 3, è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 10, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 154, comma 1, lettera *h*), e 158.

CAPO II - ILLECITI PENALI

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Art. 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

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

Art. 170. Inosservanza di provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera *c*), è punito con la reclusione da tre mesi a due anni.

Art. 171. Altre fattispecie

1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

Art. 172. Pene accessorie

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

TITOLO IV - DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

CAPO I - DISPISIZIONI DI MODIFICA

Art. 173. Convenzione di applicazione dell'Accordo di Schengen

1. La 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, è così modificata:

a) il comma 2 dell'articolo 9 è sostituito dal seguente: "2. Le richieste di accesso, rettifica o cancellazione, nonché di verifica, di cui, rispettivamente, agli articoli 109, 110 e 114, paragrafo 2, della Convenzione, sono rivolte all'autorità di cui al comma 1.";

b) il comma 2 dell'articolo 10 è soppresso;

c) l'articolo 11 è sostituito dal seguente:

"11. 1. L'autorità di controllo di cui all'articolo 114 della Convenzione è il Garante per la protezione dei dati personali. Nell'esercizio dei compiti ad esso demandati per legge, il Garante esercita il controllo sui trattamenti di dati in applicazione della Convenzione ed esegue le verifiche previste nel medesimo articolo 114, anche su segnalazione o reclamo dell'interessato all'esito di un inidoneo riscontro alla richiesta rivolta ai sensi dell'articolo 9, comma 2, quando non è possibile fornire al medesimo interessato una risposta sulla base degli elementi forniti dall'autorità di cui all'articolo 9, comma 1.

2. Si applicano le disposizioni dell'articolo 10, comma 5, della legge 1 aprile 1981, n. 121, e successive modificazioni.";

d) l'articolo 12 è abrogato.

Art. 174. Notifiche di atti e vendite giudiziarie

1. All'articolo 137 del codice di procedura civile, dopo il secondo comma, sono inseriti i seguenti:

"Se la notificazione non può essere eseguita in mani proprie del destinatario, tranne che nel caso previsto dal secondo comma dell'articolo 143, l'ufficiale giudiziario consegna o deposita la copia dell'atto da notificare in busta che provvede a sigillare e su cui trascrive il numero cronologico della notificazione, dandone atto nella relazione in calce all'originale e alla copia dell'atto stesso. Sulla busta non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto. Le disposizioni di cui al terzo comma si applicano anche alle comunicazioni effettuate con biglietto di cancelleria ai sensi degli articoli 133 e 136.".

2. Al primo comma dell'articolo 138 del codice di procedura civile, le parole da: "può sempre eseguire" a "destinatario," sono sostituite dalle seguenti: "esegue la notificazione di regola mediante consegna della copia nelle mani proprie del destinatario, presso la casa di abitazione oppure, se ciò non è possibile,".

3. Nel quarto comma dell'articolo 139 del codice di procedura civile, la parola: "l'originale" è sostituita dalle seguenti: "una ricevuta".

4. Nell'articolo 140 del codice di procedura civile, dopo le parole: "affigge avviso del deposito" sono inserite le seguenti: "in busta chiusa e sigillata".

5. All'articolo 142 del codice di procedura civile sono apportate le seguenti modificazioni:

a) il primo e il secondo comma sono sostituiti dal seguente:

"Salvo quanto disposto nel secondo comma, se il destinatario non ha residenza,

dimora o domicilio nello Stato e non vi ha eletto domicilio o costituito un procuratore a norma dell'articolo 77, l'atto è notificato mediante spedizione al destinatario per mezzo della posta con raccomandata e mediante consegna di altra copia al pubblico ministero che ne cura la trasmissione al Ministero degli affari esteri per la consegna alla persona alla quale è diretta.";

b) nell'ultimo comma le parole: "ai commi precedenti" sono sostituite dalle seguenti: "al primo comma".

6. Nell'articolo 143, primo comma, del codice di procedura civile, sono soppresse le parole da: ", e mediante" fino alla fine del periodo.

7. All'articolo 151, primo comma, del codice di procedura civile dopo le parole: "maggiore celerità" sono aggiunte le seguenti: ", di riservatezza o di tutela della dignità".

8. All'articolo 250 del codice di procedura civile dopo il primo comma è aggiunto il seguente:

"L'intimazione di cui al primo comma, se non è eseguita in mani proprie del destinatario o mediante servizio postale, è effettuata in busta chiusa e sigillata.".

9. All'articolo 490, terzo comma, del codice di procedura civile è aggiunto, in fine, il seguente periodo: "Nell'avviso è omessa l'indicazione del debitore".

10. All'articolo 570, primo comma, del codice di procedura civile le parole: "del debitore," sono soppresse e le parole da: "informazioni" fino alla fine sono sostituite dalle seguenti: "informazioni, anche relative alle generalità del debitore, possono essere fornite dalla cancelleria del tribunale a chiunque vi abbia interesse".

11. All'articolo 14, quarto comma, della legge 24 novembre 1981, n. 689, e successive modificazioni, è aggiunto, in fine, il seguente periodo: "Quando la notificazione non può essere eseguita in mani proprie del destinatario, si osservano le modalità previste dall'articolo 137, terzo comma, del medesimo codice.".

12. Dopo l'articolo 15 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è inserito il seguente: "Articolo 15-*bis*. (Notificazioni di atti e documenti, comunicazioni ed avvisi) 1. Alla notificazione di atti e di documenti da parte di organi delle pubbliche amministrazioni a soggetti diversi dagli interessati o da persone da essi delegate, nonché a comunicazioni ed avvisi circa il relativo contenuto, si applicano le disposizioni contenute nell'articolo 137, terzo comma, del codice di procedura civile. Nei biglietti e negli inviti di presentazione sono indicate le informazioni strettamente necessarie a tale fine.".

13. All'articolo 148 del codice di procedura penale sono apportate le seguenti modificazioni:

a) il comma 3 è sostituito dal seguente: "3. L'atto è notificato per intero, salvo che la legge disponga altrimenti, di regola mediante consegna di copia al destinatario oppure, se ciò non è possibile, alle persone indicate nel presente titolo. Quando la notifica non può essere eseguita in mani proprie del destinatario, l'ufficiale giudiziario o la polizia giudiziaria consegnano la copia dell'atto da notificare, fatta eccezione per il caso di notificazione al difensore o al domiciliatario, dopo averla inserita in busta che provvedono a sigillare trascrivendovi il numero cronologico della notificazione e dandone atto nella relazione in calce all'originale e alla copia dell'atto.";

b) dopo il comma 5 è aggiunto il seguente: "5-*bis*. Le comunicazioni, gli avvisi ed ogni altro biglietto o invito consegnati non in busta chiusa a persona diversa dal destinatario recano le indicazioni strettamente necessarie.".

14. All'articolo 157, comma 6, del codice di procedura penale le parole: "è scritta all'esterno del plico stesso" sono sostituite dalle seguenti: "è effettuata nei modi previsti dall'articolo 148, comma 3".

15. All'art. 80 delle disposizioni di attuazione del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, il comma 1 è sostituito dal seguente:

"1. Se la copia del decreto di perquisizione locale è consegnata al portiere o a chi ne fa le veci, si applica la disposizione di cui all'articolo 148, comma 3, del codice.".

16. Alla legge 20 novembre 1982, n. 890, sono apportate le seguenti modificazioni:
a) all'articolo 2, primo comma, è aggiunto, in fine, il seguente periodo: "Sulle buste non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto.";
b) all'articolo 8, secondo comma, secondo periodo, dopo le parole: "L'agente postale rilascia avviso" sono inserite le seguenti: ", in busta chiusa, del deposito".

Art. 175. Forze di polizia

1. Il trattamento effettuato per il conferimento delle notizie ed informazioni acquisite nel corso di attività amministrative ai sensi dell'articolo 21, comma 1, della legge 26 marzo 2001, n. 128, e per le connessioni di cui al comma 3 del medesimo articolo è oggetto di comunicazione al Garante ai sensi dell'articolo 39, commi 2 e 3.

2. I dati personali trattati dalle forze di polizia, dagli organi di pubblica sicurezza e dagli altri soggetti di cui all'articolo 53, comma 1, senza l'ausilio di strumenti elettronici anteriormente alla data di entrata in vigore del presente codice, in sede di applicazione del presente codice possono essere ulteriormente trattati se ne è verificata l'esattezza, completezza ed aggiornamento ai sensi dell'articolo 11.

3. L'articolo 10 della legge 1 aprile 1981, n. 121, e successive modificazioni, è sostituito dal seguente:

"Art. 10 (Controlli)

1. Il controllo sul Centro elaborazione dati è esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.
2. I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità precedente ne dà notizia al Garante per la protezione dei dati personali.
3. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera *a)* del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intellegibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.
4. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali.
5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi.".

Art. 176. Soggetti pubblici

1. Nell'articolo 24, comma 3, della legge 7 agosto 1990, n. 241, dopo le parole: "mediante strumenti informatici" sono inserite le seguenti: ", fuori dei casi di accesso a dati personali da parte della persona cui i dati si riferiscono,".

2. Nell'articolo 2 del decreto legislativo 30 marzo 2001, n. 165, in materia di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, dopo il comma 1 è inserito il

seguente: "1-*bis*. I criteri di organizzazione di cui al presente articolo sono attuati nel rispetto della disciplina in materia di trattamento dei dati personali.".

3. L'articolo 4, comma 1, del decreto legislativo 12 febbraio1993, n. 39, e successive modificazioni, è sostituito dal seguente: "1. È istituito il Centro nazionale per l'informatica nella pubblica amministrazione, che opera presso la Presidenza del Consiglio dei ministri per l'attuazione delle politiche del Ministro per l'innovazione e le tecnologie, con autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e con indipendenza di giudizio.".

4. Al Centro nazionale per l'informatica nella pubblica amministrazione continuano ad applicarsi l'articolo 6 del decreto legislativo 12 febbraio 1993, n. 39, nonché le vigenti modalità di finanziamento nell'ambito dello stato di previsione del Ministero dell'economia e delle finanze.

5. L'articolo 5, comma 1, del decreto legislativo n. 39 del 1993, e successive modificazioni, è sostituito dal seguente: "1. Il Centro nazionale propone al Presidente del Consiglio dei ministri l'adozione di regolamenti concernenti la sua organizzazione, il suo funzionamento, l'amministrazione del personale, l'ordinamento delle carriere, nonché la gestione delle spese nei limiti previsti dal presente decreto.".

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

Art. 177. Disciplina anagrafica dello stato civile e delle liste elettorali

1. Il comune può utilizzare gli elenchi di cui all'articolo 34, comma 1, del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, per esclusivo uso di pubblica utilità anche in caso di applicazione della disciplina in materia di comunicazione istituzionale.

2. Il comma 7 dell'articolo 28 della legge 4 maggio 1983, n. 184, e successive modificazioni, è sostituito dal seguente: "7. L'accesso alle informazioni non è consentito nei confronti della madre che abbia dichiarato alla nascita di non volere essere nominata ai sensi dell'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396.".

3. Il rilascio degli estratti degli atti dello stato civile di cui all'articolo 107 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396 è consentito solo ai soggetti cui l'atto si riferisce, oppure su motivata istanza comprovante l'interesse personale e concreto del richiedente a fini di tutela di una situazione giuridicamente rilevante, ovvero decorsi settanta anni dalla formazione dell'atto.

4. Nel primo comma dell'articolo 5 del decreto del Presidente della Repubblica 20 marzo 1967, n. 223, sono soppresse le lettere *d*) ed *e*).

5. Nell'articolo 51 del decreto del Presidente della Repubblica 20 marzo 1967, n. 223, il quinto comma è sostituto dal seguente: "Le liste elettorali possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso.".

Art. 178. Disposizioni in materia sanitaria

1. Nell'articolo 27, terzo e quinto comma, della legge 23 dicembre 1978, n. 833, in materia di libretto sanitario personale, dopo le parole: "il Consiglio sanitario nazionale" e prima della virgola sono inserite le seguenti: "e il Garante per la protezione dei dati personali".

2. All'articolo 5 della legge 5 giugno 1990, n. 135, in materia di AIDS e infezione da HIV, sono apportate le seguenti modifiche:

a) il comma 1 è sostituito dal seguente: "1. L'operatore sanitario e ogni altro soggetto che viene a conoscenza di un caso di AIDS, ovvero di un caso di infezione da HIV, anche non accompagnato da stato morboso, è tenuto a prestare la necessaria assistenza e ad adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della relativa dignità.";

b) nel comma 2, le parole: "decreto del Ministro della sanità" sono sostituite dalle

seguenti: "decreto del Ministro della salute, sentito il Garante per la protezione dei dati personali".

3. Nell'articolo 5, comma 3, del decreto legislativo 30 dicembre 1992, n. 539, e successive modificazioni, in materia di medicinali per uso umano, è inserito, infine, il seguente periodo: "Decorso tale periodo il farmacista distrugge le ricette con modalità atte ad escludere l'accesso di terzi ai dati in esse contenuti.".

4. All'articolo 2, comma 1, del decreto del Ministro della sanità in data 11 febbraio 1997, pubblicato sulla Gazzetta Ufficiale n. 72 del 27 marzo 1997, in materia di importazione di medicinali registrati all'estero, sono soppresse le lettere *f*) ed *h*).

5. Nel comma 1, primo periodo, dell'articolo 5-*bis* del decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94, le parole da: "riguarda anche" fino alla fine del periodo sono sostituite dalle seguenti: "è acquisito unitamente al consenso relativo al trattamento dei dati personali".

Art. 179. Altre modifiche

1. Nell'articolo 6 della legge 2 aprile 1958, n. 339, sono soppresse le parole: "; mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare" e: "garantire al lavoratore il rispetto della sua personalità e della sua libertà morale;".

2. Nell'articolo 38, primo comma, della legge 20 maggio 1970, n. 300, sono soppresse le parole: "4," e ",8".

3. Al comma 3 dell'articolo 12 del decreto legislativo 22 maggio 1999, n. 185, in materia di contratti a distanza, sono aggiunte infine le seguenti parole: ", ovvero, limitatamente alla violazione di cui all'articolo 10, al Garante per la protezione dei dati personali".

CAPO II - DISPOSIZIONI TRANSITORIE

Art. 180. Misure di sicurezza

1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 31 marzo 2006.

2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.

3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro il 30 giugno 2006.

Art. 181. Altre disposizioni transitorie

1. Per i trattamenti di dati personali iniziati prima del 1 gennaio 2004, in sede di prima applicazione del presente codice:

a) l'identificazione con atto di natura regolamentare dei tipi di dati e di operazioni ai sensi degli articoli 20, commi 2 e 3, e 21, comma 2, è effettuata, ove mancante, entro il *31 luglio 2006*(1);

b) la determinazione da rendere nota agli interessati ai sensi dell'articolo 26, commi 3, lettera *a*), e 4, lettera *a*), è adottata, ove mancante, entro il 30 giugno 2004;

c) le notificazioni previste dall'articolo 37 sono effettuate entro il 30 aprile 2004;

d) le comunicazioni previste dall'articolo 39 sono effettuate entro il 30 giugno 2004;

e) *[lettera abrogata]*

f) l'utilizzazione dei modelli di cui all'articolo 87, comma 2, è obbligatoria a decorrere dal 1 gennaio 2005.

(1) *Nota redazionale*: alla data di stampa del presente volume il testo risulta così modificato dal decreto-legge 12 maggio 2006, n. 173, ancora non convertito

2. Le disposizioni di cui all'articolo 21-*bis* del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, introdotto dall'articolo 9 del decreto legislativo 30 luglio 1999, n. 281, restano in vigore fino alla data di entrata in vigore del presente codice.

3. L'individuazione dei trattamenti e dei titolari di cui agli articoli 46 e 53, da riportare nell'allegato C), è effettuata in sede di prima applicazione del presente codice entro il 30 giugno 2004.

4. Il materiale informativo eventualmente trasferito al Garante ai sensi dell'articolo 43, comma 1, della legge 31 dicembre 1996, n. 675, utilizzato per le opportune verifiche, continua ad essere successivamente archiviato o distrutto in base alla normativa vigente.

5. L'omissione delle generalità e degli altri dati identificativi dell'interessato ai sensi dell'articolo 52, comma 4, è effettuata sulle sentenze o decisioni pronunciate o adottate prima dell'entrata in vigore del presente codice solo su diretta richiesta dell'interessato e limitatamente ai documenti pubblicati mediante rete di comunicazione elettronica o sui nuovi prodotti su supporto cartaceo o elettronico. I sistemi informativi utilizzati ai sensi dell'articolo 51, comma 1, sono adeguati alla medesima disposizione entro dodici mesi dalla data di entrata in vigore del presente codice.

6. Le confessioni religiose che, prima dell'adozione del presente codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'articolo 26, comma 3, lettera *a)*, possono proseguire l'attività di trattamento nel rispetto delle medesime.

6-*bis*. Fino alla data in cui divengono efficaci le misure e gli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, per la conservazione del traffico telefonico si osserva il termine di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171.

Art. 182. Ufficio del Garante

1. Al fine di assicurare la continuità delle attività istituzionali, in sede di prima applicazione del presente codice e comunque non oltre il 31 marzo 2004, il Garante:

a) può individuare i presupposti per l'inquadramento in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilità di organico, del personale appartenente ad amministrazioni pubbliche o ad enti pubblici in servizio presso l'Ufficio del Garante in posizione di fuori ruolo o equiparato alla data di pubblicazione del presente codice;

b) può prevedere riserve di posti nei concorsi pubblici, unicamente nel limite del trenta per cento delle disponibilità di organico, per il personale non di ruolo in servizio presso l'Ufficio del Garante che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

CAPO III - ABROGAZIONI

Art. 183. Norme abrogate

1. Dalla data di entrata in vigore del presente codice sono abrogati:

a) la legge 31 dicembre 1996, n. 675;
b) la legge 3 novembre 2000, n. 325;
c) il decreto legislativo 9 maggio 1997, n. 123;
d) il decreto legislativo 28 luglio 1997, n. 255;
e) l'articolo 1 del decreto legislativo 8 maggio 1998, n. 135;
f) il decreto legislativo 13 maggio 1998, n. 171;
g) il decreto legislativo 6 novembre 1998, n. 389;
h) il decreto legislativo 26 febbraio 1999, n. 51;
i) il decreto legislativo 11 maggio 1999, n. 135;
l) il decreto legislativo 30 luglio 1999, n. 281, ad eccezione degli articoli 8, comma 1, 11 e 12;
m) il decreto legislativo 30 luglio 1999, n. 282;
n) il decreto legislativo 28 dicembre 2001, n. 467;
o) il decreto del Presidente della Repubblica 28 luglio 1999, n. 318.

2. Dalla data di entrata in vigore del presente codice sono abrogati gli articoli 12, 13, 14, 15, 16, 17, 18, 19 e 20 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501.

3. Dalla data di entrata in vigore del presente codice sono o restano, altresì, abrogati:

a) l'art. 5, comma 9, del decreto del Ministro della sanità 18 maggio 2001, n. 279, in materia di malattie rare;
b) l'articolo 12 della legge 30 marzo 2001, n. 152;
c) l'articolo 4, comma 3, della legge 6 marzo 2001, n. 52, in materia di donatori midollo osseo;
d) l'articolo 16, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, in materia di certificati di assistenza al parto;
e) l'art. 2, comma 5, del decreto del Ministro della sanità 27 ottobre 2000, n. 380, in materia di flussi informativi sui dimessi dagli istituti di ricovero;
f) l'articolo 2, comma 5-*quater* 1, secondo e terzo periodo, del decreto-legge 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge 26 maggio 2000, n. 137, e successive modificazioni, in materia di banca dati sinistri in ambito assicurativo;
g) l'articolo 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;
h) l'articolo 330-*bis* del decreto legislativo 16 aprile 1994, n. 297, in materia di diffusione di dati relativi a studenti;
i) l'articolo 8, quarto comma, e l'articolo 9, quarto comma, della legge 1 aprile 1981, n. 121.

4. Dalla data in cui divengono efficaci le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 118, i termini di conservazione dei dati personali individuati ai sensi dell'articolo 119, eventualmente previsti da norme di legge o di regolamento, si osservano nella misura indicata dal medesimo codice.

CAPO IV - NORME FINALI

Art. 184. Attuazione di direttive europee

1. Le disposizioni del presente codice danno attuazione alla direttiva 96/45/Ce del Parlamento europeo e del Consiglio, del 24 ottobre 1995, e alla direttiva 2002/58/Ce del Parlamento europeo e del Consiglio, del 12 luglio 2002.

2. Quando leggi, regolamenti e altre disposizioni fanno riferimento a disposizioni comprese nella legge 31 dicembre 1996, n. 675, e in altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente codice secondo la tavola di corrispondenza riportata in allegato.

3. Restano ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

Art. 185. Allegazione dei codici di deontologia e di buona condotta

1. L'allegato A) riporta, oltre ai codici di cui all'articolo 12, commi 1 e 4, quelli promossi ai sensi degli articoli 25 e 31 della legge 31 dicembre 1996, n. 675, e già pubblicati nella Gazzetta Ufficiale della Repubblica italiana alla data di emanazione del presente codice.

Art. 186. Entrata in vigore

1. Le disposizioni di cui al presente codice entrano in vigore il 1 gennaio 2004, ad eccezione delle disposizioni di cui agli articoli 156, 176, commi 3, 4, 5 e 6, e 182, che entrano in vigore il giorno successivo alla data di pubblicazione del presente codice. Dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli articoli 149, comma 8, e 150, comma 2.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. É fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 30 giugno 2003

PAGINA BIANCA

TAVOLA DI CORRISPONDENZA DEI RIFERIMENTI PREVIGENTI

PAGINA BIANCA

Tavola di corrispondenza dei riferimenti previgenti al Codice in materia di protezione dei dati personali

Articolato del Codice	*Riferimento previgente*
Parte I - Disposizioni generali	
Titolo I - Principi generali	
Art. 1. Diritto alla protezione dei dati personali	—
Art. 2. Finalità	
comma 1	cfr. art. 1, direttiva 95/46/Ce del Parlamento europeo e del Consiglio
	art. 1, comma 1, legge 31 dicembre 1996, n. 675
comma 2	—
Art. 3. Principio di necessità del trattamento dei dati	
comma 1	—
Art. 4. Definizioni	
comma 1, lett. *a)*	cfr. art. 2, dir. 95/46/Ce
	art. 1, comma 2, lett. *b)*, l. n. 675/1996
lett. *b)*	art. 1, comma 2, lett. *c)*, l. n. 675/1996
lett. *c)*	art. 10, comma 5, d.lg. 30 luglio 1999, n. 281
lett. *d)*	cfr. art. 22, comma 1, l. n. 675/1996
lett. *e)*	cfr. art. 24, comma 1, l. n. 675/1996
lett. *f)*	art. 1, comma 2, lett. *d)*, l. n. 675/1996
lett. *g)*	art. 1, comma 2, lett. *e)*, l. n. 675/1996
lett. *h)*	cfr. art. 19, l. n. 675/1996
lett. *i)*	art. 1, comma 2, lett. *f)*, l. n. 675/1996
lett. *l)*	art. 1, comma 2, lett. *g)*, l. n. 675/1996
lett. *m)*	art. 1, comma 2, lett. *h)*, l. n. 675/1996
lett. *n)*	art. 1, comma 2, lett. *i)*, l. n. 675/1996
lett. o)	art. 1, comma 2, lett. *l)*, l. n. 675/1996
lett. *p)*	art. 1, comma 2, lett. *a)*, l. n. 675/1996
lett. *q)*	art. 1, comma 2, lett. *m)*, l. n. 675/1996
comma 2, lett. *a)*	cfr. art. 2, par. 2, lett. *d)*, direttiva 2002/58/Ce del Parlamento europeo e del Consiglio
lett. *b)*	cfr. art. 2, lett. *e)*, dir. 2002/58/Ce
lett. *c)*	cfr. art. 2, par. 1, lett. *a)*, direttiva 2002/21/Ce del Parlamento europeo e del Consiglio
lett. *d)*	cfr. art. 2, par. 1, lett. *d)*, dir. n. 2002/21/Ce
lett. *e)*	cfr. art. 2, par. 1, lett. *c)*, dir. n. 2002/21/Ce
lett. *f)*	cfr. art. 2, par. 1, lett. *k)*, dir. n. 2002/21/Ce
lett. *g)*	cfr. art. 2, par. 2, lett. *a)*, dir. n. 2002/58/Ce
lett. *h)*	cfr. art. 2, par. 2, lett. *b)*, dir. n. 2002/58/Ce
lett. *i)*	cfr. art. 2, par. 2, lett. *c)*, dir. n. 2002/58/Ce
lett. *l)*	cfr. art. 2, par. 2, lett. *g)*, dir. n. 2002/58/Ce
lett. *m)*	cfr. art. 2, par. 2, lett. *h)*, dir. n. 2002/58/Ce
comma 3, lett. *a)*	art. 1, comma 1, lett. *a)*, d.P.R. n. 28 luglio 1999, n. 318
lett. *b)*	art. 1, lett. *b)*, d.P.R. n. 318/1999
lett. *c)*	—
lett. *d)*	—
lett. *e)*	—
lett. *f)*	—

lett. *g)*	—
comma 4, lett. *a)*	art. 1, comma 2, lett. *a)*, decreto legislativo 30 luglio 1999, n. 281
lett. *b)*	art. 1, comma 2, lett. *c)*, d.lg. n. 281/1999
lett. *c)*	art. 1, comma 2, lett. *b)*, d.lg. n. 281/1999

Art. 5. Oggetto ed ambito di applicazione

comma 1	cfr. art. 4, dir. 95/46/Ce
	artt. 2, comma 1, e 6, comma 1, l. n. 675/1996
comma 2	art. 2, commi 1-*bis*, e 1-*ter*, l. n. 675/1996
comma 3	cfr. art. 3, par. 2, (secondo periodo), dir. 95/46/Ce
	art. 3, l. n. 675/1996

Art. 6. Disciplina del trattamento —

TITOLO II - DIRITTI DELL'INTERESSATO

Art. 7. Diritto di accesso ai dati personalied altri diritti

comma 1	cfr. art. 12, dir. 95/46/Ce
	art. 13, comma 1, lett. *c)*, punto 1, -prima parte-, l. n. 675/1996
comma 2	art. 13, comma 1, lett. *b)* e *c)*, punto 1, -seconda parte-, l. n. 675/1996
comma 3	art. 13, comma 1, lett. *c)*, punti 2, 3 e 4, l. n. 675/1996
comma 4	art. 13, comma 1, lett. *d)* ed *e)*, l. n. 675/1996

Art. 8. Esercizio dei diritti

comma 1	cfr. art. 13, dir. 95/46/Ce
	art. 17, comma 1, d.P.R. 31 marzo 1998, n. 501
comma 2	art. 14, comma 1, lett. *a)*, *b)*, *c)*, *d')*, *e)* ed e-*bis*), l. n. 675/1996
comma 3	art. 14, comma 2, l. n. 675/1996
comma 4	—

Art. 9. Modalità di esercizio

comma 1	art. 17, comma 3, d.P.R. n. 501/1998
comma 2	art. 13, comma 4, l. n. 675/1996;
	art. 17, comma 4, d.P.R. n. 501/1998
comma 3	art. 13, comma 3, l. n. 675/1996
comma 4	art. 17, comma 2, d.P.R. n. 501/1998
comma 5	art. 13, comma 1, lett. *c)*, punto 1, (secondo periodo), l. n. 675/1996

Art. 10. Riscontro all'interessato

comma 1	art. 17, comma 9, d.P.R. n. 501/1998
comma 2	art. 17, comma 6, d.P.R. n. 501/1998
comma 3	art. 17, comma 5, d.P.R. n. 501/1998
comma 4	—
comma 5	—
comma 6	—
comma 7	art. 13, comma 2, l. n. 675/1996;
	art. 17, comma 7, d.P.R. n. 501/1998
comma 8	art. 17, comma 7, d.P.R. n. 501/1998
comma 9	art. 17, comma 8, d.P.R. n. 501/1998

TITOLO III - REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

CAPO I - REGOLE PER TUTTI I TRATTAMENTI

Art. 11. Modalità del trattamento e requisiti dei dati

comma 1	cfr. art. 6, dir. 95/46/Ce
	art. 9, comma 1, l. n. 675/1996
comma 2	—

Art. 12. Codici di deontologia e di buona condotta

comma 1	cfr. art. 27, dir. 95/46/Ce
	art. 31, comma 1, lett. *h)*, l. n. 675/1996

comma 2	art. 20, comma 4, decreto legislativo 28 dicembre 2001, n. 467
comma 3	art. 20, comma 3, d.lg. n. 467/2001
comma 4	—

Art. 13. Informativa

comma 1	cfr. art. 10, dir. 95/46/Ce
	art. 10, comma 1, l. n. 675/1996
comma 2	art. 10, comma 2, l. n. 675/1996
comma 3	—
comma 4	art. 10, comma 3, l. n. 675/1996
comma 5	art. 10, comma 4, l. n. 675/1996

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

comma 1	cfr. art. 15, dir. 95/46/Ce
	art. 17, comma 1, l. n. 675/1996
comma 2	art. 17, comma 2, l. n. 675/1996

Art. 15. Danni cagionati per effetto del trattamento

comma 1	cfr. art. 23, dir. 95/46/Ce
	art. 18, l. n. 675/1996
comma 2	art. 29, comma 9, l. n. 675/1996

Art. 16. Cessazione del trattamento

comma 1	cfr. art. 19, par. 2, dir. 95/46/Ce
	art. 16, comma 2, l. n. 675/1996
comma 2	art. 16, comma 3, l. n. 675/1996

Art. 17. Trattamento che presenta rischi specifici

comma 1	cfr. art. 20, dir. 95/46/Ce
	art. 24-*bis*, comma 1, l. n. 675/1996
comma 2	art. 24-*bis*, comma 2, l. n. 675/1996

CAPO II - REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

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

comma 1	—
comma 2	cfr. art. 27, comma 1, l. n. 675/1996
comma 3	cfr. art. 27, comma 1, l. n. 675/1996
comma 4	—
comma 5	—

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

comma 1	art. 7, par. 1, lett. *e*), dir. 95/46/Ce;
	art. 27, comma 1, l. n. 675/1996
comma 2	art. 27, comma 2, l. n. 675/1996
comma 3	art. 27, comma 3, l. n. 675/1996

Art. 20. Principi applicabili al trattamento di dati sensibili

comma 1	cfr. art. 8, dir. 95/46/Ce
	art. 22, comma 3, (primo periodo), l. n. 675/1996
comma 2	art. 22, comma 3-*bis*, l. n. 675/1996;
	art. 5, comma 5, decreto legislativo 11 maggio 1999, n. 135
comma 3	art. 22, comma 3, (secondo periodo), l. n. 675/1996
comma 4	art. 22, comma 3-*bis*, l. n. 675/1996

Art. 21. Principi applicabili al trattamento di dati giudiziari

comma 1	cfr. art. 8, par. 5, dir. 95/46/Ce
	art. 24, comma 1, l. n. 675/1996
comma 2	art. 5, comma 5-*bis*, d.lg. n. 135/1999

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

comma 1	—
comma 2	art. 2, comma 2, d.lg. n. 135/1999
comma 3	art. 3, comma 1, d.lg. n. 135/1999
comma 4	art. 3, comma 2, d.lg. n. 135/1999
comma 5	art. 3, comma 3, d.lg. n. 135/1999
comma 6	art. 3, comma 4, d.lg. n. 135/1999
comma 7	art. 3, comma 5, d.lg. n. 135/1999
comma 8	art. 23, comma 4, l. n. 675/1996
comma 9	art. 4, comma 1, d.lg. n. 135/1999
comma 10	art. 4, comma 2, d.lg. n. 135/1999
	art. 3, comma 6, d.lg. n. 135/1999
comma 11	art. 4, comma 3, d.lg. n. 135/1999
comma 12	art. 1, comma 2, lett. *c*), d.lg. n. 135/1999

CAPO III - REGOLE ULTERIORI PER I PRIVATI ED ENTI PUBBLICI ECONOMICI

Art. 23. Consenso

comma 1	cfr. art. 7, par. 1, lett. *a*), dir. 95/46/Ce
	art. 11, comma 1 e 20, comma 1, lett. *a*), l. n. 675/1996
comma 2	art. 11, comma 2, l. n. 675/1996
comma 3	art. 11, comma 3, l. n. 675/1996
comma 4	cfr. art. 22, comma 1, l. n. 675/1996

Art. 24. Casi nei quali può essere effettuato il trattamento senza il consenso

comma 1, lett. *a*)	cfr. art. 7, dir. 95/46/Ce
	artt. 12, comma 1, lett. *a*) e 20, comma 1, lett. *c*), l. n. 675/1996
lett. *b*)	artt. 12, comma 1, lett. *b*) e 20, comma 1, lett. a-*bis*), l. n. 675/1996
lett. *c*)	artt. 12, comma 1, lett. *c*) e 20, comma 1, lett. *b*), l. n. 675/1996
lett. *d*)	artt. 12, comma 1, lett. *f*) e 20, comma 1, lett. *e*), l. n. 675/1996
lett. *e*)	art. 7, par. 1, lett. *d*), dir. 95/46/Ce
	artt. 12, comma 1, lett. *g*) e 20 comma 1, lett. *f*), l. n. 675/1996
lett. *f*)	artt. 12, comma 1, lett. *h*) e 20, comma 1, lett. *g*), l. n. 675/1996
lett. *g*)	artt. 12, comma 1, lett. h-*bis*) e 20, comma 1, lett. *h*) ed h-*bis*), l. n. 675/1996
lett. *h*)	—
lett. *i*)	artt. 12, comma 1, lett. *d*) e 21, comma 4, lett. *a*), l. n. 675/1996
	art. 7, comma 4, d.lgs. n. 281/1999

Art. 25. Divieti di comunicazione e diffusione

comma 1	art. 21, commi 1 e 2, l. n. 675/1996
comma 2	art. 21, comma 4, lett. *b*), l. n. 675/1996

Art. 26. Garanzie per i dati sensibili

comma 1	cfr. art. 8, dir. 95/46/Ce
	art. 22, comma 1, l. n. 675/1996
comma 2	art. 22, comma 2, l. n. 675/1996
comma 3, lett. *a*)	art. 22, comma 1-*bis*, l. n. 675/1996
comma 3, lett. *b*)	art. 22, comma 1-*ter*, l. n. 675/1996
comma 4	art. 22, comma 4, l. n. 675/1996
comma 5	art. 23, comma 4, l. n. 675/1996

Art. 27. Garanzie per i dati giudiziari

comma 1	cfr. art. 8, par. 5, dir. 95/46/Ce
	art. 24, comma 1, l. n. 675/1996

TITOLO IV - I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art. 28. Titolare del trattamento

comma 1	—

Art. 29. Responsabile del trattamento

comma 1	cfr. art. 16, dir. 95/46/Ce
	art. 8, comma 1, l. n. 675/1996
comma 2	art. 8, comma 1, l. n. 675/1996
comma 3	art. 8, comma 3, l. n. 675/1996
comma 4	art. 8, comma 4, l. n. 675/1996
comma 5	art. 8, comma 2, l. n. 675/1996

Art. 30. Incaricati del trattamento

comma 1	cfr. art. 17, par. 3, dir. 95/46/Ce
	artt. 8, comma 5, e 19, l. n. 675/1996
comma 2	art. 19, l. n. 675/1996

TITOLO V - SICUREZZA DEI DATI E DEI SISTEMI

CAPO I - MISURE DI SICUREZZA — cfr. art. 17, dir. 95/46/Ce

Art. 31. Obblighi di sicurezza — art. 15, comma 1, l. n. 675/1996

Art. 32. Particolari titolari

comma 1	art. 2, comma 1, decreto legislativo 13 maggio 1998, n. 171
comma 2	art. 2, comma 2, d.lg. 171/1998
comma 3	art. 2, comma 3, d.lg. 171/1998

CAPO II - MISURE MINIME

Art. 33. Misure minime — cfr. art. 15, comma 2, l. n. 675/1996

Art. 34. Trattamenti con strumenti elettronici —

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

Art. 36. Adeguamento — cfr. art. 15, comma 3, l. n. 675/1996

TITOLO VI - ADEMPIMENTI

Art. 37. Notificazione del trattamento

comma 1	art. 18, dir. 95/46/Ce;
	cfr. art. 7, comma 1, l. n. 675/1996
comma 2	—
comma 3	art. 28, comma 7, (secondo periodo), l. n. 675/1996
comma 4	art. 13, commi 1, 2, 3, 4, d.P.R. n. 501/1998

Art. 38. Modalità di notificazione

comma 1	art. 19, dir. 95/46/Ce
	art. 7, comma 2, (primo periodo), l. n. 675/1996
comma 2	art. 12, comma 1, (primo periodo), d.P.R. n. 501/1998
comma 3	art. 12, comma 1, (secondo periodo), d.P.R. n. 501/1998
comma 4	art. 7, comma 2, (secondo periodo) e art. 16, comma 1, l. n. 675/1996
comma 5	art. 12, comma 6, d.P.R. n. 501/1998
comma 6	—

Art. 39. Obblighi di comunicazione

comma 1, lett. *a*)	art. 7, par. 1, lett. *e*), dir. 95/46/Ce
	art. 27, comma 2, l. n. 675/1996
lett. *b*)	—
comma 2	—
comma 3	—

Art. 40. Autorizzazioni generali

comma 1	art. 41, comma 7, l. n. 675/1996;
	art. 14, comma 1, d.P.R. n. 501/1998

Art. 41. Richieste di autorizzazione	
comma 1	—
comma 2	art. 14, comma 2, d.P.R. n. 501/1998
comma 3	art. 14, comma 3, d.P.R. n. 501/1998
comma 4	art. 14, comma 4, d.P.R. n. 501/1998
comma 5	art. 14, comma 5, d.P.R. n. 501/1998
TITOLO VII - TRASFERIMENTO DEI DATI ALL'ESTERO	cfr. artt. 25 e 26, dir. 95/46/Ce
Art. 42. Trasferimenti all'interno dell'Unione europea	
comma 1	—
Art. 43. Trasferimenti consentiti in Paesi terzi	
alinea del comma 1	art. 28, comma 1, l. n. 675/1996
comma 1	artt. 28, comma 4, eccetto la lett. *g*), e 26, comma 2, l. n. 675/1996 art. 7, comma 4, d.lg n. 281/1999
Art. 44. Altri trasferimenti consentiti	art. 28, comma 4, lett. *g*), l. n. 675/1996
Art. 45. Trasferimenti vietati	art. 28, comma 3, l. n. 675/1996
PARTE II - DISPOSIZIONI RELATIVE A SPECIFICI SETTORI	
TITOLO I - TRATTAMENTI IN AMBITO GIUDIZIARIO	
CAPO I - PROFILI GENERALI	cfr. art. 3, dir. 95/46/Ce
Art. 46. Titolari dei trattamenti	—
Art. 47. Trattamenti per ragioni di giustizia	art. 3, par. 2, (primo periodo), dir. 95/46/Ce art. 4, comma 1, lett. *c*) e *d*) e comma 2, l. n. 675/1996
Art. 48. Banche di dati di uffici giudiziari	—
Art. 49. Disposizioni di attuazione	—
CAPO II - MINORI	
Art. 50. Notizie o immagini relative ai minori	—
CAPO III - INFORMATICA GIURIDICA	
Art. 51. Principi generali	—
Art. 52. Dati identificativi degli interessati	—
TITOLO II - TRATTAMENTI DA PARTE DI FORZE DI POLIZIA	cfr. art. 3, dir. 95/46/Ce
CAPO I - PROFILI GENERALI	
Art. 53. Ambito applicativo e titolari dei trattamenti	art. 3, par. 2, (primo periodo), dir. 95/46/Ce; art. 4, comma 1, lett. *a*) ed *e*) e comma 2, l. n. 675/1996
Art. 54. Modalità di trattamento e flussi di dati	—
Art. 55. Particolari tecnologie	—
Art. 56. Tutela dell'interessato	—
Art. 57. Disposizioni di attuazione	—
TITOLO III - DIFESA E SICUREZZA DELLO STATO	
CAPO I - PROFILI GENERALI	art. 3, dir. 95/46/Ce
Art. 58. Disposizioni applicabili	
comma 1	art. 4, commi 1, lett. *b*) e 2, l. n. 675/1996

comma 2	art. 4, commi 1, lett. *e*) e 2, l. n. 675/1996
comma 3	art. 15, comma 4, l. n. 675/1996
comma 4	—

TITOLO IV - TRATTAMENTI IN AMBITO PUBBLICO

CAPO I - ACCESSO A DOCUMENTI AMMINISTRATIVI

Art. 59. Accesso a documenti amministrativi	art. 43, comma 2, l. n. 675/1996; art. 16, comma 1, lett. *c*), d.lg. n. 135/1999
Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale	art. 16, comma 2, d.lg. n. 135/1999

CAPO II - REGISTRI PUBBLICI E ALBI PROFESSIONALI

Art. 61. Utilizzazione di dati pubblici	
comma 1	art. 20, comma 1, lett. *f*), d.lg. n. 467/2001
comma 2	—
comma 3	—
comma 4	—

CAPO III - STATO CIVILE, ANAGRAFI E LISTE ELETTORALI

Art. 62. Dati sensibili e giudiziari	art. 6, d.lg. n. 135/1999
Art. 63. Consultazione di atti	—

CAPO IV - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 64. Cittadinanza, immigrazione e condizione dello straniero	
comma 1	art. 7, comma 1, d.lg. n. 135/1999
comma 2	art. 7, comma 3, d.lg. n. 135/1999
comma 3	art. 7, comma 2, d.lg. n. 135/1999
Art. 65. Diritti politici e pubblicità dell'attività di organi	
comma 1	art. 8, commi 1 e 2, d.lg. n. 135/1999
comma 2	art. 8, comma 3, d.lg. n. 135/1999
comma 3	art. 8, comma 4, d.lg. n. 135/1999
comma 4	art. 8, comma 5, d.lg. n. 135/1999
comma 5	art. 8, comma 6, d.lg. n. 135/1999
Art. 66. Materia tributaria e doganale	
comma 1	art. 10, comma 1, d.lg. n. 135/1999
comma 2	art. 10, comma 2, d.lg. n. 135/1999
Art. 67. Attività di controllo e ispettive	
comma 1, lett. *a*)	art. 11, comma 1, d.lg. n. 135/1999
lett. *b*)	art. 11, comma 3, d.lg. n. 135/1999
Art. 68. Benefici economici ed abilitazioni	
comma 1	art. 13, comma 1, d.lg. n. 135/1999
comma 2	art. 13, comma 2, d.lg. n. 135/1999
comma 3	art. 13, comma 3, d.lg. n. 135/1999
Art. 69. Onorificenze, ricompense e riconoscimenti	art. 14, d.lg. n. 135/1999
Art. 70. Volontariato e obiezione di coscienza	
comma 1	art. 15, comma 1, d.lg. n. 135/1999
comma 2	art. 15, comma 2, d.lg. n. 135/1999
Art. 71. Attività sanzionatorie e di tutela	
comma 1	art. 16, comma 1, lett. *a*) e *b*), d.lg. n. 135/1999
comma 2	art. 16, comma 2, d.lg. n. 135/1999

Art. 72. Rapporti con enti di culto art. 21, d.lg. n. 135/1999

Art. 73. Altre finalità in ambito amministrativo e sociale Provv. Garante n. 1/P/2000 del 30 dicembre 1999 - 13 gennaio 2000

CAPO V - PARTICOLARI CONTRASSEGNI

Art. 74. Contrassegni su veicoli e accessi a centri storici —

TITOLO V - TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

CAPO I - PRINCIPI GENERALI cfr. art. 8, dir. 95/46/Ce

Art. 75. Ambito applicativo art. 1, decreto legislativo 30 luglio 1999, n. 282

Art. 76. Esercenti professioni sanitarie e organismi sanitari pubblici

comma 1 art. 23, comma 1, l. n. 675/1996
comma 2 —
comma 3 art. 23, comma 3, (primo periodo), l. n. 675/1996

CAPO II - MODALITÀ SEMPLIFICATE PER INFORMATIVA E CONSENSO

Art. 77. Casi di semplificazione —

Art. 78. Informativa del medico di medicina generale o del pediatra —

Art. 79. Informativa da parte di organismi sanitari —

Art. 80. Informativa da parte di altri soggetti pubblici —

Art. 81. Prestazione del consenso —

Art. 82. Emergenze e tutela della salute e dell'incolumità fisica

comma 1 —
comma 2 art. 23, comma 1-*quater*, l. n. 675/1996
comma 3 —
comma 4 —

Art. 83. Altre misure per il rispetto dei diritti degli interessati —

Art. 84. Comunicazione di dati all'interessato

comma 1 art. 23, comma 2, l. n. 675/1996
comma 2 —

CAPO III - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 85. Compiti del Servizio sanitario nazionale

comma 1 art. 17, comma 1, d.lg. n. 135/1999
comma 2 —
comma 3 —
comma 4 art. 17, comma 2, d.lg. n. 135/1999

Art. 86. Altre finalità di rilevante interesse pubblico

comma 1
lett. *a*) art. 18, d.lg. n. 135/1999
lett. *b*) art. 19, d.lg. n. 135/1999
lett. *c*) art. 20, d.lg. n. 135/1999

CAPO IV - PRESCRIZIONI MEDICHE

Art. 87. Medicinali a carico del Servizio sanitario nazionale art. 4, comma 2, d.lg. n. 282/1999

Art. 88. Medicinali non a carico del Servizio sanitario nazionale art. 4, comma 1, d.lg. n. 282/1999

Art. 89. Casi particolari
comma 1 —
comma 2 art. 4, comma 4, d.lg. n. 282/1999

CAPO V - DATI GENETICI
Art. 90. Trattamento dei dati genetici e donatori di midollo osseo
comma 1 art. 17, comma 5, d.lg. n. 135/1999
comma 2 —
comma 3 art. 4, comma 3, legge 6 marzo 2001, n. 52

CAPO VI - DISPOSIZIONI VARIE
Art. 91. Dati trattati mediante carte —

Art. 92. Cartelle cliniche —

Art. 93. Certificato di assistenza al parto
comma 1 art. 16, comma 2, d.P.R. 28 dicembre 2000, n. 445
comma 2 —
comma 3 —

Art. 94. Banche di dati, registri e schedari in ambito sanitari —

TITOLO VI - ISTRUZIONE
CAPO I - PROFILI GENERALI
Art. 95. Dati sensibili e giudiziari art. 12, d.lg. n. 135/1999

Art. 96. Trattamento di dati relativi a studenti
comma 1 art. 330-*bis*, (primo e secondo periodo), decreto legislativo 16 aprile 1994, n. 297
comma 2 art. 330-*bis*, (terzo periodo), d.lg. n. 297/1994

TITOLO VII - TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI
CAPO I - PROFILI GENERALI cfr. artt. 6, 11, par. 2, 13, par. 2, dir. 95/46/Ce
Art. 97. Ambito applicativo —

Art. 98. Finalità di rilevante interesse pubblico artt. 22 e 23, d.lg. n. 135/1999

Art. 99. Compatibilità tra scopi e durata del trattamento
comma 1 art. 9, comma 1-*bis*, l. n. 675/1996
comma 2 art. 9, comma 1-*bis*, l. n. 675/1996
comma 3 art. 16, comma 2, lett. c-*bis*), l. n. 675/1996

Art. 100. Dati relativi ad attività di studio e di ricerca art. 6, comma 4, decreto legislativo 5 giugno 1998, n. 204

CAPO II - TRATTAMENTO PER SCOPI STORICI
Art. 101. Modalità di trattamento
comma 1 art. 7, comma 1, d.lg. n. 281/1999
comma 2 art. 7, comma 2, d.lg. n. 281/1999
comma 3 art. 7, comma 3, d.lg. n. 281/1999

Art. 102. Codice di deontologia e di buona condotta
comma 1 art. 6, comma 1, d.lg. n. 281/1999
comma 2 art. 7, comma 5, d.lg. n. 281/1999

Art. 103. Consultazione di documenti conservati in archivi —

CAPO III - TRATTAMENTO PER SCOPI STATISTICI O SCIENTIFICI

Art. 104. Ambito applicativo e dati identificativi per scopi statistici o scientifici

comma 1	art. 10, comma 1, d.lg. n. 281/1999
comma 2	art. 10, comma 5, d.lg. n. 281/1999

Art. 105. Modalità di trattamento

comma 1	art. 10, comma 3, d.lg. n. 281/1999
comma 2	art. 10, comma 2, d.lg. n. 281/1999
comma 3	—
comma 4	—

Art. 106. Codici di deontologia e di buona condotta

comma 1	art. 6, comma 1, d.lg. n. 281/1999
comma 2	art. 10, comma 6, d.lg. n. 281/1999

Art. 107. Trattamento di dati sensibili

comma 1	art. 10, comma 4, d.lg. n. 281/1999

Art. 108. Sistema statistico nazionale —

Art. 109. Dati statistici relativi all'evento della nascita —

Art. 110. Ricerca medica, biomedica ed epidemiologica

comma 1	art. 5, comma 1, d.lg. n. 282/1999
comma 2	art. 5, comma 2, d.lg. n. 282/1999

TITOLO VIII - LAVORO E PREVIDENZA SOCIALE

CAPO I - PROFILI GENERALI

Art. 111. Codice di deontologia e di buona condotta

comma 1	art. 20, comma 2, lett. *b*), d.lg. n. 467/2001

Art. 112. Finalità di rilevante interesse pubblico

comma 1	art. 9, comma 1, d.lg. n. 135/1999
comma 2	art. 9, comma 2, d.lg. n. 135/1999
comma 3	art. 9, comma 4, d.lg. n. 135/1999

CAPO II - ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO

Art. 113. Raccolta di dati e pertinenza cfr. art. 8, legge 20 maggio 1970, n. 300

CAPO III - DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO

Art. 114. Controllo a distanza cfr. art. 4, comma 1, l. n. 300/1970

Art. 115. Telelavoro e lavoro a domicilio

comma 1 e 2	art. 6, legge 2 aprile 1958, n. 339

CAPO IV - ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE

Art. 116. Conoscibilità di dati su mandato dell'interessato

commi 1 e 2	art. 12, legge 30 marzo 2001, n. 152

TITOLO IX - SISTEMA BANCARIO, FINANZIARIO ED ASSICURATIVO

CAPO I - SISTEMI INFORMATIVI

Art. 117. Affidabilità e puntualità nei pagamenti

comma 1	art. 20, comma 1, lett. *e*), d.lg. n. 467/2001

Art. 118. Informazioni commerciali

comma 1	art. 20, comma 1, lett. *d*), d.lg. n. 467/2001

Art. 119. Dati relativi al comportamento debitorio —

Art. 120. Sinistri art. 2, comma 5-*quater* 1, decreto-legge 28 marzo 2000, n. 70, nel testo modificato dalla legge 26 maggio 2000, n. 137 di conversione

TITOLO X - COMUNICAZIONI ELETTRONICHE

CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121. Servizi interessati	cfr. art. 3, dir. 2002/58/Ce
Art. 122. Informazioni raccolte nei riguardi dell'abbonato e dell'utente	cfr. art. 5, par. 3, dir. 2002/58/Ce
Art. 123. Dati relativi al traffico	
comma 1	cfr. art. 6, dir. 2002/58/Ce
	art. 4, comma 1, d.lg. n. 171/1998
comma 2	art. 4, comma 2, d.lg. n. 171/1998
comma 3	art. 4, comma 3, d.lg. n. 171/1998
comma 4	—
comma 5	art. 4, comma 4, d.lg. n. 171/1998
comma 6	art. 4, comma 5, d.lg. n. 171/1998
Art. 124. Fatturazione dettagliata	
comma 1	cfr. art. 7, dir. 2002/58/Ce
	art. 5, comma 3, (primo periodo), d.lg. n. 171/1998
comma 2	art. 5, comma 1, d.lg. n. 171/1998
comma 3	art. 5, comma 2, d.lg. n. 171/1998
comma 4	art. 5, comma 3, (secondo periodo), d.lg. n. 171/1998
comma 5	—
Art. 125. Identificazione della linea	
comma 1	cfr. art. 8, dir. 2002/58/Ce
	art. 6, comma 1, d.lg. n. 171/1998
comma 2	art. 6, comma 2, d.lg. n. 171/1998
comma 3	art. 6, comma 3, d.lg. n. 171/1998
comma 4	art. 6, comma 4, d.lg. n. 171/1998
comma 5	art. 6, comma 5, d.lg. n. 171/1998
comma 6	art. 6, comma 6, d.lg. n. 171/1998
Art. 126. Dati relativi all'ubicazione	cfr. art. 9, dir. 2002/58/Ce
Art. 127. Chiamate di disturbo e di emergenza	
comma 1	cfr. art. 10, dir. 2002/58/Ce
	art. 7, comma 1, d.lg. n. 171/1998
comma 2	art. 7, comma 2, d.lg. n. 171/1998
comma 3	—
comma 4	art. 7, comma 2-*bis*, d.lg. n. 171/1998
Art. 128. Trasferimento automatico della chiamata	
comma 1	cfr. art. 11, dir. 2002/58/Ce; art. 8, comma 1, d.lg. n. 171/1998
Art. 129. Elenchi di abbonati	cfr. art. 12, dir. 2002/58/Ce
	art. 9, d.lg. n. 171/1998
Art. 130. Comunicazioni indesiderate	cfr. art. 13, dir. 2002/58/Ce; art. 10, d.lg. n. 171/1998
Art. 131. Informazioni ad abbonati e utenti	art. 3, d.lg. n. 171/1998
Art. 132. Conservazione di dati di traffico per altre finalità	cfr. art. 15, dir. 2002/58/Ce

CAPO II - INTERNET E RETI TELEMATICHE

Art. 133. Codice di deontologia e di buona condotta	art. 20, comma 2, lett. *a*), d.lg. n. 467/2001

CAPO III - VIDEOSORVEGLIANZA

Art. 134. Codice di deontologia e di buona condotta	art. 20, comma 2, lett. *g*), d.lg. n. 467/2001

TITOLO XI - LIBERE PROFESSIONI E INVESTIGAZIONE PRIVATA
CAPO I - PROFILI GENERALI

Art. 135. Codice di deontologia e di buona condotta — art. 22, comma 4, lett. *c*), (secondo periodo), l. n. 675/1996

TITOLO XII - GIORNALISMO ED ESPRESSIONE LETTERARIA ED ARTISTICA
CAPO I - PROFILI GENERALI — cfr. art. 9, dir. 95/46/Ce

Art. 136. Finalità giornalistiche ed altre manifestazioni del pensiero

comma 1, lett. *a*)	art. 25, comma 1, l. n. 675/1996
lett. *b*) e *c*)	art. 25, comma 4-*bis*, l. n. 675/1996

Art. 137. Disposizioni applicabili

comma 1, lett. *a*)	art. 25, comma 1, l. n. 675/1996
lett. *b*)	art. 25, comma 1, l. n. 675/1996
lett. *c*)	art. 28, comma 6, l. n. 675/1996
comma 2	art. 12, comma 1, lett. *e*), l. n. 675/1996; art. 25, comma 1, l. n. 675/1996
comma 3	art. 20, comma 1, lett. *d*), e art. 25, comma 1, l. n. 675/1996

Art. 138. Segreto professionale — art. 13, comma 5, l. n. 675/1996

CAPO II - CODICE DI DEONTOLOGIA

Art. 139. Codice di deontologia relativo ad attività giornalistiche — art. 25, commi 2, 3 e 4, l. n. 675/1996

TITOLO XIII - MARKETING DIRETTO
CAPO I - PROFILI GENERALI

Art. 140. Codice di deontologia e di buona condotta — art. 20, comma 2, lett. *c*), d.lg. n. 467/2001

PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

TITOLO I - TUTELA AMMINISTRATIVA E GIURISDIZIONALE
CAPO I - TUTELA DINANZI AL GARANTE

Sezione I - Principi generali — cfr. art. 22, dir. 95/46/Ce

Art. 141. Forme di tutela — —

Sezione II - Tutela amministrativa

Art. 142. Proposizione dei reclami — —

Art. 143. Procedimento per i reclami — art. 21, comma 3, l. n. 675/1996; art. 31, comma 1, lett. *c*) e *l*), l. n. 675/1996

Art. 144. Segnalazioni — —

Sezione III - Tutela alternativa a quella giurisdizionale

Art. 145. Ricorsi

comma 1	art. 29, comma 1, (primo periodo), l. n. 675/1996
comma 2	art. 29, comma 1, (secondo periodo), l. n. 675/1996
comma 3	art. 29, comma 2, (secondo periodo), l. n. 675/1996

Art. 146. Interpello preventivo

comma 1	art. 29, comma 2, (primo periodo), l. n. 675/1996
comma 2	art. 29, comma 2, (primo periodo), l. n. 675/1996
comma 3	—

Art. 147. Presentazione del ricorso

comma 1, lett. *a*)	art. 18, comma 1, lett. *a*), d.P.R. n. 501/1998
lett. *b*)	art. 18, comma 1, lett. *c*), -seconda parte-, d.P.R. n. 501/1998
lett. *c*)	art. 18, comma 1, lett. *d*), d.P.R. n. 501/1998
lett. *d*)	art. 18, comma 1, lett. *c*), -prima parte-, d.P.R. n. 501/1998

lett. *e*)	art. 18, comma 1, lett. *b*), d.P.R. n. 501/1998
alinea del comma 2	art. 18, comma 1, lett. *e*), d.P.R. n. 501/1998
lett. *a*), *b*) e *c*)	art. 18, comma 3, d.P.R. n. 501/1998
comma 3	art. 18, comma 4, d.P.R. n. 501/1998
comma 4	art. 18, comma 2, d.P.R. n. 501/1998
comma 5	art. 18, alinea del comma 1, d.P.R. n. 501/1998

Art. 148. Inammissibilità del ricorso

comma 1	art. 19, comma 1, d.P.R. n. 501/1998
comma 2	art. 18, comma 5, d.P.R. n. 501/1998

Art. 149. Procedimento relativo al ricorso

comma 1	art. 20, comma 1, d.P.R. n. 501/1998
comma 2	art. 20, comma 2, d.P.R. n. 501/1998
comma 3	art. 29, comma 3, l. n. 675/1996; art. 20, comma 3, d.P.R. n. 501/1998
comma 4	—
comma 5	art. 20, comma 4, d.P.R. n. 501/1998
comma 6	art. 20, comma 5, d.P.R. n. 501/1998
comma 7	art. 20, comma 8, d.P.R. n. 501/1998
comma 8	art. 29, comma 6-*bis*, l. n. 675/1996

Art. 150. Provvedimenti a seguito del ricorso

comma 1	art. 29, comma 5, l. n. 675/1996
comma 2	art. 29, comma 4, l. n. 675/1996
comma 3	—
comma 4	art. 20, comma 6, d.P.R. n. 501/1998
comma 5	art. 20, comma 11, d.P.R. n. 501/1998
comma 6	—

Art. 151. Opposizione

comma 1	art. 29, comma 6, l. n. 675/1996
comma 2	—

CAPO II - TUTELA GIURISDIZIONALE

Art. 152. Autorità giudiziaria ordinaria

comma 1	art. 29, comma 8, l. n. 675/1996
comma 2	—
comma 3	—
comma 4	—
comma 5	—
comma 6	—
comma 7	—
comma 8	—
comma 9	—
comma 10	—
comma 11	—
comma 12	art. 29, comma 7, (primo periodo), l. n. 675/1996
comma 13	art. 29, comma 7, (secondo periodo), l. n. 675/1996
comma 14	—

TITOLO II - L'AUTORITÀ

CAPO I - IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI cfr. art. 28, dir. 95/45/Ce

Art. 153. Il Garante

comma 1	art. 30, comma 2, l. n. 675/1996
comma 2	art. 30, comma 3, (primo e terzo periodo), l. n. 675/1996
comma 3	art. 30, comma 3, (secondo periodo), l. n. 675/1996
comma 4	art. 30, comma 4, l. n. 675/1996
comma 5	art. 30, comma 5, l. n. 675/1996
comma 6	art. 30, comma 6, l. n. 675/1996

comma 7	art. 33, (prima frase), l. n. 675/1996

Art. 154. Compiti

alinea del comma 1	art. 31, alinea, l. n. 675/1996
lett. *a*)	art. 31, comma 1, lett. *b*), l. n. 675/1996
lett. *b*)	art. 31, comma 1, lett. *d*), l. n. 675/1996
lett. *c*)	art. 31, comma 1, lett. *c*), l. n. 675/1996
lett. *d*)	art. 31, comma 1, lett. *e*) ed *l*), l. n. 675/1996
lett. *e*)	art. 31, comma 1, lett. *h*), l. n. 675/1996
lett. *f*)	art. 31, comma 1, lett. *m*), l. n. 675/1996
lett. *g*)	—
lett. *h*)	art. 31, comma 1, lett. *i*), l. n. 675/1996
lett. *i*)	art. 31, comma 1, lett. *g*), l. n. 675/1996
lett. *l*)	art. 31, comma 1, lett. *a*), l. n. 675/1996
lett. *m*)	art. 31, comma 1, lett. *n*), l. n. 675/1996
comma 2	art. 31, comma 1, lett. o), l. n. 675/1996
comma 3	art. 31, commi 5 e 6, l. n. 675/1996
comma 4	art. 31, comma 2, l. n. 675/1996
comma 5	—
comma 6	art. 40, l. n. 675/1996

CAPO II - L'UFFICIO DEL GARANTE

Art. 155. Principi applicabili

comma 1	art. 33, comma 1-*sexies*, l. n. 675/1996

Art. 156. Ruolo organico e personale

comma 1	art. 33, comma 1, (ultimo periodo), l. n. 675/1996
comma 2	—
comma 3	art. 33, commi 1-*bis* e 1-*quater*, l. n. 675/1996
comma 4	art. 33, comma 1-*ter*, l. n. 675/1996
comma 5	art. 33, comma 1-*quinquies*, l. n. 675/1996
comma 6	—
comma 7	art. 33, comma 4, l. n. 675/1996
comma 8	art. 33, comma 6, l. n. 675/1996
comma 9	art. 33, comma 6-*bis*, l. n. 675/1996
comma 10	art. 33, comma 2, l. n. 675/1996

CAPO III - ACCERTAMENTI E CONTROLLI

Art. 157. Richiesta di informazioni e di esibizione di documenti

comma 1	art. 32, comma 1, l. n. 675/1996

Art. 158. Accertamenti

comma 1	art. 32, comma 2, l. n. 675/1996
comma 2	art. 32, comma 2, l. n. 675/1996
comma 3	art. 32, comma 3, l. n. 675/1996; art. 15, comma 1, d.P.R. n. 501/1998

Art. 159. Modalità

comma 1	art. 15, commi 6, e 7, (secondo periodo), d.P.R. n. 501/1998
comma 2	art. 32, comma 4, l. n. 675/1996; art. 15, comma 5, d.P.R. n. 501/1998
comma 3	art. 15, commi 2, e 7, (primo periodo), d.P.R. n. 501/1998
comma 4	art. 15, comma 4, d.P.R. n. 501/1998
comma 5	art. 15, comma 8, d.P.R. n. 501/1998
comma 6	art. 32, comma 5, l. n. 675/1996

Art. 160. Particolari accertamenti

comma 1	art. 32, comma 6, (primo periodo), l. n. 675/1996
comma 2	art. 32, comma 6, (secondo periodo), l. n. 675/1996
comma 3	art. 32, comma 7, (primo e secondo periodo), l. n. 675/1996

comma 4	art. 32, comma 7, (terzo periodo), l. n. 675/1996
comma 5	—
comma 6	—

TITOLO III - SANZIONI

CAPO I - VIOLAZIONI AMMINISTRATIVE — cfr. art. 24, dir. 95/46/Ce

Art. 161. Omessa o inidonea informativa all'interessato

comma 1	art. 39, comma 2, (primo periodo), l. n. 675/1996

Art. 162. Altre fattispecie

comma 1	art. 16, comma 3, l. n. 675/1996
comma 2	art. 39, comma 2, (secondo periodo), l. n. 675/1996

Art. 163. Omessa o incompleta notificazione

comma 1	art. 34, comma 1, l. n. 675/1996

Art. 164. Omessa informazione o esibizione al Garante

comma 1	art. 39, comma 1, l. n. 675/1996

Art. 165. Pubblicazione del provvedimento del Garante

comma 1	—

Art. 166. Procedimento di applicazione

comma 1	art. 39, comma 3, l. n. 675/1996

CAPO II - ILLECITI PENALI

Art. 167. Trattamento illecito di dati

comma 1	art. 35, comma 1, l. n. 675/1996; art. 11, d.lg. 171/1998
comma 2	art. 35, comma 2, l. n. 675/1996

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

comma 1	art. 37-*bis*, comma 1, l. n. 675/1996

Art. 169. Misure di sicurezza

comma 1	art. 36, comma 1, l. n. 675/1996
comma 2	art. 36, comma 2, l. n. 675/1996

Art. 170. Inosservanza di provvedimenti del Garante

comma 1	art. 37, comma 1, l. n. 675/1996

Art. 171. Altre fattispecie —

Art. 172. Pene accessorie

comma 1	art. 38, comma 1, l. n. 675/1996

TITOLO IV - DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

CAPO I - DISPOSIZIONI DI MODIFICA

Art. 173. Convenzione di applicazione dell'Accordo di Schengen —

Art. 174. Notifiche di atti e vendite giudiziarie —

Art. 175. Forze di Polizia —

Art. 176. Soggetti pubblici —

Art. 177. Disciplina anagrafica, dello stato civile e delle liste elettorali —

Art. 178. Disposizioni in materia sanitaria

comma 1	—

comma 2	—
comma 3	art. 4, comma 5, d.lg. n. 282/1999
comma 4	—
comma 5	—
Art. 179. Altre modifiche	—
CAPO II - DISPOSIZIONI TRANSITORIE	
Art. 180. Misure di sicurezza	—
Art. 181. Altre disposizioni transitorie	
comma 1	—
comma 2	—
comma 3	—
comma 4	art. 13, comma 5, d.P.R. n. 501/1998
comma 5	—
comma 6	—
Art. 182. Ufficio del Garante	—
CAPO III - ABROGAZIONI	
Art. 183. Norme abrogate	—
CAPO IV - NORME FINALI	
Art. 184. Attuazione di direttive europee	
comma 1	—
comma 2	—
comma 3	art. 43, comma 2, (secondo periodo), l. n. 675/1996
Art. 185. Allegazione dei codici di deontologia e di buona condotta	—
Art. 186. Entrata in vigore	—

ALLEGATI

PAGINA BIANCA

Codici di deontologia

A.1. Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Visto l'art. 25 della legge 31 dicembre 1996, n. 675, come modificato dall'art. 12 del decreto legislativo 13 maggio 1998, n. 171, secondo il quale il trattamento dei dati personali nell'esercizio della professione giornalistica deve essere effettuato sulla base di un apposito codice di deontologia, recante misure ed accorgimenti a garanzia degli interessati rapportati alla natura dei dati, in particolare per quanto riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale;

Visto il comma 4-*bis* dello stesso art. 25, secondo il quale tale codice è applicabile anche all'attività dei pubblicisti e dei praticanti giornalisti, nonché a chiunque tratti temporaneamente i dati personali al fine di utilizzarli per la pubblicazione occasionale di articoli, di saggi e di altre manifestazioni di pensiero;

Visto il comma 2 del medesimo art. 25, secondo il quale il codice di deontologia è adottato dal Consiglio nazionale dell'ordine dei giornalisti in cooperazione con il Garante, il quale ne promuove l'adozione e ne cura la pubblicazione nella *Gazzetta Ufficiale*;

Vista la nota prot. n. 89/GAR del 26 maggio 1997, con la quale il Garante ha invitato il Consiglio nazionale dell'ordine ad adottare il codice entro il previsto termine di sei mesi dalla data di invio della nota stessa;

Vista la nota prot. n. 4640 del 24 novembre 1997, con il quale il Garante ha aderito alla richiesta di breve differimento del predetto termine di sei mesi, presentata il 19 novembre dal presidente del Consiglio nazionale dell'ordine;

Visto il provvedimento prot. n. 5252 del 18 dicembre 1997, con il quale il Garante ha segnalato al Consiglio nazionale dell'ordine alcuni criteri da tenere presenti nel bilanciamento delle libertà e dei diritti coinvolti dall'attività giornalistica;

Vista la nota prot. n. 314 del 23 gennaio 1998, con la quale il Garante ha formulato altre osservazioni sul primo schema di codice elaborato dal Consiglio nazionale dell'ordine e trasmesso al Garante con nota prot. n. 7182 del 30 dicembre 1997;

Vista la nota prot. n. 204 del 15 gennaio 1998, con la quale il Garante, sulla base della prima esperienza di applicazione della legge n. 675/1996 e dello schema di codice elaborato, ha rappresentato al Ministro di grazia e giustizia l'opportunità di una revisione dell'art. 25 della legge, che è stato poi modificato con il citato decreto legislativo n. 171 del 13 maggio 1998;

Vista la nota prot. n. 5876 del 30 giugno 1998, con la quale il Garante ha invitato il Consiglio nazionale dell'ordine ad apportare alcune residuali modifiche all'ulteriore schema approvato dallo stesso Consiglio nella seduta del 26 e 27 marzo 1998 e trasmesso al Garante con nota prot. n. 1074 dell'8 aprile;

(*) Provvedimento del Garante del 29 luglio 1998, *G.U.* 3 agosto 1998, n. 179

Constatata l'idoneità delle misure e degli accorgimenti a garanzia degli interessati previsti dallo schema definitivo del codice di deontologia trasmesso al Garante dal Consiglio nazionale dell'ordine con nota prot. n. 2210 del 15 luglio 1998;

Considerato che, ai sensi dell'art. 25, comma 2, della legge n. 675/1996, il codice deve essere pubblicato nella *Gazzetta Ufficiale*, a cura del Garante, e diviene efficace quindici giorni dopo la sua pubblicazione;

Dispone:

La trasmissione del codice di deontologia che figura in allegato all'ufficio pubblicazione leggi e decreti del Ministero di grazia e giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 29 luglio 1998

IL PRESIDENTE
Rodotà

CODICE DI DEONTOLOGIA RELATIVO AL TRATTAMENTO DEI DATI PERSONALI NELL'ESERCIZIO DELL'ATTIVITÀ GIORNALISTICA (*)

Art. 1. Principi generali

1. Le presenti norme sono volte a contemperare i diritti fondamentali della persona con il diritto dei cittadini all'informazione e con la libertà di stampa.

2. In forza dell'art. 21 della Costituzione, la professione giornalistica si svolge senza autorizzazioni o censure. In quanto condizione essenziale per l'esercizio del diritto dovere di cronaca, la raccolta, la registrazione, la conservazione e la diffusione di notizie su eventi e vicende relativi a persone, organismi collettivi, istituzioni, costumi, ricerche scientifiche e movimenti di pensiero, attuate nell'ambito dell'attività giornalistica e per gli scopi propri di tale attività, si differenziano nettamente per la loro natura dalla memorizzazione e dal trattamento di dati personali ad opera di banche dati o altri soggetti. Su questi principi trovano fondamento le necessarie deroghe previste dai paragrafi 17 e 37 e dall'art. 9 della direttiva 95/46/Ce del Parlamento europeo e del Consiglio dell'Unione europea del 24 ottobre 1995 e dalla legge n. 675/1996.

Art. 2. Banche dati di uso redazionale e tutela degli archivi personali dei giornalisti

1. Il giornalista che raccoglie notizie per una delle operazioni di cui all'art. 1, comma 2, lettera *b)*, della legge n. 675/1996 rende note la propria identità, la propria professione e le finalità della raccolta, salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; evita artifici e pressioni indebite. Fatta palese tale attività, il giornalista non è tenuto a fornire gli altri elementi dell'informativa di cui all'art. 10, comma 1, della legge n. 675/1996.

2. Se i dati personali sono raccolti presso banche dati di uso redazionale, le imprese editoriali sono tenute a rendere noti al pubblico, mediante annunci, almeno due volte l'anno, l'esistenza dell'archivio e il luogo dove è possibile esercitare i diritti previsti dalla legge n. 675/1996. Le imprese editoriali indicano altresì fra i dati della gerenza il responsabile del trattamento al quale le persone interessate possono rivolgersi per esercitare i diritti previsti dalla legge n. 675/1996.

3. Gli archivi personali dei giornalisti, comunque funzionali all'esercizio della professione e per l'esclusivo perseguimento delle relative finalità, sono tutelati, per quanto concerne le fonti delle notizie, ai sensi dell'art. 2 della legge n. 69/1963 e dell'art. 13, comma 5, della legge n. 675/1996.

4. Il giornalista può conservare i dati raccolti per tutto il tempo necessario al perseguimento delle finalità proprie della sua professione.

Art. 3. Tutela del domicilio

1. La tutela del domicilio e degli altri luoghi di privata dimora si estende ai luoghi di cura, detenzione o riabilitazione, nel rispetto delle norme di legge e dell'uso corretto di tecniche invasive.

Art. 4. Rettifica

1. Il giornalista corregge senza ritardo errori e inesattezze, anche in conformità al dovere di rettifica nei casi e nei modi stabiliti dalla legge.

Art. 5. Diritto all'informazione e dati personali

1. Nel raccogliere dati personali atti a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dati atti a rivelare le condizioni di salute e la sfera sessuale, il giornalista garantisce il diritto all'informazione su fatti di interesse pubblico, nel rispetto dell'essenzialità dell'informazione, evi-

(*) In conformità all'articolo 184, comma 2, d.lg. 30 giugno 2003, n. 196, i riferimenti a disposizioni della legge n. 675/1996 o ad altre disposizioni abrogate, devono intendersi riferiti alle corrispondenti nuove disposizioni in vigore, secondo la tavola di corrispondenza

tando riferimenti a congiunti o ad altri soggetti non interessati ai fatti.

2. In relazione a dati riguardanti circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico, è fatto salvo il diritto di addurre successivamente motivi legittimi meritevoli di tutela.

Art. 6. Essenzialità dell'informazione

1. La divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

2. La sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica.

3. Commenti e opinioni del giornalista appartengono alla libertà di informazione nonché alla libertà di parola e di pensiero costituzionalmente garantita a tutti.

Art. 7. Tutela del minore

1. Al fine di tutelarne la personalità, il giornalista non pubblica i nomi dei minori coinvolti in fatti di cronaca, né fornisce particolari in grado di condurre alla loro identificazione.

2. La tutela della personalità del minore si estende, tenuto conto della qualità della notizia e delle sue componenti, ai fatti che non siano specificamente reati.

3. Il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca; qualora, tuttavia, per motivi di rilevante interesse pubblico e fermo restando i limiti di legge, il giornalista decida di diffondere notizie o immagini riguardanti minori, dovrà farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi e i limiti stabiliti dalla "Carta di Treviso".

Art. 8. Tutela della dignità delle persone

1. Salva l'essenzialità dell'informazione, il giornalista non fornisce notizie o pubblica immagini o fotografie di soggetti coinvolti in fatti di cronaca lesive della dignità della persona, né si sofferma su dettagli di violenza, a meno che ravvisi la rilevanza sociale della notizia o dell'immagine.

2. Salvo rilevanti motivi di interesse pubblico o comprovati fini di giustizia e di polizia, il giornalista non riprende né produce immagini e foto di persone in stato di detenzione senza il consenso dell'interessato.

3. Le persone non possono essere presentate con ferri o manette ai polsi, salvo che ciò sia necessario per segnalare abusi.

Art. 9. Tutela del diritto alla non discriminazione

1. Nell'esercitare il diritto dovere di cronaca, il giornalista è tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali.

Art. 10. Tutela della dignità delle persone malate

1. Il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico.

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e sempre nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica.

Art. 11. Tutela della sfera sessuale della persona

1. Il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona, identificata o identificabile.

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica.

Art. 12. Tutela del diritto di cronaca nei procedimenti penali

1. Al trattamento dei dati relativi a procedimenti penali non si applica il limite previsto dall'art. 24 della legge n. 675/1996.

2. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'art. 686, commi 1, lettere *a*) e *d*), 2 e 3, del codice di procedura penale è ammesso nell'esercizio del diritto di cronaca, secondo i principi di cui all'art. 5.

Art. 13. Ambito di applicazione, sanzioni disciplinari

1. Le presenti norme si applicano ai giornalisti professionisti, pubblicisti e praticanti e a chiunque altro, anche occasionalmente, eserciti attività pubblicistica.

2. Le sanzioni disciplinari, di cui al titolo III della legge n. 69/1963, si applicano solo ai soggetti iscritti all'albo dei giornalisti, negli elenchi o nel registro.

A.2. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visto l'art. 31, comma 1, lettera *h)* della legge 31 dicembre 1996, n. 675, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare il relativo art. 6, comma 1, il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici;

Visto l'articolo 7, comma 5, del medesimo decreto legislativo n. 281/1999, relativo ad alcuni profili che devono essere individuati dal codice per i trattamenti di dati per scopi storici;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla *Gazzetta Ufficiale* n. 46 del 25 febbraio 2000, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi del trattamento di dati personali per scopi storici effettuati da archivisti e utenti ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione del medesimo codice in base al principio di rappresentatività a darne comunicazione al Garante entro il 31 marzo 2000;

Viste le comunicazioni pervenute al Garante in risposta al provvedimento del 10 febbraio 2000, con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare alla redazione del codice e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro composto da componenti della Commissione consultiva per le questioni inerenti la consultabilità degli atti d'archivio riservati, del Centro di documentazione ebraica, del Ministero per i beni e le attività culturali, dell'Associazione delle istituzioni culturali italiane, dell'Associazione nazionale archivistica italiana, dell'Istituto nazionale per la storia del movimento di liberazione in Italia, della Società per lo studio della storia contemporanea, dell'Istituto storico italiano per l'età moderna e contemporanea, della Società per gli studi di storia delle istituzioni, della Società italiana delle storiche, dell'Istituto romano per la storia d'Italia dal fascismo alla resistenza;

Considerato che il testo del codice è stato oggetto di ampia diffusione, anche attraverso la sua pubblicazione su alcuni siti Internet, al fine di favorire il più ampio dibattito e di per-

(*) Provvedimento del Garante n. 8/P/20001 del 14 marzo 2001, *G.U.* del 5 aprile 2001, n. 80

mettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

Vista la nota del 28 febbraio 2001 con cui il gruppo di lavoro ha trasmesso il testo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici approvato e sottoscritto in pari data;

Rilevato che il rispetto delle disposizioni contenute nel codice costituisce condizione essenziale per la liceità del trattamento dei dati personali;

Constatata la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, ed in particolare all'art. 31, comma 1, lettera *h*) della legge n. 675/1996, nonché agli artt. 6 e 7 del decreto legislativo n. 281/1999;

Considerato che, ai sensi dell'art. 6, comma 1, del decreto legislativo n. 281/1999, il codice deve essere pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante;

Rilevato che anche dopo tale pubblicazione il codice potrà essere eventualmente sottoscritto da altri soggetti pubblici e privati, società scientifiche ed associazioni professionali interessati;

Vista la documentazione in atti;

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

Relatore il prof. Ugo De Siervo;

Dispone:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici che figura in allegato all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 14 marzo 2001

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI PER SCOPI STORICI (*)

Preambolo

I sottoindicati soggetti pubblici e privati sottoscrivono il presente codice sulla base delle seguenti premesse:

1) Chiunque accede ad informazioni e documenti per scopi storici utilizza frequentemente dati di carattere personale per i quali la legge prevede alcune garanzie a tutela degli interessati. In considerazione dell'interesse pubblico allo svolgimento di tali trattamenti, il legislatore -con specifico riguardo agli archivi pubblici e a quelli privati dichiarati di notevole interesse storico ai sensi dell'art. 36 del d.P.R. 30 settembre 1963 n. 1409- ha esentato i soggetti che utilizzano dati personali per le suddette finalità dall'obbligo di richiedere il consenso degli interessati ai sensi degli artt. 12, 20 e 28 della legge (l. 31 dicembre 1996, n. 675, in particolare art. 27; dd.lg. 11 maggio 1999, n. 135 e 30 luglio 1999, n. 281, in particolare art. 7, comma 4; d.P.R. 30 settembre 1963, n. 1409, e successive modificazioni e integrazioni).

2) L'utilizzazione di tali dati da parte di utenti ed archivisti deve pertanto rispettare le previsioni di legge e quelle del presente codice di deontologia e di buona condotta, l'osservanza del quale, oltre a rappresentare un obbligo deontologico, costituisce condizione essenziale per la liceità del trattamento dei dati (art. 31, comma 1, lettera *h*), l. 31 dicembre 1996, n. 675; art. 6, d.lg. 30 luglio 1999, n.281).

3) L'osservanza di tali regole non deve pregiudicare l'indagine, la ricerca, la documentazione e lo studio ovunque svolti, in relazione a figure, fatti e circostanze del passato.

4) I trattamenti di dati personali concernenti la conservazione, l'ordinamento e la comunicazione dei documenti conservati negli Archivi di Stato e negli archivi storici degli enti pubblici sono considerati di rilevante interesse pubblico (art. 23, d.lg. 11 maggio 1999, n. 135).

5) La sottoscrizione del presente codice è promossa per legge dal Garante, nel rispetto del principio di rappresentatività dei soggetti pubblici e privati interessati. Il codice è espressione delle associazioni professionali e delle categorie interessate, ivi comprese le società scientifiche, ed è volto ad assicurare l'equilibrio delle diverse esigenze connesse alla ricerca e alla rappresentazione di fatti storici con i diritti e le libertà fondamentali delle persone interessate (art. 1, l. 31 dicembre 1996, n. 675).

6) Il presente codice, sulla base delle prescrizioni di legge, individua in particolare: a) alcune regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, armonizzate con quelle che riguardano il diritto di cronaca e la manifestazione del pensiero; b) 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; c) modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati per scopi storici (art. 7, comma 5, d.lg. 30 luglio 1999, n. 281).

7) La sottoscrizione del presente codice è effettuata ispirandosi, oltre agli artt. 21 e 33 della Costituzione della Repubblica italiana, alle pertinenti fonti e documenti internazionali in materia di ricerca storica e di archivi e in particolare:

a) agli artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;
b) alla Raccomandazione R (2000) 13 del 13 luglio 2000 del Consiglio d'Europa;
c) agli artt. 1, 7, 8, 11 e 13 della Carta dei diritti fondamentali dell'Unione europea;
d) ai Principi direttivi per una legge sugli archivi storici e gli archivi correnti, individuati dal Consiglio internazionale degli archivi al congresso di Ottawa nel 1996, e al Codice internazionale di deontologia degli archivisti approvato nel congresso internazionale degli archivi, svoltosi a Pechino nel 1996.

(*) In conformità all'articolo 184, comma 2, d.lg. 30 giugno 2003, n. 196, i riferimenti a disposizioni della legge n. 675/1996 o ad altre disposizioni abrogate, devono intendersi riferiti alle corrispondenti nuove disposizioni in vigore, secondo la tavola di corrispondenza.

CAPO I - PRINCIPI GENERALI

Art. 1. Finalità e ambito di applicazione

1. Le presenti norme sono volte a garantire che l'utilizzazione di dati di carattere personale acquisiti nell'esercizio della libera ricerca storica e del diritto allo studio e all'informazione, nonché nell'accesso ad atti e documenti, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

2. Il presente codice detta disposizioni per i trattamenti di dati personali effettuati per scopi storici in relazione ai documenti conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico. Il codice si applica, senza necessità di sottoscrizione, all'insieme dei trattamenti di dati personali comunque effettuati dagli utenti per scopi storici.

3. Il presente codice reca, altresì, principi-guida di comportamento dei soggetti che trattano per scopi storici dati personali conservati presso archivi pubblici e archivi privati dichiarati di notevole interesse storico, e in particolare:

a) nei riguardi degli archivisti, individua regole di correttezza e di non discriminazione nei confronti degli utenti, indipendentemente dalla loro nazionalità, categoria di appartenenza, livello di istruzione;
b) nei confronti degli utenti, individua cautele per la raccolta, l'utilizzazione e la diffusione dei dati contenuti nei documenti.

4. La competente sovrintendenza archivistica riceve comunicazione da parte di proprietari, possessori e detentori di archivi privati non dichiarati di notevole interesse storico o di singoli documenti di interesse storico, i quali manifestano l'intenzione di applicare il presente codice nella misura per essi compatibile.

Art. 2. Definizioni

1. Nell'applicazione del presente codice si tiene conto delle definizioni e delle indicazioni contenute nella disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni citate nel preambolo. Ai medesimi fini si intende, altresì:

a) per "archivista", chiunque, persona fisica o giuridica, ente o associazione, abbia responsabilità di controllare, acquisire, trattare, conservare, restaurare e gestire archivi storici, correnti o di deposito della pubblica amministrazione, archivi privati dichiarati di notevole interesse storico, nonché gli archivi privati di cui al precedente art. 1, comma 4;
b) per "utente", chiunque chieda di accedere o acceda per scopi storici a documenti contenenti dati personali, anche per finalità giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero;
c) per "documento", qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali.

CAPO II - REGOLE DI CONDOTTA PER GLI ARCHIVISTI E LICEITÀ DEI RELATIVI TRATTAMENTI

Art. 3. Regole generali di condotta

1. Nel trattare i dati di carattere personale e i documenti che li contengono, gli archivisti adottano, in armonia con la legge e i regolamenti, le modalità più opportune per favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati.

2. Gli archivisti di enti o istituzioni pubbliche si adoperano per il pieno rispetto, anche da parte dei terzi con cui entrano in contatto per ragioni del proprio ufficio o servizio, delle disposizioni di legge e di regolamento in materia archivistica e, in particolare, di quanto previsto negli artt. 21 e 21-*bis* del d.P.R. 30 settembre 1963, n. 1409, come modificati dal d.lg. 30 luglio 1999, n. 281, dall'art. 7 del medesimo d.lg. n. 281, e successive modificazioni ed integrazioni.

3. I soggetti che operano presso enti pubblici svolgendo funzioni archivistiche, nel trattare dati di carattere personale si attengono ai doveri di lealtà, correttezza, imparzialità, onestà e diligenza propri dell'esercizio della professione e della qualifica o livello ricoperti. Essi conformano il proprio operato al principio di trasparenza della attività amministrativa.

4. I dati personali trattati per scopi storici possono essere ulteriormente utilizzati per tali scopi, e sono soggetti in linea di principio alla medesima disciplina indipendentemente dal documento in cui sono contenuti e dal luogo di conservazione, ferme restando le cautele e le garanzie previste per particolari categorie di dati o di trattamenti.

Art. 4. Conservazione e tutela

1. Gli archivisti si impegnano a:
   a) favorire il recupero, l'acquisizione e la tutela dei documenti. A tal fine, operano in conformità con i principi, i criteri metodologici e le pratiche della professione generalmente condivisi ed accettati, curando anche l'aggiornamento sistematico e continuo delle proprie conoscenze storiche, amministrative e tecnologiche;
   b) tutelare l'integrità degli archivi e l'autenticità dei documenti, anche elettronici e multimediali, di cui promuovono la conservazione permanente, in particolare di quelli esposti a rischi di cancellazione, dispersione ed alterazione dei dati;
   c) salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;
   d) assicurare il rispetto delle misure di sicurezza previste dall'art. 15 della legge 31 dicembre 1996, n. 675 e dal d.P.R. 28 luglio 1999, n. 318 e successive integrazioni e modificazioni, sviluppando misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, e adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati.

Art. 5. Comunicazione e fruizione

1. Gli archivi sono organizzati secondo criteri tali da assicurare il principio della libera fruibilità delle fonti.

2. L'archivista promuove il più largo accesso agli archivi e, attenendosi al quadro della normativa vigente, favorisce l'attività di ricerca e di informazione nonché il reperimento delle fonti.

3. L'archivista informa il ricercatore sui documenti estratti temporaneamente da un fascicolo perché esclusi dalla consultazione.

4. In caso di rilevazione sistematica dei dati realizzata da un archivio in collaborazione con altri soggetti pubblici o privati, per costituire banche dati di intere serie archivistiche, la struttura interessata sottoscrive una apposita convenzione per concordare le modalità di fruizione e le forme di tutela dei soggetti interessati, attenendosi alle disposizioni della legge, in particolare per quanto riguarda il rapporto tra il titolare, il responsabile e gli incaricati del trattamento, nonché i rapporti con i soggetti esterni interessati ad accedere ai dati.

Art. 6. Impegno di riservatezza

1. Gli archivisti si impegnano a:
   a) non fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attività anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati. Nel caso in cui l'archivista svolga ricerche per fini personali o comunque estranei alla propria attività professionale, è soggetto alle stesse regole e ai medesimi limiti previsti per gli utenti;
   b) mantenere riservate le notizie e le informazioni concernenti i dati personali apprese nell'esercizio delle proprie attività.

2. L'archivista osserva tali doveri di riserbo anche dopo la cessazione dalla propria attività.

Art. 7. Aggiornamento dei dati

1. L'archivista favorisce l'esercizio del diritto degli interessati all'aggiornamento, alla rettifica o all'integrazione dei dati, garantendone la conservazione secondo modalità che assicurino la distinzione delle fonti originarie dalla documentazione successivamente acquisita.

2. Ai fini dell'applicazione dell'art. 13 della legge n. 675/1996, in presenza di eventuali richieste generalizzate di accesso ad un'ampia serie di dati o documenti, l'archivista pone a disposizione gli strumenti di ricerca e le fonti pertinenti fornendo al richiedente idonee indicazioni per una loro agevole consultazione.

3. In caso di esercizio di un diritto, ai sensi dell'art. 13, comma 3, della legge n. 675/1996, da parte di chi vi abbia interesse in relazione a dati personali che riguardano persone decedute e documenti assai risalenti nel tempo, la sussistenza dell'interesse è valutata anche in riferimento al tempo trascorso.

Art. 8. Fonti orali

1. In caso di trattamento di fonti orali, è necessario che gli intervistati abbiano espresso il proprio consenso in modo esplicito, eventualmente in forma verbale, anche sulla base di una informativa semplificata che renda nota almeno l'identità e l'attività svolta dall'intervistatore nonché le finalità della raccolta dei dati.

2. Gli archivi che acquisiscono fonti orali richiedono all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti nell'intervista stessa e del relativo consenso manifestato dagli intervistati.

CAPO III - REGOLE DI CONDOTTA PER GLI UTENTI E CONDIZIONI PER LA LICEITÀ DEI RELATIVI TRATTAMENTI

Art. 9. Regole generali di condotta

1. Nell'accedere alle fonti e nell'esercitare l'attività di studio, ricerca e manifestazione del pensiero, gli utenti, quando trattino i dati di carattere personale, secondo quanto previsto dalla legge e dai regolamenti, adottano le modalità più opportune per favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate.

2. In applicazione del principio di cui al comma 1, gli utenti utilizzano i documenti sotto la propria responsabilità e conformandosi agli scopi perseguiti e delineati nel progetto di ricerca, nel rispetto dei principi di pertinenza ed indispensabilità di cui all'art. 7, del d.lg. 30 luglio 1999, n. 281.

Art. 10. Accesso agli archivi pubblici

1. L'accesso agli archivi pubblici è libero. Tutti gli utenti hanno diritto ad accedere agli archivi con eguali diritti e doveri.

2. Fanno eccezione, ai sensi delle leggi vigenti, i documenti di carattere riservato relativi alla politica interna ed estera dello Stato che divengono consultabili cinquanta anni dopo la loro data e quelli contenenti i dati di cui agli artt. 22 e 24 della legge n. 675/1996, che divengono liberamente consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute o la vita sessuale oppure rapporti riservati di tipo familiare.

3. L'autorizzazione alla consultazione dei documenti di cui al comma 2 può essere rilasciata prima della scadenza dei termini dal Ministro dell'interno, previo parere del direttore dell'Archivio di Stato o del sovrintendente archivistico competenti e udita la Commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati istituita presso il Ministero dell'interno, secondo la procedura dettata dagli artt. 8 e 9 del decreto legislativo n. 281/1999.

4. In caso di richiesta di autorizzazione a consultare i documenti di cui al comma 2 prima della scadenza dei termini, l'utente presenta all'ente che li conserva un progetto di ricerca che, in relazione alle fonti riservate per le quali chiede l'autorizzazione, illustri le finalità della ricerca e le modalità di diffusione dei dati. Il richiedente ha facoltà di presentare ogni altra documentazione utile.

5. L'autorizzazione di cui al comma 3 alla consultazione è rilasciata a parità di condizioni ad ogni altro richiedente. La valutazione della parità di condizioni avviene sulla base del progetto di ricerca di cui al comma 4.

6. L'autorizzazione alla consultazione dei documenti, di cui al comma 3, prima dello scadere dei termini, può contenere cautele volte a consentire la comunicazione dei dati senza ledere i diritti, le libertà e la dignità delle persone interessate.

7. Le cautele possono consistere anche, a seconda degli obiettivi della ricerca desumibili dal progetto, nell'obbligo di non diffondere i nomi delle persone, nell'uso delle sole iniziali dei nominativi degli interessati, nell'oscuramento dei nomi in una banca dati, nella sottrazione temporanea di singoli documenti dai fascicoli o nel divieto di riproduzione dei documenti. Particolare attenzione è prestata al principio della pertinenza e all'indicazione di fatti o circostanze che possono rendere facilmente individuabili gli interessati.

8. L'autorizzazione di cui al comma 3 è personale e il titolare dell'autorizzazione non può delegare altri al conseguente trattamento dei dati. I documenti mantengono il loro carattere riservato e non possono essere ulteriormente utilizzati da altri soggetti senza la relativa autorizzazione.

Art. 11. Diffusione

1. L'interpretazione dell'utente, nel rispetto del diritto alla riservatezza, del diritto all'identità personale e della dignità degli interessati, rientra nella sfera della libertà di parola e di manifestazione del pensiero costituzionalmente garantite.

2. Nel far riferimento allo stato di salute delle persone l'utente si astiene dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad una determinata persona identificata o identificabile.

3. La sfera privata delle persone note o che abbiano esercitato funzioni pubbliche deve essere rispettata nel caso in cui le notizie o i dati non abbiano alcun rilievo sul loro ruolo o sulla loro vita pubblica.

4. In applicazione di quanto previsto dall'art. 7, comma 2, del d.lg. n. 281/1999, al momento della diffusione dei dati il principio della pertinenza è valutato dall'utente con particolare riguardo ai singoli dati personali contenuti nei documenti, anziché ai documenti nel loro complesso. L'utente può diffondere i dati personali se pertinenti e indispensabili alla ricerca e se gli stessi non ledono la dignità e la riservatezza delle persone.

5. L'utente non è tenuto a fornire l'informativa di cui all'art. 10, comma 3, della legge n. 675/1996 nei casi in cui tale adempimento comporti l'impiego di mezzi manifestamente sproporzionati.

6. L'utente può utilizzare i dati elaborati o le copie dei documenti contenenti dati personali, accessibili su autorizzazione, solo ai fini della propria ricerca, e ne cura la riservatezza anche rispetto ai terzi.

Art. 12. Applicazione del codice

1. I soggetti pubblici e privati, comprese le società scientifiche e le associazioni professionali, che siano tenuti ad applicare il presente codice si impegnano, con i modi e nelle forme previste dai propri ordinamenti, a promuoverne la massima diffusione e la conoscenza, nonché ad assicurarne il rispetto.

2. Nel caso degli archivi degli enti pubblici e degli archivi privati dichiarati di notevole interesse storico, le sovrintendenze archivistiche promuovono la diffusione e l'applicazione del codice.

Art. 13. Violazione delle regole di condotta

1. Nell'ambito degli archivi pubblici le amministrazioni competenti applicano le sanzioni previste dai rispettivi ordinamenti.

2. Le società e le associazioni tenute ad applicare il presente codice adottano, sulla base dei propri ordinamenti e regolamenti, le opportune misure in caso di violazione del codice stesso, ferme restando le sanzioni di legge.

3. La violazione delle prescrizioni del presente codice da parte degli utenti è comunicata agli organi competenti per il rilascio delle autorizzazioni a consultare documenti riservati prima del decorso dei termini di legge, ed è considerata ai fini del rilascio dell'autorizzazione medesima. L'Amministrazione competente, secondo il proprio ordinamento, può altresì escludere temporaneamente dalle sale di studio i soggetti responsabili della violazione delle regole del presente codice. Gli stessi possono essere esclusi da ulteriori autorizzazioni alla consultazione di documenti riservati.

4. Oltre a quanto previsto dalla legge per la denuncia di reato cui sono tenuti i pubblici ufficiali, i soggetti di cui ai commi 1 e 2 possono segnalare al Garante le violazioni delle regole di condotta per l'eventuale adozione dei provvedimenti e delle sanzioni di competenza.

Art. 14. Entrata in vigore

1. Il presente codice si applica a decorrere dal quindicesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

A.3. Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Visto l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visto l'art. 31, comma 1, lettera *h)* della legge 31 dicembre 1996, n. 675, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare il relativo art. 6, comma 1, il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi di statistica e di ricerca scientifica;

Visto l'articolo 10, comma 6, del medesimo decreto legislativo n. 281/1999, relativo ad alcuni profili che devono essere individuati dal codice per i trattamenti di dati per scopi statistici e di ricerca scientifica;

Visto altresì l'articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322, come modificato dall'articolo 12, comma 6, del decreto legislativo n. 281/1999, nel quale si prevede che la Commissione per la garanzia dell'informazione statistica debba essere sentita ai fini della sottoscrizione dei codici di deontologia e di buona condotta relativi al trattamento dei dati personali nell'ambito del Sistema statistico nazionale;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla *Gazzetta Ufficiale* n. 46 del 25 febbraio 2000, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi del trattamento di dati personali per scopi statistici e di ricerca scientifica ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività a darne comunicazione al Garante entro il 31 marzo 2000;

Viste le comunicazioni pervenute al Garante in risposta al provvedimento del 10 febbraio 2000, con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare alla redazione dei codici e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro, composto, fra gli altri, da rappresentanti dei seguenti soggetti pubblici: Istituto nazionale di statistica - Istat, Istituto di studi e analisi economica - Isae, Istituto per lo sviluppo della formazione profes-

(*) Provvedimento del Garante n. 13 del 31 luglio 2002, *G.U.* 1° ottobre 2002, n. 230

sionale dei lavoratori - Isfol, Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica;

Considerato che il testo del codice è stato oggetto di ampia consultazione nell'ambito dei soggetti interessati, che hanno avuto modo di far pervenire osservazioni e proposte;

Visto il decreto del Presidente del Consiglio dei ministri 9 marzo 2000, n. 152 contenente le norme per la definizione dei criteri e delle procedure per l'individuazione dei soggetti privati partecipanti al Sistema statistico nazionale (Sistan) ai sensi dell'articolo 2, comma 1, della legge 28 aprile 1998, n. 125;

Visto il decreto del Presidente del Consiglio dei ministri 9 maggio 2001 in materia di circolazione dei dati all'interno del Sistema statistico nazionale;

Visto il decreto del Presidente del Consiglio dei ministri 28 maggio 2002 sull'inserimento di altri uffici di statistica nell'ambito del Sistan;

Vista la nota del 2 aprile 2001 con cui il Presidente dell'Istat, su mandato del Comitato di indirizzo e coordinamento dell'informazione statistica, ha trasmesso il testo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, sottoscritto dallo stesso a nome dei soggetti interessati;

Vista la deliberazione di questa Autorità n. 23 del 4 luglio 2001 sull'esame preliminare del codice;

Ritenuto opportuno procedere all'esame definitivo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici effettuati nell'ambito del Sistan, anche separatamente rispetto al codice che, a norma degli articoli 6, comma 1, e 10, comma 6, del d.lg. n. 281/1999, deve disciplinare l'utilizzo dei dati personali a fini statistici al di fuori del Sistan;

Sentita la Commissione per la garanzia nell'informazione statistica ai sensi dell'articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322 e sulla base degli approfondimenti curati d'intesa con l'Istat;

Rilevato che il rispetto delle disposizioni contenute nel codice costituisce condizione essenziale per la liceità del trattamento dei dati personali;

Constatata la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, ed in particolare all'art. 31, comma 1, lettera *h*) della legge n. 675/1996, nonché agli artt. 6 e 10, 11 e 12 del decreto legislativo n. 281/1999;

Considerato che, ai sensi dell'art. 6, comma 1, del decreto legislativo n. 281/1999, il codice deve essere pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante;

Vista la documentazione in atti;

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

Relatore il prof. Gaetano Rasi;

Dispone:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico

nazionale, che figura in allegato, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 31 luglio 2002

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI A SCOPI STATISTICI E DI RICERCA SCIENTIFICA EFFETTUATI NELL'AMBITO DEL SISTEMA STATISTICO NAZIONALE (*)

Preambolo

Il presente codice è volto a garantire che l'utilizzazione di dati di carattere personale per scopi di statistica, considerati dalla legge di rilevante interesse pubblico e fonte dell'informazione statistica ufficiale intesa quale patrimonio della collettività, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

Il codice è sottoscritto in attuazione degli articoli 6 e 10, comma 6, del decreto legislativo 30 luglio 1999, n. 281 e si applica ai trattamenti per scopi statistici effettuati nell'ambito del Sistema statistico nazionale, per il perseguimento delle finalità di cui al decreto legislativo 6 settembre 1989, n. 322.

La sua sottoscrizione è effettuata ispirandosi alle pertinenti fonti e documenti internazionali in materia di attività statistica e, in particolare:

a) alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;
b) alla Carta dei diritti fondamentali dell'Unione europea del 18 dicembre 2000, con specifico riferimento agli artt. 7 e 8;
c) alla Convenzione n. 108 adottata a Strasburgo il 28 gennaio 1981, ratificata in Italia con legge 21 febbraio 1989, n. 98;
d) alla direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio dell'Unione europea del 24 ottobre 1995;
e) alla Raccomandazione del Consiglio d'Europa R(97)18, adottata il 30 settembre 1997;
f) all'articolo 10 del Regolamento (CE) n. 322/97 del Consiglio dell'Unione europea del 17 febbraio 1997.

Gli enti, gli uffici e i soggetti che applicano il seguente codice sono chiamati ad osservare anche il principio di imparzialità e di non discriminazione nei confronti di altri utilizzatori, in particolare, nell'ambito della comunicazione per scopi statistici di dati depositati in archivi pubblici e trattati da enti pubblici o sulla base di finanziamenti pubblici.

CAPO I - AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

Art. 1. Ambito di applicazione

1. Il codice si applica ai trattamenti di dati personali per scopi statistici effettuati da:

a) enti ed uffici di statistica che fanno parte o partecipano al Sistema statistico nazionale, per l'attuazione del programma statistico nazionale o per la produzione di informazione statistica, in conformità ai rispettivi ambiti istituzionali;
b) strutture diverse dagli uffici di cui alla lettera a), ma appartenenti alla medesima amministrazione o ente, qualora i relativi trattamenti siano previsti dal programma statistico nazionale e gli uffici di statistica attestino le metodologie adottate, osservando le disposizioni contenute nei decreti legislativi 6 settembre 1989, n. 322 e 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni, nonché nel presente codice.

Art. 2. Definizioni

1. Ai fini del presente codice si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675 (di seguito denominata "Legge"), nel decreto legislativo 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni. Ai fini medesimi, si intende inoltre per:

a) "trattamento per scopi statistici", qualsiasi trattamento effettuato per finalità di indagine statistica o di produzione, conservazione e diffusione di risultati statistici in attuazione del programma statistico nazionale o per effettuare informazione

(*) In conformità all'articolo 184, comma 2, d.lg. 30 giugno 2003, n. 196, i riferimenti a disposizioni della legge n. 675/1996 o ad altre disposizioni abrogate, devono intendersi riferiti alle corrispondenti nuove disposizioni in vigore, secondo la tavola di corrispondenza

statistica in conformità agli ambiti istituzionali dei soggetti di cui all'articolo 1;

b) "risultato statistico", l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;

c) "variabile pubblica", il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;

d) "unità statistica", l'entità alla quale sono riferiti o riferibili i dati trattati.

Art. 3. Identificabilità dell'interessato

1. Agli effetti dell'applicazione del presente codice:

a) un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati identificativi della medesima;

b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
- risorse economiche;
- risorse di tempo;
- archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
- archivi, anche non nominativi, che forniscano ulteriori informazioni oltre a quelle oggetto di comunicazione o diffusione;
- risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
- conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;

c) in caso di comunicazione e di diffusione, l'interessato può ritenersi non identificabile se il rischio di identificazione, in termini di probabilità di identificare l'interessato stesso tenendo conto dei dati comunicati o diffusi, è tale da far ritenere sproporzionati i mezzi eventualmente necessari per procedere all'identificazione rispetto alla lesione o al pericolo di lesione dei diritti degli interessati che può derivarne, avuto altresì riguardo al vantaggio che se ne può trarre.

Art. 4. Criteri per la valutazione del rischio di identificazione

1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto dei seguenti criteri:

a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;

b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;

c) i risultati statistici relativi a sole variabili pubbliche non sono soggetti alla regola della soglia;

d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;

e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;

f) si presume che sia adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentino la medesima modalità di una variabile.

2. Nel programma statistico nazionale sono individuate le variabili che possono essere diffuse in forma disaggregata, ove ciò risulti necessario per soddisfare particolari esigenze conoscitive anche di carattere internazionale o comunitario.

3. Nella comunicazione di collezioni campionarie di dati, il rischio di identificazione deve essere per quanto possibile contenuto. Tale limite e la metodologia per la stima del rischio di identificazione sono individuati dall'Istat che, attenendosi ai criteri di cui all'art. 3, comma 1, lett. *d*), definisce anche le modalità di rilascio dei dati dandone comunicazione alla Commissione per la garanzia dell'informazione statistica.

Art. 5. Trattamento di dati sensibili da parte di soggetti privati

1. I soggetti privati che partecipano al Sistema statistico nazionale ai sensi della legge 28 aprile 1998, n. 125, raccolgono o trattano ulteriormente dati sensibili per scopi statistici di regola in forma anonima, fermo restando quanto previsto dall'art. 6-*bis*, comma 1, del decreto legislativo 6 settembre 1989, n. 322, come introdotto dal decreto legislativo 30 luglio 1999, n. 281, e successive modificazioni e integrazioni.

2. In casi particolari in cui scopi statistici, legittimi e specifici, del trattamento di dati sensibili non possono essere raggiunti senza l'identificazione anche temporanea degli interessati, per garantire la legittimità del trattamento medesimo è necessario che concorrano i seguenti presupposti:

a) l'interessato abbia espresso liberamente il proprio consenso sulla base degli elementi previsti per l'informativa;
b) il titolare adotti specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo che ciò risulti irragionevole o richieda uno sforzo manifestamente sproporzionato;
c) il trattamento risulti preventivamente autorizzato dal Garante, anche sulla base di un'autorizzazione relativa a categorie di dati o tipologie di trattamenti, o sia compreso nel programma statistico nazionale.

3. Il consenso è manifestato per iscritto. Qualora la raccolta dei dati sensibili sia effettuata con particolari modalità quali interviste telefoniche o assistite da elaboratore che rendano particolarmente gravoso per l'indagine acquisirlo per iscritto, il consenso, purché espresso, può essere documentato per iscritto. In tal caso, la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso è conservata dal titolare del trattamento per tre anni.

CAPO II - INFORMATIVA, COMUNICAZIONE E DIFFUSIONE

Art. 6. Informativa

1. Oltre alle informazioni di cui all'art. 10 della Legge, all'interessato o alle persone presso le quali i dati personali dell'interessato sono raccolti per uno scopo statistico è rappresentata l'eventualità che essi possono essere trattati per altri scopi statistici, in conformità a quanto previsto dai decreti legislativi 6 settembre 1989, n. 322 e 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni.

2. Quando il trattamento riguarda dati personali non raccolti presso l'interessato e il conferimento dell'informativa a quest'ultimo richieda uno sforzo sproporzionato rispetto al diritto tutelato, in base a quanto previsto dall'art. 10, comma 4 della Legge, l'informativa stessa si considera resa se il trattamento è incluso nel programma statistico nazionale o è oggetto di pubblicità con idonee modalità da comunicare preventivamente al Garante il quale può prescrivere eventuali misure ed accorgimenti.

3. Nella raccolta di dati per uno scopo statistico, l'informativa alla persona presso la quale i dati sono raccolti può essere differita per la parte riguardante le specifiche finalità, le modalità del trattamento cui sono destinati i dati, qualora ciò risulti necessario per il raggiungimento dell'obiettivo dell'indagine –in relazione all'argomento o alla natura della stessa– e purché il trattamento non riguardi dati sensibili. In tali casi, il completamento dell'informativa deve essere fornito all'interessato non appena vengano a cessare i motivi che ne avevano ritardato la comunicazione, a meno che ciò comporti un impiego di mezzi palesemente sproporzionato. Il soggetto responsabile della

ricerca deve redigere un documento –successivamente conservato per almeno due anni dalla conclusione della ricerca e reso disponibile a tutti i soggetti che esercitano i diritti di cui all'art. 13 della Legge– in cui siano indicate le specifiche motivazioni per le quali si è ritenuto di differire l'informativa, la parte di informativa differita, nonché le modalità seguite per informare gli interessati quando sono venute meno le ragioni che avevano giustificato il differimento.

4. Quando le circostanze della raccolta e gli obiettivi dell'indagine 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 può essere data anche per il tramite del soggetto rispondente.

Art. 7. Comunicazione a soggetti non facenti parte del Sistema statistico nazionale

1. Ai soggetti che non fanno parte del Sistema statistico nazionale possono essere comunicati, sotto forma di collezioni campionarie, dati individuali privi di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalità che rendano questi ultimi non identificabili.

2. La comunicazione di dati personali a ricercatori di università o ad istituti o enti di ricerca o a soci di società scientifiche a cui si applica il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati fuori dal Sistema statistico nazionale, di cui all'articolo 10, comma 6, del decreto legislativo 30 luglio 1999, n. 281 e successive modificazioni e integrazioni, è consentita nell'ambito di specifici laboratori costituiti da soggetti del Sistema statistico nazionale, a condizione che:

a) i dati siano il risultato di trattamenti di cui i medesimi soggetti del Sistema statistico nazionale siano titolari;
b) i dati comunicati siano privi di dati identificativi;
c) le norme in materia di segreto statistico e di protezione dei dati personali, contenute anche nel presente codice, siano rispettate dai ricercatori che accedono al laboratorio anche sulla base di una preventiva dichiarazione di impegno;
d) l'accesso al laboratorio sia controllato e vigilato;
e) non sia consentito l'accesso ad archivi di dati diversi da quello oggetto della comunicazione;
f) siano adottate misure idonee affinché le operazioni di immissione e prelievo di dati siano inibite ai ricercatori che utilizzano il laboratorio;
g) il rilascio dei risultati delle elaborazioni effettuate dai ricercatori che utilizzano il laboratorio sia autorizzato solo dopo una preventiva verifica, da parte degli addetti al laboratorio stesso, del rispetto delle norme di cui alla lettera c).

3. Nell'ambito di progetti congiunti, finalizzati anche al perseguimento di compiti istituzionali del titolare del trattamento che ha originato i dati, i soggetti del Sistema statistico nazionale possono comunicare dati personali a ricercatori operanti per conto di università, altre istituzioni pubbliche e organismi aventi finalità di ricerca, purché sia garantito il rispetto delle condizioni seguenti:

a) i dati siano il risultato di trattamenti di cui i medesimi soggetti del Sistema statistico nazionale sono titolari;
b) i dati comunicati siano privi di dati identificativi;
c) la comunicazione avvenga sulla base di appositi protocolli di ricerca sottoscritti da tutti i ricercatori che partecipano al progetto;
d) nei medesimi protocolli siano esplicitamente previste, come vincolanti per tutti i ricercatori che partecipano al progetto, le norme in materia di segreto statistico e di protezione dei dati personali contenute anche nel presente codice.

4. È vietato ai ricercatori ammessi alla comunicazione dei dati di effettuare trattamenti per fini diversi da quelli esplicitamente previsti dal protocollo di ricerca, di conservare i dati comunicati oltre i termini di durata del progetto, di comunicare ulteriormente i dati a terzi.

Dna dell'imputato

o dell'indagato

Art. 8. Comunicazione dei dati tra soggetti del Sistema statistico nazionale

1. La comunicazione di dati personali, privi di dati identificativi, tra i soggetti del Sistema statistico nazionale è consentita per i trattamenti statistici, strumentali al perseguì-

mento delle finalità istituzionali del soggetto richiedente, espressamente determinati all'atto della richiesta, fermo restando il rispetto dei principi di pertinenza e di non eccedenza.

2. La comunicazione anche dei dati identificativi di unità statistiche tra i soggetti del Sistema statistico nazionale è consentita, previa motivata richiesta in cui siano esplicitate le finalità perseguite ai sensi del decreto legislativo 6 settembre 1989, n. 322, ivi comprese le finalità di ricerca scientifica per gli enti di cui all'art. 2 del decreto legislativo medesimo, qualora il richiedente dichiari che non sia possibile conseguire altrimenti il medesimo risultato statistico e, comunque, nel rispetto dei principi di pertinenza e di stretta necessità.

3. I dati comunicati ai sensi dei commi 1 e 2 possono essere trattati dal soggetto richiedente, anche successivamente, per le sole finalità perseguite ai sensi del decreto legislativo 6 settembre 1989, n. 322, ivi comprese le finalità di ricerca scientifica per gli enti di cui all'art. 2 del decreto legislativo medesimo, nei limiti previsti dal decreto legislativo 30 luglio 1999, n. 281, e nel rispetto delle misure di sicurezza previste dall'art. 15 della Legge e successive modificazioni e integrazioni.

Art. 9. Autorità di controllo

1. La Commissione per la garanzia dell'informazione statistica di cui all'articolo 12 del decreto legislativo 6 settembre 1989, n. 322 contribuisce alla corretta applicazione delle disposizioni del presente codice e, in particolare, di quanto previsto al precedente art. 8, segnalando al Garante i casi di inosservanza.

CAPO III - SICUREZZA E REGOLE DI CONDOTTA

Art. 10. Raccolta dei dati

1. I soggetti di cui all'art. 1 pongono specifica attenzione nella selezione del personale incaricato della raccolta dei dati e nella definizione dell'organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del presente codice e la tutela dei diritti degli interessati, procedendo altresì alla designazione degli incaricati del trattamento, secondo le modalità di legge.

2. In ogni caso, il personale incaricato della raccolta si attiene alle disposizioni contenute nel presente codice e alle istruzioni ricevute. In particolare:

a) rende nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;
b) fornisce le informazioni di cui all'art. 10 della Legge e di cui all'art. 6 del presente codice, nonché ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici o indebite pressioni;
c) non svolge contestualmente presso gli stessi interessati attività di rilevazione di dati per conto di più titolari, salvo espressa autorizzazione;
d) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;
e) assicura una particolare diligenza nella raccolta di dati personali di cui agli articoli 22, 24 e 24-*bis* della Legge.

Art. 11. Conservazione dei dati

1. I dati personali possono essere conservati anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, in conformità all'art. 9 della Legge e all'art. 6-*bis* del decreto legislativo 6 settembre 1989, n. 322 e successive modificazioni e integrazioni. In tali casi, i dati identificativi possono essere conservati fino a quando risultino necessari per:

- indagini continue e longitudinali;
- indagini di controllo, di qualità e di copertura;
- definizione di disegni campionari e selezione di unità di rilevazione;
- costituzione di archivi delle unità statistiche e di sistemi informativi;
- altri casi in cui ciò risulti essenziale e adeguatamente documentato per le finalità perseguite.

2. Nei casi di cui al comma 1, i dati identificativi sono conservati separatamente da ogni altro dato, in modo da consentirne differenti livelli di accesso, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o comporti un impiego di mezzi manifestamente sproporzionati rispetto al diritto tutelato.

Art. 12. Misure di sicurezza

1. Nell'adottare le misure di sicurezza di cui all'art. 15, comma 1, della Legge e di cui al regolamento previsto dal comma 2 del medesimo articolo, il titolare del trattamento determina anche i differenti livelli di accesso ai dati personali con riferimento alla natura dei dati stessi e alle funzioni dei soggetti coinvolti nei trattamenti.

2. I soggetti di cui all'art. 1 adottano le cautele previste dagli articoli 3 e 4 del decreto legislativo 11 maggio 1999, n. 135 in riferimento ai dati di cui agli articoli 22 e 24 della Legge.

Art. 13. Esercizio dei diritti dell'interessato

1. In caso di esercizio dei diritti di cui all'art.13 della Legge, l'interessato può accedere agli archivi statistici contenenti i dati che lo riguardano per chiederne l'aggiornamento, la rettifica o l'integrazione, sempre che tale operazione non risulti impossibile per la natura o lo stato del trattamento, o comporti un impiego di mezzi manifestamente sproporzionati.

2. In attuazione dell'art. 6-*bis*, comma 8, del decreto legislativo 6 settembre 1989, n. 322, il responsabile del trattamento annota in appositi spazi o registri le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio, qualora tali operazioni non producano effetti significativi sull'analisi statistica o sui risultati statistici connessi al trattamento. In particolare, non si procede alla variazione se le modifiche richieste contrastano con le classificazioni e con le metodologie statistiche adottate in conformità alle norme internazionali comunitarie e nazionali.

Art. 14. Regole di condotta

1. I responsabili e gli incaricati del trattamento che, anche per motivi di lavoro, studio e ricerca abbiano legittimo accesso ai dati personali trattati per scopi statistici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti all'atto della progettazione del trattamento;
b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute;
c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attività statistica o di attività ad essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui;
d) il lavoro svolto deve essere oggetto di adeguata documentazione;
e) le conoscenze professionali in materia di protezione dei dati personali devono essere adeguate costantemente all'evoluzione delle metodologie e delle tecniche;
f) la comunicazione e la diffusione dei risultati statistici devono essere favorite, in relazione alle esigenze conoscitive degli utenti, purché nel rispetto delle norme sulla protezione dei dati personali.

2. I responsabili e gli incaricati del trattamento di cui al comma 1 sono tenuti a conformarsi alle disposizioni del presente codice, anche quando non siano vincolati al rispetto del segreto d'ufficio o del segreto professionale. I titolari del trattamento adottano le misure opportune per garantire la conoscenza di tali disposizioni da parte dei responsabili e degli incaricati medesimi.

3. I comportamenti non conformi alle regole di condotta dettate dal presente codice devono essere immediatamente segnalati al responsabile o al titolare del trattamento.

A.4. Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Visto l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visto l'art. 12 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto l'art. 106, comma 1, del Codice il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi statistici o scientifici;

Visto l'art. 106, comma 2, del medesimo Codice relativo a taluni profili che, sulla base di alcune garanzie, devono essere individuati dal codice di deontologia e di buona condotta per i trattamenti di dati per scopi statistici e scientifici;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla *Gazzetta Ufficiale* della Repubblica italiana 25 febbraio 2000, n. 46, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi al trattamento di dati personali per scopi statistici e di ricerca scientifica ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività a darne comunicazione al Garante;

Viste le comunicazioni pervenute al Garante in risposta al citato provvedimento del 10 febbraio 2000, con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare all'adozione dei codici e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro, composto, in particolare, da rappresentanti dei seguenti soggetti: Conferenza dei rettori delle università italiane; Associazione italiana di epidemiologia; Associazione italiana di sociologia; Consiglio italiano per le scienze sociali; Società italiana degli economisti; Società italiana di biometria; Società italiana di demografia storica; Società italiana di igiene, medicina preventiva e sanità pubblica; Società italiana di statistica; Società italiana di statistica medica ed epidemiologia clinica; Associazione tra istituti di ricerche di mercato, sondaggi di opinione, ricerca sociale;

Considerato che il testo del codice è stato oggetto di ampia diffusione anche attraverso la sua pubblicazione sul sito Internet di questa Autorità, resa nota tramite avviso sulla

(*) Provvedimento del Garante n. 2 del 16 giugno 2004, *G.U.* 14 agosto 2004, n. 190.

Gazzetta Ufficiale della Repubblica italiana 20 maggio 2004, n. 117, al fine di favorire il più ampio dibattito e di permettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

Viste le osservazioni pervenute secondo quanto disposto dal citato avviso;

Rilevato che il rispetto delle disposizioni contenute nel codice di deontologia e di buona condotta costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici (art. 12, comma 3, del Codice);

Constatata la conformità del codice di deontologia e di buona condotta alle leggi e ai regolamenti in materia di protezione dei dati personali, anche in relazione a quanto previsto dagli artt. 12 e 104 e seguenti del Codice;

Considerato che, ai sensi dell'art. 12, comma 2, del Codice, il codice di deontologia e di buona condotta deve essere pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, riportato nell'allegato A) al medesimo Codice;

Vista la documentazione in atti;

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

Relatore il prof. Gaetano Rasi;

Dispone:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, che figura in allegato, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana, nonché al Ministro della giustizia per essere riportato nell'allegato A) al Codice.

Roma, 16 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI PER SCOPI STATISTICI E SCIENTIFICI

sottoscritto da:
- Conferenza dei rettori delle università italiane
- Associazione italiana di epidemiologia
- Associazione italiana di sociologia
- Consiglio italiano per le scienze sociali
- Società italiana degli economisti
- Società italiana di biometria
- Società italiana di demografia storica
- Società italiana di igiene, medicina preventiva e sanità pubblica
- Società italiana di statistica
- Società italiana di statistica medica ed epidemiologia clinica
- Associazione tra istituti di ricerche di mercato, sondaggi di opinione, ricerca sociale

Preambolo

I sottoindicati soggetti pubblici e privati sottoscrivono il presente codice, adottato sulla base di quanto previsto dall'art. 106 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali (di seguito denominato "decreto"), sulla base delle seguenti premesse:

1) le disposizioni del presente codice di deontologia e di buona condotta sono volte ad assicurare l'equilibrio tra i diritti e le libertà fondamentali della persona, in particolare il diritto alla protezione dei dati personali e il diritto alla riservatezza, con le esigenze della statistica e della ricerca scientifica, quali risultano dal principio della libertà di ricerca costituzionalmente garantito, presupposto per lo sviluppo della scienza, per il miglioramento delle condizioni di vita degli individui e per la crescita di una società democratica;

2) i ricercatori, singoli o associati, che operano nell'ambito di università, enti ed istituti di ricerca e società scientifiche, conformano al presente codice ogni fase dei trattamenti di dati personali effettuati a fini statistici o scientifici, indipendentemente dalla sottoscrizione del codice stesso da parte dei rispettivi enti e società scientifiche;

3) nell'applicazione del presente codice, i soggetti che ne sono destinatari osservano i princìpi contenuti nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, ratificata con legge 4 agosto 1955, n. 848, nella direttiva 95/46/Ce del Parlamento europeo e del Consiglio dell'Unione europea, nelle Raccomandazioni del Consiglio d'Europa R (83)10 adottata il 23 settembre del 1983 e R (97)18 adottata il 30 settembre 1997, nonché nelle altre disposizioni normative comunitarie e internazionali relative al trattamento dei dati personali a fini statistici e scientifici. Essi operano nel rispetto dei princìpi di pertinenza e di non eccedenza, intesa come non ridondanza del trattamento progettato rispetto agli scopi perseguiti, avuto riguardo ai dati disponibili ed ai trattamenti già effettuati dallo stesso titolare;

4) per quanto non disciplinato nel presente codice, si applicano le disposizioni previste dalla normativa in materia di dati personali, anche in relazione alla natura pubblica o privata del soggetto titolare del trattamento (artt. 18 e s. e 23 e s. del decreto). In particolare, i dati personali trattati per scopi statistici o scientifici non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura;

5) per trattamento per scopi statistici si intende qualsiasi trattamento effettuato per le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici (art. 4 del decreto);

6) per trattamento per scopi scientifici si intende qualsiasi trattamento effettuato per le

finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore (art. 4 del decreto);

7) gli enti e i soggetti che applicano il presente codice osservano il principio di imparzialità e di non discriminazione nei confronti degli altri soggetti che trattano i dati per scopi statistici o scientifici. La sottoscrizione del presente codice è effettuata avendo riguardo, in particolare, alla rilevanza di tale principio in materia di comunicazione per scopi statistici o scientifici di dati depositati in archivi pubblici o che sono stati trattati sulla base di finanziamenti pubblici;

8) il decreto e il presente codice non si applicano ai dati anonimi;

9) ai trattamenti finalizzati alla realizzazione di attività di informazione commerciale e di comunicazione commerciale, nonché alle correlate ricerche di mercato si applicano le disposizioni dei codici di deontologia e di buona condotta previsti dagli articoli 118 e 140 del decreto.

CAPO I - AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

Art. 1. Definizioni

1. Ai fini del presente codice si applicano le definizioni elencate nell'art. 4 del decreto con le seguenti integrazioni:

a) "risultato statistico", l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;
b) "unità statistica", l'entità alla quale sono riferiti o riferibili i dati trattati;
c) "dato identificativo indiretto", un insieme di modalità di caratteri associati o associabili ad una unità statistica che ne consente l'identificazione con l'uso di tempi e risorse ragionevoli, secondo i princìpi di cui all'art. 4;
d) "variabile pubblica", il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;
e) "istituto o ente di ricerca", un organismo pubblico o privato per il quale la finalità di statistica o di ricerca scientifica risulta dagli scopi dell'istituzione e la cui attività scientifica è documentabile;
f) "società scientifica", un'associazione che raccoglie gli studiosi di un ambito disciplinare, ivi comprese le relative associazioni professionali.

2. Salvo quando diversamente specificato, il riferimento a trattamenti per scopi statistici si intende comprensivo anche dei trattamenti per scopi scientifici.

Art. 2. Ambito di applicazione

1. Il presente codice si applica all'insieme dei trattamenti effettuati per scopi statistici e scientifici –conformemente agli *standard* metodologici del pertinente settore disciplinare–, di cui sono titolari università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e soci di dette società scientifiche.

2. Il presente codice non si applica ai trattamenti per scopi statistici e scientifici connessi con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attività comparabili in termini di significativa ricaduta personalizzata sull'interessato, che restano regolati dalle pertinenti disposizioni.

Art. 3. Presupposti dei trattamenti

1. La ricerca è effettuata sulla base di un progetto redatto conformemente agli *standard* metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici.

2. Il progetto di ricerca di cui al comma 1, inoltre:

a) specifica le misure da adottare nel trattamento di dati personali, al fine di garantire il rispetto del presente codice, nonché della normativa in materia di protezione dei dati personali;
b) individua gli eventuali responsabili del trattamento;
c) contiene una dichiarazione di impegno a conformarsi alle disposizioni del presente codice sottoscritta dai soggetti coinvolti. Un'analoga dichiarazione è sottoscritta anche dai soggetti –ricercatori, responsabili e incaricati del trattamento– che fossero coinvolti nel prosieguo della ricerca, e conservata conformemente a quanto previsto al comma 3.

3. Il titolare deposita il progetto presso l'università o ente di ricerca o società scientifica cui afferisce, la quale ne cura la conservazione, in forma riservata (essendo la consultazione del progetto possibile ai soli fini dell'applicazione della normativa in materia di dati personali), per cinque anni dalla conclusione programmata della ricerca.

4. Nel trattamento di dati idonei a rivelare lo stato di salute, i soggetti coinvolti osservano le regole di riservatezza e di sicurezza cui sono tenuti gli esercenti le professioni sanitarie o regole di riservatezza e sicurezza comparabili.

Art. 4. Identificabilità dell'interessato

1. Agli effetti dell'applicazione del presente codice:
a) un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati identificativi della medesima;
b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
- risorse economiche;
- risorse di tempo;
- archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
- archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;
- risorse *hardware* e *software* per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al *software* di controllo adottati;
- conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;
c) in caso di comunicazione e di diffusione, l'interessato può ritenersi non identificabile se il rischio di identificazione, in termini di probabilità di identificare l'interessato stesso tenendo conto dei dati comunicati o diffusi, è tale da far ritenere sproporzionati i mezzi eventualmente necessari per procedere all'identificazione rispetto alla lesione o al pericolo di lesione dei diritti degli interessati che può derivarne, avuto altresì riguardo al vantaggio che se ne può trarre.

Art. 5. Criteri per la valutazione del rischio di identificazione

1. Ai fini della comunicazione e diffusione di dati, la valutazione del rischio di identificazione tiene conto dei seguenti criteri:
a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;
b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;
c) i risultati statistici relativi a sole variabili pubbliche non sono soggette alla regola della soglia;

d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;
e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;
f) si presume adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentano la medesima modalità di una variabile.

CAPO II - INFORMATIVA, COMUNICAZIONE E DIFFUSIONE

Art. 6. Informativa

1. Nella raccolta di dati per uno scopo statistico, nell'ambito delle informazioni di cui all'art. 13 del decreto è rappresentata all'interessato l'eventualità che i dati personali possono essere conservati e trattati per altri scopi statistici o scientifici, per quanto noto adeguatamente specificati anche con riguardo alle categorie di soggetti ai quali i dati potranno essere comunicati.

2. Nella raccolta di dati per uno scopo statistico, l'informativa alla persona presso la quale i dati sono raccolti può essere differita per la parte riguardante le specifiche finalità e le modalità del trattamento cui sono destinati i dati, qualora ciò risulti necessario per il raggiungimento dell'obiettivo dell'indagine –in relazione all'argomento o alla natura della stessa– e il trattamento non riguardi dati sensibili o giudiziari. In tali casi, l'informativa all'interessato è completata non appena cessano i motivi che ne avevano ritardato la comunicazione, a meno che ciò risulti irragionevole o comporti un impiego di mezzi manifestamente sproporzionato. Il soggetto responsabile della ricerca redige un documento –successivamente conservato per tre anni dalla conclusione della raccolta e reso disponibile agli interessati che esercitano i diritti di cui all'art. 7 del decreto–, in cui sono indicate le specifiche motivazioni per le quali si è ritenuto di differire l'informativa, la parte di informativa differita, nonché le modalità seguite per informare gli interessati quando sono venuti meno i motivi che avevano giustificato il differimento, ovvero le ragioni portate per il mancato completamento dell'informativa.

3. Quando, con riferimento a parametri scientificamente attendibili, gli obiettivi dell'indagine, la natura dei dati e le circostanze della raccolta 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 può essere data per il tramite del soggetto rispondente, purché il trattamento non riguardi dati sensibili o giudiziari.

4. Quando i dati sono raccolti presso terzi, ovvero il trattamento effettuato per scopi statistici o scientifici riguarda dati raccolti per altri scopi, e l'informativa comporta uno sforzo sproporzionato rispetto al diritto tutelato, il titolare adotta forme di pubblicità con le seguenti modalità:

- per trattamenti riguardanti insiemi numerosi di soggetti distribuiti sull'intero territorio nazionale, inserzione su almeno un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale;
- per trattamenti riguardanti insiemi numerosi di soggetti distribuiti su un'area regionale (o provinciale), inserzione su un quotidiano di larga diffusione regionale (o provinciale) o annuncio presso un'emittente radiotelevisiva a diffusione regionale (o provinciale);
- per trattamenti riguardanti insiemi di specifiche categorie di soggetti, identificate da particolari caratteristiche demografiche e/o da particolari condizioni formative o occupazionali o analoghe, inserzione in strumenti informativi di cui gli interessati sono normalmente destinatari.

Della modalità di pubblicità adottata, il titolare dà preventiva informazione al Garante.

5. Qualora il titolare ritenga di non utilizzare le forme di pubblicità di cui al comma 4, anche in considerazione della natura dei dati raccolti o delle modalità del trattamento, ovvero degli oneri che comportano rispetto al tipo di ricerca svolta, il titolare medesimo può individuare idonee forme di pubblicità da comunicare preventivamente al Garante, il quale può, in ogni caso, prescrivere eventuali misure ed accorgimenti.

Art. 7. Consenso

1. Il trattamento per scopi statistici o scientifici può essere effettuato da un soggetto privato senza il consenso dell'interessato qualora non riguardi dati sensibili o giudiziari e l'informativa ai sensi dell'art. 13 del decreto, nella parte riguardante la natura obbligatoria o meno del conferimento dei dati, evidenzi in dettaglio e specificamente le ragioni per le quali il conferimento è facoltativo.

Art. 8. Comunicazione e diffusione dei dati

1. È consentito diffondere anche mediante pubblicazione risultati statistici soltanto in forma aggregata ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti, salvo che la diffusione riguardi variabili pubbliche.

2. I dati personali trattati per un determinato scopo statistico possono essere comunicati, privi di dati identificativi, a un'università o istituto o ente di ricerca o a un ricercatore per altri scopi statistici chiaramente determinati per iscritto nella richiesta dei dati. Il soggetto richiedente, nel predisporre il pertinente progetto di ricerca ai sensi dell'art. 3, si impegna a non effettuare trattamenti per fini diversi da quelli indicati nella richiesta e a non comunicare ulteriormente i dati a terzi; allega inoltre al progetto copia della richiesta di comunicazione. Il soggetto richiesto, titolare del trattamento originario, deposita la richiesta di comunicazione e il connesso progetto presso l'università o ente di ricerca o società scientifica cui afferisce, la quale ne cura la conservazione, in forma riservata, per cinque anni dalla conclusione programmata della ricerca.

3. Nel caso in cui il richiedente dichiari che non è possibile conseguire altrimenti il risultato statistico di interesse, dandone espressa motivazione nella richiesta di cui al precedente comma 2, è consentita anche la comunicazione dei dati identificativi. Il soggetto richiesto, valutata la motivazione, fornisce i dati nel rispetto del principio di pertinenza e di stretta necessità. Resta fermo quanto previsto dall'art. 9.

4. Le disposizioni di cui ai commi 2 e 3 si applicano anche alla comunicazione, e al conseguente trasferimento anche temporaneo, di dati personali a università o istituti o enti di ricerca o ricercatori residenti in un Paese appartenente all'Unione europea o il cui ordinamento assicuri comunque un livello di tutela delle persone adeguato.

5. Quando il trattamento per un determinato scopo statistico comporta il trasferimento anche temporaneo dei dati personali in un Paese, non appartenente all'Unione europea, il cui ordinamento non assicura un livello di tutela delle persone adeguato, il trasferimento è consentito sulla base di garanzie per i diritti dell'interessato comparabili a quelle del presente codice, prestate dall'ente o dal ricercatore destinatario del trasferimento medesimo tramite un contratto redatto secondo una tipologia autorizzata dal Garante ai sensi dell'art. 40 del decreto, anche su proposta di enti e società scientifiche.

Art. 9. Trattamento dei dati sensibili o giudiziari

1. I dati sensibili o giudiziari trattati per scopi statistici e scientifici devono essere di regola in forma anonima.

2. Quando gli scopi statistici e scientifici, legittimi e specifici, del trattamento di dati sensibili o giudiziari non possono essere raggiunti senza l'identificazione anche temporanea degli interessati, il titolare adotta specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato.

3. Quando i dati di cui al comma 1 sono contenuti in elenchi, registri o banche dati tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente non intelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

4. I soggetti di cui all'art. 2, comma 1, aventi natura privata possono trattare dati sensibili per scopi statistici e scientifici quando:

a) l'interessato ha espresso liberamente il proprio consenso sulla base degli elementi previsti per l'informativa;

b) il consenso è manifestato per iscritto. Quando la raccolta dei dati sensibili è effettuata con modalità –quali interviste telefoniche o assistite da elaboratore o simili– che rendono particolarmente gravoso per l'indagine acquisirlo per iscritto, il consenso, purché esplicito, può essere documentato per iscritto. In tal caso, la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso è conservata dal titolare del trattamento per tre anni;

c) il trattamento risulti preventivamente autorizzato dal Garante, a seguito di specifica richiesta ai sensi dell'art. 26, comma 1, del decreto ovvero sulla base di un'autorizzazione generale relativa a determinate categorie di titolari o di trattamenti, rilasciata ai sensi dell'art. 40 del decreto, anche su proposta di enti e società scientifiche.

5. Il trattamento di dati giudiziari da parte dei soggetti di cui all'art. 2, comma 1, aventi natura privata è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante emanato ai sensi dell'art. 27 del decreto.

6. I soggetti cui all'art. 2, comma 1, aventi natura pubblica possono trattare dati sensibili o giudiziari:

a) per scopi scientifici, nel rispetto dell'art. 22 del decreto, qualora provvedano con atto di natura regolamentare ad individuare e rendere pubblici i tipi di dati e di operazioni strettamente pertinenti e necessarie in relazione alle finalità perseguite nei singoli casi, aggiornando tale individuazione periodicamente, secondo quanto previsto dall'art. 20, commi 2 e 4, del decreto;

b) per scopi statistici, nel rispetto dell'art. 22 del decreto, qualora siano soddisfatte le condizioni di cui all'art. 20, commi 2, 3 e 4 del decreto medesimo.

Art. 10. Dati genetici

1. Il trattamento di dati genetici è consentito nei soli casi e modi previsti da apposita autorizzazione del Garante ai sensi dell'art. 90 del decreto.

Art. 11. Disposizioni particolari per la ricerca medica, biomedica ed epidemiologica

1. La ricerca medica, biomedica ed epidemiologica è sottoposta all'applicazione del presente codice nei limiti di cui all'art. 2, comma 2.

2. La ricerca di cui al comma 1 si svolge nel rispetto degli orientamenti e delle disposizioni internazionali e comunitarie in materia, quali la Convenzione sui diritti dell'uomo e sulla biomedicina del 4 aprile 1997, ratificata con legge 28 marzo 2001, n. 145, la Raccomandazione del Consiglio d'Europa R(97)5 adottata il 13 febbraio 1997 relativa alla protezione dei dati sanitari e la dichiarazione di Helsinki dell'Associazione medica mondiale sui princìpi per la ricerca che coinvolge soggetti umani.

3. Nella ricerca di cui al comma 1, l'informativa mette in grado gli interessati di distinguere le attività di ricerca da quelle di tutela della salute.

4. Nel manifestare il proprio consenso ad un'indagine medica o epidemiologica, l'interessato è richiesto di dichiarare se vuole conoscere o meno eventuali scoperte inattese che emergano a suo carico durante la ricerca. In caso positivo, l'interessato è informato secondo quanto previsto dall'art. 84 del decreto. Quando, per i motivi di cui al successivo comma 5, il consenso non può essere richiesto, tali eventi sono comunque comunicati all'interessato nel rispetto dell'art. 84 del decreto qualora rivestano un'importanza rilevante per la tutela della salute dello stesso.

5. Nella ricerca di cui al comma 1, il consenso dell'interessato non è necessario quando, ai sensi dell'art. 110 del decreto, sono soddisfatti i seguenti requisiti:

a) non è possibile informare l'interessato per motivi etici (ignoranza dell'interessato

sulla propria condizione), ovvero per motivi metodologici (necessità di non comunicare al soggetto le ipotesi dello studio o la sua posizione di elezione), ovvero per motivi di impossibilità organizzativa;

b) il programma di ricerca è stato oggetto di motivato parere favorevole del competente comitato etico;

c) il trattamento è autorizzato dal Garante, anche ai sensi dell'art. 40 del decreto anche su proposta di enti e società scientifiche pertinenti.

Art. 12. Attività di controllo

1. Le università, gli altri istituti o enti di ricerca e le società scientifiche conservano la documentazione relativa ai progetti di ricerca presentati e agli impegni sottoscritti dai ricercatori ai sensi dell'art. 3, commi 1 e 2, e dell'art. 8, comma 2 del presente codice.

2. Gli enti di cui al comma 1:

a) assicurano la diffusione e il rispetto del presente codice fra tutti coloro che, all'interno o all'esterno dell'organizzazione, sono in qualunque forma coinvolti nel trattamento dei dati personali realizzato nell'ambito delle ricerche, anche adottando opportune misure sulla base dei propri statuti e regolamenti;

b) segnalano al Garante le violazioni del codice di cui vengono a conoscenza.

CAPO III - SICUREZZA E REGOLE DI CONDOTTA

Art. 13. Raccolta dei dati

1. I soggetti di cui all'art. 2, comma 1, pongono specifica attenzione nella selezione del personale incaricato della raccolta dei dati e nella definizione dell'organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del presente codice e la tutela dei diritti degli interessati.

2. Il personale incaricato della raccolta si attiene alle disposizioni contenute nel presente codice e alle istruzioni ricevute. In particolare:

a) rende nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;

b) fornisce le informazioni di cui all'art. 13 del decreto ed all'art. 6 del presente codice, nonché ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici ed indebite pressioni;

c) non svolge contestualmente presso gli stessi interessati attività di rilevazione di dati personali per conto di più titolari, salvo espressa autorizzazione;

d) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;

e) assicura una particolare diligenza nella raccolta di dati sensibili o giudiziari.

Art. 14. Conservazione dei dati

1. I dati personali possono essere conservati per scopi statistici o scientifici anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, in conformità all'art. 99 del decreto. In tali casi, i dati identificativi possono essere conservati fino a quando risultino necessari per:

a) indagini continue e longitudinali;

b) indagini di controllo, di qualità e di copertura;

c) definizione di disegni campionari e selezione di unità di rilevazione;

d) costituzione di archivi delle unità statistiche e di sistemi informativi;

e) altri casi in cui ciò risulti essenziale e adeguatamente documentato per le finalità perseguite.

2. Nei casi di cui al comma 1, i dati identificativi sono conservati separatamente da ogni altro dato, in modo da consentirne differenti livelli di accesso, salvo ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

Art. 15. Misure di sicurezza

1. Nell'adottare le misure di sicurezza dei dati e dei sistemi di cui agli artt. 31 e seguenti del decreto e al disciplinare tecnico contenuto nel relativo Allegato B), i titolari dei trattamenti di dati per scopi statistici curano anche i livelli di accesso ai dati personali con riferimento alla natura dei dati stessi ed alle funzioni dei soggetti coinvolti nei trattamenti.

Art. 16. Esercizio dei diritti dell'interessato

1. In caso di esercizio dei diritti di cui all'art. 7 del decreto in riferimento a dati trattati per scopi statistici e scientifici, l'interessato può accedere agli archivi che lo riguardano per chiederne l'aggiornamento, la rettifica o l'integrazione, sempre che tale operazione non risulti impossibile per la natura o lo stato del trattamento o comporti un impiego di mezzi manifestamente sproporzionato.

2. Qualora tali modifiche non producano effetti significativi sui risultati statistici connessi al trattamento, il responsabile del trattamento provvede ad annotare, in appositi spazi o registri, le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio.

Art. 17. Regole di condotta

1. I responsabili e gli incaricati del trattamento che, per motivi di lavoro e ricerca, abbiano legittimo accesso ai dati personali trattati per scopi statistici e scientifici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti nel progetto di ricerca di cui all'art. 3;

b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute;

c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attività statistica o di attività ad essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui;

d) il lavoro svolto è oggetto di adeguata documentazione;

e) le conoscenze professionali in materia di protezione dei dati personali sono adeguate costantemente all'evoluzione delle metodologie e delle tecniche;

f) la comunicazione e la diffusione dei risultati statistici sono favorite, in relazione alle esigenze conoscitive della comunità scientifica e dell'opinione pubblica, nel rispetto della disciplina sulla protezione dei dati personali;

g) i comportamenti non conformi alle regole di condotta dettate dal presente codice sono immediatamente segnalati al responsabile o al titolare del trattamento.

Art. 18. Adeguamento

1. La corrispondenza delle disposizioni del codice alla normativa, anche di carattere internazionale, introdotta in materia di protezione dei dati personali trattati a fini di statistica e di ricerca scientifica è verificata nel tempo anche su segnalazione dei soggetti che lo hanno sottoscritto. Ciò ai fini dell'introduzione nel codice medesimo delle modifiche necessarie al fine del coordinamento con dette fonti, ovvero, qualora tali modifiche incidano in maniera apprezzabile sulla disciplina del presente codice, del pronunciamento di un nuovo codice ai sensi dell'art. 12 del decreto.

Art. 19. Entrata in vigore

1. Il presente codice si applica a decorrere dal 1° ottobre 2004.

A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

VISTO l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

VISTI gli artt. 12 e 154, comma 1, lett. *e*) del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), i quali attribuiscono al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

VISTO l'art. 117 del Codice con il quale è stato demandato al Garante il compito di promuovere la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo, nonché riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati;

VISTO il provvedimento generale del Garante adottato il 31 luglio 2002 (in *Bollettino* n. 30/2002, p. 47) con il quale, nelle more dell'adozione del predetto codice di deontologia e di buona condotta, sono state nel frattempo prescritte, ai soggetti privati che gestiscono sistemi informativi di rilevazione di rischi creditizi, nonché alle banche e società finanziarie che vi accedono, alcune prime misure da adottare al fine di conformare il relativo trattamento ai principi in materia di protezione dei dati personali;

VISTO il provvedimento del 10 aprile 2002, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana 8 maggio 2002, n. 106, con il quale il Garante ha promosso la sottoscrizione del codice di deontologia e di buona condotta;

VISTE le comunicazioni pervenute al Garante in risposta al citato provvedimento del 10 aprile 2002, con le quali diversi soggetti privati, associazioni di categoria ed associazioni di consumatori hanno manifestato la volontà di partecipare all'adozione di tale codice e rilevato che si è anche formato un apposito gruppo di lavoro composto da rappresentanti dei predetti soggetti;

CONSIDERATO che il testo del codice di deontologia e di buona condotta è stato oggetto di ampia diffusione anche attraverso la sua pubblicazione sul sito Internet di questa Autorità, resa nota tramite avviso sulla *Gazzetta Ufficiale* della Repubblica italiana 18 agosto 2004, n. 193, al fine di favorire il più ampio dibattito e di permettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

(*) Provvedimento del Garante n. 8 del 16 novembre 2004, *G.U.* 23 dicembre 2004, n. 300, come modificato dall'*errata corrige* pubblicata *G.U.* 9 marzo 2005, n. 56

VISTE le osservazioni pervenute a seguito di tale avviso e le modifiche apportate allo schema del codice, poi sottoscritto il 12 novembre 2004;

CONSTATATA la conformità del codice di deontologia e di buona condotta alle leggi ed ai regolamenti anche in relazione a quanto previsto dall'art. 12 del Codice;

VISTO l'art. 5 del codice di deontologia e di buona condotta;

CONSIDERATO che dalle predette consultazioni sono emersi anche alcuni dettagli operativi che rendono necessario indicare modalità di attuazione idonee ed efficaci delle disposizioni in materia di informativa da rendere agli interessati ai sensi dell'art. 13 del Codice;

RITENUTO pertanto indispensabile prescrivere, ai sensi dell'art. 154, comma 1, lett. *c)*, del Codice, un modello unico per l'informativa, basato su espressioni chiare, semplici e di agevole comprensione, e da adottare da tutti i soggetti privati titolari dei trattamenti di dati personali effettuati, in modo effettivo ed uniforme;

RILEVATO che il rispetto delle disposizioni contenute nel codice di deontologia e di buona condotta costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici (art. 12, comma 3, del Codice);

RILEVATO altresì che i titolari del trattamento sono tenuti a fare uso del modello unico di informativa che il presente provvedimento prescrive, al quale potranno apportarvi eventuali modifiche sostanziali o integrazioni con esso compatibili, unicamente previo assenso di questa Autorità, salvi eventuali adattamenti meramente formali;

CONSIDERATO che, ai sensi dell'art. 12, comma 2, del Codice, il codice di deontologia e di buona condotta deve essere pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, riportato nell'allegato A) al medesimo Codice;

VISTA la documentazione in atti;

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

Relatore il dott. Mauro Paissan;

TUTTO CIÒ PREMESSO IL GARANTE:

a) dispone la trasmissione del codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti, che figura in allegato, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana, nonché al Ministro della giustizia per essere riportato nell'allegato A) al Codice;

b) individua, in allegato alla presente deliberazione, il modello di informativa contenente i requisiti minimi che, ai sensi dell'art. 154, comma 1, lett. *c)*, del Codice, prescrive a tutti i titolari del trattamento interessati di utilizzare nei termini di cui in motivazione.

Roma, 16 novembre 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITÀ E PUNTUALITÀ NEI PAGAMENTI

Preambolo

I sottoindicati soggetti privati sottoscrivono il presente codice di deontologia e di buona condotta sulla base delle seguenti premesse:

1) il trattamento di dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di credito al consumo o comunque riguardanti l'affidabilità e la puntualità dei pagamenti, deve svolgersi nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identità personale;
2) con il presente codice sono individuate adeguate garanzie e modalità di trattamento a tutela dei diritti degli interessati da osservare nel perseguire finalità di tutela del credito e di contenimento dei relativi rischi, in modo da agevolare anche l'accesso al credito al consumo e ridurre il rischio di eccessivo indebitamento da parte degli interessati;
3) la sottoscrizione del presente codice è promossa dal Garante per la protezione dei dati personali nell'ambito delle associazioni rappresentative degli operatori del settore, ai sensi degli artt. 12 e 117 del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196);
4) tutti coloro che utilizzano dati personali per le finalità sopra indicate devono osservare le regole di comportamento stabilite dal presente codice come condizione essenziale per la liceità e la correttezza del trattamento;
5) gli stessi operatori del settore devono rispettare, altresì, le garanzie previste dal predetto Codice, in particolare in tema di manifestazione del consenso e di altri presupposti di liceità;
6) il presente codice non riguarda sistemi informativi di cui sono titolari soggetti pubblici e, in particolare, il servizio di centralizzazione dei rischi gestito dalla Banca d'Italia (artt. 13, 53, comma 1, lett. *b*), 60, comma 1, 64, 67, comma 1, lett. *b*), 106, 107, 144 e 145 del decreto legislativo 1° settembre 1993, n. 385 –Testo unico delle leggi in materia bancaria e creditizia–; delibera Cicr del 29 marzo 1994; provvedimento Banca d'Italia 10 agosto 1995; circolare Banca d'Italia 11 febbraio 1991, n. 139 e successivi aggiornamenti). Al sistema centralizzato di rilevazione dei rischi di importo contenuto istituito con deliberazione Cicr del 3 maggio 1999 (in *Gazzetta Ufficiale* 8 luglio 1999, n. 158) si applicano alcuni principi stabiliti dal presente codice in tema di informativa agli interessati e di esercizio dei diritti, in quanto compatibili con la specifica disciplina di riferimento (v., in particolare, le istruzioni della Banca d'Italia in *Gazzetta Ufficiale* 21 novembre 2000, n. 272).

Art. 1. Definizioni

1. Ai fini del presente codice di deontologia e di buona condotta, si applicano le definizioni elencate nel Codice in materia di protezione dei dati personali (art. 4 decreto legislativo 30 giugno 2003, n. 196), di seguito denominato "Codice". Ai medesimi fini, si intende inoltre per:

a) "richiesta/rapporto di credito": qualsiasi richiesta o rapporto riguardanti la concessione, nell'esercizio di un'attività commerciale o professionale, di credito sotto forma di dilazione di pagamento, di finanziamento o di altra analoga facilitazione finanziaria ai sensi del Testo unico delle leggi in materia bancaria e creditizia (decreto legislativo 1° settembre 1993, n. 385);
b) "regolarizzazione degli inadempimenti": l'estinzione delle obbligazioni pecuniarie inadempiute (derivanti sia da un mancato pagamento, sia da un ritardo), senza perdite o residui anche a titolo di interessi e spese o comunque a seguito di vicende estintive diverse dall'adempimento, in particolare a seguito di transazioni o concordati;
c) "sistema di informazioni creditizie": ogni banca di dati concernenti richieste/rapporti di credito, gestita in modo centralizzato da una persona giuridica, un ente, un'associazione o un altro organismo in ambito privato e consultabile solo dai soggetti che comunicano le informazioni in essa registrate e che partecipano al

relativo sistema informativo. Il sistema può contenere, in particolare:

1) informazioni creditizie di tipo negativo, che riguardano soltanto rapporti di credito per i quali si sono verificati inadempimenti;
2) informazioni creditizie di tipo positivo e negativo, che attengono a richieste/rapporti di credito a prescindere dalla sussistenza di inadempimenti registrati nel sistema al momento del loro verificarsi;

d) "gestore": il soggetto privato titolare del trattamento dei dati personali registrati in un sistema di informazioni creditizie e che gestisce tale sistema stabilendone le modalità di funzionamento e di utilizzazione;

e) "partecipante": il soggetto privato titolare del trattamento dei dati personali raccolti in relazione a richieste/rapporti di credito, che in virtù di contratto o accordo con il gestore partecipa al relativo sistema di informazioni creditizie e può utilizzare i dati presenti nel sistema, obbligandosi a comunicare al gestore i predetti dati personali relativi a richieste/rapporti di credito in modo sistematico, in un quadro di reciprocità nello scambio di dati con gli altri partecipanti. Fatta eccezione di soggetti che esercitano attività di recupero crediti, il partecipante può essere:

1) una banca;
2) un intermediario finanziario;
3) un altro soggetto privato che, nell'esercizio di un'attività commerciale o professionale, concede una dilazione di pagamento del corrispettivo per la fornitura di beni o servizi;

f) "consumatore": la persona fisica che, in relazione ad una richiesta/rapporto di credito, agisce per scopi non riferibili all'attività imprenditoriale o professionale eventualmente svolta;

g) "tempo di conservazione dei dati": il periodo nel quale i dati personali relativi a richieste/rapporti di credito rimangono registrati in un sistema di informazioni creditizie ed utilizzabili dai partecipanti per le finalità di cui al presente codice;

h) "tecniche o sistemi automatizzati di *credit scoring*": le modalità di organizzazione, aggregazione, raffronto od elaborazione di dati personali relativi a richieste/rapporti di credito, consistenti nell'impiego di sistemi automatizzati basati sull'applicazione di metodi o modelli statistici per valutare il rischio creditizio, e i cui risultati sono espressi in forma di giudizi sintetici, indicatori numerici o punteggi, associati all'interessato, diretti a fornire una rappresentazione, in termini predittivi o probabilistici, del suo profilo di rischio, affidabilità o puntualità nei pagamenti.

Art. 2. Finalità del trattamento

1. Il trattamento dei dati personali contenuti in un sistema di informazioni creditizie è effettuato dal gestore e dai partecipanti esclusivamente per finalità correlate alla tutela del credito e al contenimento dei relativi rischi e, in particolare, per valutare la situazione finanziaria e il merito creditizio degli interessati o, comunque, la loro affidabilità e puntualità nei pagamenti.

2. Non può essere perseguito alcun altro scopo, specie se relativo a ricerche di mercato e promozione, pubblicità o vendita diretta di prodotti o servizi.

Art. 3. Requisiti e categorie dei dati

1. Il trattamento effettuato nell'ambito di un sistema di informazioni creditizie riguarda solo dati riferiti al soggetto che chiede di instaurare o è parte di un rapporto di credito con un partecipante e al soggetto coobbligato, anche in solido, la cui posizione è chiaramente distinta da quella del debitore principale.

2. Il trattamento non può riguardare i dati sensibili e quelli giudiziari, e concerne dati personali di tipo obiettivo, strettamente pertinenti e non eccedenti rispetto alle finalità perseguite, relativi ad una richiesta/rapporto di credito, e concernenti anche ogni vicenda intervenuta a qualsiasi titolo o causa fino alla regolarizzazione degli inadempimenti, nel rispetto dei tempi di conservazione stabiliti dall'art. 6.

3. Per ogni richiesta/rapporto di credito segnalato ad un sistema di informazioni creditizie possono essere trattate le seguenti categorie di dati, che il gestore indica in un elenco

reso agevolmente disponibile su un proprio sito della rete di comunicazione, nonché comunica analiticamente agli interessati su loro richiesta:

a) dati anagrafici, codice fiscale o partita Iva;
b) dati relativi alla richiesta/rapporto di credito, descrittivi, in particolare, della tipologia di contratto, dell'importo del credito, delle modalità di rimborso e dello stato della richiesta o dell'esecuzione del contratto;
c) dati di tipo contabile relativi ai pagamenti, al loro andamento periodico, all'esposizione debitoria anche residua e alla sintesi dello stato contabile del rapporto;
d) dati relativi ad attività di recupero del credito o contenziose, alla cessione del credito o a eccezionali vicende che incidono sulla situazione soggettiva o patrimoniale di imprese, persone giuridiche o altri enti.

4. Le codifiche ed i criteri eventualmente utilizzati per registrare dati in un sistema di informazioni creditizie e per facilitarne il trattamento sono diretti esclusivamente a fornire una rappresentazione oggettiva e corretta degli stessi dati, nonché delle vicende del rapporto di credito segnalato. L'utilizzo di tali codifiche e criteri è accompagnato da precise indicazioni circa il loro significato, fornite dal gestore, osservate dai partecipanti e rese agevolmente disponibili da entrambi, anche a richiesta degli interessati.

5. Nel sistema di informazioni creditizie sono registrati gli estremi identificativi del partecipante che ha comunicato i dati personali relativi alla richiesta/rapporto di credito. Tali estremi sono accessibili al gestore o agli interessati e non anche agli altri partecipanti.

Art. 4. Modalità di raccolta e registrazione dei dati

1. Salvo quanto previsto dal comma 5, il gestore acquisisce esclusivamente dai partecipanti i dati personali da registrare nel sistema di informazioni creditizie.

2. Il partecipante adotta idonee procedure di verifica per garantire la lecita utilizzabilità nel sistema, la correttezza e l'esattezza dei dati comunicati al gestore.

3. All'atto del ricevimento dei dati, il gestore verifica la loro congruità attraverso controlli di carattere formale e logico e, se i dati risultano incompleti od incongrui, li ritrasmette al partecipante che li ha comunicati, ai fini delle necessarie integrazioni e correzioni. All'esito dei controlli e delle eventuali integrazioni e correzioni, i dati sono registrati nel sistema di informazioni creditizie e resi disponibili a tutti i partecipanti.

4. Il partecipante verifica con cura i dati da esso trattati e risponde tempestivamente alle richieste di verifica del gestore, anche a seguito dell'esercizio di un diritto da parte dell'interessato.

5. Eventuali operazioni di eliminazione, integrazione o modificazione dei dati registrati in un sistema di informazioni creditizie sono disposte direttamente dal partecipante che li ha comunicati, ove tecnicamente possibile, ovvero dal gestore su richiesta del medesimo partecipante o d'intesa con esso, anche a seguito dell'esercizio di un diritto da parte dell'interessato, oppure in attuazione di un provvedimento dell'autorità giudiziaria o del Garante.

6. I dati relativi al primo ritardo nei pagamenti in un rapporto di credito sono utilizzati e resi accessibili agli altri partecipanti nel rispetto dei seguenti termini:

a) nei sistemi di informazioni creditizie di tipo negativo, dopo almeno centoventi giorni dalla data di scadenza del pagamento o in caso di mancato pagamento di almeno quattro rate mensili non regolarizzate;
b) nei sistemi di informazioni creditizie di tipo positivo e negativo:
    1) qualora l'interessato sia un consumatore, decorsi sessanta giorni dall'aggiornamento mensile di cui al successivo comma 8, oppure in caso di mancato pagamento di almeno due rate mensili consecutive, oppure quando il ritardo si riferisce ad una delle due ultime scadenze di pagamento. Nel secondo caso i dati sono resi accessibili dopo l'aggiornamento mensile relativo alla seconda rata consecutivamente non pagata;
    2) negli altri casi, dopo almeno trenta giorni dall'aggiornamento mensile di cui al successivo comma 8 o in caso di mancato pagamento di una rata.

7. Al verificarsi di ritardi nei pagamenti, il partecipante, anche unitamente all'invio di solleciti o di altre comunicazioni, avverte l'interessato circa l'imminente registrazione dei dati in uno o più sistemi di informazioni creditizie. I dati relativi al primo ritardo di cui al comma 6 possono essere resi accessibili ai partecipanti solo decorsi almeno quindici giorni dalla spedizione del preavviso all'interessato.

8. Fermo restando quanto previsto dal comma 6, i dati registrati in un sistema di informazioni creditizie sono aggiornati periodicamente, con cadenza mensile, a cura del partecipante che li ha comunicati.

Art. 5. Informativa

1. Al momento della raccolta dei dati personali relativi a richieste/rapporti di credito, il partecipante informa l'interessato ai sensi dell'art. 13 del Codice anche con riguardo al trattamento dei dati personali effettuato nell'ambito di un sistema di informazioni creditizie.

2. L'informativa di cui al comma 1 reca in modo chiaro e preciso, nell'ambito della descrizione delle finalità e delle modalità del trattamento, nonché degli altri elementi di cui all'art. 13 del Codice, le seguenti indicazioni:

a) estremi identificativi dei sistemi di informazioni creditizie cui sono comunicati i dati personali e dei rispettivi gestori;
b) categorie di partecipanti che vi accedono;
c) tempi di conservazione dei dati nei sistemi di informazioni creditizie cui sono comunicati;
d) modalità di organizzazione, raffronto ed elaborazione dei dati, nonché eventuale uso di tecniche o sistemi automatizzati di *credit scoring*;
e) modalità per l'esercizio da parte degli interessati dei diritti previsti dall'art. 7 del Codice.

3. L'informativa di cui al comma 2 è fornita agli interessati per iscritto secondo il modello allegato alla deliberazione che verifica la conformità del presente codice e, se inserita in un modulo utilizzato dal partecipante, è adeguatamente evidenziata e collocata in modo autonomo ed unitario, in parti o riquadri distinti da quelli relativi ad eventuali altre finalità del trattamento effettuato dal medesimo partecipante.

4. L'informativa dovuta per effetto di eventuali aggiornamenti o modifiche relativi alle indicazioni rese ai sensi del comma 2, anche in caso di cambiamento della denominazione e della sede del gestore, è fornita attraverso comunicazioni periodiche, nonché su uno o più siti Internet e a richiesta degli interessati.

5. Ad integrazione dell'informativa resa dai partecipanti singolarmente ad ogni interessato, il gestore fornisce un'informativa più dettagliata attraverso modalità ulteriori di diffusione delle informazioni al pubblico, anche mediante strumenti telematici.

6. Quando la richiesta di credito non è accolta, il partecipante comunica all'interessato se, per istruire la richiesta di credito, ha consultato dati personali relativi ad informazioni creditizie di tipo negativo in uno o più sistemi, indicandogli gli estremi identificativi del sistema da cui sono state rilevate tali informazioni e del relativo gestore.

7. Il partecipante fornisce all'interessato le altre notizie di cui agli articoli 9, comma 1, lett. *d*), e 10, comma 1, lett. *c*).

Art. 6. Conservazione e aggiornamento dei dati

1. I dati personali riferiti a richieste di credito, comunicati dai partecipanti, possono essere conservati in un sistema di informazioni creditizie per il tempo necessario alla relativa istruttoria e comunque non oltre centottanta giorni dalla data di presentazione delle richieste medesime. Se la richiesta di credito non è accolta o è oggetto di rinuncia il partecipante ne dà notizia al gestore con l'aggiornamento mensile di cui all'articolo 4, comma 8. In tal caso, i dati personali relativi alla richiesta cui l'interessato ha rinunciato o che non è stata accolta possono

essere conservati nel sistema non oltre trenta giorni dalla data del loro aggiornamento.

2. Le informazioni creditizie di tipo negativo relative a ritardi nei pagamenti, successivamente regolarizzati, possono essere conservate in un sistema di informazioni creditizie fino a:

a) dodici mesi dalla data di registrazione dei dati relativi alla regolarizzazione di ritardi non superiori a due rate o mesi;
b) ventiquattro mesi dalla data di registrazione dei dati relativi alla regolarizzazione di ritardi superiori a due rate o mesi.

3. Decorsi i periodi di cui al comma 2, i dati sono eliminati dal sistema di informazioni creditizie se nel corso dei medesimi intervalli di tempo non sono registrati dati relativi ad ulteriori ritardi o inadempimenti.

4. Il partecipante ed il gestore aggiornano senza ritardo i dati relativi alla regolarizzazione di inadempimenti di cui abbiano conoscenza, avvenuta dopo la cessione del credito da parte del partecipante ad un soggetto che non partecipa al sistema, anche a seguito di richiesta dell'interessato munita di dichiarazione del soggetto cessionario del credito o di altra idonea documentazione.

5. Le informazioni creditizie di tipo negativo relative a inadempimenti non successivamente regolarizzati possono essere conservate nel sistema di informazioni creditizie non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto oppure, in caso di altre vicende rilevanti in relazione al pagamento, dalla data in cui è risultato necessario il loro ultimo aggiornamento, o comunque dalla data di cessazione del rapporto.

6.[1] Le informazioni creditizie di tipo positivo relative ad un rapporto che si è esaurito con estinzione di ogni obbligazione pecuniaria, possono essere conservate nel sistema non oltre ventiquattro mesi dalla data di cessazione del rapporto o di scadenza del relativo contratto, ovvero dal primo aggiornamento effettuato nel mese successivo a tali date. Tenendo conto del requisito della completezza dei dati in rapporto alle finalità perseguite (art. 11, comma 1, lett. *d*) del Codice), le predette informazioni di tipo positivo possono essere conservate ulteriormente nel sistema qualora in quest'ultimo risultino presenti, in relazione ad altri rapporti di credito riferiti al medesimo interessato, informazioni creditizie di tipo negativo concernenti ritardi od inadempimenti non regolarizzati. In tal caso, le informazioni creditizie di tipo positivo sono eliminate dal sistema allo scadere del termine previsto dal comma 5 per la conservazione delle informazioni di tipo negativo registrate nel sistema in riferimento agli altri rapporti di credito con l'interessato.

7. Qualora il consumatore interessato comunichi al partecipante la revoca del consenso al trattamento delle informazioni di tipo positivo, nell'ambito del sistema di informazioni creditizie, il partecipante ne dà notizia al gestore con l'aggiornamento mensile di cui all'articolo 4, comma 8. In tal caso, e in quello in cui la revoca gli sia stata comunicata direttamente dall'interessato, il gestore registra la notizia nel sistema ed elimina le informazioni non oltre novanta giorni dall'aggiornamento o dalla comunicazione.

8. Prima dell'eliminazione dei dati dal sistema di informazioni creditizie nei termini indicati ai precedenti commi, il gestore può trasporre i dati su altro supporto, ai fini della limitata conservazione per il tempo necessario, esclusivamente in relazione ad esigenze di difesa di un proprio diritto in sede giudiziaria, nonché della loro eventuale elaborazione statistica in forma anonima.

9. Le disposizioni del presente articolo non riguardano la conservazione ad uso interno, da parte del partecipante, della documentazione contrattuale o contabile contenente i dati personali relativi alla richiesta/rapporto di credito.

Art. 7. Utilizzazione dei dati

1. Il partecipante può accedere al sistema di informazioni creditizie anche mediante consultazione di copia della relativa banca dati, rispetto a dati per i quali sussiste un suo giustificato interesse, riguardanti esclusivamente:

(1) *v.* Nota redazionale p. 134

a) consumatori che chiedono di instaurare o sono parte di un rapporto di credito con il medesimo partecipante e soggetti coobbligati, anche in solido;
b) soggetti che agiscono nell'ambito della loro attività imprenditoriale o professionale per i quali sia stata avviata un'istruttoria per l'instaurazione di un rapporto di credito o comunque per l'assunzione di un rischio di credito, oppure che siano già parte di un rapporto di credito con il medesimo partecipante;
c) soggetti aventi un collegamento di tipo giuridico con quelli di cui alla lettera *b)*, in particolare in quanto obbligati in solido o appartenenti a gruppi di imprese, sempre che i dati personali cui il partecipante intende accedere risultino oggettivamente necessari per valutare la situazione finanziaria e il merito creditizio dei soggetti di cui alla stessa lettera *b)*.

2. Il sistema di informazioni creditizie è accessibile dal partecipante e dal gestore solo da un numero limitato, rispetto all'intera organizzazione del titolare, di responsabili ed incaricati del trattamento designati per iscritto, con esclusivo riferimento ai dati strettamente necessari, pertinenti e non eccedenti in rapporto alle finalità indicate nell'articolo 2, in relazione alle specifiche esigenze derivanti dall'istruttoria di una richiesta di credito o dalla gestione di un rapporto, concretamente verificabili sulla base degli elementi in possesso dei partecipanti medesimi. Nei soli limiti e con le medesime modalità appena indicate, il sistema è accessibile anche da banche ed intermediari finanziari appartenenti al gruppo bancario del partecipante all'esclusivo fine di curare l'istruttoria per l'instaurazione del rapporto di credito con l'interessato o comunque per l'assunzione del relativo rischio.

3. I partecipanti accedono al sistema di informazioni creditizie attraverso le modalità e gli strumenti anche telematici individuati per iscritto con il gestore, nel rispetto della normativa sulla protezione dei dati personali. I dati personali relativi a richieste/rapporti di credito registrati in un sistema di informazioni creditizie sono consultabili con modalità di accesso graduale e selettivo, attraverso uno o più livelli di consultazione di informazioni sintetiche o riepilogative dei dati riferiti all'interessato, prima della loro visione in dettaglio e con riferimento anche ad eventuali dati riferiti a soggetti coobbligati o collegati ai sensi del comma 1. Sono, in ogni caso, precluse, anche tecnicamente, modalità di accesso che permettano interrogazioni di massa o acquisizioni di elenchi di dati concernenti richieste/rapporti di credito relativi a soggetti diversi da quelli che hanno chiesto di instaurare o sono parte di un rapporto di credito con il partecipante.

4. Non è inoltre consentito l'accesso ad un sistema di informazioni creditizie da parte di terzi, fatte salve le richieste da parte di organi giudiziari e di polizia giudiziaria per ragioni di giustizia, oppure da parte di altre istituzioni, autorità, amministrazioni o enti pubblici nei soli casi previsti da leggi, regolamenti o normative comunitarie e con l'osservanza delle norme che regolano la materia.

Art. 8. Accesso ed esercizio di altri diritti degli interessati

1. In relazione ai dati personali registrati in un sistema di informazioni creditizie, gli interessati possono esercitare i propri diritti secondo le modalità stabilite dal Codice, sia presso il gestore, sia presso i partecipanti che li hanno comunicati. Tali soggetti garantiscono, anche attraverso idonee misure organizzative e tecniche, un riscontro tempestivo e completo alle richieste avanzate.

2. Nella richiesta con la quale esercita i propri diritti, l'interessato indica anche, ove possibile, il codice fiscale e/o la partita Iva, al fine di agevolare la ricerca dei dati che lo riguardano nel sistema di informazioni creditizie.

3. Il terzo al quale l'interessato conferisce, per iscritto, delega o procura per l'esercizio dei propri diritti, può trattare i dati personali acquisiti presso un sistema di informazioni creditizie esclusivamente per finalità di tutela dei diritti dell'interessato, con esclusione di ogni altro scopo perseguito dal terzo medesimo o da soggetti ad esso collegati.

4. Il partecipante, al quale è rivolta una richiesta con cui è esercitato taluno dei diritti di cui all'articolo 7 del Codice relativamente alle informazioni creditizie registrate in un

sistema, fornisce direttamente riscontro nei termini previsti dall'art. 146, commi 2 e 3 del Codice e dispone le eventuali modifiche ai dati ai sensi dell'articolo 4, comma 5. Se la richiesta è rivolta al gestore, quest'ultimo provvede anch'esso direttamente nei medesimi termini, consultando ove necessario il partecipante.

5. Qualora sia necessario svolgere ulteriori o particolari verifiche con il partecipante, il gestore informa l'interessato di tale circostanza entro il termine di quindici giorni previsto dal Codice ed indica un altro termine per la risposta, che non può essere superiore ad ulteriori quindici giorni. Durante il periodo necessario ad effettuare le ulteriori verifiche con il partecipante, il gestore:

a) nell'arco dei primi quindici giorni, mantiene nel sistema di informazioni creditizie l'indicazione relativa allo svolgimento delle verifiche, tramite specifica codifica o apposito messaggio da apporre in corrispondenza dei dati oggetto delle richieste dell'interessato;
b) negli ulteriori quindici giorni, sospende la visualizzazione nel sistema di informazioni creditizie dei dati oggetto delle verifiche.

6. In caso di richieste di cui al comma 4 riguardanti effettive contestazioni relative ad inadempimenti del venditore/fornitore dei beni o servizi oggetto del contratto sottostante al rapporto di credito, il gestore annota senza ritardo nel sistema di informazioni creditizie, su richiesta dell'interessato, del partecipante o informando quest'ultimo, la notizia relativa all'esistenza di tali contestazioni, tramite l'inserimento di una specifica codifica da apporre in corrispondenza dei dati relativi al rapporto di credito.

Art. 9. Uso di tecniche o sistemi automatizzati di *credit scoring*

1. Nei casi in cui i dati personali contenuti in un sistema di informazioni creditizie siano trattati anche mediante l'impiego di tecniche o sistemi automatizzati di *credit scoring*, il gestore e i partecipanti assicurano il rispetto dei seguenti principi:

a) le tecniche o i sistemi, messi a disposizione dal gestore o impiegati per conto dei partecipanti, possono essere utilizzati solo per l'istruttoria di una richiesta di credito o per la gestione dei rapporti di credito instaurati;
b) i dati relativi a giudizi, indicatori o punteggi associati ad un interessato sono elaborati e comunicati dal gestore al solo partecipante che ha ricevuto la richiesta di credito dall'interessato o che ha precedentemente comunicato dati riguardanti il relativo rapporto di credito e, comunque, non sono conservati nel sistema di informazioni creditizie ai sensi dell'art. 6 del presente codice, né resi accessibili agli altri partecipanti;
c) i modelli o i fattori di analisi statistica, nonché gli algoritmi di calcolo dei giudizi, indicatori o punteggi sono verificati periodicamente con cadenza almeno annuale ed aggiornati in funzione delle risultanze di tali verifiche;
d) quando la richiesta di credito non è accolta, il partecipante comunica all'interessato se, per istruire la richiesta di credito, ha consultato dati relativi a giudizi, indicatori o punteggi di tipo negativo ottenuti mediante l'uso di tecniche o sistemi automatizzati di *credit scoring* e, su sua richiesta, gli fornisce tali dati, nonché una spiegazione delle logiche di funzionamento dei sistemi utilizzati e delle principali tipologie di fattori tenuti in considerazione nell'elaborazione.

Art. 10. Trattamento di dati provenienti da fonti pubbliche

1. Nei casi in cui il gestore di un sistema di informazioni creditizie, direttamente o per il tramite di società collegate o controllate, effettua in ogni forma il trattamento di dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque o comunque fornisce ai partecipanti servizi per accedere ai dati provenienti da tali fonti, fermi restando i limiti e le modalità che le leggi stabiliscono per la loro conoscibilità e pubblicità, nonché le disposizioni di cui all'art. 61, comma 1, del Codice, il gestore e i partecipanti assicurano il rispetto dei seguenti principi:

a) i dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, se registrati, devono figurare in banche di dati personali separate dal sistema di informazioni creditizie e non interconnesse a tale sistema;
b) nel caso di accesso del partecipante a dati personali contenuti sia in un sistema di informazioni creditizie, sia in una delle banche di dati di cui alla lett. *a*), il

gestore adotta le adeguate misure tecniche ed organizzative al fine di assicurare la separazione e la distinguibilità dei dati provenienti dal sistema di informazioni creditizie rispetto a quelli provenienti da altre banche dati, anche attraverso l'inserimento di idonee indicazioni, eliminando ogni possibilità di equivoco circa la diversa natura ed origine dei dati oggetto dell'accesso;

c) quando la richiesta di credito non è accolta, il partecipante comunica all'interessato se, per istruire la richiesta di credito, ha consultato anche dati personali di tipo negativo nelle banche di dati di cui alla lett. *a)* e, su sua richiesta, specifica la fonte pubblica da cui provengono i dati medesimi.

Art. 11. Misure di sicurezza dei dati

1. I dati personali oggetto di trattamento nell'ambito di un sistema di informazioni creditizie hanno carattere riservato e non possono essere divulgati a terzi, al di fuori dei casi previsti dal Codice e nei precedenti articoli.

2. Le persone fisiche che, in qualità di responsabili o di incaricati del trattamento designati dal gestore o dai partecipanti, hanno accesso al sistema di informazioni creditizie, mantengono il segreto sui dati personali acquisiti e rispondono della violazione degli obblighi di riservatezza derivanti da un'utilizzazione dei dati o una divulgazione a terzi per finalità diverse o incompatibili con le finalità di cui all'art. 2 del presente codice o comunque non consentite.

3. Il gestore e i partecipanti adottano le misure tecniche, logiche, informatiche, procedurali, fisiche ed organizzative idonee ad assicurare la sicurezza, l'integrità e la riservatezza dei dati personali e delle comunicazioni elettroniche in conformità alla disciplina in materia di protezione dei dati personali.

4. Il gestore adotta adeguate misure di sicurezza al fine di garantire il corretto e regolare funzionamento del sistema di informazioni creditizie, nonché il controllo degli accessi. Questi ultimi sono registrati e memorizzati nel sistema informativo del gestore medesimo o di ogni partecipante presso cui risieda copia della stessa banca dati.

5. In relazione al rispetto degli obblighi di sicurezza, riservatezza e segretezza di cui al presente articolo, il gestore e i partecipanti impartiscono specifiche istruzioni per iscritto ai rispettivi responsabili ed incaricati del trattamento e vigilano sulla loro puntuale osservanza, anche attraverso verifiche da parte di idonei organismi di controllo.

Art. 12. Misure sanzionatorie

1. Ferme restando le sanzioni amministrative, civili e penali previste dalla normativa vigente, i gestori e i partecipanti prevedono d'intesa tra di loro, anche per il tramite delle associazioni che sottoscrivono il presente codice, idonei meccanismi per l'applicazione, in particolare da parte delle associazioni di categoria che sottoscrivono il presente codice o dell'organismo di cui all'art. 13, comma 7, previa informativa al Garante, di misure sanzionatorie graduate a seconda della gravità della violazione. Le misure comprendono il richiamo formale, la sospensione o la revoca dell'autorizzazione ad accedere al sistema di informazioni creditizie e, nei casi più gravi, anche la pubblicazione della notizia della violazione su uno o più quotidiani o periodici nazionali, a spese del contravventore.

Art. 13. Disposizioni transitorie e finali

1. Le misure necessarie per l'applicazione del presente codice di deontologia e di buona condotta sono adottate dai soggetti tenuti a rispettarlo al più tardi entro il 30 aprile 2005.

2. Entro il termine di cui al comma 1, il gestore del sistema centralizzato di rilevazione dei rischi di importo contenuto, istituito con deliberazione Cicr del 3 maggio 1999 (pubblicata in *Gazzetta Ufficiale* 8 luglio 1999, n. 158), nonché i relativi partecipanti, adottano le misure necessarie per l'applicazione degli artt. 5 e 8, commi 1, 2, 3, 4 e 5, primo periodo, del presente codice in tema di informativa agli interessati e di esercizio dei diritti, ad integrazione di quanto previsto nel punto 3 delle istruzioni della Banca d'Italia (pubblicate in *Gazzetta Ufficiale* 21 novembre 2000, n. 272).

3. I partecipanti forniscono entro i tre mesi successivi al termine di cui al comma 1, nell'ambito delle comunicazioni periodiche inviate alla clientela, le informazioni di cui all'art. 5, commi 1 e 2, del presente codice eventualmente non comprese nelle informative precedentemente rese agli interessati i cui dati personali risultino già registrati in un sistema di informazioni creditizie.

4.[1] In sede di prima applicazione delle disposizioni di cui all'art. 6, comma 6, i gestori riducono entro il 30 giugno 2005, ad un termine non superiore a trentasei mesi, i tempi di conservazione dei dati personali relativi ad informazioni creditizie di tipo positivo. Entro il 31 dicembre 2005 l'organismo di cui al comma 7 valuta, con atto motivato, se l'esperienza maturata e l'incidenza delle misure previste dal presente codice sui diritti degli interessati, tenuto anche conto dell'efficienza dei sistemi di informazioni creditizie, giustifichino il mantenimento del predetto termine di trentasei mesi. Il medesimo termine si intende mantenuto qualora il Garante, su richiesta del predetto organismo o di propria iniziativa, non disponga diversamente. Entro il 31 gennaio 2006 il Garante dispone la pubblicazione sulla *Gazzetta Ufficiale* del proprio provvedimento o di un avviso indicante il termine da osservare.

5. Al fine di consentire il controllo sulla corretta attuazione delle disposizioni del presente codice, ogni gestore comunica al Garante, non oltre due mesi dal termine di cui al comma 1 e secondo le modalità indicate da quest'ultimo:

a) oltre ai propri estremi identificativi e recapiti, una descrizione generale delle modalità di funzionamento del sistema di informazioni creditizie e di accesso da parte dei partecipanti, che permetta di valutare l'adeguatezza delle misure, anche tecniche ed organizzative, adottate per l'applicazione del presente codice;
b) in relazione alle parti aventi riflessi in materia di protezione dei dati personali e di applicazione del presente codice, i modelli di contratti, accordi, convenzioni, regolamenti o istruzioni che disciplinano le modalità di partecipazione ed accesso dei partecipanti al sistema di informazioni creditizie, nonché la documentazione circa le misure adottate in tema di sicurezza, riservatezza e segretezza dei dati;
c) i documenti di cui agli articoli 3, commi 3 e 4, 5, commi 4 e 5, e di cui al successivo comma 7.

6. Le comunicazioni di cui al comma 5 sono inviate al Garante, anche successivamente al predetto termine, da qualsiasi titolare che, in qualità di gestore di un sistema di informazioni creditizie, intenda procedere ad un trattamento di dati personali soggetto all'ambito di applicazione del presente codice. I gestori trasmettono al Garante eventuali variazioni delle comunicazioni e dei documenti precedentemente inviati, non oltre la fine dell'anno in cui sono avvenute le variazioni.

7. Il gestore effettua verifiche periodiche, con cadenza almeno annuale, sulla liceità e correttezza del trattamento, controllando l'esattezza e completezza dei dati riferiti ad un congruo numero di richieste/rapporti di credito, estratti a campione. Il controllo è eseguito da un organismo composto da almeno un rappresentante del gestore, un rappresentante dei partecipanti designato a rotazione e un rappresentante delle associazioni dei consumatori designato dal Consiglio nazionale dei consumatori ed utenti. Il verbale dei controlli è trasmesso al Garante.

8. Allo scopo di vigilare sulla puntuale osservanza delle disposizioni contenute nel presente codice e fermi restando i poteri previsti dal Codice in materia di accertamenti e controlli, il Garante può concordare con il gestore l'esecuzione di altre verifiche periodiche presso i luoghi ove si svolge il trattamento dei dati personali, con eventuali accessi, anche a campione, al sistema di informazioni creditizie. Il Garante può eseguire analoghi controlli concordati sugli accessi effettuati da parte dei partecipanti.

9. Le associazioni di categoria che sottoscrivono il presente codice e i gestori avviano forme di collaborazione con le associazioni dei consumatori e con il Garante, al fine di individuare sia soluzioni operative per il rispetto del presente codice, sia sistemi alternativi di risoluzione delle controversie derivanti dall'applicazione del presente codice.

(1) *v.* Nota redazionale p. 134

10. Il Garante, anche su richiesta delle associazioni di categoria che sottoscrivono il presente codice, promuove il periodico riesame e l'eventuale adeguamento alla luce del progresso tecnologico, dell'esperienza acquisita nella sua applicazione o di novità normative.

Art. 14. Entrata in vigore

1. Il presente codice si applica a decorrere dal 1° gennaio 2005.

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITÀ E PUNTUALITÀ NEI PAGAMENTI (ART. 117 DEL CODICE)

Sottoscritto da:

- AISReC - Associazione italiana delle società di referenza creditizia
- ABI - Associazione bancaria italiana
- FEDERCASSE - Federazione italiana delle banche di credito cooperativo
- ASSOFIN - Associazione italiana del credito al consumo e immobiliare
- ASSILEA - Associazione italiana leasing
- CTC - Consorzio per la tutela del credito
- ADICONSUM - Associazione difesa consumatori e ambiente
- ADOC - Associazione per la difesa e l'orientamento dei consumatori
- ADUSBEF - Associazione difesa utenti servizi bancari finanziari assicurativi e postali
- CODACONS - Coordinamento delle associazioni per la difesa dell'ambiente e la tutela dei diritti di utenti e di consumatori
- FEDERCONSUMATORI - Federazione nazionale consumatori e utenti

MODELLO UNICO DI INFORMATIVA
(G.U. 23 dicembre 2004, n. 300)

Come utilizziamo i Suoi dati
(art. 13 del Codice sulla protezione dei dati personali
art. 5 del codice deontologico sui sistemi di informazioni creditizie)

Gentile Cliente,

per concederLe il finanziamento richiesto, utilizziamo alcuni dati che La riguardano. Si tratta di informazioni che Lei stesso ci fornisce o che otteniamo consultando alcune banche dati. Senza questi dati, che ci servono per valutare la Sua affidabilità, potrebbe non esserLe concesso il finanziamento.

Queste informazioni saranno conservate presso di noi; alcune saranno comunicate a grandi banche dati istituite per valutare il rischio creditizio, gestite da privati e consultabili da molti soggetti. Ciò significa che altre banche o finanziarie a cui Lei chiederà un altro prestito, un finanziamento, una carta di credito, ecc., anche per acquistare a rate un bene di consumo, potranno sapere se Lei ha presentato a noi una recente richiesta di finanziamento, se ha in corso altri prestiti o finanziamenti e se paga regolarmente le rate.

Qualora Lei sia puntuale nei pagamenti, la conservazione di queste informazioni da parte delle banche dati richiede il Suo consenso(1). In caso di pagamenti con ritardo o di omessi pagamenti, oppure nel caso in cui il finanziamento riguardi la Sua attività imprenditoriale o professionale, tale consenso non è necessario.

Lei ha diritto di conoscere i Suoi dati e di esercitare i diversi diritti relativi al loro utilizzo (rettifica, aggiornamento, cancellazione, ecc.).

Per ogni richiesta riguardante i Suoi dati, utilizzi nel Suo interesse il fac-simile presente sul sito ... inoltrandolo alla nostra società:

Banca ... Recapiti utili (indirizzo, telefono, fax, e-mail)

e/o alle società sotto indicate, cui comunicheremo i Suoi dati:

Troverà qui sotto i loro recapiti ed altre spiegazioni.

Conserviamo i Suoi dati presso la nostra società per tutto ciò che è necessario per gestire il finanziamento e adempiere ad obblighi di legge.

Al fine di meglio valutare il rischio creditizio, ne comunichiamo alcuni *(dati anagrafici, anche della persona eventualmente coobbligata, tipologia del contratto, importo del credito, modalità di rimborso)* ai sistemi di informazioni creditizie, i quali sono regolati dal relativo codice deontologico del 2004 (*Gazzetta Ufficiale* ... novembre 2004, n. ... ; sito *web www*.....). I dati sono resi accessibili anche ai diversi operatori bancari e finanziari partecipanti, di cui indichiamo di seguito le categorie.

I dati che La riguardano sono aggiornati periodicamente con informazioni acquisite nel corso del rapporto *(andamento dei pagamenti, esposizione debitoria residuale, stato del rapporto).*

Nell'ambito dei sistemi di informazioni creditizie, i Suoi dati saranno trattati secondo modalità di organizzazione, raffronto ed elaborazione strettamente indispensabili per perseguire le finalità sopra descritte, e in particolare saranno... [INDICARE IN SINTESI].

(1) Tale consenso non è necessario qualora Lei lo abbia già fornito sulla base di una nostra precedente informativa

I Suoi dati sono/non sono oggetto di particolari elaborazioni statistiche al fine di attribuirLe un giudizio sintetico o un punteggio sul Suo grado di affidabilità e solvibilità (cd. *credit scoring*), tenendo conto delle seguenti principali tipologie di fattori: ... . Alcune informazioni aggiuntive possono esserLe fornite in caso di mancato accoglimento di una richiesta di credito.

I sistemi di informazioni creditizie cui noi aderiamo sono gestiti da:

1) ESTREMI IDENTIFICATIVI: ...*(denominazione, sede, recapiti anche telematici, indicare la tipologia di sistema: p/n o n)*/PARTECIPANTI: ...*(indicare le categorie, ad es.: banche, società finanziarie, società di leasing...)*/TEMPI DI CONSERVAZIONE DEI DATI: ...*(evidenziare specificità rispetto ai tempi indicati nel codice di deontologia)*/USO DI SISTEMI AUTOMATIZZATI DI *CREDIT SCORING*: SI-NO/ALTRO: ...

2) ESTREMI IDENTIFICATIVI: ...*(denominazione, sede, recapiti anche telematici, indicare la tipologia di sistema: p/n o n)*/PARTECIPANTI: ...*(indicare le categorie, ad es.: banche, società finanziarie, società di leasing...)*/TEMPI DI CONSERVAZIONE DEI DATI: ... *(evidenziare specificità rispetto ai tempi indicati nel codice di deontologia)*/USO DI SISTEMI AUTOMATIZZATI DI *CREDIT SCORING*: SI-NO/ALTRO: ...

3) .....

Lei ha diritto di accedere in ogni momento ai dati che La riguardano. Si rivolga alla nostra società [INDICARE L'UNITÀ O PERSONA RESPONSABILE PER IL RISCONTRO ALLE ISTANZE DI CUI ALL'ART. 7 DEL CODICE], oppure ai gestori dei sistemi di informazioni creditizie, ai recapiti sopra indicati.

Allo stesso modo può richiedere la correzione, l'aggiornamento o l'integrazione dei dati inesatti o incompleti, ovvero la cancellazione o il blocco per quelli trattati in violazione di legge, o ancora opporsi al loro utilizzo per motivi legittimi da evidenziare nella richiesta *(art. 7 del Codice; art. 8 del codice deontologico).*

Tempi di conservazione dei dati nei sistemi di informazioni creditizie:

richieste di finanziamento	***6 mesi**, qualora l'istruttoria lo richieda, o **1 mese** in caso di **rifiuto** della richiesta o **rinuncia** alla stessa*
morosità di due rate o di due mesi** poi **sanate	***12 mesi** dalla regolarizzazione*
***ritardi superiori sanati** anche su transazione*	***24 mesi** dalla regolarizzazione*
eventi negativi** (ossia morosità, gravi inadempimenti, sofferenze) **non sanati	***36 mesi** dalla data di scadenza contrattuale del rapporto o dalla data in cui è risultato necessario l'ultimo aggiornamento (in caso di successivi accordi o altri eventi rilevanti in relazione al rimborso)*
***rapporti** che si sono svolti **positivamente** (senza ritardi o altri eventi negativi)*	***36 mesi** in presenza di altri rapporti con eventi negativi non regolarizzati. Nei restanti casi, nella prima fase di applicazione del codice di deontologia, il termine sarà di **36 mesi** dalla data di cessazione del rapporto o di scadenza del contratto, ovvero dal primo aggiornamento effettuato nel mese successivo a tali date (nel secondo semestre del 2005, dopo la valutazione del Garante, tale termine rimarrà a 36 mesi o verrà ridotto a 24 mesi: si veda il ns. sito www.....)* [1]

(1) Nota redazionale
La valutazione del Garante è stata espressa con: **"Avviso relativo ai termini di conservazione dei dati personali presso i sistemi di informazioni creditizie"** In relazione al codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (Del. Garante 16 novembre 2004, n. 8, nella *G.U.* 23 dicembre 2004, n. 300; art. 6, comma 6, del predetto codice ivi allegato), esaminate anche le valutazioni espresse dall'organismo di verifica previsto dal medesimo codice (art. 13, commi 4 e 7), ha disposto la pubblicazione del presente avviso per indicare che i dati personali relativi ad informazioni creditizie di tipo positivo restino conservati nei sistemi di informazione creditizie per un termine non superiore a 36 mesi.
(*G.U.* 6 marzo 2006, n. 54)

Misure minime di sicurezza

B. Disciplinare tecnico in materia di misure minime di sicurezza (*)

TRATTAMENTI CON STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

SISTEMA DI AUTENTICAZIONE INFORMATICA

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con

(*) Artt. da 33 a 36 del Codice.

le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

SISTEMA DI AUTORIZZAZIONE

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

ALTRE MISURE DI SICUREZZA

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La for-

mazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

MISURE DI TUTELA E GARANZIA

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

C. Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia (*)

Si tratta di un allegato che, allo stato, non comprende ancora i decreti in fase di adozione:

- decreto del Ministro della giustizia da adottare ai sensi dell'art. 46 del Codice;
- decreto del Ministro dell'interno da adottare ai sensi dell'art. 53 del Codice.

(*) Artt. 46 e 53 del Codice

PAGINA BIANCA

RELAZIONE PER L'ANNO 2005

Diritto alla protezione dei dati personali: garanzie per i cittadini e sicurezza dei sistemi

PAGINA BIANCA

I. STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Il quadro normativo

1.1. Il Codice e la "stabilizzazione" delle regole per la protezione dei dati

1.2. Le modifiche apportate

1.3. Il monitoraggio delle leggi regionali

1.4. Altre novità normative con riflessi in materia di protezione di dati personali

II. L'ATTIVITÀ SVOLTA DAL GARANTE

2. Trattamenti effettuati in ambito pubblico

2.1. Profili introduttivi

2.2. Regolamenti sui trattamenti di dati sensibili e giudiziari

2.3. Trasparenza dell'attività amministrativa e accesso ai documenti

2.4. Il principio del "pari rango"

2.5. Pubblici registri, elenchi, atti e documenti conoscibili da chiunque

2.6. Documentazione anagrafica e materia elettorale

2.7. Istruzione

2.8. Notificazioni di atti e comunicazioni

2.9. Attività fiscale, tributaria e doganale

2.10. Trattamenti effettuati presso regioni ed enti locali

2.11. Attività giudiziaria

3. Sanità

3.1. Trattamento di dati idonei a rivelare lo stato di salute

4. Dati genetici

4.1. Le informazioni genetiche

5. Ricerca statistica e scientifica

5.1. Ricerca statistica

5.2. Ricerca medica, biomedica ed epidemiologica

6. Attività di polizia

6.1. Il controllo sul Centro elaborazione dati del Dipartimento di pubblica sicurezza

6.2. Controllo sui trattamenti effettuati dai servizi di informazione e di sicurezza

6.3. Il controllo sul Sistema informativo Schengen (Sis)

7. Attività giornalistica e mezzi di informazione

7.1. Tutela dei minori

7.2. Cronache giudiziarie

7.3. Dati idonei a rivelare lo stato di salute

7.4. Libertà di informazione e personaggi pubblici

7.5. Esercizio dei diritti e diritto all'oblìo

8. Associazioni, movimenti politici e partiti

8.1. Associazioni

8.2. Movimenti politici e propaganda elettorale

9. Attività economiche

9.1. Credito

9.2. Assicurazioni

9.3. *Marketing*

9.4. Impresa

9.5. Trasferimento dei dati personali all'estero

9.6. Lavoro

9.7. Condomini

10. Libere professioni

10.1. Attività forense. Ordini e collegi professionali

11. Concessionari di pubblici servizi

11.1. Servizi di riscossione tributi

12. Rapporto di lavoro e previdenza

12.1. Rapporti di lavoro in ambito pubblico

12.2. Previdenza

13. Videosorveglianza

13.1. Videosorveglianza in ambito pubblico

14. Altre iniziative nel settore pubblico

14.1. Utilizzo di dati biometrici

14.2. Ulteriori iniziative dell'Ufficio

15. Reti di comunicazione elettronica

15.1. Conservazione dei dati di traffico

15.2. I nuovi elenchi telefonici

15.3. Elenchi telefonici *cd.* "categorici"

15.4. *Spamming*
15.5. Videochiamate
15.6. Chiamate in entrata
15.7. Intercettazioni
15.8. Servizi telefonici non richiesti
15.9. Informativa con modalità diverse da quelle ordinarie
15.10. Il codice deontologico
15.11. Motori di ricerca e diritto all'oblìo
15.12. Televisione digitale: i servizi interattivi
15.13. *Pornosquatting*
15.14. *Rfid*

16. La sicurezza dei dati e dei sistemi

17. Registro dei trattamenti

18. La trattazione dei ricorsi

18.1. Considerazioni generali
18.2. Profili procedurali
18.3. Brevi cenni sulla casistica

19. Contenzioso giurisdizionale

19.1. Considerazioni generali
19.2. Profili procedurali
19.3. Profili di merito
19.4. Opposizione ai provvedimenti del Garante
19.5. Intervento del Garante in giudizi relativi all'applicazione del Codice

20. Attività ispettive e applicazione di sanzioni amministrative

20.1. Il potenziamento del dispositivo di controllo
20.2. La collaborazione con la Guardia di finanza
20.3. Settori oggetto dei controlli e casi più rilevanti
20.4. L'attività sanzionatoria del Garante
20.5. Alcuni riferimenti statistici

21. Relazioni istituzionali

21.1. L'Autorità e le attività di sindacato ispettivo e di indirizzo del Parlamento
21.2. L'attività consultiva del Garante sugli atti del Governo
21.3. Altra collaborazione con la Presidenza del Consiglio dei ministri

22. Relazioni internazionali

22.1. La cooperazione tra autorità garanti nell'Ue: il Gruppo art. 29

22.2. Cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni

22.3. Partecipazione ad altri comitati e gruppi di lavoro

23. Attività di ricerca, comunicazione e formazione

23.1. La comunicazione del Garante: profili generali

23.2. Prodotti informativi

23.3. Prodotti editoriali

23.4. Incontri internazionali

23.5. Il sito Internet dell'Autorità

23.6. Ufficio per le relazioni con il pubblico

23.7. Manifestazioni e conferenze

23.8. L'attività di studio, ricerca e documentazione

III. L'UFFICIO DEL GARANTE

24. La gestione amministrativa dell'Ufficio

24.1. Il bilancio e gli impegni di spesa

24.2. L'attività contrattuale

24.3. Le novità legislative e regolamentari e l'organizzazione dell'Ufficio

24.4. Il personale e i collaboratori esterni

24.5. Il settore informatico e tecnologico

24.6. Il monitoraggio dell'efficacia e dell'efficienza e il supporto al controllo interno

25. Dati statistici

25.1. Tabelle e grafici

DOCUMENTAZIONE

Provvedimenti del Garante

26. Autorizzazione n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro

27. Autorizzazione n. 2/2005 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale

28. Autorizzazione n. 3/2005 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni

29. Autorizzazione n. 4/2005 al trattamento dei dati sensibili da parte dei liberi professionisti

30. Autorizzazione n. 5/2005 al trattamento dei dati sensibili da parte di diverse categorie di titolari
31. Autorizzazione n. 6/2005 al trattamento dei dati sensibili da parte degli investigatori privati
32. Autorizzazione n. 7/2005 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici
33. Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento dei dati personali verso l'Argentina
34. Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento di dati personali dal territorio dello Stato all'Ufficio statunitense "Cbp" del Ministero della sicurezza interna (Department of Homeland Security)
35. Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso Paesi terzi
36. Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento dei dati personali verso l'Isola di Man
37. Investigazioni difensive: riapertura dei lavori sul codice deontologico
38. Avviso relativo ai termini di conservazione dei dati personali presso i sistemi di informazioni creditizie
39. *"Fidelity card"* e garanzie per i consumatori
40. TV interattiva e trattamento dei dati
41. Disposizioni in materia di comunicazione e di propaganda politica
42. Trattamento dei dati sensibili nella pubblica amministrazione
43. Sicurezza presso il C.e.d. del Dipartimento della pubblica sicurezza
44. Elenchi telefonici: semplificate le procedure per i "categorici"
45. Ricette mediche, tessera sanitaria e monitoraggio della spesa
46. Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro
47. Portfolio: garanzie nei processi formativi degli alunni
48. Procreazione assistita - Registro nazionale delle strutture sanitarie
49. Passaporto elettronico
50. Servizi di radiotaxi
51. Propaganda elettorale: il "decalogo" del Garante
52. Il caso Laziomatica. Prescrizioni a tutti i comuni sulla gestione delle anagrafi
53. Strutture sanitarie: rispetto della dignità
54. Liceità, correttezza e pertinenza nell'attività di recupero crediti
55. Luoghi di lavoro: accertamenti della tossicodipendenza per particolari addetti

Unione europea

56. Conservazione dei dati trattati nell'ambito della fornitura di servizi di comunicazione elettronica

57. Miglioramento della cooperazione di polizia, con particolare riferimento ai confini interni (modifica della Convenzione di applicazione Schengen)
58. Decisione sull'istituzione del Sistema informativo Schengen di seconda generazione (Sis II)
59. Regolamento sull'istituzione del Sistema informativo Schengen di seconda generazione (Sis II)
60. Accesso al Sistema informativo Schengen di seconda generazione (Sis II) per l'emissione delle carte di circolazione dei veicoli
61. Protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale
62. Scambio di informazioni in virtù del principio di disponibilità
63. Formato uniforme per i permessi di soggiorno dei cittadini di Paesi terzi

Consiglio dell'Unione europea

64. Requisiti minimi comuni di sicurezza per le carte di identità nazionali
65. Convenzione di Prüm sulla lotta al terrorismo, al crimine transfrontaliero e all'immigrazione clandestina

Gruppo art. 29

66. Livello di protezione garantito in Canada ai fini della trasmissione, da parte delle compagnie aeree, dei dati sui viaggiatori
67. Questioni di protezione dati relative ai diritti di proprietà intellettuale
68. Protezione dati e tecnologie *Rfid*
69. Notificazione dei trattamenti di dati e ruolo dei *privacy officer*
70. Trasferimento all'estero di dati e "regole vincolanti nell'impresa"
71. Modello di richiesta ai fini dell'approvazione di "regole vincolanti nell'impresa"
72. Sistema di informazione visti (Vis) e scambio di dati sui visti per soggiorni di breve durata
73. Caratteristiche di sicurezza ed elementi biometrici nei passaporti e nei documenti di viaggio
74. Conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica
75. Trasferimento all'estero dei dati e adeguatezza: linee di interpretazione armonizzata
76. Uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto
77. Istituzione del Sis II e accesso per il rilascio delle carte di circolazione
78. Linee guida per i *terminated merchant database*
79. Rapporto annuale per il 2004

Garante europeo per la protezione dei dati

80. Sistema di informazione visti (Vis) e scambio di dati tra Stati membri sui visti per brevi soggiorni

81. Accordo tra la Comunità europea e il Governo del Canada sul trattamento delle informazioni sui passeggeri

82. Istituzione del Sis II e accesso per il rilascio delle carte di circolazione

83. Accesso alla documentazione amministrativa e protezione dati

84. Relazione annuale per il 2005

Autorità di controllo Schengen

85. Base giuridica proposta per il Sis II

86. Accertamenti svolti sull'inserimento delle segnalazioni nel Sis ai sensi dell'art. 96 della Convenzione

Consiglio d'Europa

87. Applicazione della Convenzione ETS 108 al trattamento di dati biometrici

Corte europea dei diritti dell'uomo

88. Diffusione di foto segnaletiche nell'attività di polizia

Rete Ue di esperti indipendenti

89. Diritti fondamentali e misure di prevenzione del reclutamento di potenziali terroristi

90. Relazione annuale per il 2005

Autorità di controllo Europol

91. Accesso di Europol al Sis II

92. Livello di tutela dei dati in Australia

27ma Conferenza dei Garanti privacy

93. Dichiarazione di Montreux

94. Risoluzione sull'utilizzo della biometria per passaporti, carte di identità e titoli di viaggio

95. Risoluzione sull'utilizzo di dati personali per la comunicazione politica

Conferenza di primavera 2005

96. Dichiarazione sulla lotta al terrorismo internazionale

Elenco delle abbreviazioni

La presente Relazione è riferita al 2005 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 15 giugno 2005, relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	ad esempio
art.	articolo
Bollettino	Bollettino del Garante per la protezione dei dati personali "Cittadini e Società dell'Informazione"
c.c.	codice civile
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cd.	cosiddetto/a
cfr.	confronta
Cost.	Costituzione
d.l.	decreto legge
d.lg.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.G.p.	decreto del Presidente della Giunta provinciale
d.P.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
P.a.	Pubblica amministrazione
par.	paragrafo
Provv.	provvedimento
Relazione	Relazione del Garante per la protezione dei dati personali
r.d.	regio decreto
reg.	regolamento
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

PAGINA BIANCA

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Il quadro normativo

1.1. *Il Codice e la "stabilizzazione" delle regole per la protezione dei dati*

Nella *Relazione* del Garante per l'anno 2004 si è già ampiamente evidenziato come il Codice in materia di protezione dei dati personali entrato in vigore il 1° gennaio di tale anno (d.lg. 30 giugno 2003, n. 196) abbia consolidato il quadro di rafforzate garanzie per i diritti fondamentali della persona che sono state introdotte negli anni scorsi rispetto al trattamento dei dati personali. In particolare, si è richiamata l'attenzione sull'importante e solenne riconoscimento del diritto alla protezione dei dati personali, affermato già nell'art. 1 del Codice, diritto già contemplato nella Carta dei diritti fondamentali dell'Unione europea e nel Trattato per la Costituzione europea.

Nella stessa *Relazione* (p. 3) si erano tuttavia posti in luce alcuni interventi modificativi del Codice che erano stati avviati nel 2004 in alcuni settori di rilievo, da analizzare con cura stante l'esigenza di evitare possibili passi in parziale controtendenza rispetto al processo di consolidamento e di "stabilizzazione" delle garanzie dei cittadini che nel Codice aveva trovato ampia esplicazione. In questa prospettiva ci si era riferiti, in particolare, alle modifiche normative sulla conservazione dei dati del traffico telefonico e all'ambito sanitario (d.l. 24 dicembre 2003, n. 354, convertito dalla l. 26 febbraio 2004, n. 45; d.l. 29 marzo 2004, n. 81, convertito dalla l. 26 maggio 2004, n. 138), nonché alle diverse proroghe dei termini per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili delle pubbliche amministrazioni.

Analoghi interventi normativi si sono registrati anche nel corso del 2005, interventi dei quali viene effettuata di seguito una sintesi.

1.2. *Le modifiche apportate*

Specifico rilievo hanno assunto, anzitutto, le ulteriori modifiche apportate al Codice (art. 132) e ad alcune disposizioni ad esso collegate, relativamente alla disciplina della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e di repressione dei reati (d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale: art. 6).

Dati di traffico

Le modifiche introdotte hanno riguardato, in particolare, la tipologia dei dati personali oggetto di necessaria conservazione, la durata di tale conservazione e le modalità di acquisizione, accesso ed utilizzazione dei dati medesimi. In questo quadro:

a) la conservazione dei dati di traffico telefonico per finalità di accertamento e repressione dei reati è stata estesa ai dati concernenti le "chiamate senza risposta";

b) è stato introdotto l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare anche i dati relativi al "traffico telematico", esclusi i contenuti delle comunicazioni, per un periodo di sei mesi, nonché per ulteriori sei mesi per esclusive finalità di accertamento e repressione di delitti di particolare gravità (indicati all'art. 407, comma 2, lett. a), c.p.p. o commessi in danno di sistemi informatici o telematici) (art. 132, commi 1 e 2, del Codice, come modificato dall'art. 6, comma 2, d.l. n. 144/2005);

c) è stata sospesa fino al 31 dicembre 2007 l'applicazione di tutte le disposizioni normative o amministrative che prescrivano o consentano la cancellazione dei dati del traffico telefonico o telematico; questi debbono essere quindi conservati fino alla medesima data del 31 dicembre 2007 limitatamente, per quanto riguarda i dati di traffico telematico, alle "informazioni che consentono la tracciabilità degli accessi, nonché qualora disponibili, dei servizi", rimanendo del pari esclusa la conservazione dei contenuti delle conversazioni (art. 6, comma 1, d.l. n. 144/2005).

Il d.l. n. 144/2005 ha previsto, altresì, che le modalità e i tempi di attuazione delle predette modifiche all'art. 132 del Codice siano individuati con regolamento governativo, adottato previo parere del Garante (art. 6, comma 4, d.l. n. 144/2005). A tale regolamento si aggiunge –e, per certi versi, potrebbe in parte "sovrapporsi"– il provvedimento che l'Autorità dovrà adottare, in base al medesimo articolo 132 del Codice, per disciplinare le modalità di trattamento presso i fornitori e di accesso ai dati conservati per le finalità accertamento e repressione dei reati, nonché per individuare ulteriori e più incisive misure di sicurezza necessarie a garantire maggiormente che la conservazione di tale categoria delicata di dati sia effettuata nel pieno rispetto dei diritti fondamentali della persona.

La piena attuazione di tali modalità e misure protettive si è affiancata al dibattito relativo all'ampliamento dei tempi di conservazione e delle categorie di dati da conservare anche relativamente alle comunicazioni telematiche. Sebbene le modifiche apportate abbiano in parte un'efficacia temporale limitata, resta sul tappeto il rapporto tra la predetta conservazione e il principio relativo alle finalità per le quali i dati sono o dovrebbero essere trattati dai fornitori, nonché il tema della proporzionalità rispetto alle finalità di polizia e di giustizia da perseguire. In materia dovranno essere peraltro effettuate a breve nuove valutazioni di carattere anche normativo, per effetto del prossimo recepimento della direttiva 2006/24/Ce del Parlamento e dal Consiglio dell'Unione europea approvata il 15 marzo 2006 sempre in tema di *data retention*, direttiva la quale prevede un periodo di conservazione dei dati (compreso fra i sei mesi e i due anni) che, oltre ad essere più breve rispetto a quello attualmente previsto in Italia, è stato oggetto di rilievi critici nel parere espresso preventivamente dalle autorità europee per la protezione dei dati personali (parere elaborato da un sottogruppo che è stato coordinato dall'Autorità italiana: parere del Gruppo art. 29 WP 113, 21 ottobre 2005).

Esercizi di telefonia ed Internet point

Il d.l. n. 144/2005 ha introdotto altre disposizioni di rilievo per la protezione dei dati personali.

Per finalità di lotta al terrorismo, sono stati ad esempio previsti, nei confronti

di titolari e gestori di esercizi pubblici di telefonia e Internet, alcuni obblighi orientati ad un maggiore controllo delle comunicazioni effettuate con strumenti telematici o telefonici, come l'identificazione del cliente, il monitoraggio delle operazioni dell'utente e l'archiviazione dei relativi dati (art. 7 d.l. n. 144/2005). In relazione a tali obblighi, il Ministero dell'interno, sentito il Garante, ha poi adottato il previsto decreto di attuazione recante la disciplina delle misure che il gestore è tenuto ad osservare, nonché delle modalità di trattamento dei dati (*v.* anche par. 21.2).

Dna dell'indagato e banca di dati

A parziale modifica dell'art. 349 c.p.p., sono stati previsti, con il d.l. n. 144/2005, nuovi poteri per la polizia giudiziaria al fine di identificare la persona nei cui confronti vengono svolte indagini, prevedendo che si possa procedere, previa autorizzazione del pubblico ministero, al prelievo coattivo di capelli o saliva anche senza il consenso dell'interessato. Nel corso dei lavori di conversione del decreto, il Governo ha accettato un ordine del giorno parlamentare che lo impegna ad istituire una banca dati nella quale raccogliere i dati relativi al Dna acquisiti ai sensi del predetto art. 349 c.p.p., ovvero attraverso altri accertamenti effettuati da reparti di polizia scientifica. Secondo l'o.d.g., tale banca dati dovrebbe operare sotto la vigilanza del Garante, il quale potrebbe fissare limiti e condizioni alla consultazione dei dati relativi a soggetti per i quali non sia già intervenuta una sentenza di condanna. Appare evidente che si tratta di una tematica particolarmente delicata in relazione alla quale ogni iniziativa richiederà un'attenta valutazione delle diverse implicazioni che, anche sul piano costituzionale, potrebbero derivarne per i diritti fondamentali della persona e, in particolare, per la riservatezza e la dignità degli interessati.

Adozione delle misure minime di sicurezza

Le altre modifiche apportate al Codice hanno riguardato la reiterazione di proroghe, già disposte nel corso del 2004, con le quali erano stati differiti i termini per adempiere a pur importanti obblighi posti a garanzia dell'interessato, in relazione all'applicazione delle "nuove" misure minime di sicurezza e all'adozione dei regolamenti in materia di dati sensibili e giudiziari da parte dei soggetti pubblici.

Per quanto riguarda le misure minime di sicurezza, la scadenza originariamente fissata al 30 giugno 2004 (art. 180, comma 1, del Codice), era stata prorogata due volte già nel corso del 2004, inizialmente al 31 dicembre 2004 (d.l. 24 giugno 2004, n. 158, convertito, con modificazioni, dalla l. 27 luglio 2004, n. 188) e, quindi, al 30 giugno 2005 (d.l. 9 novembre 2004, n. 266, convertito, con modificazioni, dalla l. 27 dicembre 2004, n. 306). Con successivi interventi adottati sempre in via d'urgenza nel 2005, il termine è stato ulteriormente prorogato, una prima volta al 31 dicembre 2005 (d.l. 30 dicembre 2004, n. 314, convertito, con modificazioni, dalla l. 1° marzo 2005, n. 26) e, da ultimo, al 31 marzo 2006 (d.l. 30 dicembre 2005, n. 273, convertito, con modificazioni, dalla l. 23 febbraio 2006, n. 51). Analogamente, è stato prorogato anche il termine per adottare le misure di sicurezza da parte dei soggetti che, alla data di entrata in vigore del Codice, disponevano di strumenti elettronici "obsoleti": prima al 31 marzo 2005, poi al 30 settembre 2005, quindi al 31 marzo 2006 e, da ultimo, al 30 giugno 2006 (d.l. n. 273/2005 cit.).

Adozione dei regolamenti sul trattamento dei dati sensibili e giudiziari

Il già citato d.l. n. 158/2004 aveva, inoltre, prorogato al 31 dicembre 2005 il termine per l'adozione e pubblicazione, da parte delle pubbliche amministrazioni, dei regolamenti in materia di dati sensibili e giudiziari, originariamente fissato dal Codice alla data del 31 dicembre 2004 (art. 181, comma 1, lett. *a*)). La citata l. 23 febbraio 2006, n. 51, di conversione del d.l. n. 273/2005, ha poi prorogato ulteriormente il termine in questione al 15 maggio 2006 (da ultimo prorogato ancora al 31 luglio 2006 con d.l. 12 maggio 2006, n. 173).

1.3. *Il monitoraggio delle leggi regionali*

Nel quadro normativo di riferimento dell'attività di monitoraggio sugli atti delle regioni e degli enti locali, si deve evidenziare il testo di legge costituzionale recante modifiche alla Parte II della Costituzione approvato dal Parlamento, pubblicato sulla *Gazzetta Ufficiale* 18 novembre 2005, n. 269, e sottoposto a *referendum* confermativo ai sensi dell'art. 138 Cost. (*v.* anche par. 1.3). Per quanto attiene ai rapporti tra Stato e regioni (capo V del testo, artt. 37-50), non vi sono particolari innovazioni rispetto a quanto statuito dalla Corte costituzionale con l'importante sentenza n. 271/2005 (sulla quale v. anche par. 21.3), circa la titolarità esclusiva dello Stato a legiferare in materia della protezione di dati personali in quanto "*essenzialmente riferibile, all'interno delle materie legislative di cui all'art. 117 Cost., alla categoria dell'ordinamento civile*".

La pronuncia della Corte è intervenuta su una questione complessa e dibattuta anche in sede parlamentare successivamente alla modifica del titolo V della Costituzione. La materia in esame, ha affermato la Corte, rientra tra le situazioni nella titolarità esclusiva del potere legislativo da parte dello Stato. L'adozione da parte delle regioni, nell'esercizio della loro potestà legislativa esclusiva o concorrente, di norme attinenti direttamente alla protezione dei dati personali, se può apparire giustificata e legittimata dalla natura "trasversale" della normativa sulla *privacy* e in ragione del suo vasto e articolato ambito di applicazione, deve tuttavia limitarsi a meglio specificare i principi o le norme generali già contenuti nella legislazione statale.

Su questi presupposti, anche nel 2005 l'Autorità ha proseguito l'attività di monitoraggio svolta anche in passato con finalità essenzialmente conoscitive e di ricognizione di nodi problematici, imperniata anche sulla verifica della conformità degli atti normativi e regolamentari delle regioni alla normativa statale sulla protezione dei dati personali.

I profili tematici e problematici emersi dall'esame dei numerosi testi normativi effettuato nel 2005 sono, in gran parte, sostanzialmente analoghi a quelli già evidenziati nella *Relazione* 2004; particolare attenzione è stata rivolta all'applicazione del principio di pertinenza e non eccedenza, specialmente per quanto riguarda il trattamento di dati sensibili da parte di soggetti pubblici.

Per assicurare il rispetto della ripartizione costituzionale di competenze, si è tra gli altri criteri utilizzato frequentemente, nei casi dubbi, quello proposto anche in dottrina, consistente nel verificare se le norme regionali definiscano le posizioni soggettive e i rapporti giuridici dei soggetti coinvolti in termini diversi rispetto a quelli stabiliti dal legislatore nazionale, attribuendosi in tal caso alle stesse una valenza privatistica che le ascriverebbe alla materia dell'ordinamento civile, sottratta quindi alla competenza regionale.

In questo quadro è emersa, come rilevato dal presidente del Garante nel corso di un'audizione svoltasi il 26 maggio 2005 presso la Commissione affari costituzionali del Senato della Repubblica, l'opportunità di prevedere e, comunque, di realizzare adeguate modalità di raccordo e scambio di valutazioni anche fra il Garante e le regioni; meritano una citazione, come momento di raccordo, le collaborazioni informali con gli organismi rappresentativi delle autonomie locali e territoriali in vista del parere sullo schema tipo di regolamento sul trattamento dei dati sensibili e giudiziari, di cui più dettagliatamente si riferisce in altra parte di questa *Relazione* (*v.* par. 2.2.1).

1.4. *Altre novità normative con riflessi in materia di protezione di dati personali*

Nel corso dell'anno sono stati approvati altri provvedimenti normativi riguardanti la materia del trattamento dei dati personali e l'attività del Garante.

In proposito, vanno ricordati, in particolare:

Costituzione

a) la predetta legge costituzionale di modifica della Parte II della Costituzione, che menziona espressamente le autorità indipendenti nella Carta costituzionale. Il nuovo art. 98-*bis* Cost. prevede infatti che, per lo svolgimento di attività di garanzia o di vigilanza in materia di diritti di libertà garantiti dalla Costituzione e su materie di competenza dello Stato, si possano istituire con legge apposite autorità indipendenti, stabilendone la durata del mandato, i requisiti di eleggibilità e le condizioni di indipendenza. Le autorità riferiscono alle Camere sui risultati delle attività svolte. La legge costituzionale, approvata a maggioranza assoluta, ma inferiore ai due terzi dei componenti di ciascuna Camera, e pubblicata nella *G.U.* 18 novembre 2005, n. 269, è come è noto in procinto di essere sottoposta a *referendum* popolare confermativo ai sensi dell'art. 138 Cost.;

"Dematerializzazione" della corrispondenza nella pubblica amministrazione

b) la l. 23 dicembre 2005, n 266 (legge finanziaria per il 2006), la quale reca una delicata previsione che consente una "dematerializzazione" della corrispondenza delle pubbliche amministrazioni (art. 1, comma 51). La disposizione mira a collocarsi nel solco del processo di informatizzazione della pubblica amministrazione e, in particolare, dell'automatizzazione delle procedure, mediante la formazione dei documenti in formato elettronico, il trasferimento su supporto digitale della documentazione cartacea, l'utilizzo del protocollo informatico e dei sistemi di classificazione e di fascicolazione elettronica. Peraltro, il "Codice dell'amministrazione digitale" contiene già una norma sulla dematerializzazione dei documenti delle pubbliche amministrazioni, in base alla quale le amministrazioni sono tenute a valutare in termini di rapporto costi-benefici il recupero su supporto informatico dei documenti cartacei dei quali sia necessaria o opportuna la conservazione, predisponendo i conseguenti piani di sostituzione degli archivi cartacei con archivi informatici (art. 42 d.lg. n. 82/2005). La disposizione contenuta nella legge finanziaria sembra andare oltre tale previsione, consentendo alle pubbliche amministrazioni anche di stipulare convenzioni con soggetti pubblici o privati per il trasferimento su supporto informatico degli invii di corrispondenza da e per gli uffici pubblici, ed individuando nel concessionario del servizio pubblico universale un soggetto abilitato a tale dematerializzazione. La norma richiede altresì che le pubbliche amministrazioni si avvalgano, in ogni caso, di servizi informatici e telematici che assicurino l'integrità del messaggio nella fase di trasmissione informatica, attraverso la certificazione tramite firma digitale o altri strumenti che garantiscano l'integrità legale del contenuto, la marca temporale e l'identità dell'ente certificatore che presidia il processo. Il concessionario del servizio postale viene obbligato, poi, ad individuare i dirigenti preposti alla certificazione di conformità del documento informatico riproduttivo del documento originale cartaceo. È di tutta evidenza la particolare delicatezza di questi processi, che richiedono approfondite valutazioni per contemperare le esigenze di potenziamento dell'efficienza delle P.a. con una rigorosa serie di cautele volte a prevenire la dispersione o l'utilizzo di dati per finalità non consentite o comunque indebito, considerato anche l'incisivo ruolo previsto per soggetti esterni alla P.a.;

Tecniche di comunicazione a distanza

c) il d.l. 30 dicembre 2005, n. 273 (cui si è fatto già riferimento a proposito delle proroghe dei termini in materia di misure di sicurezza e di regolamenti sui dati sensibili e giudiziari, al par. 1.1), convertito, con modificazioni, dalla l. n. 51/2006, il cui art. 19-*bis* modifica l'art. 58, comma 2, del "Codice del consumo" (d.lg. 6 settembre 2005, n. 206), prevedendo che le disposizioni che individuano i limiti di utilizzo di tecniche di comunicazione per la conclusione di contratti a distanza si applichino anche in deroga alle norme previste dal Codice;

Attività delle autorità indipendenti in materia di tutela del risparmio

d) la l. 28 dicembre 2005, n. 262, recante "*Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*", la quale prevede (art. 21) forme di collaborazione tra la Banca d'Italia, la Commissione nazionale per la società e la borsa (Consob), l'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Isvap), la Commissione di vigilanza sui fondi pensione (Covip) e l'Autorità garante della concorrenza e del mercato, anche mediante scambio di informazioni, al fine di agevolare l'esercizio delle rispettive funzioni. D'interesse per il Garante appaiono, in particolare, le disposizioni generali sui procedimenti di competenza delle autorità e, in particolare, l'articolo 23, il quale disciplina i procedimenti per l'adozione di atti regolamentari e generali da parte delle citate autorità indipendenti;

Nuova disciplina delle attività trasfusionali

e) la l. 21 ottobre 2005, n. 219, recante nuove norme in materia di attività trasfusionali e di produzione degli emoderivati, la quale disciplina le attività trasfusionali comportanti la raccolta, oltre che del sangue e degli emocomponenti, anche delle cellule staminali. La legge prevede l'istituzione di un sistema informativo dei servizi trasfusionali, le cui caratteristiche saranno definite con decreto del Ministro della salute, al quale è demandata anche l'individuazione di un sistema di codifica che, *"nel rispetto delle norme sulla tutela e riservatezza dei dati sensibili"*, identifichi il donatore e il ricevente, nonché gli emocomponenti e le strutture trasfusionali. Il Garante dovrà fornire indicazioni sulle garanzie e cautele da adottare nel trattamento di tali dati in occasione dell'espressione del parere sullo schema di decreto, previsto ai sensi dell'articolo 154, comma 4, del Codice;

Misure di contrasto all'evasione fiscale

f) il d.l. 30 settembre 2005, n. 203 (*cd.* "collegato" alla manovra finanziaria per il 2006), convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248, recante misure di contrasto dell'evasione fiscale. Il decreto ha introdotto alcune disposizioni volte ad agevolare l'accesso dei comuni a banche di dati, nonché quello dei "concessionari" a dati personali utili ai fini della riscossione dei tributi. Il Garante, nel corso della discussione parlamentare del decreto e nell'esercizio del proprio compito di segnalazione al Parlamento, ha richiamato l'attenzione della Commissione finanze del Senato sull'esigenza di coordinare tali disposizioni con quelle previste dal Codice, in particolare per quanto riguarda il principio di pertinenza e non eccedenza dei dati accessibili per finalità istituzionali, e per ciò che attiene all'obbligo per i "concessionari" di informare i debitori ai sensi dell'articolo 13 del Codice. La necessità di procedere ad un'idonea informativa degli interessati è stata richiamata dal Garante anche con un *provvedimento* generale del 25 maggio 2005 [doc. *web* n. 1131826] riguardante alcune disposizioni della legge finanziaria del 2005 –che hanno aumentato il patrimonio informativo a disposizione degli organi preposti alla riscossione dei tributi– al fine di assicurare che le esigenze di riscossione dei crediti pubblici possano essere soddisfatte, ma rispettando pienamente, al tempo stesso, le garanzie e i diritti fondamentali dei soggetti interessati (sul punto *v.*, *amplius*, il par. 2.9);

Frodi e carte di pagamento

g) la l. 17 agosto 2005, n. 166, che ha introdotto un sistema di prevenzione delle frodi mediante carte di pagamento, istituendo una apposita banca dati presso l'Ufficio centrale antifrode dei mezzi di pagamento (Uncamp) del Ministero dell'economia e delle finanze (art. 1). Nell'archivio dovranno confluire, tra l'altro, i dati identificativi dei punti di vendita e dei rappresentanti legali degli esercizi commerciali nei cui confronti venga revocata la convenzione di negoziazione delle carte di pagamento, nonché i dati di tutte le transazioni contestate dai titolari delle carte concluse presso un determinato punto vendita (art. 2) ed altre informazioni relative al rischio di frode (art. 3). L'art. 7 della legge prevede inoltre l'adozione di un decreto di attuazione che dovrà individuare in dettaglio i dati e le informazioni da inserire nell'archivio, stabilendo le modalità di accesso ai dati da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno. Il medesimo decreto dovrà infine regolare i termini e le modalità per la comunicazione e la gestione dei dati e delle informazioni, i livelli di accesso all'archivio informatizzato e le modalità di consultazione delle informazioni ivi contenute. Pur non essendo prevista espressamente dalla legge in esame la consultazione del Garante, l'amministrazione competente dovrà acquisire comunque il parere dell'Autorità, ai sensi dell'articolo 154, comma 4, del Codice;

***Cd.* "abusi di mercato"**

h) la l. 18 aprile 2005, n. 62 (legge comunitaria 2004), il cui art. 9 ha recepito la direttiva n. 2003/6/Ce del Parlamento europeo e del Consiglio dell'Unione europea del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (*cd.* "abusi di mercato"). La disposizione attribuisce alla Consob poteri di informazione e di indagine, in relazione ai quali –nel corso dei lavori parlamentari– questa Autorità ha suggerito alla competente Commissione della Camera alcune proposte emendative volte ad armonizzare il testo con la disciplina in materia di protezione dei dati personali, in particolare per quanto riguarda l'applicazione delle previste garanzie in caso di comunicazione o diffusione dei dati e di acquisizione di dati di traffico. La legge, inoltre, ha conferito delega al Governo per recepire la direttiva n. 2003/98/Ce del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo dell'informazione nel settore pubblico. Tale delega è stata attuata con d.lg. 24 gennaio 2006, n. 36, in relazione al quale il Garante ha fornito alla Presidenza del Consiglio dei ministri gli elementi di valutazione richiesti (*cfr.*, sul punto, quanto riportato a p. 10);

Modifiche al codice di procedura civile

i) il d.l. 14 marzo 2005, n. 35 (*cd.* "sulla competitività"), convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80, e successivamente modificato dalla l. 28 dicembre 2005, n. 263, che ha conferito, fra l'altro, una delega al Governo per apportare talune modifiche al codice di procedura civile per una riforma organica della disciplina delle procedure concorsuali. In tale contesto, sono stati ulteriormente modificati gli artt. 490 e 570 c.p.c. in materia di pubblicità degli avvisi concernenti l'esecuzione forzata –norme sulle quali era già intervenuto il Codice, prevedendo disposizioni a garanzie della riservatezza del debitore esecutato (art. 174, commi 9 e 10, del Codice). Le nuove modifiche rendono pubblicabili su specifici siti Internet individuati dal Ministero della giustizia, oltre che l'avviso dell'esecuzione –opportunamente privato delle generalità del debitore– la copia dell'ordinanza del giudice e la relazione di stima del bene oggetto di esecuzione (art. 490, secondo comma, c.p.c.). Il pubblico avviso, in caso di espropriazione immobiliare, deve contenere l'indicazione del nome e del recapito

telefonico del custode nominato in sostituzione del debitore (art. 570 c.p.c.). É inoltre consentito all'ufficiale giudiziario, ai fini della ricerca di cose da sottoporre ad esecuzione e previa autorizzazione del giudice, di rivolgere una richiesta ai soggetti gestori dell'anagrafe tributaria e di altre banche dati pubbliche (art. 492 c.p.c.);

Disciplina dell'accesso ai documenti amministrativi

l) la l. 11 febbraio 2005, n. 15, di riforma della l. 7 agosto 1990, n. 241, la quale reca alcune importanti disposizioni di coordinamento con le norme del Codice, volte a disciplinare l'accesso ai dati personali, in particolare di natura sensibile, e ad istituire una "collaborazione" fra il Garante e la Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei ministri, nei procedimenti per i quali rilevino, allo stesso tempo, questioni concernenti l'accesso ai documenti e il trattamento dei dati personali. Nel corso dei lavori parlamentari, la Commissione affari costituzionali del Senato ha recepito alcuni suggerimenti dell'Autorità per un miglior coordinamento delle disposizioni della legge con quelle del Codice;

Documenti elettronici

m) il d.l. 31 gennaio 2005, n. 7 (*cd.* "*omnibus*"), convertito, con modificazioni, dalla l. 31 marzo 2005, n. 43, che ha fissato al 1° gennaio 2006 la data a decorrere dalla quale devono essere rilasciati in formato elettronico il passaporto, il visto, il permesso di soggiorno e la carta d'identità (art. 7-*vicies ter* d.l. n. 7/2005).

Risultano di interesse per la protezione dei dati personali anche diversi decreti legislativi adottati dal Governo in base a specifiche deleghe, conferite per il riassetto della normativa in importanti settori. In alcuni casi il Governo, nel quadro di una collaborazione istituzionale che ha dato diversi frutti, ha richiesto all'Autorità di formulare osservazioni o indicazioni sui profili della protezione dei dati personali, che sono state tenute in considerazione ai fini della redazione del testo poi approvato (*v.* anche par. 21.2.).

Fra gli altri, vanno ricordati, in particolare:

Riutilizzo di documenti nel settore pubblico

a) il d.lg. 24 gennaio 2006, n. 36, relativo al riutilizzo di documenti nel settore pubblico e adottato in attuazione della direttiva 2003/98/Ce che individua le condizioni e le modalità affinché il riutilizzo delle informazioni e dei documenti nel settore pubblico avvenga con modalità non discriminatorie e in termini rispettosi dei diritti della persona. Il Garante, nel formulare il richiesto parere, ha espresso alcune osservazioni sui profili riguardanti la protezione dei dati personali, che sono state sostanzialmente recepite (*Parere* 27 ottobre 2005 [doc *web* n. 1185170]);

Codice del consumo

b) il d.lg. 6 settembre 2005, n. 206, recante il "Codice del consumo", in attuazione della delega attribuita al Governo dall'art. 7 della l. n. 229/2003 (legge di semplificazione 2001), che incide solo formalmente sull'articolo 179, comma 3, del Codice, lasciando inalterata la potestà sanzionatoria del Garante in caso di mancato rilascio dell'informativa all'interessato nei contratti a distanza;

Codice delle assicurazioni private

c) il d.lg. 2 settembre 2005 n. 209, recante il "Codice delle assicurazioni private", in attuazione della delega attribuita al Governo dall'art. 4 della predetta l. n. 229/2003, nel quale sono state trasfuse le disposizioni relative al funzionamento della Banca dati sinistri e del Centro di informazione italiano, già istituiti presso l'Isvap, nonché quelle in materia di accesso agli atti detenuti dalle imprese di assicurazione;

Codice dell'amministrazione digitale

d) il d.lg. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale", in attuazione della delega prevista dall'art. 10 della medesima l. n. 229/2003, volto ad incrementare la modernizzazione della pubblica amministrazione attraverso l'utilizzo delle tecnologie e a riconoscere nuovi

diritti ai cittadini, anche attraverso una più ampia partecipazione ai procedimenti amministrativi ed una più efficace accessibilità ai servizi in rete. Le osservazioni formulate dall'Autorità sullo schema di decreto sono state in parte recepite (*Note* 14 febbraio e 1° marzo 2005);

Sistema pubblico di connettività

e) il d.lg. 28 febbraio 2005, n. 42, che istituisce il Sistema pubblico di connettività (Spc) e la Rete internazionale della pubblica amministrazione, destinati a sostituire la Rete unitaria della pubblica amministrazione (Rupa). Il Spc tende a sviluppare la condivisione e la circolarità del patrimonio informativo della pubblica amministrazione, attraverso infrastrutture tecnologiche che assicurino l'interoperabilità dei sistemi informatici e dei flussi informativi e garantiscano, allo stesso tempo, la sicurezza e la riservatezza delle informazioni. Anche in relazione a tale atto normativo, l'Autorità ha formulato alcune osservazioni sugli aspetti concernenti la protezione dei dati personali (*Nota* 10 febbraio 2005).

PAGINA BIANCA

L'ATTIVITÀ SVOLTA DAL GARANTE

PAGINA BIANCA

II - L'attività svolta dal Garante

2 Trattamenti effettuati in ambito pubblico

2.1. *Profili introduttivi*

L'anno trascorso ha contraddistinto una fase di rilievo per le pubbliche amministrazioni, chiamate ad attivarsi più incisivamente del passato nel riconoscere e rendere pubbliche alcune garanzie previste, in particolare, per il trattamento dei dati sensibili e giudiziari.

Le nuove scadenze di legge previste a conclusione di un periodo transitorio sproporzionatamente lungo, caratterizzato da numerose e ingiustificate proroghe, pur imponendo alle amministrazioni pubbliche di concludere l'*iter* per l'adozione dei necessari atti di natura regolamentare per il trattamento dei dati sensibili e giudiziari, hanno esposto il nostro Paese a procedure di infrazione per la violazione del diritto comunitario. L'utilizzo delle predette informazioni è soggetto, infatti, a rigorose cautele in base alla disciplina comunitaria, la quale vieta in linea di principio il loro trattamento a meno che, in chiave di assoluta eccezione, ricorrano specifici motivi di interesse pubblico rilevante e siano altresì assicurate adeguate garanzie (art. 8 direttiva n. 95/46/Ce).

La predisposizione dei predetti regolamenti, oltre a costituire un adempimento necessario in base al Codice, ha offerto all'intera amministrazione pubblica un'occasione significativa per proseguire, anche sotto il profilo delle garanzie e della trasparenza, il sofferto processo di modernizzazione delle proprie strutture, rendendo possibile un adeguamento del proprio assetto organizzativo e funzionale anche in riferimento al rispetto dei diritti e delle libertà fondamentali della persona, che trovano un immediato riflesso in ogni settore di attività della pubblica amministrazione.

L'Autorità è stata chiamata nuovamente a verificare il rispetto della disciplina in materia di protezione dei dati personali in diversi settori della P.a. in cui sono peraltro intervenute nuove disposizioni speciali. Si è potuto, così, registrare una più marcata consapevolezza nel corpo sociale della necessità di tutelare maggiormente e in termini più specifici il diritto fondamentale alla protezione dei dati personali, anche in particolari ambiti che, finora, non erano stati oggetto di espressa valutazione.

Quest'opera più analitica di controllo sul corretto trattamento dei dati da parte dei soggetti pubblici ha permesso peraltro di riscontrare alcuni ritardi e incertezze applicative, talvolta fisiologici, talaltra connessi a ingiustificate preoccupazioni o letture normative connaturate solo in parte alla necessità di coniugare l'innovativo quadro di garanzie per i diritti e le libertà fondamentali nel trattamento dei dati con specifiche procedure proprie di singole amministrazioni legate anche a norme risalenti nel tempo.

2.2. *Regolamenti sui trattamenti di dati sensibili e giudiziari*

I soggetti pubblici possono trattare i dati sensibili esclusivamente in base ad un'espressa disposizione di legge che lo consenta espressamente, individuando i tipi di dati utilizzabili, le operazioni eseguibili e il carattere di rilevante interesse pubblico delle finalità perseguite (artt. 20, comma 1, e 21, comma 1, del Codice); riguardo ai dati giudiziari, il trattamento può essere autorizzato anche in base ad un provvedimento del Garante (art. 21, comma 1).

Come già evidenziato in passato, laddove siano specificate per legge solo le "rilevanti finalità di interesse pubblico", l'amministrazione interessata può trattare i dati sensibili e giudiziari qualora adotti un apposito atto di reale natura regolamentare che identifichi i tipi di dati utilizzati e di operazioni su di essi eseguibili, conformandosi al parere reso in proposito dal Garante (artt. 20, comma 2, e 21, comma 2, del Codice); tale parere può essere espresso dall'Autorità anche su schemi-tipo, nella prospettiva di rispettare il principio di semplificazione (art. 2, comma 2, del Codice) e di armonizzare un livello elevato di tutela dei diritti rispetto all'operato delle singole amministrazioni.

In merito, nonostante l'emanazione dei regolamenti fosse stata già imposta vigente la legge n. 675/1996, il Codice, prevedendo un ulteriore periodo transitorio di adeguamento a favore delle amministrazioni, aveva indicato, in un primo tempo, il 30 settembre 2004 quale nuova scadenza per adottare i predetti regolamenti. Tale scadenza è stata successivamente differita al 31 dicembre 2005 (l. 27 luglio 2004, n. 188, di conversione del d.l. 24 giugno 2004, n. 158) e nel corrente anno, giova evidenziarlo, il termine è stato ulteriormente prorogato (dapprima al 28 febbraio 2006, poi al 15 maggio 2006 e, infine, al 31 luglio 2006: art. 181 del Codice, come modificato dall'art. 10 d.l. 30 dicembre 2005, n. 273, convertito, con modificazioni, con l. 23 febbraio 2006, n. 51 e dal d.l. 12 maggio 2006, n. 173).

Provvedimento generale sui regolamenti per il trattamento dei dati sensibili e giudiziari nella P.a.

Nel corso del 2005, in previsione della predetta scadenza, il Garante ha adottato un *provvedimento* generale con il quale ha fornito nuove indicazioni a tutti i soggetti pubblici per favorire una migliore ricognizione dei trattamenti e la predisposizione del contenuto degli atti regolamentari in questione (*Provv.* 30 giugno 2005 [doc. *web* n. 1144445], pubblicato in *G.U.* 23 luglio 2005, n. 170).

Il Garante ha in primo luogo segnalato alle amministrazioni che la prosecuzione del trattamento di dati sensibili e giudiziari in carenza del necessario supporto normativo, dopo la menzionata scadenza, concretizzerebbe un illecito (con conseguenti responsabilità di diverso ordine, anche contabile e per danno erariale), e potrebbe inoltre comportare sia l'inutilizzabilità dei dati trattati indebitamente, sia il possibile intervento di provvedimenti anche giudiziari di blocco o di divieto del trattamento (art. 154 del Codice; art. 11, commi 1, lett. *a*), e 2, del Codice). Analoga riflessione è stata svolta in riferimento ai trattamenti di dati che non saranno menzionati nei regolamenti, trattamenti che non potranno essere effettuati.

L'Autorità ha poi evidenziato la possibilità, prevista nel Codice, di procedere alla predisposizione di schemi-tipo operanti per insiemi omogenei di amministrazioni, rispetto ai quali può essere pertanto espresso dal Garante un unico parere, al fine sia di rendere più organiche le garanzie in riferimento ad altre amministrazioni, sia di semplificare l'*iter* di approvazione degli atti.

L'Autorità ha in seguito sottolineato che le pubbliche amministrazioni che adottano un regolamento conforme allo schema-tipo approvato dal Garante non devono chiedere singolarmente al Garante di esprimere il parere previsto ai sensi degli artt. 20, comma 2, 21, comma 2 e 154, comma 5, del Codice (*Nota* 16 febbraio 2005). Le medesime amministrazioni devono invece sottoporre al Garante

uno schema di regolamento per il parere qualora manchi uno schema-tipo sul quale si sia già espressa favorevolmente l'Autorità, oppure nell'ipotesi in cui l'amministrazione intenda apportare a tale schema-tipo già esaminato modifiche sostanziali o integrazioni non formali, che riguardino categorie di dati o tipologie rilevanti di operazioni, precedentemente non considerati (*Nota* 11 novembre 2005).

L'Autorità ha inoltre fornito ulteriori chiarimenti sulla natura della disciplina regolamentare prevista dal Codice, segnalando che le amministrazioni pubbliche (quali, ad esempio, taluni enti vigilati o controllati) non possono avvalersi di atti e decreti che, pur essendo a volte denominati quali "regolamenti", non abbiano in base alla legge la necessaria natura di reale fonte normativa suscettibile di incidere su diritti e libertà fondamentali di terzi. Le amministrazioni non possono in particolare avvalersi di meri regolamenti interni od organizzativi che non abbiano, in base alla legge, i necessari caratteri di innovatività nell'ordinamento, generalità ed astrattezza, dovendo assicurare comunque l'adozione di un atto di effettiva natura regolamentare, promuovendone quindi, se necessario, l'adozione da parte della competente amministrazione di riferimento (*Note* 23 e 24 gennaio 2006).

Collaborazione per la predisposizione di schemi di regolamento

Al fine di contribuire alla corretta applicazione del Codice, il Garante, in vista delle scadenze di legge, ha in ogni caso intensificato la collaborazione finalizzata alla predisposizione degli schemi (come pure di schemi-tipo) di regolamento, alcuni dei quali da tempo in fase di studio; ciò, con organismi rappresentativi di regioni, autonomie locali ed università, nonché, in riferimento alle rispettive funzioni istituzionali, con la Presidenza del Consiglio dei ministri ed altri soggetti pubblici.

Infine, l'Autorità, a seguito di interpelli anche informali, ha fornito innumerevoli chiarimenti e delucidazioni a diversi soggetti pubblici (ministeri, autorità indipendenti, istituti di ricerca, istituti previdenziali ed assicurativi), in ordine alla corretta predisposizione degli schemi di regolamento di competenza. Si è così favorita una maggiore conformità al Codice degli schemi sottoposti al parere già nella fase della loro elaborazione, con conseguente incremento dei pareri favorevoli che hanno constatato il già intervenuto recepimento di indicazioni fornite nel quadro dei contatti tra le amministrazioni interpellanti e l'Ufficio del Garante.

L'esame comparato di un elevato numero di schemi di regolamento ha permesso all'Autorità di disporre di un orizzonte più ampio per valutazioni organiche sul modo con cui le P.a. trattano dati delicati per la sfera delle persone.

Si è potuta, tra l'altro, rilevare la frequente ricorrenza di alcuni profili critici che non hanno a volte consentito di valutare positivamente gli schemi sottoposti per il parere o, più spesso, di esprimere un parere favorevole in termini generali, ma con varie "condizioni" che hanno impegnato a fondo l'attività istruttoria del parere risultata particolarmente onerosa per l'Autorità. Si è ad esempio riscontrata la tendenza di talune amministrazioni a "legalizzare" mediante lo schema predisposto un insieme di trattamenti che non rientrava tra le attribuzioni istituzionali di riferimento, oppure di modalità di trattamento obiettivamente sproporzionate in rapporto alle finalità perseguite.

In numerosi casi si è reso necessario richiamare l'attenzione delle pubbliche amministrazioni in ordine alla necessità di prendere in considerazione nei regolamenti le sole, specifiche finalità di rilevante interesse pubblico, perseguite di volta in volta dall'ente in rapporto alle attività istituzionali svolte, già individuate specificamente dal Codice o, come quest'ultimo prevede, da un'espressa previsione di legge che, anche se collocata fuori del Codice, le evidenzi comunque puntualmente nei termini richiesti (art. 20 e parte II del Codice). Per altro verso, si è non di rado rilevato l'inserimento, negli schemi, di richiami generici alla normativa vigente, oppure a non meglio precisate "finalità pubbliche", con conseguente prescrizione da parte

dell'Autorità dell'inserimento di richiami più puntuali alla disciplina di riferimento.

Si è altresì esaminata un'ulteriore problematica di fondo, riguardante la possibilità per determinati soggetti di adottare atti aventi effettiva natura regolamentare: si pensi agli organismi strumentali dotati unicamente di autonomia gestionale, costituiti dagli enti locali per la cura associata di uno o più servizi e funzioni pubblici locali, ovvero alle aziende di servizi alla persona con personalità giuridica di diritto pubblico. In tali ipotesi, è stato necessario rilevare che le amministrazioni non possono avvalersi, nel caso di specie, di meri atti che, anche se denominati regolamenti, non hanno, anche per la loro eventuale rilevanza solo interna, la necessaria natura di fonte regolamentare suscettibile di incidere su diritti e libertà fondamentali di terzi. Tali soggetti sono stati pertanto invitati ad assicurare l'utilizzazione di un atto di natura effettivamente regolamentare, promuovendone se del caso l'adozione da parte delle competenti amministrazioni di riferimento le quali esercitino, ad esempio, poteri di indirizzo e controllo (*Note* 15 novembre e 2 dicembre 2005).

Particolarmente impegnativa è stata, per l'Autorità, la verifica dell'indispensabilità del trattamento delle tipologie di informazioni sensibili e giudiziarie individuate negli schemi-tipo (art. 22, comma 3, del Codice). In numerosi casi, si è conseguentemente reso necessario depennare categorie di dati sensibili o giudiziari o di operazioni di trattamento individuate negli schemi.

In particolare, è stata rivolta l'attenzione sulle operazioni che possono spiegare effetti maggiormente significativi per l'interessato, e per le quali devono pertanto essere assicurate opportune garanzie. Spesso, infatti, non è risultata comprovata l'indispensabilità delle operazioni di interconnessione con altri titolari del trattamento, pubblici o privati: non sono mancati i casi in cui si è registrata la carenza di una rigorosa delimitazione in conformità al principio di indispensabilità, ovvero dell'individuazione della base normativa che autorizza le predette operazioni (art. 22, commi 9 e 11 del Codice). Il Garante ha quindi richiesto di verificare di volta in volta se l'operazione consistesse effettivamente in una interconnessione o in un diverso tipo di collegamento per via telematica volto ad ottenere informazioni o certificazioni dal medesimo o da altri titolari del trattamento, senza una consultazione diretta di banche dati.

Oggetto di attente verifiche sono state, altresì, le operazioni di comunicazione e diffusione individuate: con riferimento alle prime, si è reso necessario richiamare l'attenzione delle amministrazioni pubbliche in ordine alla necessità di delimitarle ed evidenziarle rigorosamente in considerazione del principio di stretta indispensabilità, indicando il motivo per cui si effettua la predetta operazione, nonché l'eventuale base normativa; con riferimento alle seconde, è stata sempre evidenziata la necessità di riportare l'espressa disposizione di legge che le autorizzi (art. 22, comma 11, del Codice).

Si è reso poi necessario sottolineare, in diverse occasioni, che con l'atto di natura regolamentare vanno identificati unicamente i tipi di dati sensibili e giudiziari trattati, nonché i tipi di operazioni su di essi eseguibili, e non altri aspetti riguardanti il rispetto della normativa in materia di protezione dei dati personali. Spesso, infatti, le amministrazioni pubbliche hanno disciplinato con l'atto in questione le modalità di esercizio del diritto di accesso ai propri dati personali da parte dell'interessato (artt. 7-10 del Codice); l'informativa (art. 13); l'individuazione ed i compiti del titolare, di eventuali responsabili e degli incaricati del trattamento (artt. 28-30); l'esercizio del diritto di accesso ai documenti amministrativi (artt. 59 e 60); l'adozione delle misure di sicurezza (artt. 31-36). Nelle predette ipotesi, l'Autorità ha osservato che non deve pertanto essere effettuata alcuna comunicazione al Garante in ordine ai predetti adempimenti e che dalla circostanza che l'Autorità abbia ricevuto even-

tuali note in proposito, il titolare del trattamento non può desumere alcun assenso o autorizzazione a proseguire il trattamento dei dati con le modalità dichiarate.

Occorre altresì evidenziare che, in numerosi casi, l'Autorità è stata interpellata in ordine a trattamenti di dati sensibili già disciplinati in sede legislativa ovvero, nel caso dei dati giudiziari, anche con provvedimento del Garante, per i quali, pertanto, è stato rilevato che il soggetto pubblico non deve provvedere con proprio regolamento.

2.2.1. *Enti locali*

Nel quadro della collaborazione instaurata con organismi rappresentativi di comuni, comunità montane e province, è stata ultimata la predisposizione dei rispettivi schemi-tipo di regolamento.

Comuni

Per quanto riguarda, in particolare, i comuni, l'Anci (Associazione nazionale dei comuni italiani), in collaborazione con il Garante, ha elaborato nel 2005 il relativo schema-tipo di regolamento anche alla luce delle proposte di modifica e delle integrazioni prospettate durante la fase della consultazione pubblica effettuata nel 2004. Il Garante ha poi espresso parere positivo (*Parere* 21 settembre 2005 [doc. *web* n. 1170239]) sullo schema definitivo [doc *web* n. 1174532].

In considerazione dei numerosi trattamenti di dati sensibili e giudiziari effettuati in un'amministrazione con articolate competenze come quella comunale, lo schema-tipo di regolamento per i comuni è corredato da trentacinque schede comprensive di diverse finalità di rilevante interesse pubblico individuate nel Codice (artt. 62-73, 86, 90, 95 e 112).

In particolare, le schede riguardano i trattamenti relativi alla gestione del personale impiegato a vario titolo presso il comune e quelli relativi ai servizi demografici, anagrafici, di stato civile ed elettorale; si riferiscono, inoltre, ai trattamenti di dati sensibili e giudiziari rinvenibili presso i servizi sociali, alle attività amministrative curate dalla polizia municipale, così come a quelle esperite per il patrocinio e la difesa in giudizio dell'amministrazione. Infine, un'ulteriore serie di schede censisce le attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione.

Comunità montane

L'Uncem (Unione nazionale comuni comunità enti montani) ha redatto il proprio schema-tipo di regolamento utilizzando il predetto schema-tipo predisposto per i comuni dal quale sono state espunte alcune schede in considerazione delle specifiche e rilevanti finalità di interesse pubblico perseguite per legge dalle comunità montane. Anche in questo caso, il parere del Garante è risultato positivo (*Parere* 19 ottobre 2005 [doc. *web* nn. 1182188]). Lo schema-tipo [doc *web* n. 1182195] si compone pertanto di un articolato integrato solo da diciannove schede che individuano i tipi di dati e di operazioni in relazione alla gestione del personale dipendente, all'attuazione di servizi sociali, all'espletamento dei servizi di istruzione e cultura, di polizia municipale, dell'avvocatura e relativi alle politiche del lavoro.

Province

Lo schema-tipo di regolamento riguardante i trattamenti di dati sensibili e giudiziari effettuati presso le province [doc *web* n. 1175584] è frutto della collaborazione con l'Upi (Unione delle province d'Italia). Anche in questo caso, il progetto di schema-tipo, nell'ambito di una consultazione pubblica, è stato messo a disposizione delle province, dal 20 aprile al 15 maggio 2005, al fine di sollecitare eventuali proposte di modifica o integrazioni; sulla versione definitiva il Garante si è espresso positivamente (*Parere* 7 settembre 2005 [doc. *web* nn. 1174562]).

Lo schema-tipo di regolamento per le province contiene, anch'esso, un articolato, cui fanno seguito quindici schede corrispondenti alla gestione dei dati nei rapporti di lavoro dipendente di qualunque tipo, da parte degli organi dell'ente, nonché del difensore civico. Le schede riguardano, inoltre, la gestione delle attività relative all'incontro domanda/offerta di lavoro e al contenzioso; le attività concernenti

le erogazioni di benefici a vario titolo, di vigilanza in materia ambientale e di sicurezza stradale; le attività attinenti al rilascio di autorizzazioni, abilitazioni ed iscrizioni agli albi; la protezione civile; l'organizzazione del servizio scolastico, la gestione delle biblioteche e dei centri di documentazione, nonché le attività riguardanti le iniziative di democrazia diretta.

Ulteriori specifiche attività

Diversi enti locali hanno successivamente richiesto un parere dell'Autorità in ordine al trattamento di dati sensibili e giudiziari per ulteriori attività (protezione civile, agevolazioni tributarie, volontariato, attività ricreative) che non figuravano, per tipologia di dati o di operazioni, negli schemi-tipo di regolamento già predisposti dall'Anci, dall'Upi e dall'Uncem.

Il Garante ha unificato la trattazione delle varie istanze pervenute esprimendo un unico parere nel quale ha previsto che tutti gli altri enti locali interessati a svolgere i medesimi trattamenti con le stesse modalità, possono effettuarli adottando o integrando i regolamenti di pertinenza sulla base delle indicazioni fornite dall'Autorità, senza che sia necessario sottoporre singolarmente all'Autorità ciascuno schema (*Parere* 29 dicembre 2005 [doc. *web* n. 1213424]).

In base a questo parere dell'Autorità, gli enti locali possono trattare informazioni sullo stato di salute dei cittadini nell'ambito delle competenze loro attribuite dalla legge in materia di protezione civile per programmare piani di emergenza e dare attuazione, in caso di calamità, a piani di evacuazione. I dati sull'origine razziale e etnica, opinioni politiche e religiose, salute e dati giudiziari possono essere utilizzati da comuni e province nell'ambito delle attività per il conferimento di onorificenze e ricompense, concessioni di patrocini e patronati. Le stesse tipologie di dati sono utilizzabili dai comuni per l'iscrizione di associazioni ed organizzazioni di volontariato negli albi comunali.

Oltre al trattamento dei dati sensibili già individuati nello schema-tipo Anci, i comuni possono trattare dati personali relativi alle convinzioni religiose e filosofiche nei casi in cui essi concedano agevolazioni tributarie o utilizzino fondi per interventi relativi ad edifici di culto, di partito o di associazioni.

Nei confronti di un altro cospicuo numero di enti locali, i quali avevano richiesto anch'essi il parere su schemi di regolamento, l'Autorità ha, invece, evidenziato che alcune tipologie di trattamento specificato nei medesimi schemi sono già ricomprese negli schemi-tipo. Si è fatto riferimento, in particolare, alle attività relative alla protocollazione ed archiviazione (*Nota* 23 febbraio 2006); al trattamento di dati idonei a rivelare lo stato di salute finalizzato alla concessione di contributi per l'abbattimento delle barriere architettoniche (*Nota* 3 marzo 2006); al trattamento di dati giudiziari per l'applicazione delle norme in materia di sanzioni amministrative e ricorsi, con particolare riferimento ai condoni edilizi (*Nota* 14 marzo 2006); al trattamento di dati sensibili dei volontari di protezione civile effettuato per gestire forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato (*Nota* 8 marzo 2006).

È stato inoltre rilevato che taluni dei trattamenti di dati sensibili sottoposti all'esame dell'Autorità risultavano già disciplinati in sede legislativa ovvero, nel caso dei dati giudiziari, in base ad un provvedimento del Garante, non occorrendo, per tali casi, che l'amministrazione provveda ad una specifica disciplina con regolamento. Tali ipotesi hanno riguardato i dati giudiziari trattati per adempiere ad obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o per espletare procedure relative a gare d'appalto (*Nota* 23 febbraio 2006); la notificazione di atti contenenti dati sensibili o giudiziari effettuata su delega dell'autorità giudiziaria (*Nota* 14 marzo 2006); il trattamento di dati sensibili e giudiziari effettuato nell'ambito del Programma statistico nazionale-Psn (*Nota* 31 marzo 2006); i

trattamenti di dati sensibili effettuati da farmacie comunali (*Nota* 14 marzo 2006).

L'Autorità è stata poi chiamata ad esprimere un parere anche in ordine al trattamento dei dati svolto da parte delle comunità comprensoriali.

Comunità comprensoriali

In proposito, nel rilevare che tali comunità sono enti di diritto pubblico (ai quali si applicano le norme di legge relative alle comunità montane che non siano incompatibili con le disposizioni della normativa di riferimento: art. 1, comma 2, d.P.G.p. 9 novembre 1981, n. 20-60/Legisl., recante "*Approvazione del testo unico delle leggi provinciali concernenti l'ordinamento e l'attività dei comprensori*"), l'Autorità ha adottato un provvedimento collegiale (*Parere* 30 novembre 2005 [doc. *web* n. 1202243]) con il quale ha segnalato che tali soggetti, anche in relazione alle competenze svolte per conto di comuni, possono avvalersi degli schemi-tipo di regolamento predisposti dall'Uncem per le comunità montane e dall'Anci per i comuni, sui quali il Garante ha espresso parere favorevole. I comprensori richiedenti sono stati quindi invitati a conformare lo schema di regolamento alle indicazioni fornite con il parere stesso, segnatamente per quanto concerne le operazioni di interconnessione, raffronto, comunicazione e diffusione.

2.2.2. *Regioni e province autonome*

L'Autorità aveva avviato nel 2004 una collaborazione con la Conferenza delle regioni e delle province autonome per la redazione di uno schema-tipo di regolamento sul trattamento dei dati personali sensibili e giudiziari effettuato presso regioni e province autonome, aziende sanitarie locali, enti e agenzie regionali e provinciali, nonché enti vigilati da regioni e province autonome.

Lo schema-tipo di regolamento sottoposto al parere del Garante alla fine del 2005 ha però evidenziato alcuni profili problematici che sono stati tuttavia approfonditi nel quadro del rapporto di collaborazione istituzionale tra gli uffici prima che il parere fosse espresso (*Nota* 30 dicembre 2005).

I profili di maggiore criticità hanno riguardato i trattamenti di dati personali connessi all'esercizio dell'attività epidemiologica del servizio sanitario regionale, ovvero l'ipotizzata attivazione verso l'amministrazione regionale di un flusso informativo sistematico di dati sulla salute degli assistiti, identificabili anche attraverso il codice fiscale, da parte dei soggetti erogatori dell'assistenza sanitaria territoriale. Al riguardo, è emersa l'esigenza di una revisione della bozza di schema-tipo consentendo comunque l'efficace esercizio delle funzioni di organizzazione, programmazione, valutazione e controllo dell'attività sanitaria da parte delle regioni nel pieno rispetto, però, delle garanzie previste dalla disciplina in materia di protezione dei dati personali.

Un'ulteriore problematica emersa nell'esame dello schema-tipo di regolamento riguardava l'ipotizzato svolgimento, da parte delle regioni, di un'attività amministrativa di *follow-up* nei confronti dei singoli assistiti, realizzata sulla base del predetto flusso informativo; attività che deve invece rimanere, anche in base ai principi del Codice, di esclusiva competenza delle strutture sanitarie.

A seguito dei rilievi formulati preliminarmente dall'Autorità, il testo aggiornato dello schema-tipo di regolamento è stato sottoposto all'esame del Garante con esito positivo (*Provv.* 13 aprile 2006 [doc. *web* n. 1272225]).

Le regioni e le province autonome hanno potuto pertanto avvalersi di tale schema-tipo in conformità al quale è stata resa possibile l'adozione dei necessari atti regolamentari sul trattamento di dati di pertinenza dei medesimi enti, nonché delle aziende sanitarie, degli enti e agenzie regionali/provinciali e degli enti vigilati dalla regione/provincia autonoma.

Sempre in riferimento ai trattamenti di dati sensibili e giudiziari svolti presso le regioni e le province autonome, il Garante ha esaminato un ulteriore schema-tipo

di regolamento predisposto dalla Conferenza dei Presidenti dell'assemblea, dei consigli regionali e delle province autonome, riguardante i trattamenti in ambito anch'esso regionale, ma effettuati presso assemblee e consigli regionali e provinciali. Il Garante ha espresso parere condizionato al rispetto di alcune indicazioni (*Provv.* 29 dicembre 2005 [doc. *web* n. 1210939]).

Per quanto riguarda, infine, la pubblicità immobiliare, è stata avviata una collaborazione con la Regione Friuli Venezia Giulia e le province autonome di Trento e Bolzano, al fine di elaborare una scheda-tipo da allegare al regolamento dei medesimi enti per i trattamenti di dati sensibili e giudiziari connessi con l'impianto e la tenuta dei libri fondiari, secondo il sistema in vigore nei territori già appartenenti all'impero austro-ungarico.

2.2.3. *Ministeri*

Accanto alle prime iniziative in materia intraprese dalle autonomie locali, nel 2005 alcune amministrazioni centrali hanno sottoposto anch'esse all'esame dell'Autorità propri schemi di regolamento su cui è stato espresso il parere nella prima parte del 2006.

Ministero della difesa

Il parere reso dal Garante all'amministrazione della difesa ha riguardato, in particolare, l'identificazione dei tipi di dati e di operazioni eseguibili in relazione ad una serie di trattamenti effettuati presso l'amministrazione, tra i quali quelli riguardanti il reclutamento, le assunzioni e l'impiego del personale civile e militare, la redazione e la tenuta dei documenti caratteristici, matricolari e dei fascicoli personali, il monitoraggio sanitario, le attività amministrative connesse alla tutela della salute dei dipendenti, l'assistenza sanitaria e l'attività medico-legale anche in favore di terzi, nonché la gestione del contenzioso giudiziale e stragiudiziale (*Parere* 9 marzo 2006 [doc. *web* n. 1259655]).

Altri ministeri

L'Autorità ha espresso parere positivo anche sullo schema di regolamento per i trattamenti dei dati sensibili e giudiziari effettuati presso il Ministero dell'istruzione, dell'università e della ricerca, le istituzioni scolastiche ed educative, gli istituti di alta formazione artistica, musicale e coreutica e gli istituti regionali di ricerca educativa (*Parere* 16 marzo 2006 [doc. *web* n. 1259641]), nonché presso il Ministero delle infrastrutture e dei trasporti (*Parere* 23 marzo 2006 [doc. *web* n. 1269037]). Per quest'ultima amministrazione, in particolare, oltre alla gestione del personale e al contenzioso, sono stati presi in considerazione i trattamenti relativi al rilascio delle patenti, alla gestione del demanio marittimo e alle attività di controllo in materia di immigrazione clandestina, ambiente, trasporto terrestre e marittimo, nonché alle operazioni di ricerca e soccorso in mare.

2.2.4. *Altri soggetti pubblici*

Pareri su schemi-tipo

Va segnalato anche il parere conforme espresso dall'Autorità in ordine allo schema-tipo di regolamento sul trattamento dei dati sensibili e giudiziari predisposto dalla Crui (Conferenza dei rettori delle università italiane) (*Parere* 17 novembre 2005 [doc. *web* nn. 1198369 e 1201343]). La Conferenza ha coordinato il lavoro preparatorio degli atenei offrendo un supporto per interpretare e applicare la normativa sulla tutela dei dati sensibili e giudiziari. Lo schema-tipo di regolamento ha individuato i dati sensibili e giudiziari che vengono di consueto trattati presso le università pubbliche italiane per diverse finalità tra le quali figurano, in particolare, quelle connesse alle attività di ricerca e all'attività didattica e di gestione dei percorsi formativi degli studenti. Analogamente a quanto avviene per altri schemi-tipo, tutte le università pubbliche possono utilizzare lo schema approvato dal Garante per adottare il proprio regolamento, senza dover richiedere autonomamente uno specifico parere dell'Autorità.

Il Garante ha inoltre espresso parere positivo sullo schema-tipo di regolamento predisposto da Assoporti, per le autorità portuali (*Parere* 7 dicembre 2005 [doc. *web* n. 1212485]) e da Unioncamere, per conto delle camere di commercio (*Parere* 15 dicembre 2005 [doc. *web* n. 1202978]), oltre che sullo schema di regolamento relativo al trattamento di dati sensibili e giudiziari effettuato dalla stessa Unioncamere (*Parere* 30 novembre 2005 [doc. *web* n. 1202969]).

Anche il Ministero dell'ambiente e della tutela del territorio ha sottoposto all'esame dell'Autorità uno schema di regolamento, predisposto dall'Ente parco delle dolomiti bellunesi, ai fini dell'adozione quale schema-tipo per i trattamenti dei dati sensibili e giudiziari da effettuarsi presso gli enti parco nazionali. Nel parere reso, il Garante ha fornito alcune indicazioni, in conformità alle quali lo schema dovrà essere riformulato (*Parere* 9 marzo 2006 [doc *web* n. 1269050]).

Si dà conto di seguito di pronunciamenti dell'Autorità che, pur essendo in taluni casi intervenuti nella prima parte del 2006, fanno seguito ad un'attività istruttoria svoltasi nell'anno oggetto della presente *Relazione*.

Pareri su specifici schemi di regolamento

Sono diverse le amministrazioni che, a causa del peculiare settore di competenza e, quindi, della specificità dei trattamenti di dati effettuati, non hanno potuto avvalersi di schemi-tipo di regolamento predisposti da organi rappresentativi ed hanno dovuto pertanto presentare al Garante una richiesta di parere su uno specifico schema di regolamento.

Di seguito, anche in questi casi, a forme di collaborazione informale con l'Ufficio del Garante, l'Autorità ha espresso il proprio parere positivo in ordine a richieste pervenute e riguardanti gli schemi predisposti dai seguenti enti: Enit-Ente nazionale italiano per il turismo (*Parere* 21 dicembre 2005 [doc. *web* n. 1212477]); Enac-Ente nazionale per l'aviazione civile (*Parere* 12 gennaio 2006 [doc. *web* n. 1218208]); Cnipa-centro nazionale per l'informatica nella pubblica amministrazione (*Parere* 12 gennaio 2006 [doc. *web* n. 1218226]); Avvocatura generale dello Stato (*Parere* 18 gennaio 2006 [doc. *web* n. 1218216]); Ansv-Agenzia nazionale per la sicurezza del volo (*Parere* 23 febbraio 2006 [doc. *web* n. 1245373]).

Analogamente, l'Autorità si è espressa sulle richieste di parere rivolte da taluni istituti previdenziali ed assicurativi relativamente, soprattutto, ad attività relative alla gestione del personale, ad attività assicurative ed assistenziali in favore dei propri iscritti, nonché di difesa in giudizio dell'amministrazione: parere positivo è stato espresso in quest'ambito nei riguardi delll'Ipost-Istituto postelegrafonici (*Parere* 16 febbraio 2006 [doc. *web* n. 1244658]) e dell'Enam-Ente nazionale di assistenza magistrale (*Parere* 16 marzo 2006 [doc. *web* n. 1259665]).

Tra gli enti di ricerca, l'Infn (Istituto nazionale di fisica nucleare) (*Parere* 19 ottobre 2005 [doc. *web* n. 1182760]), l'Asi-Agenzia spaziale italiana (*Parere* 27 gennaio 2006 [doc. *web* n. 1244630]), l'Inaf-Istituto nazionale di astrofisica (*Parere* 27 gennaio 2006 [doc. *web* n. 1244643]) e il Consorzio per l'area di ricerca scientifica e tecnologica di Trieste (*Parere* 2 marzo 2006 [doc. *web* n. 1246876]), hanno chiesto ed ottenuto dal Garante parere positivo in ordine ai rispettivi schemi di regolamento. La peculiarità e, al contempo, l'elemento comune di tali atti regolamentari è costituita dal fatto che in essi, oltre ai trattamenti di informazioni sensibili e giudiziarie effettuati nell'ambito della gestione dei rapporti di lavoro e del contenzioso, sono stati disciplinati i trattamenti finalizzati alla formazione professionale o universitaria.

È stato espresso un parere positivo anche in ordine al regolamento presentato dall'Istat-Istituto nazionale di statistica, tenendo conto della specifica disciplina prevista per i trattamenti di dati per scopi di ricerca statistica effettuati dai soggetti che fanno parte o partecipano al Sistema statistico nazionale ed inseriti nel Programma

statistico nazionale-Psn. In tale caso, l'articolo 6-*bis*, comma 2, del decreto legislativo 6 settembre 1989, n. 322 prevede infatti che nel Programma statistico nazionale, sul quale il Garante esprime un parere specifico, siano indicati i dati sensibili e giudiziari, le rilevazioni per le quali essi sono trattati e le relative modalità del trattamento (*Parere* 15 dicembre 2005 [doc. *web* n. 1212493]).

Autorità amministrative indipendenti

Tra le autorità amministrative indipendenti che hanno chiesto un parere specifico, poi espresso in senso positivo dal Garante, si annoverano l'Isvap-Istituto sulla vigilanza per le assicurazioni private e di interesse collettivo (*Parere* 30 novembre 2005 [doc. *web* n. 1212464]), la Covip-Commissione di vigilanza sui fondi pensione (*Parere* 2 febbraio 2006 [doc. *web* n. 1225873]); l'Autorità garante della concorrenza e del mercato (*Parere* 7 dicembre 2005 [doc. *web* n. 1212081]) e la Consob-Commissione nazionale per le società e la borsa (*Parere* 15 dicembre 2005 [doc. *web* n. 1202986]). Tali regolamenti individuano, in particolare, i tipi di dati sensibili e giudiziari e le operazioni eseguibili in relazione ai trattamenti posti in essere dalle citate autorità per svolgere le funzioni istituzionali, anche di controllo e vigilanza, nell'ambito dei rispettivi settori di competenza.

Anche il Garante ha adottato il proprio regolamento per il trattamento dei dati sensibili e giudiziari [doc. *web* n. 1249212], con deliberazione 29 dicembre 2005, n. 26, pubblicata in *Gazzetta Ufficiale* 22 marzo 2006, n. 68.

Regolamento Isvap sul Centro di informazioni

L'Autorità ha prestato la propria collaborazione, esprimendo parere favorevole, in relazione all'adozione del regolamento Isvap concernente le modalità di funzionamento del "Centro di informazioni", da adottare ai sensi degli artt. 5 e 10 del d.lg. 30 giugno 2003, n. 190 (ora previsto dagli artt. 154 e 155 d.lg. 7 settembre 2005, n. 209, recante il Codice delle assicurazioni private) in attuazione della direttiva 2000/26/Ce, in materia di assicurazione della responsabilità civile risultante dalla circolazione di autoveicoli. Il Centro informazioni istituito presso l'Isvap (*cfr.* art. 5 d.lg. n. 190/2003) svolge attività a favore dei soggetti residenti nel territorio della Repubblica, danneggiati da sinistri della circolazione stradale provocati da veicoli stazionanti abitualmente e assicurati in un Stato diverso da quello di residenza, i quali possono chiedere nel proprio Stato di residenza il risarcimento a seguito di un sinistro derivante dalla circolazione dei veicoli a motore. Il Centro è chiamato anche a trattare dati personali relativi a soggetti assicurati in Italia per agevolare il reperimento da parte dei danneggiati delle informazioni necessarie a far valere la richiesta di indennizzo (finalità esclusiva nella prospettiva del legislatore comunitario per l'istituzione dei "centri" sopra descritti). Le informazioni destinate a confluire nel Centro saranno in parte fornite dalle singole imprese di assicurazione, anche attraverso l'associazione nazionale di categoria (Ania), a tal fine designata responsabile del trattamento (art. 29 del Codice).

Particolari indicazioni fornite in sede di parere

In alcuni casi, l'Autorità ha condizionato il proprio parere favorevole al rispetto di talune condizioni.

Per quanto concerne lo schema curato dal Consiglio nazionale delle ricerche-Cnr, il Garante ha sollecitato modifiche ed integrazioni anche in riferimento alle indicazioni normative menzionate nel medesimo schema. Alcune di esse sono apparse infatti non pertinenti (in quanto relative alla previdenza del personale degli enti locali), o da sopprimere o incomplete (con riferimento ai principi fondamentali in materia di libertà ed attività sindacale); è stata evidenziata anche la non corretta individuazione di alcune disposizioni del Codice relative alle finalità di rilevante interesse pubblico perseguite dall'ente.

Ulteriori condizioni sono state fissate dall'Autorità a proposito della necessità di enucleare distinte schede per disciplinare le attività effettuate a fini di ricerca scientifica (distinguendo ulteriormente quelle di ricerca medica, biomedica ed epidemiologica

dalle altre relative alla restante attività di ricerca) e quelle di natura amministrativa correlate ad attività di prevenzione, diagnosi e cura della salute dei soggetti assistiti dal Servizio sanitario nazionale. Il Garante ha fornito altresì indicazioni in ordine alla necessità di specificare, anche per categorie, i destinatari delle comunicazioni dei dati, di eliminare il riferimento a trattamenti di dati giudiziari già oggetto dell'*autorizzazione generale* n. 7/2005 [doc. *web* n. 1203942] e di comprovare l'indispensabilità dell'utilizzo di dati relativi alle convinzioni religiose per perseguire le attività connesse all'esercizio di libertà ed attività sindacali (*Parere* 8 febbraio 2006 [doc. *web* n. 1244717]).

Analoga valutazione sull'indispensabilità dei dati è stata prescritta ad un altro ente di ricerca (la Stazione zoologica "Anton Dohrn"), a proposito di alcune comunicazioni di dati prospettate, e in relazione all'utilizzo di informazioni attinenti all'origine razziale o etnica per perseguire attività relative all'instaurazione e gestione dei rapporti di lavoro, nonché di promozione e formazione nella ricerca scientifica e di corresponsione di compensi e rimborsi ai componenti degli organi statutari e delle specifiche commissioni dell'ente. Inoltre, le finalità di gestione dei rapporti con i predetti componenti non sono state ritenute ricomprese in quelle di promozione e formazione nella ricerca scientifica; si è quindi evidenziata la necessità di disciplinarle in una scheda distinta (*Parere* 23 febbraio 2006 [doc. *web* n. 1246894]).

Specifiche integrazioni sono state parimenti prospettate, quale condizione per l'acquisizione di un parere favorevole, all'Istituto nazionale di alta matematica "Francesco Severi", nel cui schema di regolamento non risultavano contemplate alcune operazioni essenziali a realizzare attività indicate nello schema stesso e strettamente connesse alla finalità di instaurazione e gestione di rapporti di lavoro (*Parere* 23 febbraio 2006 [doc. *web* n. 1246888]).

Anche lo schema curato dall'Istituto nazionale economia agraria (Inea) è stato oggetto di indicazioni specifiche. Al riguardo, il Garante ha chiesto di modificare alcuni riferimenti normativi (ritenuti incompleti o inidonei a legittimare le operazioni indicate) e di integrare una scheda con l'indicazione specifica dei tipi di dati utilizzati, che venivano invece menzionati soltanto nella sintetica descrizione del trattamento (*Parere* 16 febbraio 2006 [doc. *web* n. 1244652]).

2.3. *Trasparenza dell'attività amministrativa e accesso ai documenti*

Le problematiche legate ai rapporti intercorrenti tra la trasparenza dell'attività amministrativa e la protezione dei dati personali continuano ad essere fonte di alcuni dubbi interpretativi presso taluni operatori: anche nel 2005 sono pervenuti numerosi quesiti riguardanti i limiti del diritto all'accesso ai sensi della l. 7 agosto 1990, n. 241, come pure al diritto di accesso riconosciuto ai consiglieri comunali e provinciali ai sensi dell'art. 43 del d.lg. 18 agosto 2000, n. 267.

Linee generali

Su tali aspetti, l'Autorità è stata tra l'altro interpellata da un comune, sia in ordine alla possibilità di ottemperare alla richiesta presentata da un cittadino, ai sensi della l. n. 241/1990, di rilasciare copia di documenti ed informazioni riguardanti l'esito di alcuni procedimenti disciplinari nei confronti di un dipendente, sia relativamente ad una richiesta avente analogo oggetto, formulata da un consigliere comunale ai sensi dell'art. 43 del d.lg. n. 267/2000 (*Nota* 13 luglio 2005).

Sotto il primo profilo è stato ribadito il consolidato orientamento dell'Autorità ricordando nuovamente che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60). Spetta all'amministrazione destinataria della richiesta di accesso verificare, caso per caso, l'interesse e i motivi sottesi alla relativa istanza, e valutare la sussistenza delle ragioni per le quali il docu-

mento può essere sottratto, anche temporaneamente, alla conoscenza del richiedente.

Con riferimento, invece, alla possibilità di consentire ad un consigliere comunale l'acquisizione delle predette informazioni, l'Ufficio del Garante ha ribadito che, anche in tali ipotesi, il Codice non ha abrogato o modificato la specifica disposizione di legge che riconosce ai consiglieri comunali e provinciali il diritto di ottenere dagli uffici del comune, compresi enti ed aziende collegati, informazioni utili all'espletamento del loro mandato, nel rispetto del segreto d'ufficio, ma anche del principio di pertinenza e non eccedenza nel trattamento dei dati.

Principi analoghi sono stati richiamati nella risposta fornita ad un cittadino, il quale si era rivolto all'Autorità lamentando la presunta illegittimità del comportamento tenuto da un comune (*Nota* 9 novembre 2005). L'ente aveva reso disponibili a terzi i documenti presentati e sottoscritti dall'interessato, il quale, nell'ambito di una segnalazione all'amministrazione comunale, aveva evidenziato problemi di edilizia privata riguardanti il condominio di propria residenza. Al riguardo, è stato sottolineato che l'amministrazione destinataria della richiesta di accesso è tenuta a valutare l'interesse e i motivi sottesi alla relativa istanza alla luce delle norme vigenti in materia di accesso ai documenti amministrativi, le quali attribuiscono il diritto di prendere visione e di estrarre copia di documenti amministrativi ai soggetti privati che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso (artt. 22 ss. l. n. 241/1990, come modificata dalla l. n. 15/2005).

Con riferimento ad una richiesta di intervento presentata da un cittadino che aveva interpellato l'Autorità al fine di vedere soddisfatta una sua istanza di accesso rivolta ad una sede Inps, è stato ricordato che le scelte effettuate dall'amministrazione, in caso di diniego dell'accesso, espresso o tacito, o del suo differimento sono più propriamente sindacabili dinanzi al tribunale amministrativo regionale, ovvero mediante richiesta di riesame della suddetta determinazione, al difensore civico competente per ambito territoriale, in base all'art. 25, l. n. 241/1990, come modificato dalla l. n. 15/2005 (*Nota* 6 dicembre 2005).

Ulteriori precisazioni in merito sono state fornite ad alcuni cittadini i quali, in qualità di richiedenti l'accesso a taluni atti amministrativi, nel lamentare la comunicazione delle loro generalità al controinteressato da parte del comune interpellato, avevano richiesto all'Autorità la determinazione del risarcimento dei danni. A tal proposito, è stato evidenziato (*Nota* 17 gennaio 2006), da un lato, che le pubbliche amministrazioni, destinatarie di una richiesta di accesso agli atti ed ai documenti da esse detenuti, sono tenute a comunicare l'avvio del procedimento ai soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti ed a quelli che per legge debbono intervenirvi (art. 7 l. n. 241/1990); dall'altro, che l'Autorità non è competente in relazione alle richieste risarcitorie, fermo restando il diritto della persona interessata, che ritenga di aver subito un danno –anche non patrimoniale– per effetto del trattamento di dati personali, di far valere le proprie pretese risarcitorie davanti all'autorità giudiziaria ordinaria, ove ne ricorrano i presupposti (art. 15 del Codice).

Beneficiari dei fondi nel settore dell'agricoltura

Ulteriori questioni interpretative sono state poste dall'Agea (Agenzia per le erogazioni in agricoltura) con riferimento alla possibilità di fornire l'elenco nominativo dei beneficiari dei fondi comuni nel settore dell'agricoltura (Feoga) ad una giornalista che intendeva diffonderli durante una trasmissione televisiva (*Nota* 30 settembre 2005).

In proposito è stata richiamata preliminarmente l'attenzione del principio generale operante per i soggetti pubblici, secondo cui i dati personali possono essere comunicati a privati richiedenti in tutti i casi in cui tale comunicazione sia prevista o consentita da una disposizione di legge o di regolamento (art. 19, comma 3, del

Codice). Nel ricordare che l'Autorità si era già espressa in passato nei confronti dell'Agea a proposito delle informazioni contenute nel Sistema informativo agricolo nazionale (Sian), rilevando che il registro delle quote-latte è consultabile integralmente da chiunque ne avesse interesse, in quanto tale regime di conoscibilità risulta espressamente disciplinato da una disposizione regolamentare (art. 3, comma 2, d.m. 31 luglio 2003 Min. politiche agricole), è stato sottolineato come debbano essere verificate anche in tal caso le disposizioni vigenti applicabili all'Agenzia, con particolare riferimento a quelle in materia di accesso.

Prestazioni e incarichi conferiti ai pubblici dipendenti

L'Autorità ha fornito indicazioni relativamente all'accesso, da parte di un giornalista, ai dati contenuti nell'anagrafe delle prestazioni e degli incarichi conferiti ai pubblici dipendenti presso il Dipartimento della funzione pubblica (art. 24, comma 1, 30 dicembre 1991, n. 412). È stato chiarito che la normativa di riferimento si limita a stabilire, per le pubbliche amministrazioni, l'obbligo di comunicare al Dipartimento i compensi percepiti dai propri dipendenti anche per incarichi relativi a compiti e doveri d'ufficio, essendo le stesse tenute, altresì, a comunicare semestralmente l'elenco dei collaboratori esterni e dei soggetti cui sono stati affidati incarichi di consulenza, con l'indicazione della ragione dell'incarico e dell'ammontare dei compensi corrisposti (artt. 7, comma 6, e 53, comma 14, d.lg. 30 marzo 2001, n. 165), senza che sia però disciplinato il profilo relativo alla conoscibilità dei dati in questione.

Pertanto, i predetti documenti possono formare oggetto di accesso ai sensi della legge n. 241/1990 e dell'art. 59 del Codice: spetta quindi al medesimo Dipartimento –quale amministrazione destinataria della richiesta di accesso– verificare se l'istanza del giornalista sia accoglibile o meno, in base all'interesse e ai motivi rappresentati, tenendo anche conto della prima giurisprudenza amministrativa formatasi a proposito del diritto di critica e di cronaca, quale "diritto" autonomo che potrebbe giustificare una richiesta di accesso a documenti. Non si pongono problemi, invece, per la pubblicazione di dati anonimi o riepilogativi attinti da tabelle a carattere esclusivamente statistico, prive di dettagli correlabili a nominativi (*cfr.* art. 53, comma 16, d.lg. n. 165/2001).

2.4. *Il principio del "pari rango"*

Le problematiche applicative derivanti dal contemperamento del diritto di accesso agli atti ed ai documenti amministrativi, da un lato, e del diritto alla riservatezza dall'altro, emergono con maggiore evidenza nell'ipotesi in cui i documenti amministrativi di cui si richiede l'ostensione contengono dati idonei a rivelare lo stato di salute o la vita sessuale. In tale ipotesi, il trattamento è consentito laddove la situazione giuridicamente rilevante, che si intende tutelare con la richiesta di accesso, sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (art. 60 del Codice) (*v.* già il *Provv.* 9 luglio 2003 [doc. *web* n. 29832], in *Relazione* 2003, p. 64).

Finalità di investigazione difensiva

In merito, l'Autorità ha rilevato in termini generali che, per il rilascio di copia della documentazione sanitaria relativa ad un ricovero ospedaliero, richiesta da un soggetto diverso dall'interessato e, in particolare, dal difensore nell'ambito delle indagini effettuate nell'interesse di due soggetti indagati per fatti connessi al ricovero medesimo, non è necessario ottenere una specifica autorizzazione del Garante laddove le richieste siano formulate nei confronti di organismi sanitari in conformità alla legge, anche sotto il profilo della disciplina delle investigazioni difensive introdotta dalla legge 7 dicembre 2000, n. 397 (*Nota* 28 aprile 2005).

In tal caso, spetta però all'amministrazione destinataria della richiesta non solo accertare, caso per caso, la sussistenza dei presupposti per l'esercizio della facoltà riconosciuta al difensore dalla citata disciplina, ma operare anche un'attenta valutazione dei diritti coinvolti, al fine di stabilire se il diritto che il soggetto intende far valere, sulla base della documentazione richiesta, possa essere appunto considerato "di pari rango" rispetto a quello della persona cui si riferiscono i dati (artt. 92, comma 2, 71 e 60 del Codice).

Cartella clinica di un dipendente infortunato in servizio

Analoghe considerazioni sono state sviluppate con riferimento alla richiesta di un'"autorizzazione" ad ottenere copia della cartella clinica redatta in riferimento allo stato di salute di un dipendente, e relativa all'accettazione in pronto soccorso per un incidente occorsogli sul luogo di lavoro, al fine di consentire la difesa in giudizio del datore di lavoro (*Nota* 8 novembre 2005).

Graduatorie di trasferimento

L'Ufficio del Garante ha evidenziato ulteriormente che, nell'ipotesi in cui venga presentata ad una amministrazione pubblica una richiesta di accesso agli atti relativi all'attribuzione del punteggio conferito a singoli dipendenti nell'ambito di una graduatoria di trasferimento provinciale, laddove il punteggio analitico attribuito nelle graduatorie di trasferimento contenga anche dati idonei a rivelare lo stato di salute, l'amministrazione interpellata può accogliere l'istanza sempreché, a seguito di una valutazione dei diritti coinvolti, valuti che il diritto che il terzo intende far valere sulla base delle informazioni o della documentazione richiesta possa essere considerato "di pari rango" rispetto a quello della persona cui si riferiscono i dati (*Nota* 17 gennaio 2006).

2.5. *Pubblici registri, elenchi, atti e documenti conoscibili da chiunque*

Casellario informatico delle imprese

Il Garante si è pronunciato su alcune questioni relative al trattamento dei dati contenuti in pubblici registri, elenchi, atti e documenti conoscibili da chiunque, con particolare riferimento al Casellario informatico delle imprese in relazione alla trasparenza negli appalti.

In sede di esame di un ricorso, il Garante si è occupato ad esempio del regime di comunicazione e di pubblicità di tale Casellario. In esso, sono contenute le attestazioni relative alle imprese appaltatrici di lavori pubblici rilasciate dagli organismi che ne accertano i requisiti, nonché le comunicazioni dei soggetti pubblici che riferiscono sull'andamento degli appalti; tra le informazioni acquisite al Casellario, rientrano anche i casi di esclusione per collegamento sostanziale, trattandosi di ipotesi ritenuta lesiva della *par condicio* tra concorrenti e della segretezza delle offerte [doc. *web* n. 1151205].

Rispetto a questa stessa ipotesi, una società ha richiesto la cancellazione delle informazioni dal Casellario, sostenendo che era illecita tanto l'iscrizione, quanto la diffusione *on-line* sul sito *web* dell'Autorità di vigilanza per i lavori pubblici, trattandosi di operazioni ritenute prive di fondamento normativo. Il Garante ha invece ritenuto lecita, alla luce della vigente normativa, l'iscrizione nel Casellario da parte dell'Autorità di vigilanza anche dei dati relativi al "collegamento sostanziale", nonché la loro comunicazione ad altri organi per fini di piena trasparenza delle operazioni di appalto. É risultata, invece, ingiustificata, secondo la disciplina vigente, la diffusione delle informazioni tramite il sito Internet della stessa Autorità, alla luce della specifica disciplina applicabile.

Dopo l'intervento del Garante, l'Autorità di vigilanza per i lavori pubblici ha quindi sospeso la visibilità in Internet dei dati oggetto del ricorso ed ha comunicato di aver istituito un gruppo di lavoro per la revisione del Casellario sotto il profilo dell'individuazione di corrette modalità di diffusione e di tempi di conservazione adeguata delle informazioni.

Ipoteche

La legge finanziaria per il 2005 ha introdotto una disposizione che vieta, di regola, la riutilizzazione commerciale delle informazioni contenute negli archivi catastali e nei pubblici registri immobiliari tenuti dagli uffici dell'Agenzia del territorio (art. 1, commi 367 e ss., l. n. 311/2004).

L'eventuale possibilità di riutilizzare per fini commerciali tali informazioni è stata subordinata alla stipula di specifiche convenzioni con la stessa Agenzia, le quali devono disciplinare, a fronte del preventivo pagamento dei tributi dovuti, le modalità e i termini della raccolta, della conservazione, dell'elaborazione dei dati, nonché il controllo del limite di riutilizzo consentito. A tale scopo, il Garante ha promosso la sottoscrizione del codice deontologico previsto in materia (artt. 61 e 118 del Codice), anche al fine di garantire il rispetto dei diritti degli interessati e del principio di compatibilità della riutilizzazione con gli scopi per i quali i dati sono stati originariamente raccolti; principio del quale l'Agenzia del territorio dovrà tenere conto qualora intenda delimitare, nel rispetto dei principi di pertinenza e non eccedenza, le modalità di riutilizzazione dei dati da parte dei soggetti convenzionati (*Provv.* 25 maggio 2005 [doc. *web* n. 1131816]).

2.6. *Documentazione anagrafica e materia elettorale*

Le problematiche riguardanti la materia anagrafica hanno impegnato l'Autorità su diversi fronti nel corso del 2005.

In particolare, in diverse occasioni l'Autorità è stata chiamata ad occuparsi della conformità al Codice della trasmissione a soggetti privati di informazioni contenute negli archivi anagrafici, con particolare riferimento allo stato di famiglia (*Note* 17 gennaio 2006).

In proposito, è stato ricordato che la specifica disposizione contemplata nel regolamento anagrafico –secondo la quale l'ufficiale dell'anagrafe rilascia, a chiunque ne faccia richiesta, i *"certificati concernenti la residenza e lo stato di famiglia"* degli iscritti all'anagrafe (art. 33 d.P.R. 30 maggio 1989, n. 223)– costituisce un'idonea fonte normativa per la comunicazione all'esterno di dati personali da parte di soggetti pubblici (art. 19, comma 3, del Codice).

Accesso delle università

Sono state poi distinte le predette ipotesi da quelle in cui si intenda attivare un flusso di dati anagrafici verso soggetti pubblici. Sul punto, è stato tra l'altro chiarito, ad esempio, che l'università può svolgere senza particolari difficoltà le proprie attività stante la possibilità di accedere, con cadenza regolare, ai dati anagrafici dei nuovi nati presso gli uffici anagrafici di un comune, al fine di poter inviare alle famiglie materiale informativo riguardante progetti di ricerca sullo sviluppo cognitivo, linguistico e socio-affettivo del bambino nei primi tre anni di vita (*Nota* 25 febbraio 2005). La possibilità del rilascio, anche periodico, di elenchi degli iscritti nell'anagrafe della popolazione residente, è infatti previsto rispetto alle pubbliche amministrazioni *"che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità"* (art. 34, comma 2, d.P.R. n. 223/1989); pertanto, ove l'amministrazione comunale interpellata valuti che la motivata richiesta dell'università di utilizzare i predetti elenchi anagrafici sia finalizzata ad un uso di pubblica utilità, si può accedere ai predetti elenchi, in conformità alla previsione dell'art. 19, comma 2, del Codice, che autorizza la comunicazione di dati personali tra soggetti pubblici qualora ciò sia previsto da norme legislative o regolamentari.

Caso "Laziomatica"

È risultato inoltre particolarmente significativo l'intervento del Garante resosi necessario a seguito di segnalazioni concernenti alcuni accessi illeciti a dati anagrafici detenuti presso il Comune di Roma, in correlazione ad un caso di falsa sotto-

scrizione di candidature alle elezioni regionali del 3 e 4 aprile 2005. L'Autorità ha effettuato una serie di accertamenti ispettivi, anche nell'esercizio di funzioni di polizia giudiziaria, che hanno portato all'adozione di un provvedimento che ha preso in esame diversi profili problematici (*Provv.* 6 ottobre 2005 [doc. *web* n. 1179484], pubblicato in *G.U.* 24 ottobre 2005, n. 248).

In primo luogo, è stato rilevato che da parte di Laziomatica S.p.A. (società per azioni a prevalente capitale regionale istituita dalla Regione Lazio per la gestione del Sistema informativo regionale-Sir: *v.* l.r. 3 agosto 2001, n. 20) erano stati effettuati accessi illeciti ad una banca dati anagrafica del Comune di Roma, che la stessa Regione sarebbe autorizzata a consultare solo per determinate finalità sanitarie, in base al "Protocollo di intesa per la cooperazione nello sviluppo dei servizi al cittadino" sottoscritto il 12 maggio 2004 allo scopo di permettere uno scambio di dati tra i due enti per effettuare verifiche attinenti solo a prestazioni sanitarie (*ticket*, scelta del medico); con la possibilità di accedere direttamente agli stessi dati anagrafici detenuti dal Comune.

Il Garante ha pertanto prescritto ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, alla Regione Lazio e Laziomatica S.p.A., di osservare le regole concernenti sia il ruolo del responsabile e degli incaricati del trattamento (artt. 29 e 30), sia la definizione dei rispettivi compiti e le rigorose istruzioni da impartire, adeguando entro 180 giorni i rapporti tra loro intercorrenti. La Regione e il Comune sono stati invitati anche a rivedere entro il medesimo termine il Protocollo di intesa, per permettere alla prima di continuare ad ottenere speditamente e *on-line* la conferma dei dati anagrafici necessari per varie prestazioni sanitarie, senza che ciò comporti la possibilità di consultare direttamente e liberamente la banca dati anagrafica della popolazione.

In secondo luogo, è emerso che, nella prassi amministrativa osservata presso il Comune di Roma nei rapporti con numerosi enti, ivi inclusa la Regione, veniva consentita la consultazione diretta per via telematica di dati anagrafici mediante un meccanismo di *cd.* "anagrafe aperta"; in altri termini, i dati anagrafici venivano riportati in un *cd.* "data base popolazione" contenente numerose ulteriori informazioni (relative anche a "vaccinazioni, elettorale, leva militare" o alla carta d'identità ed al codice fiscale). In tal modo, si era realizzato un sistema di impropria consultazione diretta di dati anagrafici da parte di personale comunale non facente parte dei servizi di anagrafe e di stato civile (centrali e dei municipi), nonché, soprattutto, da parte di numerosi soggetti esterni al Comune di Roma (amministrazioni centrali, militari e sanitarie; uffici giudiziari ed enti locali; ecc.). La consultazione diretta veniva consentita senza verificare né la concreta motivazione di pubblica utilità in base alla quale veniva richiesto di conoscere i dati anagrafici, né le singole utilizzazioni dei dati consentite a regime presso enti a struttura complessa che perseguono differenti finalità.

Il Garante ha rilevato che il predetto sistema si discostava dal quadro normativo vigente: l'ufficiale d'anagrafe può infatti rilasciare solo attestazioni o certificazioni relativamente al contenuto delle schede che compongono l'anagrafe della popolazione residente, ed entro certi limiti può anche rilasciare elenchi. Ad eccezione del personale autorizzato delle forze di polizia, le medesime schede non possono però essere consultate direttamente da parte di chi, pur facente parte del personale comunale, sia estraneo all'ufficio di anagrafe (artt. 1, 33, 34 e 37 d.P.R. 30 maggio 1989, n. 223). L'utilizzo di elenchi di dati anagrafici è consentito anche da parte del comune che detiene i dati, per fini di comunicazione istituzionale, ma sempre su motivata richiesta –questa volta "interna" all'ente– (art. 177, comma 1, del Codice). Altri soggetti anche privati possono ottenere solo dati anagrafici resi

anonimi ed aggregati, su richiesta e per fini statistici e di ricerca (art. 34, comma 2, d.P.R. n. 223/1989).

Il Codice, pur non avendo inciso sulla portata delle predette disposizioni sull'anagrafe della popolazione, ha però ribadito la necessità del perdurante rispetto delle vigenti norme che regolano la conoscibilità e la pubblicità di taluni atti (*cfr.*, *ad es.*, gli artt. 19, comma 3, 24, comma 1, lett. *c*), 59 e 61 del Codice), che subordinano la consultazione di materiale documentale al rispetto di determinati limiti temporali (*ad es.*, con esclusione dei periodi in cui un elenco è in fase di aggiornamento) o soggettivi, oppure di talune modalità (*ad es.*, documentazione dell'identità del soggetto che intende consultare un registro) o finalità (*ad es.*, fini statistici e di ricerca).

Anche in relazione a questo elemento di illiceità del trattamento, il Garante ha fissato un termine di 180 giorni, entro i quali il Comune di Roma è stato richiesto di individuare un diverso meccanismo che, pur permettendo di comunicare i dati richiesti (quali le richieste di certificazione o attestazione, oppure di rilascio di elenchi ad amministrazioni pubbliche motivato da ragioni accertate di pubblica utilità), permetta di perseguire le finalità di snellimento e di efficienza dell'azione amministrativa attraverso modalità di riscontro anche automatiche e per via telematica che escludano, però, la consultazione diretta, anche *on-line*, degli atti di provenienza anagrafica da parte di soggetti interni ed esterni diversi da quelli preposti all'ufficio anagrafe.

Comitato tecnico per la revisione della disciplina anagrafica

Nel quadro delle iniziative di aggiornamento della normativa anagrafica, l'Autorità è stata invitata dal Ministero dell'interno (Dipartimento per gli affari interni e territoriali, Direzione centrale per i servizi demografici) a partecipare ai lavori del Comitato tecnico istituito per predisporre uno studio finalizzato alla revisione della predetta normativa, alla luce soprattutto delle innovazioni riguardanti l'Indice nazionale delle anagrafi ed il sistema di accesso ed interscambio anagrafico, nonché dei provvedimenti relativi a soggetti stranieri.

Utilizzo di dati anagrafici per finalità di ricerca storica

Con riferimento poi alle finalità di ricerca storica, l'Autorità è stata poi interpellata in ordine alle modalità di raccolta di dati anagrafici e di informazioni contenute nelle liste elettorali. Ad esempio, è stato chiesto di verificare la praticabilità della creazione di una banca dati contenente informazioni, estrapolate da pubblici registri, elenchi, atti o documenti conoscibili da chiunque e risalenti sino al 1950, concernenti cittadini deceduti emigrati all'estero nel secolo scorso, al fine di agevolare la ricerca delle proprie origini da parte di discendenti degli interessati. In proposito, nel richiamare la specifica disciplina di settore relativa anche alla consultazione degli archivi storici di enti pubblici, è stato evidenziato il diverso regime di conoscibilità previsto per le liste elettorali –che possono essere rilasciate in copia "per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per i perseguimento di un interesse collettivo o diffuso" (art. 177, comma 5, del Codice, che ha sostituito l'art. 51 d.P.R. 20 marzo 1967, n. 223)– da quello relativo ai dati anagrafici, previsto dal citato art. 33 d.P.R. n. 223/1989 (*Nota* 28 gennaio 2005).

2.7. *Istruzione*

2.7.1. *Università*

Si è registrata anche una proficua collaborazione con alcune istituzioni universitarie, nelle forme e modalità previste dal Codice.

Verifica delle autocertificazioni e diritto allo studio

Un ateneo ha comunicato all'Autorità, ai sensi dell'art. 39 del Codice, l'intenzione di stipulare una convenzione con l'Azienda per il diritto alla studio universi-

tario, per consentire un reciproco accesso ai dati personali degli studenti contenuti nei rispettivi archivi, al fine di controllare la veridicità delle autocertificazioni prodotte dagli studenti riguardo alla loro condizione economica.

L'Ufficio del Garante, nel riconoscere che sussistono in capo alle suddette amministrazioni compiti istituzionali di intervento diretti a rimuovere ostacoli di ordine economico e sociale per la concreta realizzazione del diritto agli studi universitari (d.P.C.M. 9 aprile 2001), ha precisato che, in virtù dei principi di pertinenza e non eccedenza dei dati trattati rispetto alle finalità perseguite, non dovrebbe essere consentito per tali finalità l'accesso ai dati personali degli studenti per gli interventi diretti alla totalità degli iscritti, potendosi ritenere lecito esclusivamente l'accesso alle informazioni personali dei soggetti che abbiano avanzato una specifica richiesta per usufruire di determinati benefici, in funzione della loro appartenenza a talune fasce di reddito, o del possesso di individuati meriti accademici (*Nota* 3 febbraio 2005).

Graduatorie per l'ammissione ai corsi di laurea

Il Ministero dell'istruzione, dell'università e della ricerca ha sottoposto al Garante due schemi di decreto relativi alla disciplina dell'accesso ai corsi di laurea specialistica programmati a livello nazionale per l'anno accademico 2005/2006.

Nell'esprimere i pareri richiesti, l'Autorità ha evidenziato la mancanza di una disposizione legislativa che preveda la diffusione su Internet dei dati personali presenti nella graduatoria finale, come era stato invece previsto negli schemi di decreto esaminati. Si è invitato inoltre il Ministero ad individuare il ruolo del Consorzio interuniversitario Cineca in riferimento al trattamento, attesa la molteplicità delle operazioni allo stesso affidate, nonché ad integrare l'informativa da fornire ai candidati, la quale risultava priva di alcuni elementi essenziali, tra cui l'indicazione delle finalità del trattamento e l'ambito di comunicazione dei dati trattati (*Nota* 5 aprile 2005).

Nei primi mesi del 2005, in occasione dell'emanazione dei decreti del Ministro dell'istruzione, dell'università e della ricerca riguardanti le modalità e i contenuti delle prove di ammissione ai corsi di laurea specialistica programmati a livello nazionale per l'anno accademico 2006–2007, l'amministrazione ha espresso l'intenzione di pubblicare sul proprio sito Internet i punteggi riferiti ai singoli argomenti di esame e al totale complessivo ottenuto da ciascun candidato, senza l'indicazione dei dati personali di quest'ultimo. Ciò, per consentire ai candidati di accedere, utilizzando chiavi personali (*username* e *password*), ad un'area riservata del sito Internet Cineca, per visualizzare il proprio elaborato (contraddistinto da un codice identificativo) e visionare la valutazione dei singoli argomenti d'esame, nonché il punteggio complessivo ottenuto. I testi di informativa da fornire ai candidati –allegati agli schemi di decreto– sono stati considerati conformi all'art. 13 del Codice (*Parere* 6 aprile 2006 [doc. *web* n. 1269403]).

Preiscrizioni all'università per via telematica

Si è reso necessario un ulteriore intervento dell'Autorità in relazione a quanto disposto dal decreto del Ministro dell'istruzione, dell'università e della ricerca del 1° febbraio 2005, secondo il quale gli studenti iscritti all'ultimo anno della scuola secondaria superiore, interessati all'accesso ai corsi di laurea universitari, ai corsi delle istituzioni di alta formazione artistica e culturale, ai percorsi di istruzione e formazione tecnica superiore (Ifts), nonché all'inserimento nel mondo del lavoro, potevano preiscriversi all'università utilizzando un apposito modulo ad accesso libero, disponibile sul sito *web* del Ministero.

In merito a quanto previsto nel decreto citato, adottato senza la prevista consultazione del Garante, è stato osservato che la raccolta dei dati sensibili in sede di prescrizione informatica, come disciplinata dal decreto stesso, non risultava lecita alla luce del principio di indispensabilità del loro trattamento. La preiscrizione rappresenta infatti non un atto formale di iscrizione, bensì un primo strumento per l'orien-

tamento dello studente e per programmare l'offerta formativa. Un ulteriore elemento di criticità è stato ravvisato nella prevista confluenza dei moduli compilati dagli studenti in una banca dati consultabile da parte di diversi soggetti anche privati. Nella medesima occasione è stato inoltre rappresentato al Ministero l'obbligo di fornire comunque una specifica informativa agli studenti (*Nota* 18 febbraio 2005).

Infine, con riferimento allo schema di decreto relativo alle preiscrizioni universitarie per l'anno accademico 2006-2007, l'Autorità ha espresso parere favorevole riscontrando che è stata prevista soltanto la raccolta di dati personali non sensibili degli studenti. Il decreto ha inoltre disposto che i dati acquisiti siano resi accessibili (anche con modalità telematiche attraverso l'utilizzo di una specifica chiave di accesso) alle sole istituzioni formative nei riguardi delle quali lo studente abbia manifestato un interesse all'immatricolazione. Il testo dell'informativa da fornire agli studenti, allegato allo schema di decreto, è risultato conforme a quanto previsto dall'art. 13 del Codice (*Parere* 8 febbraio 2006 [doc. *web* n. 1244669]).

2.7.2. *Scuola*

Portfolio delle competenze individuali

Il Garante ha ricevuto numerosi reclami e segnalazioni da parte di genitori ed alunni, che lamentavano possibili violazioni della riservatezza in relazione alla predisposizione, da parte degli istituti scolastici, del "portfolio delle competenze individuali" (uno strumento didattico redatto dall'insegnante per ciascun alunno, che, oltre ai progressi formativi ed educativi dello studente, è stato predisposto per documentarne interessi, attitudini, aspirazioni personali emergenti nel corso degli anni scolastici).

Con il *provvedimento* generale del 26 luglio 2005 [doc. *web* n. 1155253], l'Autorità ha indicato agli istituti scolastici pubblici e privati le modalità per trattare lecitamente i dati personali in occasione della compilazione e gestione del "portfolio". L'Autorità ha stabilito che nel "portfolio" debbano essere inseriti solamente dati personali pertinenti e necessari per la valutazione e l'orientamento dell'alunno. I dati più delicati, in grado di rivelare particolari condizioni come lo stato di adozione o le malattie sofferte, possono essere annotati solo se strettamente indispensabili per la valutazione e l'orientamento dell'alunno.

In alcuni casi portati all'esame dell'Autorità, la raccolta di dati era risultata invece eccessiva ed ingiustificata, potendo far emergere informazioni particolarmente delicate sull'alunno (*ad es.* lo stato di adozione) o in quanto concernenti informazioni relative al suo profilo psicologico (descrizioni di paure e disagi), al suo stato di salute (eventuali ricoveri ospedalieri e patologie), al credo religioso, alla condizione sociale e familiare, o ad altri dati sensibili del minore.

In base alle garanzie richiamate dal Garante, ogni istituto scolastico è stato quindi richiamato ad adottare opportune misure per evitare la raccolta di dati non necessari, nonché per informare gli esercenti la potestà genitoriale sul trattamento dei dati personali dei minori. Ai genitori o ai legali rappresentanti devono essere garantiti tutti i diritti riconosciuti dal Codice (*ad es.*, accesso ai dati, aggiornamento, integrazione, ecc.). Devono essere poi predisposte idonee misure di sicurezza, e va individuato un ridotto periodo di conservazione dei dati. Il Garante ha inoltre precisato che, alla fine del corso di studi, il "portfolio" deve essere rilasciato allo studente, affinché questi lo consegni, ove previsto, al proprio nuovo istituto scolastico.

Campagne di informazione sanitaria nelle scuole

Un ulteriore intervento si è avuto a seguito della segnalazione di un genitore che lamentava la raccolta, in occasione di una campagna di prevenzione delle malattie renali rivolta a tutti i bambini frequentanti le scuole elementari di un comune pugliese, di dati personali, anche sensibili, di minori, senza la previsione di idonee garanzie in merito ai soggetti che avrebbero avuto accesso a tali informazioni.

Il progetto era stato promosso da alcuni istituti scolastici, da un circolo sportivo, da un istituto di credito e da alcune strutture sanitarie, anche private, operanti nel territorio. Nell'acquisire ulteriori elementi presso il segnalante e le predette strutture si è potuto anche rappresentare ai promotori dell'iniziativa la necessità di intervenire sulle relative modalità operative, al fine di individuare una differente procedura che consentisse ai genitori interessati di sottoporre i loro figli allo *screening* gratuito delle malattie renali, senza però dar vita a raccolte o comunicazioni di dati personali dei minori stessi non strettamente necessari.

La struttura promotrice della campagna di prevenzione ha compreso le problematiche relative al trattamento dei dati personali degli alunni e ha quindi modificato l'intero assetto del progetto, in modo da articolarlo non più attraverso la raccolta dei dati dei bambini interessati ad effettuare gratuitamente l'esame delle urine, bensì attraverso la distribuzione all'interno delle classi di un buono anonimo per l'esecuzione gratuita dell'esame, che il genitore interessato avrebbe potuto consegnare direttamente al laboratorio medico. È stato inoltre previsto che i risultati degli esami clinici effettuati fossero consegnati solo ai genitori dei bambini, non potendo, in ogni caso, essere conosciuti da parte delle strutture promotrici (*Nota* 15 aprile 2005).

Collaborazione tra istituzioni scolastiche e circoli sportivi

A seguito di una segnalazione, l'Autorità ha appreso che un'associazione sportiva, all'interno di un progetto realizzato in collaborazione con enti locali e soggetti privati, volto ad offrire tre mesi di pratica sportiva gratuita agli alunni delle scuole pubbliche elementari e medie, effettuava un dettagliato *screening* medico, psicologico e motorio degli alunni anche in relazione alla loro anamnesi familiare. L'Ufficio ha invitato l'associazione sportiva a richiedere unicamente un certificato medico di idoneità fisica all'attività sportiva, anziché anche altra documentazione sanitaria, e a distruggere gli altri dati idonei a rivelare lo stato di salute del minore o della relativa famiglia, eventualmente già raccolti. All'associazione sportiva sono stati altresì segnalati gli obblighi in materia di misure di sicurezza e la necessità di informare in modo idoneo i legali rappresentanti degli alunni coinvolti (*Nota* 23 dicembre 2005).

Ricerche universitarie svolte nelle scuole

Il Garante ha bloccato la pubblicazione di alcuni risultati di una ricerca universitaria svolta in una scuola elementare, riportati in una tesi di laurea. Ciò in quanto alunni e genitori non erano stati informati né degli scopi dell'iniziativa, né della circostanza che la loro partecipazione era facoltativa.

Il provvedimento di blocco adottato dall'Autorità ha riguardato le informazioni personali (in alcuni casi anche sensibili, in quanto idonee a rivelare aspetti della sfera psico-fisica dei genitori) raccolte tramite questionari sottoposti ad alcuni alunni delle elementari o elaborate nelle varie fasi della ricerca. Il Garante ha sottolineato che l'università, titolare del trattamento, per effettuare lecitamente la rilevazione dei dati a fini di ricerca, avrebbe dovuto informare adeguatamente i genitori delle predette circostanze (*cfr. Newsletter* 11-24 aprile 2005).

L'Autorità è intervenuta anche sulla distribuzione presso le scuole elementari di un questionario con il quale venivano raccolte informazioni sull'identità sessuale degli alunni e sugli eventuali interventi chirurgici cui essi erano stati sottoposti (*Nota* 14 luglio 2005). Dagli accertamenti effettuati è risultato che il questionario, realizzato dall'istituto di sessuologia di un'università, avrebbe dovuto essere inizialmente distribuito mantenendo l'anonimato degli alunni. Essendo stata riscontrata invece la mancanza della garanzia di anonimato, l'istituto scolastico ha bloccato la distribuzione dei suddetti questionari.

Vigilanza sull'adempimento dell'obbligo scolastico

Sollecitata da un quesito formulato da un istituto scolastico, l'Autorità ha ricordato che specifiche disposizioni di legge attribuiscono ai comuni la vigilanza sull'adempimento dell'obbligo scolastico, prevedendo che il sindaco debba trasmettere ogni anno ai direttori didattici degli istituti scolastici l'elenco dei fanciulli che per

ragioni di età sono soggetti all'obbligo scolastico, al fine di accertare l'eventuale inadempienza all'obbligo (art. 114 d.lg. 16 aprile 1994, n. 297). Tale comunicazione è risultata quindi lecita (*Nota* 17 giugno 2005).

Pubblicazione degli esiti degli scrutini

L'Autorità è nuovamente intervenuta in merito alla pubblicità dei risultati degli scrutini scolastici, essendo venuta a conoscenza da notizie stampa di iniziative promosse da alcuni presidi di istituti superiori per vietare di fotografare gli esiti finali degli scrutini pubblicati. Al riguardo, è stato precisato che nessuna norma del Codice preclude la piena pubblicità degli esiti scolastici, né la possibilità di accedere ai luoghi dove questi sono esposti e di trarne notizia prendendo appunti per usi personali, eventualmente anche attraverso foto da utilizzare ovviamente in maniera lecita. Nella medesima occasione è stato inoltre ricordato che i dati relativi agli esiti scolastici, per quanto riferiti a minori, non si qualificano di per sé come dati sensibili, non riguardando informazioni sullo stato di salute, le opinioni politiche, le appartenenze religiose, l'etnia o gli stili di vita, e consistendo piuttosto in dati "comuni" sul rendimento scolastico (*cfr. Comunicato stampa* 14 giugno 2005).

Graduatorie permanenti *on-line*

A seguito di alcune notizie stampa, l'Autorità ha appurato la presenza sul *web* di numerose graduatorie permanenti contenenti dati personali, anche sensibili, del personale A.t.a. (assistenti amministrativi, tecnici di laboratorio e collaboratori ausiliari del Ministero dell'istruzione, dell'università e della ricerca). Su sollecitazione del Garante, detto Ministero ha diramato una circolare (28 novembre 2005, n. 2100) con cui, recependo le osservazioni formulate dall'Autorità, ha invitato tutti gli uffici scolastici regionali ad inserire nella graduatoria solo il nome e cognome e la posizione dell'interessato, omettendo qualsiasi altra informazione personale come, ad esempio, il domicilio, il recapito telefonico o la presenza di eventuali invalidità.

2.8. *Notificazioni di atti e comunicazioni*

Sono pervenute ancora all'Autorità numerose segnalazioni di cittadini concernenti notifica di atti giudiziari, verbali di contravvenzione, avvisi fiscali ed atti amministrativi.

Notificazioni

L'Autorità ha ricordato che il Codice (art. 174), modificando alcune disposizioni dei codici di procedura civile e penale, oltre che di alcune leggi speciali, ha introdotto particolari modalità operanti per le notifiche da effettuare a persone diverse dal destinatario, al fine di tutelarne la riservatezza adottando accorgimenti che prevengano l'indebita conoscenza del contenuto dell'atto da parte di terzi.

Tali novità hanno riguardato in modo particolare l'obbligo di inserire la copia dell'atto da notificare in una busta sigillata su cui va apposto solo il numero cronologico della notificazione, e di annotare tale attività nella relazione in calce all'originale e alla copia dell'atto stesso. Nessun segno o indicazione da cui possa desumersi il contenuto dell'atto può essere quindi apposto sulla busta. Si tratta poi di cautele operanti nel processo sia civile, sia penale, nonché per le notificazioni di sanzioni amministrative e di atti e documenti provenienti da organi delle pubbliche amministrazioni, se effettuate a soggetti diversi dagli interessati.

Altre segnalazioni hanno riguardato notificazioni di atti giudiziari eseguite in maniera non corretta; in particolare, le doglianze concernevano notifiche effettuate a persone diverse dai destinatari attraverso la consegna di plichi non sigillati. Gli uffici addetti alla notifiche sono stati richiamati al pieno rispetto delle norme poste a tutela della riservatezza dei destinatari degli atti.

Strumenti di comunicazione tra pubbliche amministrazioni

L'Ufficio ha ricordato la liceità dell'utilizzo del fax come mezzo di comunicazione tra pubbliche amministrazioni in quanto espressamente consentito dalla legge, e di specificare che i dipendenti preposti all'invio e alla ricezione devono essere designati quali incaricati del trattamento rispettando anche le misure di sicurezza e gli obblighi di riservatezza previsti dal Codice (*Nota* 16 febbraio 2005).

Con particolare riferimento, poi, all'attività svolta da un'azienda sanitaria, l'Autorità ha affermato che il ricorso a tale mezzo di comunicazione deve avvenire osservando comunque le dovute cautele, soprattutto per quanto riguarda informazioni sensibili, assicurandosi che soggetti diversi dall'interessato o non autorizzati al trattamento dei dati personali ne vengano a conoscenza. Nel caso di specie, nel corso di un procedimento di affido, alcuni assistenti sociali avevano inviato una comunicazione riservata al numero di fax del luogo di lavoro del genitore diverso da quello espressamente indicato come recapito per la corrispondenza relativa ai rapporti con il figlio minore.

Vendite giudiziarie

Sono pervenute al Garante diverse segnalazioni relative al mancato rispetto delle nuove disposizioni relative alla pubblicità degli avvisi di vendita giudiziaria. Si è potuto quindi far notare che, con riferimento al processo esecutivo, l'art. 490 c.p.c. prevede ora l'omissione dell'indicazione del debitore, qualora l'annuncio sia inserito nei quotidiani o sia divulgato con le forme della pubblicità commerciale. Le informazioni relative al debitore possono essere comunque fornite dalla cancelleria del tribunale a chiunque vi abbia interesse, unitamente ad ogni altra ulteriore informazione ritenuta necessaria (*Provv.* 7 febbraio 2005 [doc. *web* n. 1103505]).

Restano all'attenzione dell'Autorità le questioni emergenti dalle recenti modifiche dell'art. 490 c.p.c. che prevedono la pubblicazione su siti Internet dell'avviso, dell'ordinanza del giudice e della stima, nonché il regime di pubblicità ed il contenuto dell'istanza di vendita (art. 173 disp. att. c.p.c.), effettuata a cura del creditore procedente.

2.9. *Attività fiscale, tributaria e doganale*

Il Garante è intervenuto in merito ad alcune disposizioni introdotte dalla legge finanziaria per il 2005, volte a potenziare il patrimonio informativo a disposizione degli organismi preposti ai controlli fiscali e alla riscossione dei tributi, esaminandone i profili rilevanti per il trattamento dei dati personali (*Provv.* 25 maggio 2005 [doc. *web* n. 1131826]). Il nuovo assetto normativo ha infatti ampliato sensibilmente l'ambito applicativo delle disposizioni in materia di indagini bancarie da parte dell'amministrazione finanziaria con riferimento ai dati, alle notizie e ai documenti acquisibili dagli organi di controllo, agli operatori presso i quali questi ultimi possono intraprendere accertamenti, nonché ad alcune novità procedurali.

L'Autorità ha rilevato che l'utilizzazione dei dati personali deve avvenire sulla base di un preciso quadro di riferimento anche per ciò che riguarda i flussi tra l'amministrazione finanziaria e i destinatari delle richieste di informazioni, con particolare riferimento alla possibilità di accedere e di interconnettere informazioni contenute in altri archivi, nel rispetto dei principi di necessità e di proporzionalità nel trattamento dei dati. Il passaggio ad un sistema più efficiente di trasmissione delle informazioni necessarie alle indagini bancarie, basato solo sulla via telematica, deve garantire comunque il rispetto dei presupposti normativi, i quali giustificano soltanto verifiche mirate e relative a casi individuati selettivamente.

Il Garante ha inoltre precisato che è necessario individuare precise modalità di accertamento, delineando misure ed accorgimenti volti a garantire la sicurezza dei dati e il rispetto dei principi di selettività, proporzionalità e di pertinenza delle informazioni raccolte presso gli interessati e i terzi.

Non sono risultati, poi, adeguatamente tipizzati i contenuti informativi del sistema di comunicazione introdotto dalla legge finanziaria, stante il riferimento ampio e indistinto ad ogni tipo di dato o notizia relativi a soggetti indicati anche per categorie. L'esigenza di procedere solo a richieste selettive di dati, in rapporto a necessità effettive di verifica, è stata quindi avvertita dal Garante, in particolare per informazioni richieste cumulativamente o per intere categorie, tenendo conto dell'indeterminato ambito di oggettivo di riferimento delle richieste medesime.

Comunicazioni all'anagrafe tributaria

La predetta legge finanziaria ha integrato le tipologie di dati che soggetti pubblici e privati devono trasmettere all'anagrafe tributaria (art. 7 d.P.R. n. 605/1973), prevedendo la trasmissione delle denunce di inizio attività presentate allo sportello unico comunale per l'edilizia, nonché delle informazioni catastali identificative dell'immobile contenute nei contratti di somministrazione. I decreti volti a disciplinare tali comunicazioni sono stati adottati senza il necessario interpello preventivo del Garante, circostanza che può determinare anche l'inutilizzabilità dei dati personali in tal modo raccolti, oltre che un vizio per violazione di legge.

Con il predetto *provvedimento* del 25 maggio 2005 il Garante ha quindi ravvisato l'esigenza che sia avviata, presso l'anagrafe tributaria, una verifica organica sull'effettiva necessità e proporzionalità della raccolta sistematica e generalizzata delle varie categorie di dati acquisite e disponibili, adottando anche modalità tecniche rispettose del Codice. In particolare, il Garante ha rilevato la necessità di verificare se, in rapporto alle finalità perseguite, sia sufficiente che l'Amministrazione finanziaria si limiti ad accedere per via telematica ai dati necessari alle verifiche, presenti presso banche dati pubbliche e private, evitando di duplicare in modo superfluo le medesime banche dati presso l'anagrafe tributaria, peraltro anche con possibili difficoltà di aggiornamento e nell'allineamento dei dati.

Anagrafe dei conti e dei depositi

Con il medesimo provvedimento il Garante è intervenuto anche in riferimento all'operatività dell'anagrafe dei conti e dei depositi istituita con la legge n. 413/1991.

Tutti i soggetti operanti nel settore finanziario devono rilevare e porre in evidenza i dati identificativi (compreso il codice fiscale) di tutti i soggetti che intrattengano qualsiasi rapporto o effettuino qualsiasi operazione di natura finanziaria. Ritenendo che il regolamento istitutivo della citata anagrafe debba essere modificato o integrato per essere adeguato alla nuova disciplina, il Garante ha segnalato la necessità di individuare soluzioni efficaci e rispettose dei principi in materia di protezione dei dati personali.

Comunicazioni telematiche nelle indagini bancarie

Il Garante ha espresso parere favorevole sullo schema di provvedimento predisposto dall'Agenzia delle entrate in merito all'adozione di specifiche tecniche per l'invio di comunicazioni telematiche in materia di indagini finanziarie, in attuazione di quanto previsto dalla legge finanziaria per il 2005 (*Parere* 21 dicembre 2005 [doc. *web* n. 1210095]).

Tale provvedimento, volto a ridurre i rischi di ingerenza di soggetti non autorizzati rispetto alla trasmissione cartacea delle comunicazioni, ha lasciato immutato l'*iter* procedimentale previsto per autorizzare l'inoltro delle richieste. Il provvedimento prevede che i dati acquisiti siano trattati nel rispetto dei principi di necessità, pertinenza e non eccedenza, e che la loro comunicazione avvenga mediante posta elettronica certificata. Si è incrementata così la sicurezza sulla provenienza della richiesta –anche grazie alla firma elettronica–, sull'integrità nella fase di trasporto del messaggio –attraverso la tecnica di cifratura mediante l'utilizzo di una coppia di chiavi asimmetriche–, nonché sulla ricezione esclusiva da parte dei legittimi destinatari.

Nell'ambito del medesimo provvedimento il Garante ha altresì valutato la conformità al Codice della nuova disciplina della dichiarazione stragiudiziale introdotta dalla legge finanziaria (*cfr.* par. 11.1).

2.10. *Trattamenti effettuati presso regioni ed enti locali*

Sono rimaste numerose le questioni interpretative portate all'attenzione del Garante da parte di regioni e di enti locali.

Tra le fattispecie di maggior rilievo generale, si ricorda quella evocata da una segnalazione che lamentava le modalità di gestione dei servizi pubblici presso un comune, affidata per alcune funzioni delicate –quali quelle relative alla gestione dell'ufficio anagrafe, dello stato civile e notifiche– a personale appartenente ad una società di diritto privato, nonché a volontari (*Nota* 3 agosto 2005).

Sono stati svolti anche accertamenti a seguito di una segnalazione relativa ad un comune che, nell'erogare un sussidio per mezzo di una banca convenzionata, avrebbe comunicato a quest'ultima dati sensibili del beneficiario (nella causale del mandato di pagamento era stato evidenziato il collegamento del sussidio con patologie di carattere psichiatrico: *Nota* 16 settembre 2005).

Dati di terzi in missive anonime acquisite agli atti comunali

Il Garante ha adottato una decisione a seguito di un ricorso che contestava l'inoltro ai consiglieri comunali, da parte del sindaco, della copia di una lettera anonima che denunciava la gestione, ritenuta poco trasparente, di alcuni immobili comunali affidata ad una Onlus amministrata dalla ricorrente. Quest'ultima si è rivolta al Garante chiedendo, in particolare, la cancellazione e/o il blocco dei dati. Il Garante ha ritenuto infondate le richieste della ricorrente. Dalla documentazione in atti non è risultato che il trattamento dei dati fosse in termini generali illecito, anche per quanto riguarda la conservazione della lettera, considerato che la stessa, indirizzata al sindaco del comune, era stata acquisita lecitamente al protocollo (*Provv.* 14 luglio 2005 [doc. *web* n. 1157675]). La ricorrente aveva chiesto anche di far cessare il comportamento, ritenuto illegittimo, del sindaco (inoltro della nota ai consiglieri comunali). Il ricorso è stato dichiarato infondato anche in riferimento a tale profilo, in quanto la nota riguardava una questione di indubbio interesse istituzionale, relativa alla gestione di un bene di interesse turistico e culturale del comune resistente. Pertanto, la sua comunicazione (pur potendo essere auspicabilmente preceduta da una valutazione più specifica della necessità della sua comunicazione ai consiglieri, alla luce del principio di pertinenza e non eccedenza di cui all'art. 11 del Codice) non è stata ritenuta illecita, in relazione alla volontà, attestata dal sindaco, di informare i consiglieri comunali riguardo ad un documento che, per quanto anonimo, conteneva elementi rilevanti (per quanto da verificare nella loro veridicità) su una questione di interesse istituzionale. Tale valutazione è apparsa conforme sia al generale potere di controllo politico-amministrativo che la legge attribuisce al consiglio comunale (art. 42 d.lg. 18 agosto 2000, n. 267), sia alle specifiche funzioni di controllo attribuite ai singoli consiglieri (anche in riferimento alla possibilità di chiedere la convocazione del consiglio o di presentare, sulla questione in esame, interrogazioni e mozioni ai sensi degli artt. 39, comma 2, e 43, comma 1, del citato d.lg. n. 267/2000).

Comunicazioni ed interconnessioni tra enti locali ed altre amministrazioni

Sono pervenute ancora, da regioni ed enti locali, richieste di valutazione del Garante ai sensi degli artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice, rispetto alla trasmissione ad altri soggetti pubblici di dati personali, ritenuti necessari per svolgere funzioni istituzionali da parte degli enti coinvolti in casi in cui mancano norme di legge o di regolamento che prevedano tale comunicazione.

È pervenuta ad esempio una richiesta della Comunità montana del Lazio Castelli romani e predestini per accedere agli archivi informatici Agea contenenti i dati anagrafici e produttivi delle aziende olivicole e i frantoi operanti nel territorio, relativi alle campagne olearie 2002-2003 e 2003-2004; ciò, al fine di costituire una banca dati sotto la vigilanza dell'Agea (*Nota* 2 febbraio 2005).

A tale proposito è stato ricordato che la comunicazione di dati è ammissibile se

realmente necessaria in rapporto alle funzioni istituzionali; occorre in particolare che le modalità della comunicazione, specie nel caso di accesso *on-line*, rispettino il principio di pertinenza e non determinino, presso l'amministrazione ricevente, un afflusso di dati esuberante rispetto alle finalità perseguite (art. 11 del Codice). Per permettere all'Autorità una valutazione compiuta, è stato chiesto di precisare la motivazione in base alla quale si sarebbe reso necessario, per la comunità montana, acquisire i dati presso l'Agea, chiarendo, in particolare, se le medesime informazioni fossero conoscibili mediante accesso ad altre fonti documentali detenute da soggetti pubblici, se risultassero liberamente accessibili a chiunque e se riguardassero tutte le aziende, ovvero soltanto quelle che avessero presentato domande di finanziamenti comunitari all'Agea.

L'Autorità ha fornito ulteriori chiarimenti ad un comune che aveva prospettato la necessità di effettuare una serie di trasmissioni di dati personali a terzi (*Nota* 21 marzo 2005). Con riferimento alla necessità di comunicare dati alla provincia rispetto a servizi socio-assistenziali espletati da quest'ultima in regime di convenzione con i comuni (d.l. 18 gennaio 1993, n. 9, convertito in legge, con modificazioni, dall'art. 1, comma 2, l. 18 marzo 1993, n. 67), è stato evidenziato che, laddove detta comunicazione riguardi dati sensibili e giudiziari, non è possibile avvalersi dell'art. 39 del Codice, in quanto per il trattamento di tale categoria di dati da parte dei soggetti pubblici il Codice detta una specifica disciplina particolarmente stringente (artt. 20, 21 e 22). Nella medesima fattispecie, in relazione alla prevista apertura di banche dati personali da parte del comune ad una società per azioni concessionaria per l'accertamento e la liquidazione dell'imposta sulla pubblicità e di diritti sulle pubbliche affissioni, asseritamente necessaria per permettere la gestione del servizio di riscossione dei relativi tributi, è stata parimenti rilevata l'impossibilità di avvalersi della comunicazione al Garante ai sensi dell'art. 39 del Codice, in quanto la stessa è ammessa solo tra enti pubblici. A tale proposito è stata però evidenziata la possibilità di valutare se la relazione fra il comune e la società concessionaria avrebbe potuto essere inquadrata, previa apposita designazione, nell'ambito di un rapporto fra titolare (il comune) e responsabile del trattamento (il concessionario) ai sensi dell'art. 29 del Codice, designando anche i dipendenti del concessionario preposti alle operazioni di trattamento quali incaricati del trattamento (art. 30). Per quanto concerne, infine, la necessità rappresentata dal medesimo comune di trasmettere i ruoli tributari e patrimoniali ad una società concessionaria per la riscossione dei tributi comunali e delle entrate patrimoniali dell'amministrazione locale, è stato precisato che l'uso delle informazioni dei debitori iscritti a ruolo e dei relativi coobbligati risulta consentito unicamente nei limiti e con le modalità stabilite dall'art. 18 d.lg. 13 aprile 1999, n. 112 e dal relativo decreto attuativo del Ministero delle finanze del 16 novembre 2000.

Raccolta differenziata dei rifiuti solidi urbani

L'Autorità ha concluso nel 2005 gli accertamenti avviati in relazione alle modalità di trattamento dei dati personali per finalità di gestione del servizio di raccolta differenziata dei rifiuti solidi urbani (*cfr. Relazione* 2003, p. 72). Ne è conseguita l'adozione di un provvedimento di carattere generale, risultato necessario per valutare congiuntamente il rispetto della disciplina sulla raccolta differenziata (che può comportare, quando è necessario, accertamenti sull'identità di contravventori passibili di sanzioni amministrative) con il diritto degli interessati a non subire violazioni ingiustificate della propria riservatezza, soprattutto in caso di indebita visione ed utilizzazione da parte di terzi di informazioni anche sensibili, quali quelle concernenti la salute (farmaci, prescrizioni mediche, ecc.) o le convinzioni politiche, religiose o sindacali, reperibili nei sacchetti o in contenitori analoghi di rifiuti (*Provv.* 14 luglio 2005 [doc. *web* n. 1149822]).

Con il medesimo provvedimento il Garante ha anche risposto a vari quesiti di enti locali e a numerosi reclami e segnalazioni di cittadini i quali lamentavano una violazione della propria riservatezza in relazione alle modalità di raccolta differenziata dei rifiuti e ai controlli amministrativi. L'Autorità ha così individuato un quadro di garanzie per rispettare diritti e libertà fondamentali dei cittadini, prescrivendo ai comuni, titolari dei trattamenti di dati per finalità di gestione di servizi di raccolta differenziata, di adottare alcune misure necessarie per conformarsi ai principi del Codice, sul presupposto che la raccolta differenziata, prevista da specifiche norme, risponda ad un importante interesse pubblico.

In particolare, il Garante ha ritenuto che l'obbligo imposto da alcuni enti locali di utilizzare sacchetti trasparenti, anche di diverso colore a seconda dei materiali da inserire, per la raccolta "porta a porta" –pur stimolando l'utenza ad una selezione responsabile dei materiali conferiti e favorendo il loro più efficace recupero– debba considerarsi in termini generali non proporzionato. Sproporzionata è risultata, altresì, la misura che obbligava ad applicare sul contenitore dei rifiuti targhette adesive riportanti "a vista" il nominativo e l'indirizzo della persona cui si riferiscono i rifiuti, in particolare se conferiti in strada.

Si è invece precisato che può ritenersi lecito contrassegnare il sacchetto dei rifiuti mediante un codice a barre relativo ai dati identificativi del soggetto (anche se collegato ad una banca dati anagrafica presso il comune), oppure fornire agli utenti appositi sacchetti dotati di *microchip* o, eventualmente, di dispositivi di *Radio Frequency Identification* (*Rfid*), poiché tali procedure permettono di limitare l'identificabilità del soggetto conferente ai soli casi in cui sia stata già accertata la violazione delle prescrizioni in ordine alla differenziazione. Infatti, al momento dell'apertura del sacchetto, i soggetti preposti alla verifica dell'omogeneità dei materiali inseriti vengono a conoscenza del suo contenuto, ma non anche degli elementi identificativi del soggetto conferente; per converso, i soggetti preposti all'applicazione della sanzione, mediante la decodifica del codice a barre o del *microchip*, acquisiscono il nominativo del soggetto cui il sacchetto si riferisce, in relazione all'accertata segnalazione di non conformità del conferimento, senza accedere al contenuto del sacchetto.

Il Garante ha anche ritenuto che le ispezioni dei sacchetti debbano ritenersi ammesse nei soli casi in cui il soggetto che abbia depositato i rifiuti con modalità difformi da quelle consentite non risulti in altro modo identificabile, dovendosi evitare la pratica di controlli generalizzati da parte del personale incaricato (agenti di polizia municipale; dipendenti di aziende municipalizzate) al fine di rinvenire nei sacchetti stessi elementi informativi. Tale conclusione resta valida anche quando la violazione consista nel mancato rispetto dell'orario di conferimento.

Quanto, infine, alle procedure di raccolta differenziata in apposite aree di conferimento (*cd.* ecopiazzole), è stato considerato lecito che i soggetti preposti alla loro gestione esigano l'esibizione di un documento di identità annotando il deposito del rifiuto in un registro recante il nome e l'indirizzo dei conferenti, la quantità approssimativa, nonché il tipo di materiale ricevuto, per la sola finalità di accertamento dell'effettiva residenza nel comune del conferente, nonché per evitare che lo stesso soggetto possa conferire i rifiuti in violazione dei limiti quantitativi ammessi.

Nonostante le indicazioni fornite con il citato provvedimento generale, risultano permanere tuttora comportamenti difformi rispetto a quanto prescritto, soprattutto con riferimento alla raccolta differenziata a domicilio. L'Ufficio ha in tali casi invitato il comune interessato a conformarsi entro breve termine alle prescrizioni ed a produrre ogni informazione utile a sostegno delle iniziative assunte, ricevendo un riscontro sul quale sono in corso ulteriori accertamenti (*Nota* 12 ottobre 2005).

Sponsorizzazione degli enti locali

Tra le questioni allo studio dell'Autorità concernenti l'attività degli enti locali e delle pubbliche amministrazioni in generale, è in corso di definizione quella relativa alla compatibilità con il Codice di alcuni contratti di sponsorizzazione.

2.11. *Attività giudiziaria*

Carta multiservizi giustizia

Il Ministero della giustizia ha sottoposto all'Autorità un progetto volto a realizzare un sistema sicuro di accesso del personale dipendente e dei magistrati operanti negli uffici giudiziari delle regioni meridionali ai sistemi informatici, locali (registri generali dei procedimenti penali e civili, basi dati investigative, ecc.) e centralizzati (*ad es.*, il casellario giudiziale), che trattano dati sensibili e giudiziari. Il progetto prevede l'utilizzo di una carta con microprocessore (denominata "Carta multiservizi giustizia"-Cmg), nonché di rilevatori biometrici di impronte digitali che permettano la sicura autenticazione dell'utente al momento dell'accesso.

Esprimendo, con un *provvedimento* del 27 ottobre 2005 [doc. *web* n. 1185160], le proprie valutazioni ai sensi dell'art. 17 del Codice (verifica preliminare in riferimento ai trattamenti dei dati personali diversi da quelli sensibili e giudiziari, che presentino rischi per i diritti e le libertà fondamentali nonché per la dignità dell'interessato), il Garante, attesa la finalità del progetto, ha considerato positivamente la scelta della caratteristica biometrica come credenziale di autenticazione dei soggetti abilitati, preventivamente designati quali incaricati del trattamento, ed ha apprezzato che le informazioni biometriche siano trattate solo in forma sintetizzata e compressa (*cd. template*), anziché in forma di immagine dattiloscopica, al fine di permettere un'autenticazione informatica locale.

Dopo aver richiamato la necessità del rispetto di tutte le norme contenute nel Codice in materia di misure di sicurezza (artt. 31 ss. e Disciplinare tecnico All. B) del Codice), l'Autorità ha, peraltro, ricordato che il sistema deve essere realizzato in armonia con i principi informatori del Codice, espressi in particolare nell'art. 11; ha quindi prescritto che vengano raccolti e trattati i soli dati pertinenti rispetto al perseguimento della finalità di realizzazione della Cmg, che i dati non siano utilizzati per altri scopi e che gli stessi vengano conservati per il solo tempo necessario per raggiungere la finalità dichiarata e successivamente distrutti. Il Garante ha, però, ritenuto che non sussistano esigenze di complessiva funzionalità del sistema o legate a specifiche finalità non altrimenti perseguibili (tale non potendo essere considerata, come previsto nel progetto, la finalità del rilascio di eventuali duplicati), tali da giustificare l'archiviazione delle informazioni biometriche in una banca dati centralizzata.

Metodi alternativi di risoluzione delle controversie presso la camera di commercio

L'Autorità è intervenuta nuovamente, su richiesta di una camera di commercio, al fine di individuare precise garanzie per gli interessati nel quadro dell'attuazione di un progetto per lo sviluppo di metodi alternativi di risoluzione delle controversie in collaborazione con un tribunale e un consiglio dell'ordine degli avvocati.

Rispetto alla definizione dei moduli operativi del progetto, basato comunque sull'adesione libera e volontaria degli interessati, sono state prescritte alcune misure a tutela della riservatezza, in particolare in tema di informativa, la quale dovrà essere resa più specifica, con riferimento alle modalità di trattamento e al periodo di eventuale conservazione temporanea dei dati presso la camera di commercio, anche in caso di insuccesso del tentativo di conciliazione, e sull'accessibilità dei dati personali contenuti nei fascicoli del tribunale, che non devono essere trattati dai rappresentanti della camera di commercio e dell'ordine (*Nota* 21 marzo 2005).

Mediazione penale e giustizia riparativa

Sono continuati nel 2005, e successivamente, i contatti con il Ministero della giustizia relativi al progetto volto a sperimentare un modello di giustizia riparativa nell'esecuzione penale, da realizzarsi attraverso percorsi di mediazione penale tra reo e vittima.

Nel corso dei lavori della commissione di studio "Mediazione penale e giustizia riparativa", costituita presso il Dipartimento dell'amministrazione penitenziaria, sono state di seguito sottoposte alla valutazione dell'Autorità le modalità attuative del progetto, che concernono profili che attengono alla tutela della riservatezza, soprattutto per quanto riguarda le esigenze di protezione della vittima del reato.

Acquisizione di verbali di intercettazioni da parte della giustizia sportiva

Nel luglio del 2005 il Garante ha preso in esame la segnalazione di un calciatore di una nota società, il quale contestava la comunicazione di alcuni atti da parte della Procura della Repubblica presso il Tribunale di Genova nei confronti della Federazione italiana giuoco calcio-Ufficio indagini, in relazione ad episodi di illecito sportivo. In particolare, il segnalante ha lamentato che fosse stata acquisita dalla Federazione copia di trascrizioni di intercettazioni telefoniche e ambientali, effettuate nell'ambito del procedimento penale in corso, nelle quali erano contenuti brani di conversazioni, a suo dire, attinenti esclusivamente alla propria sfera privata e non pertinenti rispetto ai fatti esaminati dagli organi della giustizia sportiva.

Nell'istruttoria, anche in base alle informazioni trasmesse sia dalla Federazione, sia dalla Procura, è tuttavia risultato, in primo luogo, che il materiale probatorio era stato formalmente richiesto e lecitamente acquisito dalla Federazione in attuazione della legge sulla correttezza nello svolgimento di manifestazioni sportive (art. 2, comma 3, l. n. 401/1989), la quale permette agli organi della disciplina sportiva di chiedere copia degli atti di un procedimento penale ai fini esclusivi della propria competenza funzionale.

In secondo luogo, il Garante ha accertato che la Procura di Genova aveva trasmesso alla Federazione stralci delle trascrizioni e dei brogliacci relativi ai fatti oggetto dell'indagine penale, dai quali erano state omesse le parti di conversazioni di natura strettamente privata. Tali brani, in effetti, sono risultati espunti dalla relazione conclusiva che l'Ufficio indagini aveva trasmesso nel mese di giugno alla Procura federale della Federazione, e di essi non vi era traccia nelle decisioni assunte dalla commissione disciplinare nel successivo mese di luglio.

All'esito di tali risultanze, tenuto altresì conto del divieto di pubblicazione degli atti trasmessi dall'autorità giudiziaria gravante sulla Federazione ai sensi dell'art. 114 c.p.p., e del fatto che per l'attività degli organi di giustizia sportiva non è prevista alcuna forma di pubblicità degli atti, il Garante ha quindi ritenuto che non fossero emersi elementi per adottare un provvedimento inibitorio dell'ulteriore trattamento dei dati personali dell'interessato da parte della Federazione, adottando così una decisione di non luogo a provvedere sulla segnalazione (*Provv.* 3 agosto 2005 [doc. *web* n. 1153792]).

Mezzi di prova

Sono inoltre pervenute all'Autorità altre segnalazioni relative all'acquisizione di mezzi di prova nell'ambito dei procedimenti giudiziari. In tali occasioni il Garante ha avuto modo di ribadire che resta riservata al giudice ogni valutazione in ordine all'ammissibilità e alla rilevanza delle prove nel processo. Premesso che, nei confronti dei trattamenti effettuati presso gli uffici giudiziari "per ragioni di giustizia", le norme a tutela della riservatezza trovano minore ambito di applicazione, come disposto dagli artt. 8, comma 2, lett. *g*) e 47 del Codice, l'Autorità ha ricordato che la validità, l'efficacia e l'utilizzabilità di atti, documenti –anche informatici– e provvedimenti nei procedimenti giudiziari, basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali civili e penali (art. 160, comma 6, del Codice).

3 Sanità

3.1. *Trattamento di dati idonei a rivelare lo stato di salute*

3.1.1. *Trattamenti per fini amministrativi*

Nel 2005 l'Autorità è intervenuta più volte in merito al trattamento dei dati sensibili, e in particolare di quelli idonei a rivelare lo stato di salute, effettuato da strutture sanitarie pubbliche per finalità di cura dei pazienti e per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione degli stessi. Si è tra l'altro evidenziato che anche quando si perseguono finalità amministrative per le quali non è necessario acquisire il consenso, è comunque ineludibile l'obbligo di informare gli interessati e di rispettare altresì le disposizioni contenute nei regolamenti sul trattamento dei dati sensibili e giudiziari (*Note* 13 gennaio e 23 febbraio 2005).

Monitoraggio della spesa e tessera sanitaria elettronica

Già nel 2004 l'Autorità aveva segnalato criticamente alla Presidenza del Consiglio dei ministri l'approvazione, in sequenza, di diversi decreti attuativi del sistema di monitoraggio della spesa sanitaria e di introduzione della tessera sanitaria, senza il prescritto parere del Garante. Nel merito sono stati anche formulati rilievi specifici sul sistema di raccolta centralizzata dei dati ricavati dalle ricette mediche e da altre prescrizioni specialistiche previsto dall'art. 50 d.l. n. 269/2003.

Nel 2005, il Garante ha ribadito tali delicati rilievi anche nei confronti del Ministro dell'economia e delle finanze, rinnovando l'invito a conformare al Codice il quadro normativo di attuazione della tessera sanitaria (*Nota* 24 gennaio 2005).

Anche in funzione dei diversi interventi del Garante, il Ministro dell'economia e delle finanze ha sottoposto al parere dell'Autorità il decreto ministeriale adottato in attuazione di quanto previsto dall'art. 50, comma 10, d.l. n. 269/2003, riguardante l'approvazione del protocollo sui dati rilevati dalle ricette mediche e registrati negli archivi del Ministero, che possono essere trasmessi al Ministero della salute e alle regioni. Le garanzie poste a tutela dei dati personali individuate da ultimo nel suddetto decreto sono state infine ritenute sufficienti dall'Autorità, la quale ha espresso pertanto avviso favorevole (*Parere* 21 luglio 2005 [doc. *web* n. 1151167]). In particolare, il predetto decreto ministeriale ha previsto che i dati ricavati dalle ricette mediche e da altre prescrizioni specialistiche siano trattati dal Ministero dell'economia e delle finanze esclusivamente per fini di liquidazione dei rimborsi dovuti alle struttura sanitarie, e che gli stessi dati siano trasmessi al Ministero della salute, all'Agenzia italiana del farmaco e alle regioni, dopo essere stati privati di ogni riferimento ad informazioni che rendano identificabili gli interessati, quali il codice fiscale o il codice a barre della tessera sanitaria (d.m. 9 marzo 2006).

Referti medici relativi ad incidenti stradali

In sede applicativa, ha costituito oggetto di specifica attenzione del Garante l'avvenuta consegna da parte di organismi sanitari alla polizia stradale dei referti medici di pazienti coinvolti in incidenti stradali. È stato precisato al riguardo che le strutture sanitarie, nel rispondere doverosamente alle richieste formulate dalle forze di polizia, sono tenute ad adottare i necessari accorgimenti affinché siano comunicate esclusivamente le informazioni oggetto dell'istanza, omettendo ogni altro dato personale che non sia strettamente indispensabile a soddisfare la richiesta.

Nella fattispecie esaminata dall'Autorità, l'azienda sanitaria, a fronte della richiesta della polizia stradale di ottenere copia del certificato relativo ad un esame alcolimetrico effettuato nei confronti di un paziente coinvolto in un incidente stradale, aveva invece rilasciato copia integrale del referto di ricovero, come tale comprensivo –oltre che del dato sull'alcolemia– anche dei risultati degli altri esami clinici compiuti (*Nota* 15 novembre 2005).

Indennizzi ad emotrasfusi danneggiati irreversibilmente

L'Autorità è stata chiamata a valutare la liceità dell'inserimento di una dicitura nella causale di bonifici bancari effettuati in caso di riconoscimento dell'indennizzo previsto dalla legge n. 210/1992 a favore di soggetti danneggiati da complicanze di tipo irreversibile a seguito di vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati. L'intervento si è reso necessario in quanto nei bonifici veniva indicata la dicitura "indennizzo di cui alla legge n. 210", idonea a rivelare lo stato di salute del beneficiario ai soggetti coinvolti nella procedura di pagamento dell'indennizzo (Banca d'Italia; istituti di credito). La Direzione provinciale del tesoro interessata ha poi individuato una modalità di pagamento più rispettosa della riservatezza degli interessati, sostituendo la dicitura con l'indicazione di un codice numerico, noto all'amministrazione del tesoro, impegnandosi a suggerire tale soluzione anche alla direzione centrale (*Nota* 14 luglio 2005).

3.1.2. *Trattamenti per fini di cura della salute*

Giornate di approfondimento presso il Garante

La peculiare disciplina del trattamento dei dati sensibili da parte delle strutture sanitarie è stata esaminata nel corso di una giornata di approfondimento sull'applicazione del Codice, sul tema "*Sanità e protezione dei dati*", organizzata dal Garante il 2 febbraio 2005.

L'incontro è stato incentrato sull'analisi di significative esperienze presso organismi sanitari pubblici e privati, delle soluzioni emerse e di alcuni risultati positivi, ispirati ai principi di semplificazione, armonizzazione ed efficacia. Si è avuto così modo di analizzare alcune specifiche modalità di applicazione delle misure di protezione adottate per garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati nell'organizzazione di prestazioni e servizi.

Diffusione di dati sanitari su siti Internet

L'Autorità ha invitato un ospedale a sospendere il trattamento di dati effettuato tramite il sito Internet della struttura all'interno del quale erano state pubblicate alcune fotografie di minori affetti da comuni patologie pediatriche (*Nota* 22 aprile 2005). L'Ufficio del Garante aveva infatti rilevato un trattamento di dati sensibili relativi a minori nei confronti dei quali l'ordinamento, oltre al divieto di diffusione di dati sensibili (art. 22 del Codice), appresta una tutela rafforzata per non pregiudicare l'armonico sviluppo della loro personalità. Anche in base al codice di deontologia per l'attività medica, il medico non può diffondere, attraverso la stampa o altri mezzi di informazione, notizie che possano consentire l'identificazione dell'interessato, e deve altresì assicurare la non identificabilità dei pazienti nelle pubblicazioni scientifiche di dati clinici o di osservazioni relative a singole persone (art. 10 codice di deontologia medica del 3 ottobre 1998).

Consegna di referti diagnostici e di certificazioni mediche

Con riferimento alla consegna di referti diagnostici, il Garante ha nuovamente precisato in termini generali che tali documenti possono essere ritirati anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante la consegna degli stessi in busta chiusa. Il personale designato come incaricato deve essere debitamente istruito anche in ordine a tali modalità di consegna dei referti medici (*Provv.* 9 novembre 2005 [doc. *web* n. 1191411]).

A seguito di segnalazione, si è poi rilevata una violazione delle regole sulle modalità di corretta consegna delle certificazioni mediche. Ciò, rispetto al comportamento tenuto da un laboratorio di analisi privato che aveva trasmesso via fax al

datore di lavoro dell'interessato copia di un referto relativo ad una radiografia effettuata a seguito di un incidente occorso sul luogo di lavoro. In tale occasione, l'Autorità ha evidenziato che gli esercenti le professioni sanitarie possono rendere noti i dati personali inerenti lo stato di salute al solo interessato, per il tramite di un medico designato dallo stesso interessato, oppure dal titolare (*Nota* 1° agosto 2005).

Prenotazione di prestazioni sanitarie

Con riferimento al trattamento dei dati idonei a rivelare lo stato di sieropositività, è stato segnalato al Garante l'utilizzo, da parte di una Asl, dei moduli di prenotazione delle prestazioni sanitarie in cui veniva indicata per esteso la natura dell'esenzione dalla partecipazione alla spesa sanitaria. Ciò, attraverso l'uso della dicitura "infezione da Hiv" in luogo dell'indicazione del codice identificativo della malattia, che rendeva immediatamente riconoscibile lo stato di salute dell'interessato. Dopo l'intervento dell'Autorità, la Asl ha ripristinato un precedente sistema in base al quale l'esenzione per patologia era indicata, correttamente, con il solo codice di esenzione, ed ha assicurato che si era trattato di una disfunzione causata dalle variazioni apportate al *software* di gestione dopo l'entrata in vigore del nuovo regime di esenzione dai *ticket* (*Nota* 21 ottobre 2005; *cfr.* anche *Newsletter* 2 febbraio 2006).

Impianto di dispositivi medici per raccolta di dati sulle condizioni cliniche

Una società farmaceutica si è rivolta all'Autorità per verificare la possibilità di trattare dati personali idonei a rivelare lo stato di salute dei soggetti cui sia impiantato un dispositivo medico, al fine di effettuare alcune registrazioni audio-video sulle relative condizioni cliniche, da diffondere in seguito presso la comunità medico-scientifica per illustrare i benefici connessi all'impiego del dispositivo medesimo.

L'Autorità, nel ricordare il generale divieto di diffusione di dati idonei a rivelare lo stato di salute, ha indicato alla società la necessità di adottare soluzioni idonee affinché i pazienti che prestano un consenso informato e specifico al trattamento di dati sensibili non siano resi identificabili da parte della comunità medico-scientifica destinataria delle suddette registrazioni (*ad es.*, attraverso l'oscuramento del volto e di altri eventuali particolari fisici che li rendano identificabili) (*Nota* 23 gennaio 2006).

3.1.3. *Strutture sanitarie e tutela della dignità delle persone*

Tutela della dignità del malato

Con un *provvedimento* generale in data 9 novembre 2005 [doc. *web* n. 1191411], il Garante ha richiamato gli organismi sanitari pubblici e privati (aziende sanitarie territoriali, aziende ospedaliere, case di cura, osservatori epidemiologici regionali e servizi di prevenzione e sicurezza sul lavoro) al necessario rispetto di una serie di misure previste dal Codice, al fine di assicurare il rispetto della dignità della persona e il massimo livello di tutela degli interessati in ambito sanitario.

Misure di organizzazione del servizio a tutela della riservatezza

In particolare, il Garante ha osservato che la tutela della dignità della persona deve essere sempre garantita, specie in riferimento a fasce deboli (disabili, minori, anziani) e a pazienti sottoposti a trattamenti medici invasivi, o per i quali è doverosa una particolare attenzione (*ad es.* interruzione della gravidanza). Specifici accorgimenti dovrebbero essere disposti, *ad es.*: nei reparti di rianimazione attraverso l'uso di paraventi o simili, volti a delimitare la visibilità dell'interessato, durante l'orario di visita, ai soli familiari e conoscenti. Ulteriori misure dirette a limitare il disagio dei pazienti sono state prescritte nei confronti di aziende ospedaliere universitarie, con riferimento alla partecipazione di studenti alle visite mediche o agli interventi sanitari: le strutture che intendono avvalersi di questa modalità devono infatti informare i pazienti, limitando la presenza degli studenti in relazione al grado di invasività del trattamento e circoscrivendo il numero degli studenti presenti, rispettando anche eventuali legittime volontà contrarie.

All'atto della prescrizione di ricette mediche o del rilascio di certificati, il personale sanitario deve evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dai locali o dalle

modalità utilizzate. Ospedali e aziende sanitarie devono predisporre "distanze di cortesia" non solo per le operazioni amministrative allo sportello (prenotazioni), ma anche per la raccolta dell'anamnesi, sensibilizzando gli utenti con cartelli, segnali ed inviti. Peraltro, il rispetto di tali misure non ostacola la possibilità di utilizzare determinate aree per più prestazioni contemporanee, quando tale modalità di organizzazione risponde all'esigenza terapeutica di diminuire l'impatto psicologico dell'intervento medico (*ad es.*, nell'ipotesi di trattamenti sanitari effettuati nei confronti di minori).

Ulteriori indicazioni sono state fornite in merito all'adozione di un "ordine di precedenza e chiamata" nell'erogazione delle prestazioni sanitarie, che prescinda preferibilmente dall'individuazione nominativa (*ad es.*, attribuendo un codice numerico o alfanumerico al momento della prenotazione o dell'accettazione). Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (*ad es.*, in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), possono essere peraltro utilizzati altri equivalenti accorgimenti come, ad esempio, il contatto diretto con il paziente.

Informazioni sui ricoveri e sulle degenze

Con riferimento alle notizie che l'organismo sanitario può fornire, anche per telefono, su una prestazione di pronto soccorso, l'Autorità ha specificato che occorre limitarsi ad indicare la circostanza della presenza di una persona nella struttura d'emergenza ai terzi legittimati (parenti, familiari o conviventi, valutate le diverse circostanze del caso). L'interessato, se cosciente e capace, deve essere comunque preventivamente informato (*ad es.* all'accettazione) e deve poter decidere a quali soggetti rendere nota la sua presenza al pronto soccorso.

Anche con riferimento alla notizia della presenza dei degenti nei reparti, è stata segnalata l'esigenza che le strutture sanitarie mettano tali informazioni a disposizione dei soli terzi legittimati (anche in riferimento a conoscenti e a personale di volontariato). In questo caso, l'interessato cosciente e capace deve essere informato al momento del ricovero, in modo da poter decidere quali soggetti possono venire a conoscenza della sua presenza nella struttura sanitaria o in un reparto di degenza.

Non è stata giudicata quindi corretta l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da effettuare, come avvenuto ad esempio per degenti che debbano subire un intervento operatorio (*Provv.* 17 marzo 2005 [doc. *web* n. 1170485]). Parimenti, non debbono essere resi visibili ad estranei documenti sulle condizioni cliniche dell'interessato, come nel caso di cartelle infermieristiche poste vicino al letto di degenza.

Altre prescrizioni

Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, per evitare che soggetti estranei possano dedurre informazioni sullo stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato. Tali cautele devono essere poste in essere anche con riferimento alla redazione delle certificazioni richieste per fini amministrativi non correlati a quelli di cura (*ad es.*, per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale).

Analoghe garanzie devono essere adottate da tutti i titolari del trattamento, ivi comprese le farmacie, affinché nella spedizione di prodotti non siano indicati, sulla parte esterna del plico postale, informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato (*ad es.*, indicazione della tipologia del contenuto del plico o del reparto dell'organismo sanitario mittente). Sulle modalità di applicazione di tali regole al settore sanitario, il Garante ha avviato una consultazione con organismi sanitari e associazioni interessate.

Spazi riservati e distanze di cortesia

L'Autorità è intervenuta con specifico riferimento alla mancata previsione di spazi riservati per la compilazione delle cartelle cliniche in una azienda sanitaria (*Nota* 26 gennaio 2005), e alla carenza di appropriate distante di cortesia per il pagamento del *ticket* sanitario agli sportelli di un ospedale pubblico (*Nota* 13 luglio 2005); si è occupata altresì di una segnalazione concernente la situazione di un'azienda ospedaliera presso la quale, per prenotare prestazioni mediche, i pazienti erano costretti ad accalcarsi presso l'unico sportello e a comunicare ad alta voce i propri dati anagrafici e clinici all'impiegato, posto al di là di un vetro spesso. Le ricette, passate "di mano in mano" lungo la coda, rimanevano depositate all'esterno dello sportello finché non venivano ritirate dall'impiegato (*Nota* 23 febbraio 2005). L'avvio di accertamenti da parte dell'Autorità ha indotto l'Azienda a rivedere la modulistica, il *software* impiegato e le modalità organizzative del servizio, prevedendo, tra l'altro, l'installazione di un sistema informatizzato per la gestione delle prenotazioni (ora possibili anche *on-line*), *box* con barriere per colloqui sanitari riservati, distanze di cortesia e percorsi differenziati (*cfr. Newsletter* 2 febbraio 2006).

3.1.4. *Protezione dei dati e procreazione medicalmente assistita*

Il Garante ha espresso parere favorevole sullo schema di decreto istitutivo, per legge, del registro nazionale dei centri autorizzati ad applicare le tecniche di procreazione assistita (*Parere* 26 luglio 2005 [doc. *web* n. 1151435]).

Il registro, previsto da un decreto del Ministro della salute in applicazione del disposto di cui all'art. 11 della legge 19 febbraio 2004, n. 40, conterrà i dati relativi alle strutture sanitarie autorizzate ad applicare le predette tecniche, necessari al loro censimento, e le informazioni concernenti le autorizzazioni di legge. L'Autorità ha richiesto che nell'allegato tecnico fosse apportata una specificazione in modo da ribadire che le unità di personale operante presso le predette strutture ("personale medico", "personale laboratorio di biologia", "medico anestesista", "infermieristico", "amministrativo") fossero registrate anch'esse con dati numerici, anziché con le generalità di ogni singolo dipendente. Sebbene il registro non contenga le generalità delle coppie interessate, sarà possibile disporre di dati statistici utili alla comprensione del fenomeno, potendosi raccogliere, comunicare o diffondere informazioni, anonime ed anche aggregate, relative alle coppie stesse, agli embrioni ed ai nati (d.m. 7 ottobre 2005, in *G.U.* 3 dicembre 2005, n. 282).

Il Garante si è riservato di valutare le modalità di raccolta e di conservazione dei dati nel registro, l'individuazione dei soggetti autorizzati a consultare i dati registrati e le relative modalità di accesso; ciò, in quanto il decreto prevede un ulteriore atto ministeriale di attuazione.

4 Dati genetici

4.1. *Le informazioni genetiche*

L'autorizzazione al trattamento

Il Codice prevede espressamente che il Garante debba rilasciare un'autorizzazione generale per il trattamento dei dati genetici, da chiunque effettuato (art. 90). Ciò, sentito il Ministero della salute, il quale provvede acquisito il parere del Consiglio superiore di sanità.

Un primo schema di autorizzazione, predisposto previo approfondimento svolto anche mediante l'acquisizione di pareri da parte di medici genetisti, è stato inoltrato il 25 gennaio 2005 al Ministero della salute per acquisire il parere predetto, riservandosi il Garante la possibilità di apportare allo stesso eventuali perfezionamenti anche all'esito delle indicazioni e suggerimenti pervenuti.

Nel corso del 2005 il Garante ha ricevuto dal Ministero della salute il parere del Consiglio superiore di sanità sul predetto schema di autorizzazione generale. Alla luce dei suggerimenti del Ministero si è avviata un'ultima fase di approfondimento sulle garanzie previste dall'autorizzazione, coinvolgendo nuovamente qualificati esperti della materia ai quali l'Autorità ha richiesto di formulare ancora proprie osservazioni e valutazioni.

Nella nuova autorizzazione, il Garante intende precisare anche la portata della nozione di "dato genetico", individuando le cautele da osservare in relazione alle informazioni genetiche e ai campioni biologici trattati a fini di tutela della salute dell'interessato o di un terzo appartenente alla stessa linea genetica, a scopi di ricerca scientifica e statistica, ovvero per finalità probatorie in un procedimento civile o penale.

Si prevede inoltre di introdurre specifiche garanzie e regole di condotta per lo svolgimento di *test* e *screening* genetici, di *test* di paternità e/o maternità, nonché di indagini medico-legali, soprattutto in relazione al contenuto e alle modalità dell'informativa, alla necessità di fornire un'appropriata consulenza genetica e psicologica all'interessato, al diritto di quest'ultimo di non conoscere i risultati dell'esame (ivi comprese eventuali "notizie inattese" che lo riguardano), alle modalità di manifestazione del consenso e al periodo di conservazione dei dati e dei campioni biologici.

Secondo lo schema provvisorio di autorizzazione, le ricerche in materia genetica dovrebbero essere effettuate con le metodologie proprie del pertinente settore disciplinare, sulla base di progetti che indichino le specifiche misure da adottare nel trattamento dei dati per garantire il rispetto dell'autorizzazione, nonché, più in generale, della normativa sulla riservatezza. Gli studi genetici condotti su popolazioni isolate potrebbero essere attuati se preceduti da un'ampia attività di informazione volta ad illustrare alle comunità interessate le caratteristiche fondamentali della ricerca. Resterebbe escluso il trattamento di dati genetici da parte di datori di lavoro ed imprese assicurative.

Nel periodo che precede il rilascio dell'autorizzazione, il trattamento di queste informazioni resta disciplinato in via transitoria dalla precedente autorizzazione generale del Garante, che consente di utilizzare i predetti dati soltanto per le finalità in essa individuate e nel rispetto di specifiche prescrizioni, come ad esempio il divieto di comunicare le informazioni genetiche a terzi (punto 2, lett. b), *autorizzazione generale* n. 2/2002).

Ricerche genetiche

A seguito di una segnalazione proveniente dall'estero, il Garante ha svolto accertamenti ispettivi per verificare il rispetto della disciplina sulla protezione dei dati personali, in ordine allo svolgimento di un'articolata ricerca genetica su popolazioni isolate in Alto Adige. Sulla base delle informazioni e dei documenti acquisiti *in loco*, pur riscontrando l'adempimento ad una larga parte degli obblighi previsti in materia, è stata accertata la violazione di alcune norme in tema di misure di sicurezza e la non conformità al Codice di alcune specifiche modalità di trattamento dei dati.

L'Autorità ha quindi adottato un provvedimento di prescrizione ai sensi dell'art. 169 del Codice (misure di sicurezza), invitando i ricercatori a cessare spontaneamente le modalità di trattamento rivelatesi in contrasto con le garanzie del Codice. In particolare, è stata segnalata la necessità di chiarire alcuni profili relativi alla titolarità del trattamento (la cui individuazione risulta essenziale anche per determinare i soggetti tenuti ad effettuare la notificazione al Garante ai sensi dell'art. 37 del Codice), di incaricare per iscritto i ricercatori, i medici e gli altri collaboratori coinvolti nelle attività di trattamento (impartendo loro le necessarie istruzioni), di configurare il programma di gestione dell'archivio elettronico, contenente i dati anagrafici, genealogici e sanitari degli interessati (in modo da escluderne l'identificazione al di fuori delle specifiche ipotesi previste dal progetto) e di verificare che i campioni biologici eventualmente trasmessi ad altri enti di ricerca associati allo studio non siano in alcun modo riferibili ad una persona identificata o identificabile.

Il Garante ha inoltre chiesto di accertare la possibilità di conseguire nel corso dello studio eventuali notizie inattese e, in tal caso, di porre in adeguata evidenza nell'informativa agli interessati il loro diritto di non conoscere i risultati della ricerca o degli esami genetici effettuati, in riferimento appunto agli eventuali *unespected finding* che li riguardino (*Nota* 29 marzo 2005).

Sulla base di alcune notizie di stampa, l'Ufficio ha poi avviato accertamenti in ordine ad un complesso progetto di ricerca genetica su popolazioni isolate in Lombardia (*Nota* 11 gennaio 2005).

Banca dati del Dna per uso forense

Il Garante è stato interpellato dalla Presidenza del Consiglio dei ministri in relazione ad un documento elaborato dal Gruppo di lavoro sulla biosicurezza, istituito con d.P.C.M. 3 marzo 2004, nell'ambito del Comitato nazionale per la biosicurezza e le biotecnologie.

Il documento in questione propone, per un verso, alcune modifiche al codice di procedura penale volte a colmare la lacuna legislativa già determinatasi a seguito della sentenza n. 238/1996 della Corte costituzionale, che aveva dichiarato parzialmente incostituzionale l'art. 224 c.p.p. nella parte in cui non disciplina i casi e i modi nei quali il giudice può disporre coattivamente accertamenti peritali sulla persona dell'imputato (*ad es.*, il prelievo di campioni biologici o altri accertamenti medici).

Per altro verso, il documento individua uno schema di disegno di legge che ipotizza l'istituzione di un archivio centrale dei profili del Dna, volto a consentire l'accertamento dell'identità degli autori degli illeciti penali e di altre persone coinvolte a vario titolo in fatti criminosi, nonché l'identificazione di persone scomparse.

Il Garante ha già approfondito preliminarmente se, e in quale misura, il progetto illustrato nel documento sia compatibile con i principi del Codice, in particolare con l'assetto sistematico delineato dall'art. 90 e dalla relativa autorizzazione in corso di predisposizione, riservandosi di formalizzare le proprie determinazioni nel caso in cui il progetto resti attuale nella nuova legislatura.

5 Ricerca statistica e scientifica

5.1. *Ricerca statistica*

Istat

Per quanto riguarda le attività di ricerca statistica svolte dai soggetti, parti o partecipanti al Sistema statistico nazionale, l'Istat, nell'adottare il Programma statistico nazionale-Psn 2005-2007, ha tenuto conto delle osservazioni formulate dall'Autorità nel parere espresso il 15 marzo 2005. Le novità introdotte hanno riguardato, in particolare, le modalità di redazione del Psn con riferimento alla sequenza delle schede relative alle rilevazioni ed elaborazioni, alle variabili da divulgare in forma disaggregata e al ricorso ad imprese di *marketing* per l'attività di raccolta dei dati, nonché la costituzione dell'ufficio di statistica da parte dei soggetti coinvolti nel Programma.

Il parere sul Programma statistico nazionale 2006-2008

Successivamente, nell'ambito del prescritto parere sul Psn 2006-2008 (*Parere* 23 novembre 2005 [doc. *web* n. 1225782]), il Garante ha puntualizzato alcuni ulteriori aspetti.

È stata in particolare evidenziata l'esigenza di specificare che in caso di raccolta di dati sensibili e giudiziari non sussiste l'obbligo di fornire i dati richiesti. Tale garanzia deve essere evidenziata sia al momento in cui è fornita l'informativa all'atto della raccolta dei dati, sia nelle schede relative a rilevazioni ed elaborazioni di dati sensibili e giudiziari, anche quando i dati sono raccolti presso terzi. Si è ribadito che la facoltatività della risposta dovrebbe essere garantita anche in caso di rilevazioni che, pur non concernendo dati sensibili o giudiziari, riguardino comunque informazioni suscettibili di ledere la dignità della persona; si è inoltre precisato che, qualora la raccolta di dati personali sia effettuata presso minori, l'informativa deve essere resa anche agli esercenti la potestà, adottando le opportune misure organizzative.

Osservatori regionali e territoriali sull'immigrazione

Il Comitato di presidenza dell'Organismo nazionale di coordinamento delle politiche di integrazione sociale dei cittadini stranieri, istituito presso il Cnel, ha avviato un tavolo di lavoro per analizzare il problema della struttura e dell'operatività degli osservatori regionali e territoriali sull'immigrazione, al fine di individuare fonti, metodologie ed indicatori comuni, anche in vista delle leggi regionali in materia di prossima emanazione.

Al tavolo di lavoro è stato invitato a partecipare anche l'Ufficio del Garante ed è stata prevista l'istituzione di un comitato ristretto per individuare in maniera unitaria, per tutte le regioni e le province autonome, l'inquadramento istituzionale e le attribuzioni degli osservatori, con particolare riferimento alle scelte metodologiche delle ricerche, alla comparabilità dei risultati e ai collegamenti con le banche dati presenti a livello nazionale e locale. In tale sede, è stata suggerita la possibilità di strutturare un modello unitario di osservatorio inquadrandolo nell'ambito di applicazione della disciplina normativa concernente la protezione dei dati personali nell'ambito delle attività di statistica e, in particolare, del codice di deontologia e buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale.

5.2. *Ricerca medica, biomedica ed epidemiologica*

Comunicazioni al Garante

Nel 2005 sono pervenute all'Autorità numerose comunicazioni, inoltrate ai sensi dell'art. 39, comma 1, lett. *b*), del Codice, riguardanti progetti di ricerca in campo medico, biomedico ed epidemiologico. L'Ufficio del Garante ha ricordato che la possibilità di trattare per scopi di ricerca dati sulla salute senza il consenso degli interessati rappresenta un'ipotesi residuale che il Codice prende in considerazione nell'eventualità che la ricerca rientri in un programma di ricerca biomedica o sanitaria. Soltanto in questo caso il titolare deve informarne preventivamente il Garante ai sensi dell'art. 39, comma 1, lett. *b*), specificando la correlazione della ricerca con un programma previsto dall'art. 12-*bis* d.lg. n. 502/1992. Il trattamento può essere avviato trascorsi 45 giorni da tale comunicazione, salvo che l'Autorità si opponga entro il medesimo termine, ovvero con successiva determinazione. Qualora il trattamento di dati personali sensibili sia preordinato a perseguire altre finalità non risulta infatti applicabile la speciale disciplina prevista dal predetto art. 39.

Sorveglianza epidemiologica e "ondate di calore"

Riguardo ai trattamenti di dati sulla salute effettuati da un'agenzia sanitaria regionale a fini di sorveglianza epidemiologica, in relazione a fenomeni di ondate di calore nell'estate scorsa, l'Autorità ha rilevato che in fase transitoria il trattamento di tali informazioni poteva ritenersi, in termini generali, lecito, qualora rispondesse a finalità di rilevante interesse pubblico individuate per legge e fosse effettuato nel rispetto del principio di indispensabilità previsto dal Codice, nonché dei presupposti e dei limiti stabiliti da altre disposizioni di legge o di regolamento (artt. 18, 20, 22, 98 e 110 del Codice). Resta quindi necessario verificare preliminarmente che l'indagine che si intende realizzare non possa essere altrimenti compiuta con l'utilizzo di dati anonimi o di dati personali non sensibili (artt. 3 e 22 del Codice). Per quanto attiene poi alle concrete modalità di trattamento dei dati e alle garanzie da osservare, l'Ufficio del Garante ha segnalato che, a decorrere dalla data di scadenza del termine per varare i regolamenti sui dati sensibili (poi fissato al 31 luglio 2006), siffatti trattamenti di dati potranno essere proseguiti se si provvederà, in conformità al Codice, ad individuare i tipi di dati e di operazioni effettuate per lo svolgimento di tali attività, in un atto di natura regolamentare adottato acquisendo il preventivo parere conforme del Garante (artt. 20, 154 e 181 del Codice).

Dati sulle dipendenze per finalità socio-assistenziali

In relazione ad un caso concernente un'azienda sanitaria l'Autorità ha precisato che la trasmissione di dati personali anagrafici e sanitari degli utenti del "Servizio territoriale dipendenze", comunicati ad enti comunali e ad altre aziende sanitarie ed ospedaliere per finalità assistenziali, è ammessa soltanto quando risulti indispensabile per perseguire finalità di rilevante interesse pubblico previste dal Codice (*ad es.*, per le finalità socio-assistenziali di cui all'art. 73, o per gli scopi di carattere amministrativo correlati alla cura e alla riabilitazione dei soggetti assistiti dal Ssn, ai sensi dell'art. 85). Occorre poi rispettare rigorosi obblighi di riservatezza –cui sono tenuti i servizi, i presidi e le strutture delle unità sanitarie locali, nonché i medici, gli assistenti sociali ed il restante personale– nel trattamento delle generalità o delle informazioni idonee ad identificare i soggetti che fanno uso di sostanze stupefacenti, i quali abbiano deciso di avvalersi dell'anonimato nei rapporti con la struttura sanitaria (artt. 120 e 121 d.P.R. n. 309/1990) (*Nota* 7 giugno 2005).

Registri di patologia

Nei lavori legati alla predisposizione dello schema-tipo di regolamento regionale per il trattamento di dati sensibili effettuati in ambito sanitario, che ha visto la partecipazione degli organismi rappresentativi degli enti regionali, delle aziende sanitarie e di rappresentanti dell'Ufficio del Garante, è stata riscontrata la proliferazione a

livello locale e/o regionale di registri di patologia (archivi contenenti informazioni identificative degli interessati in relazione a specifiche patologie), soprannumerari ed ulteriori rispetto a quelli espressamente previsti dalla legislazione nazionale.

Al riguardo, l'Autorità ha evidenziato che la moltiplicazione di tali archivi contrasta con quanto previsto dall'art. 94 del Codice, in base al quale le banche dati, i registri e gli schedari in ambito sanitario devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 del Codice).

In considerazione della particolare delicatezza delle informazioni contenute nei suddetti registri e del considerevole numero dei soggetti coinvolti, l'Autorità ha quindi segnalato che l'eventuale istituzione di tali banche dati sanitarie presuppone un delicato contemperamento tra il diritto alla riservatezza degli interessati e la tutela della salute pubblica; si tratta di una valutazione che deve essere affidata a specifiche fonti normative nazionali o regionali ovvero, eventualmente, ai piani sanitari nazionali o regionali (artt. 53, 55 e 58 l. n. 388/1978, artt. 1 e 2 d.lg. n. 502/1992). Il testo dello schema-tipo di regolamento, sottoposto all'esame del Garante e sul quale è stato espresso parere favorevole (*Parere* 13 aprile 2006 [doc. *web* n. 1272225]), ha recepito tali indicazioni.

6 Attività di polizia

6.1. *Il controllo sul Centro elaborazione dati del Dipartimento di pubblica sicurezza*

Nel contesto europeo ed internazionale, trova ampio e condiviso fondamento l'esigenza di predisporre efficaci strumenti di protezione dei dati personali e dei sistemi per finalità di polizia. Vari atti normativi e di altra natura in materia di scambi di dati e di cooperazione di polizia hanno infatti prestato notevole attenzione alla necessità di garantire, sotto vari profili, *standard* elevati di sicurezza dei dati e dei sistemi rispetto al rischio di indebite operazioni di accesso, lettura, copia o modifica delle informazioni (*v.*, in particolare, la Convenzione n. 108/1981 del Consiglio d'Europa del 28 gennaio 1981 (art. 7) e la Raccomandazione R(87)15 del Consiglio d'Europa del 17 settembre 1987, applicabili al Centro elaborazione dati del Dipartimento della pubblica sicurezza del Ministero dell'interno (C.e.d.); *v.* anche la dichiarazione del Governo italiano a margine della sottoscrizione della Convenzione di applicazione dell'Accordo di Schengen).

Su queste basi, nel quadro dello svolgimento dei compiti previsti dal Codice in materia, il Garante ha avviato nel 2005 un ciclo di verifiche presso gli archivi del C.e.d. per accertare l'effettiva rispondenza dei trattamenti di dati personali effettuati in detto ambito al rispetto delle garanzie previste dal Codice. Tale attività è stata intrapresa nei modi previsti dalla legge, per il tramite di un componente designato del Garante e con l'assistenza di personale specializzato (art. 160 del Codice), esaminati anche gli elementi forniti dal Dipartimento, che ha prestato fattivamente la collaborazione richiesta.

La complessa attività è stata suddivisa in due cicli, riservati il primo alla sicurezza dei dati e dei sistemi e, l'altro, ai più articolati profili delle modalità di trattamento dei dati e di interconnessione con banche dati pubbliche e private. Nel corso del primo ciclo di accertamenti, concretamente avviati nel mese di luglio 2005, sono stati appunto approfonditi in termini analitici i profili attinenti alla sicurezza nel trattamento dei dati e del sistema informativo nel suo complesso, prendendo in considerazione i riflessi sui diritti fondamentali delle persone interessate e gli importanti interessi pubblici coinvolti.

Dagli accertamenti non sono emersi profili di violazione degli obblighi penalmente sanzionati di adozione delle misure minime di sicurezza (artt. 33 e 169; Allegato B) del Codice). Il Garante ha però impartito al Ministero dell'interno-Dipartimento della pubblica sicurezza (*Provv.* 17 novembre 2005 [doc. *web* n. 1213309]) una prima serie di prescrizioni volte ad assicurare un rafforzamento del livello di protezione delle informazioni registrate nel C.e.d., fissando termini per attuarle e chiedendo un riscontro sui relativi esiti.

Saranno invece oggetto di un secondo provvedimento in fase di adozione nel 2006 gli altri profili concernenti le modalità e la complessiva organizzazione del trattamento dei dati personali presso il C.e.d., in particolare per quanto riguarda la qualità delle informazioni, la loro conservazione nel tempo e le menzionate interconnessioni.

6.1.1. *Altri interventi in relazione ad ulteriori attività di forze di polizia*

Cessione di fabbricati

L'Autorità si è occupata delle novità introdotte dalla legge finanziaria 2005 rispetto alle modalità di trasmissione al Ministero dell'interno delle comunicazioni di cessione di fabbricati e alla loro conoscibilità presso il C.e.d. del Dipartimento di pubblica sicurezza (art. 8 l. 1 aprile 1981, n. 121). Le nuove disposizioni di legge, oltre ad estendere l'obbligo di comunicazione ai soggetti che esercitano abitualmente l'intermediazione nel settore immobiliare, contemplano la realizzazione di un modello di comunicazione di cessione, da trasmettere in via telematica al Ministero dell'interno attraverso l'Agenzia delle entrate, anche avvalendosi di intermediari (*ad es.*, centri di assistenza fiscale e dottori commercialisti).

Questa soluzione pone seri problemi di compatibilità con la normativa comunitaria la quale non consente un'utilizzazione generalizzata e sistematica, per finalità di pubblica sicurezza, dei dati raccolti per altri scopi, oltre che con la specifica normativa di protezione dati relativa alle finalità di polizia, che vieta l'uso delle informazioni contenute nel C.e.d. per finalità diverse da quelle indicate dal legislatore nella disciplina di polizia, e stabilisce a tal fine il divieto di circolazione delle informazioni all'interno della pubblica amministrazione (art. 9 l. n. 121/1981). Il Garante ha altresì invitato il Ministro dell'interno ad intervenire per specificare il ruolo assunto dai soggetti esterni nel trattamento dei dati, al fine di rispettare la normativa di settore e il principio di finalità posto dal Codice, nonché a fornire indicazioni sui tempi di conservazione degli stessi dati (*Provv.* 25 maggio 2005 [doc. *web* n. 1131826], su cui *cfr.* anche i parr. 2.5 e 2.9).

Disciplina degli assegni bancari

Il Ministero dell'interno ha chiesto all'Autorità di chiarire alcuni aspetti applicativi della normativa in materia di assegni bancari. In particolare, si è esaminata l'organizzazione del flusso di dati tra le prefetture e l'archivio degli assegni bancari e postali delle carte di pagamento irregolari attraverso il segmento A.s.a. (la sezione dell'archivio contenente i dati relativi alle sanzioni amministrative in materia di assegni), attivo presso il Ministero e gestito dalla Società interbancaria per l'automazione-Ced Borsa (Sia) S.p.A. L'Autorità ha rilevato che tale flusso di dati risulta previsto direttamente dalla legge (art. 10-*bis* l. n. 386/1990) e che la gestione dell'archivio è stata affidata alla Sia S.p.A., responsabile del trattamento, direttamente dalla Banca d'Italia. È stata inoltre presa in considerazione l'intenzione del Ministero di avviare la sperimentazione della trasmissione telematica dei rapporti di accertamento della violazione da parte dei pubblici ufficiali in luogo di quella cartacea ai prefetti competenti ad applicare la sanzione amministrativa.

Schede d'albergo

Il Ministero dell'interno ha richiesto al Garante di esprimere il proprio parere in merito ad uno schema di decreto volto ad indicare le modalità di comunicazione all'autorità di pubblica sicurezza, in particolare attraverso reti telematiche, dei dati dei soggetti alloggiati nelle strutture ricettive (*Parere* 1° giugno 2005 [doc. *web* n. 1138725]).

Nell'esprimere il parere il Garante ha ricordato, in primo luogo, che il testo unico delle leggi di pubblica sicurezza (r.d. n. 773/1931) non prevede la conservazione delle "schedine d'albergo" da parte della struttura ricettiva la quale, una volta acquisita idonea ricevuta che dimostri di aver assolto l'obbligo di trasmissione, deve cancellare i dati del cliente con la sola eccezione delle informazioni necessarie a fini fiscali e contabili (quali, *ad es.*, i dati da inserire nella fattura o nella ricevuta). Il Garante ha affermato che la comunicazione delle informazioni deve avvenire direttamente senza il tramite di altri soggetti mentre, se avviene via Internet, sono necessarie particolari garanzie per assicurare che siano destinatarie effettivamente ed unicamente le questure. Le informazioni devono essere conservate dalle questure separatamente da ogni altra informazione detenuta per finalità di giustizia o di pubblica

sicurezza (art. 53, comma 2, del Codice), per un tempo breve, in conformità alle norme applicabili (art. 11, comma 1, lett. *e*), 53 e 57, comma 1, lett. *d*) del Codice). Le informazioni possono essere consultate dal solo personale appartenente alle forze di polizia espressamente autorizzato con apposito provvedimento, per esclusive finalità di prevenzione, accertamento e repressione dei reati o di tutela dell'ordine e della sicurezza pubblica.

Infine, l'Autorità ha rilevato che non consta, allo stato, l'esistenza di elementi che possano giustificare l'inserimento dei dati in una banca dati centralizzata, anche nell'ambito del C.e.d. del Dipartimento di pubblica sicurezza.

Osservatorio sugli appalti

È proseguita la partecipazione dell'Ufficio del Garante al tavolo di lavoro avviato dal Ministero dell'interno, finalizzato a realizzare un sistema automatizzato di supporto alle decisioni per assicurare trasparenza e sicurezza degli appalti nel Mezzogiorno, attraverso l'individuazione di soluzioni idonee a realizzare tale iniziativa nel pieno rispetto delle garanzie previste dal Codice.

6.2. *Controllo sui trattamenti effettuati dai servizi di informazione e di sicurezza*

Nel 2005 il Garante ha proseguito la periodica attività di verifica in relazione a specifici trattamenti di dati personali effettuati presso i servizi di informazione e di sicurezza e gli altri competenti organismi in materia (Sismi, Sisde e Cesis), la cui disciplina è contenuta nell'art. 58 del Codice.

Tali accertamenti, effettuati nel mese di marzo 2005, sono stati svolti dall'Autorità in relazione a specifiche segnalazioni di soggetti interessati ed in conformità alle modalità previste dal Codice (art. 160). In relazione all'esito dei controlli, che si sono svolti come di consueto con la piena collaborazione dei predetti organismi, il Garante ha fornito riscontro agli interessati nei termini previsti dal Codice.

6.3. *Il controllo sul Sistema informativo Schengen (Sis)*

Accesso diretto

Nel 2005 è diminuito notevolmente il numero delle richieste di accesso ai dati pervenute direttamente al Garante. Ciò, a seguito della "campagna informativa" condotta anche in collaborazione con il Ministero degli affari esteri e le cancellerie consolari in ordine alle nuove modalità di esercizio dei diritti introdotte dal Codice (delle quali è stata già fornita ampia descrizione nella *Relazione* 2004, p. 49), in virtù delle quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del Sis, ossia al Dipartimento della pubblica sicurezza, per l'accesso ai dati che lo riguardano registrati nell'N-Sis (*c.d.* "accesso diretto").

Dall'esame delle note inoltrate al Garante, per conoscenza, dalla Divisione N-Sis, si rileva che alcune delle indicazioni fornite dall'Autorità ai competenti uffici del Dipartimento della pubblica sicurezza possono ritenersi ormai implementate, per quanto concerne l'accesso diretto, gli altri diritti contemplati dalla Convenzione ed il conseguente riscontro.

In particolare:

a) il riscontro è fornito di solito direttamente all'interessato, non più tramite la rappresentanza diplomatica;

b) si procede a comunicare agli interessati sia il primo inserimento della segnalazione, sia gli eventuali successivi rinnovi, nonché il motivo della

segnalazione nel Sis, e cioè il provvedimento che, ai sensi degli artt. 94-100 della Convenzione, risulta presupposto dalla segnalazione medesima;

c) l'interessato è reso edotto delle facoltà riconosciutegli in relazione a sue doglianze (modalità di richiesta di revoca dell'espulsione, prova dell'uscita dal territorio, usurpazione d'identità, ricongiungimento familiare, ecc.).

Residuano alcuni aspetti da approfondire con gli uffici del Dipartimento della pubblica sicurezza e il Centro visti del Ministero degli affari esteri, circa l'ulteriore snellimento necessario per le procedure di riscontro agli interessati e per la verifica della loro effettività in caso di usurpazione d'identità.

Valutazione-Schengen in Italia

Come già riportato nella *Relazione* 2004 (p. 50) l'Italia è stata oggetto di una visita valutativa del gruppo di esperti per la valutazione-Schengen costituito dal Consiglio dell'Unione europea, il quale ha esaminato il funzionamento di tutti gli elementi che compongono il sistema (Sis, Sirene, visti e frontiere esterne), in ciascuno Stato membro.

Con il rapporto redatto dagli esperti al termine della visita è stata espressa una valutazione positiva che comprende però un invito a controllare i dati inseriti dall'Italia nel Sis ai fini delle segnalazioni di cui all'art. 96 della Convenzione per l'applicazione dell'Accordo di Schengen (che risultano numericamente superiori a quelli inseriti dagli altri Stati aderenti), verificando la necessità del loro mantenimento. Su tale aspetto si è incentrata anche la specifica azione dell'Autorità comune di controllo Schengen (Acc), nell'ambito dell'attività di verifica sulle modalità di inserimento delle segnalazioni di stranieri nel Sis al fine della non ammissione nel territorio degli Stati parti della Convenzione (su cui *v.* il par. 22.2).

7 Attività giornalistica e mezzi di informazione

7.1. *Tutela dei minori*

Dati idonei a rivelare lo status di adottato

Nel 2005 sono pervenute varie segnalazioni relative al trattamento di dati effettuato in occasione di servizi giornalistici riguardanti vicende collegate a rapporti o a procedimenti di adozione.

Il Garante ha ricordato che la diffusione di dati idonei ad identificare un minore adottato, oltre a porsi in contrasto con la disciplina sulla protezione dei dati, viola la normativa in materia di adozione nella parte in cui riconosce speciali cautele e procedure per accedere alle relative informazioni, affidando ai genitori la scelta sui modi e i termini per informare il minore della sua condizione (*cfr. Comunicato stampa* 5 maggio 2005).

Il Garante è anche intervenuto rispetto alla pubblicazione, da parte di un quotidiano locale, di dati che rendevano nel loro insieme identificabili i protagonisti di un caso di adozione; si è evidenziato che le cautele imposte rilevano anche con riferimento a vicende relative ad adottati divenuti maggiorenni (*cfr. Newsletter* 28 ottobre 2005).

7.2. *Cronache giudiziarie*

Libertà di informazione e procedimenti penali

Hanno trovato ulteriore conferma, nella giurisprudenza nazionale (Tribunale di Milano, sez. I civile, 9 novembre 2004, n. 12746) ed europea (Corte europea dei diritti dell'uomo n. 50774/99, 11 gennaio 2005), i principi affermati nell'ambito di precedenti pronunce del Garante in ordine all'illiceità della diffusione di foto segnaletiche non giustificata da scopi di giustizia e di polizia, anche quando le fotografie vengano mostrate durante conferenze stampa.

Il Garante ha esaminato anche nel 2005 numerose questioni riconducibili al tema della diffusione di dati personali relativi a procedimenti penali. Con particolare riferimento alle cronache su attività di indagine e processuali, l'Autorità, provvedendo nei confronti di una testata giornalistica che aveva pubblicato un'immagine in primo piano di una donna con le manette ai polsi imputata per omicidio, ha ricordato che la diffusione di tali immagini è vietata dalla legge (art. 114, comma 6-*bis*, c.p.p.; art. 8, comma 3, codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, Allegato A.1) del Codice).

All'esito dell'istruttoria di diverse segnalazioni e di alcuni reclami, l'Autorità ha inoltre ribadito che la pubblicazione di dati giudiziari (art. 4, comma, 1, lett. *e*) del Codice) è ammessa, pur senza il consenso dell'interessato, ma nel presupposto dell'"essenzialità dell'informazione riguardo a fatti di interesse pubblico" (art. 137, comma 3, del Codice, art. 12 del codice di deontologia per l'attività giornalistica) e nella misura in cui i dati non siano relativi ad atti coperti da segreto o non pubblicabili per legge (art. 114 c.p.p.). La sussistenza del carattere di essenzialità dell'informazione deve essere ravvisata necessariamente caso per caso, nel contesto dei fatti narrati (art. 6 codice di deontologia), come già specificato nel documento del 6 maggio 2004 inviato all'Ordine nazionale dei giornalisti (*v. Relazione* 2004, pp. 53-54).

Pubblicazione di fotografie acquisite in ambito privato

Alla luce del parametro di essenzialità dell'informazione l'Autorità non ha ravvisato violazioni nella pubblicazione di alcune fotografie a corredo di notizie riguardanti operazioni di arresto (*ad es.*, se tratte da album di famiglia), sul presupposto della loro lecita acquisizione. Una decisione del Garante ha ritenuto legittima la richiesta dell'interessato formulata ad un quotidiano allo scopo di conoscere l'origine di una propria fotografia, pubblicata nel contesto di un articolo che riferiva della richiesta di rinvio a giudizio formulata a carico dell'interessato medesimo (*Provv.* 6 ottobre 2005 [doc. *web* n. 1185330]).

Diffusione di dati sulla salute

Sempre in riferimento alla pubblicazione di fotografie su organi di stampa, l'Autorità ha ritenuto non conforme al canone dell'essenzialità la pubblicazione della foto di un giovane sieropositivo arrestato per alcuni fatti criminosi e successivamente sottoposto ad una diversa indagine per possibili lesioni nei confronti di alcune donne (*Nota* 31 marzo 2005). In tale circostanza è stato ricordato come esistano modalità differenziate, rispettose della dignità e della riservatezza degli interessati, altrettanto idonee ad "allertare", ove necessario, persone che hanno avuto rapporti con soggetti sieropositivi (ad esempio, attivando numeri verdi o altri servizi di informazione e assistenza in grado di fornire opportune informazioni).

Intercettazioni telefoniche e dati di traffico

Il rispetto del principio di "essenzialità dell'informazione" è stato altresì prescritto dal Garante nella decisione su un reclamo presentato da un noto personaggio che lamentava la diffusione, da parte di organi di stampa, di dati personali contenuti nelle trascrizioni di intercettazioni telefoniche disposte nell'ambito di indagini riguardanti delicati fatti di cronaca (*Provv.* 30 novembre 2005 [doc. *web* n. 1212642]). Il Garante ha ritenuto che l'interesse pubblico connesso alle vicende per le quali era stato instaurato il procedimento penale giustificasse, in termini generali, la possibile diffusione di alcuni dati personali contenuti in atti di indagine depositati ed acquisiti dai giornalisti secondo modalità non risultate allo stato degli atti illecite (in relazione ad atti processuali conoscibili dalle parti).

Tuttavia, non tutte le informazioni diffuse sono risultate necessarie a soddisfare essenziali esigenze di cronaca. È stata perciò ritenuta illecita la diffusione del contenuto di alcune conversazioni telefoniche intercorse tra i reclamanti le quali, diversamente da altre, non presentavano un collegamento, neanche indiretto, con le vicende economico-finanziarie oggetto di cronaca, come pure la pubblicazione del testo di due messaggi *Sms* a contenuto esclusivamente privato e del tutto personale, relativi al rapporto affettivo tra i reclamanti medesimi e che non assumevano alcun rilievo in base al ruolo e alla dimensione pubblica di questi ultimi.

In relazione alla stessa vicenda il Garante ha invece dichiarato inammissibile, per carenza dei necessari presupposti, un ulteriore ricorso presentato in via d'urgenza da uno dei due personaggi coinvolti, che lamentava un pregiudizio imminente ed irreparabile in relazione alla diffusione di notizie, ritenute false, circa la situazione patrimoniale e finanziaria delle aziende del gruppo societario di cui era proprietario.

Eccedente il diritto di cronaca, e quindi illecita, è stata ritenuta anche la riproduzione, a margine di articoli di cronaca sulle indagini relative all'omicidio del vice presidente del Consiglio regionale della Calabria, di parti di documenti recanti dati personali relativi al traffico di utenze telefoniche –compresi alcuni dati accessori e quelli relativi agli intestatari– riportati in una consulenza tecnica disposta nell'ambito di una precedente indagine; siffatta riproduzione aveva infatti comportato la diffusione di dati personali relativi anche a soggetti estranei ai fatti criminosi oggetto di cronaca.

Conferenza internazionale su giustizia e mezzi di comunicazione

Il tema dei rapporti "giustizia e media" è stato al centro di una riflessione a livello europeo nell'ambito della 2ª Conferenza europea dei giudici del Consiglio d'Europa (Cracovia, 25 e 26 aprile 2005) le cui conclusioni (consultabili all'indirizzo *web* *www.coe.int*, unitamente al rapporto della delegazione italiana) evidenziano la neces-

sità di adottare misure che concilino le diverse esigenze di trasparenza della giustizia e di libero convincimento dei giudici, con la tutela della dignità umana, della *privacy*, della reputazione e con la garanzia della presunzione di innocenza.

Vittime di reati e resoconti sui decessi

Vari ricorsi, segnalazioni e reclami pervenuti nel periodo di riferimento hanno riguardato la pubblicazione di dati personali relativi a vittime di episodi criminosi.

Il Garante ha in primo luogo ricordato l'esistenza di limiti precisi dettati dalla legge in relazione a crimini specifici, ad esempio a tutela delle vittime di reati sessuali (art. 734-*bis* c.p.); ha conseguentemente vietato ad un settimanale di pubblicare i dati identificativi di una giovane donna vittima di un tentativo di violenza (*Provv.* 13 luglio 2005 [doc. *web* n. 1152088]).

Rispondendo ad alcune segnalazioni e richieste di parere, l'Autorità ha poi segnalato che, anche fuori dei casi in cui sussistano specifici limiti di legge, i mezzi di informazione sono tenuti pur sempre ad osservare un particolare rigore nel valutare l'essenzialità dell'informazione rispetto a fatti di cronaca e nel fare riferimento alle vittime di azioni delittuose (furti, rapine, aggressioni, ecc.).

All'attenzione dell'Autorità sono pervenuti anche diversi articoli, relativi soprattutto alla cronaca locale, che riferivano di decessi avvenuti in contesti o per cause particolari (uso di sostanze stupefacenti, malori, incidenti). In alcuni casi è stata riscontrata la violazione del limite di "essenzialità dell'informazione", come nel caso della pubblicazione di dati personali relativi alla sfera personale del deceduto e di quella dei suoi familiari, risultati eccedenti e non pertinenti rispetto all'evento narrato, ovvero in relazione alla pubblicazione di articoli contenenti descrizioni particolarmente impressionanti del delitto (art. 8, comma 1, codice di deontologia). L'Autorità ha altresì ricordato che, in simili del genere, i diritti di cui all'art. 7 del Codice possono essere esercitati legittimamente dai familiari del deceduto, anche in riferimento ai dati personali dello stesso, mentre eventuali azioni di risarcimento dei danni restano esercitabili, ove ne ricorrano i presupposti, solo dinanzi all'autorità giudiziaria ordinaria (*Provv.* 21 dicembre 2005 [doc. *web* n. 1217538]).

Infine, in occasione del decesso di un personaggio noto nell'ambiente sportivo, avvenuto nel corso di una diretta televisiva, il Garante, nell'immediatezza del fatto, ha allertato i mezzi di informazione affinché si astenessero dal pubblicare foto o dal mandare in onda filmati lesivi della dignità e della riservatezza dell'interessato. L'Autorità ha poi dato atto che gli stessi mezzi di informazione si erano autonomamente attenuti a tali cautele, essendosi limitati a diffondere immagini con inquadrature a distanza (*Comunicati stampa* 4 ottobre e 18 novembre 2005).

Atti terroristici e deontologia del giornalista

Il tema dell'informazione in connessione con lo sviluppo tecnologico è rimasto d'attualità anche in relazione a vicende terroristiche e all'uso del *web* per divulgare messaggi ed attività eversive. L'Assemblea parlamentare del Consiglio d'Europa ha sollecitato l'elaborazione di un codice di condotta per i giornalisti ed ha chiesto ai professionisti del settore di *"astenersi dal pubblicare immagini scioccanti di atti terroristici che violano la* privacy *e la dignità delle vittime"* (Raccomandazione 1706(2005) del 20 giugno 2005).

7.3. *Dati idonei a rivelare lo stato di salute*

Pubblicazione di dati sulla salute e dignità della persona

È stato esaminato un caso significativo in relazione al servizio di cronaca pubblicato da un quotidiano a tiratura nazionale, incentrato sulla vicenda di una donna, in coma irreversibile e in stato di gravidanza, e sulla decisione dei medici e dei familiari di tenerla se necessario in vita artificialmente per consentire la nascita prematura di un figlio.

Il Garante ha ritenuto illecito il servizio che aveva portato a pubblicare dati non indispensabili che nel loro insieme avevano reso identificabili gli interessati, specie nel loro contesto territoriale, fornendo informazioni di natura strettamente clinica relative alla donna, nonché a possibili convinzioni etico-religiose dei suoi familiari (in violazione degli artt. 5 e 10 del codice di deontologia). Il Garante ha stigmatizzato, altresì, il comportamento tenuto dalla struttura sanitaria dalla quale erano evidentemente state attinte tali informazioni, rilevando che, in assenza di un preciso consenso da parte dei familiari a siffatta comunicazione, i sanitari avrebbero dovuto attenersi al rispetto del segreto professionale (*Provv.* 13 luglio 2005 [doc. *web* n. 1152080]).

È stata riscontrata un'altra grave violazione in riferimento alle modalità con le quali alcune testate giornalistiche, anche attraverso il proprio sito *web*, hanno diffuso informazioni concernenti una persona in condizioni di salute particolarmente critiche (indicata, a seconda delle testate, mediante le generalità o altri riferimenti idonei a renderla agevolmente identificabile), con specifici riferimenti anche ai sintomi della patologia e alle ipotesi formulate sulla diagnosi (sindrome di Creutzfeldt-Jakob e sue varianti, comunemente note come morbo della "mucca pazza"). Come già avvenuto in passato in un caso analogo (*Relazione* 2002, p. 95), il Garante ha precisato che la circostanza che l'illecita pubblicazione trovasse origine in notizie diramate da talune agenzie di stampa –le quali non avevano omesso di indicare le generalità dell'interessato– non esimeva comunque altre testate giornalistiche dal dovere di garantire l'anonimato dell'interessato (*Provv.* 23 novembre 2005 [doc. *web* n. 1225898]).

Si è poi concluso il procedimento relativo ad un servizio trasmesso da un' emittente televisiva e concernente un soggetto "senza fissa dimora" (*Provv.* 7 luglio 2005 [doc. *web* n. 1170284]). Dopo un temporaneo provvedimento di blocco (*v. Relazione* 2004, p. 55) il Garante ha vietato all'emittente di diffondere alcune immagini che mostravano l'interessato in un evidente stato di difficoltà fisica e psichica, ritenendole lesive della sua dignità, oltre che raccolte in violazione dei principi di correttezza e di trasparenza (art. 11, comma 1, lett. *a*) del Codice; art. 2 del menzionato codice di deontologia).

7.4. *Libertà di informazione e personaggi pubblici*

Rispetto alle persone note, o che esercitano funzioni pubbliche, il giornalista dispone di margini più ampi nella diffusione di informazioni personali ove queste assumano rilievo in base al ruolo o al carattere pubblico dell'attività dei soggetti interessati (*cfr.* anche *Relazione* 2004, p. 55). Il principio è stato ribadito dall'Ufficio del Garante nel rispondere a diverse segnalazioni pervenute nel corso dell'anno, inoltrate da esponenti del mondo politico, di quello giornalistico e dello spettacolo (*Provvedimenti* 7 luglio 2005 [doc. *web* n. 1170291 e n. 1170297]).

Figli minorenni di personaggi pubblici

Il rilievo pubblico di una persona non può affievolire la tutela riconosciuta a congiunti e, in particolare, ai minori. Il principio è stato riaffermato dal Garante nel riconoscere la fondatezza di una segnalazione e di un reclamo con cui si lamentava l'illiceità della pubblicazione delle generalità di minori e di altri soggetti nel contesto di articoli incentrati su vicende riguardanti esponenti politici locali.

L'Autorità è poi intervenuta nei confronti di un settimanale che, nel dare notizia di un presunto legame sentimentale di un noto personaggio, aveva pubblicato un articolato servizio fotografico in cui comparivano componenti della sua famiglia ritratti in alcuni momenti di vita privata. In particolare, oltre alle immagini della

moglie, della suocera e dei figli –dei quali almeno uno risultava riconoscibile, poiché il suo volto era stato solo parzialmente oscurato–, il settimanale aveva pubblicato diversi altri dati personali, unitamente alle foto del luogo di residenza e della palazzina di famiglia. Sulla questione pende un contenzioso dinanzi all'autorità giudiziaria ordinaria, essendosi impugnato il provvedimento con cui il Garante ha vietato la pubblicazione di tali fotografie (art. 152 del Codice) (*Provv.* 23 novembre 2005 [doc. *web* n. 1200112]).

Dati personali contenuti in denunzie e atti pubblici

Si è ritenuto che concretizzassero una violazione dei limiti del diritto di critica e di cronaca anche i riferimenti personali contenuti in un ampio servizio giornalistico pubblicato da un giornale locale, concernente la denuncia di un possibile giro di usura nell'ambito di alcune case da gioco. Secondo il Garante, la diffusione di diversi dati personali relativi all'autore della denuncia –presidente di un'associazione, conosciuto anche per le sue prese di posizione pubbliche– aveva violato il principio di essenzialità dell'informazione che comporta anche il dovere del giornalista di evitare riferimenti a congiunti o ad altri soggetti non interessati ai fatti riportati (art. 5, comma 1, codice di deontologia; *Provv.* 7 luglio 2005 [doc. *web* n. 1170311]).

A seguito della segnalazione di un giornalista che opera per Rai-Radio televisione italiana S.p.A., l'Ufficio del Garante ha poi ribadito l'orientamento dell'Autorità in ordine alla conoscibilità di classi stipendiali, indennità ed altri emolumenti corrisposti ad amministratori, dirigenti e lavoratori dipendenti ed autonomi da concessionari di pubblici servizi, atteso anche l'interesse pubblico ad ottenere notizie sulle prassi in atto presso tali enti e sull'utilizzo delle relative risorse.

Non è stato invece ravvisato un analogo interesse in riferimento alla pubblicazione dell'indirizzo completo dell'abitazione privata di una giornalista, diffuso nella rubrica di posta di una rivista in risposta alla richiesta di una lettrice. Nel fornire riscontro alla segnalazione, l'Ufficio del Garante ha rilevato che la finalità informativa perseguita dal settimanale poteva essere soddisfatta senza diffondere tale informazione, fornendo semmai una risposta diretta e privata alla sola lettrice interessata.

In relazione ai ripetuti servizi giornalistici dedicati al grave malore e al ricovero di un noto imprenditore per cause legate all'abuso di sostanze stupefacenti, il Garante ha poi ricordato che, anche quando si tratti di figure pubbliche, stampa e media devono rispettare la dignità delle persone e la loro sfera più intima, astenendosi dal diffondere dettagli non indispensabili ed evitando spettacolarizzazioni e accanimenti morbosi; ha quindi ritenuto illecita –e vietato– la pubblicazione di alcuni dettagli eccedenti, idonei a rivelare possibili abitudini sessuali dell'interessato (*Provv.* 12 gennaio 2006 [doc. *web* n.1213631]). Anche questo provvedimento è stato impugnato, da una delle testate interessate.

7.5. *Esercizio dei diritti e diritto all'oblìo*

Concludendo la relativa istruttoria, il Garante ha ritenuto illecita la nuova diffusione, nel corso di una trasmissione televisiva, delle immagini di un processo –già mandate in onda sedici anni prima–, che ritraevano una donna mentre reagiva vivacemente alla richiesta di condanna, formulata dal pubblico ministero nei confronti di persona a cui la stessa era all'epoca legata sentimentalmente. L'Autorità ha ravvisato in questo caso la necessità l'esigenza di garantire il diritto all'oblìo e all'identità personale; ha infatti rilevato che le immagini erano state riproposte senza tenere in debito conto il diritto dell'interessata a veder rispettata la propria attuale dimensione sociale e affettiva, ed erano state diffuse anche in vio-

lazione del principio dell'essenzialità dell'informazione (*Provv.* 7 luglio 2005 [doc. *web* n. 1148642]).

Diritto all'oblìo, tutela dell'identità personale e informazione *on-line*

Garantire un'effettiva tutela del "diritto all'oblìo" risulta più difficile nel caso di notizie diffuse attraverso siti Internet. Il Garante ha affrontato al riguardo il caso di una donna che si era rivolta ad un quotidiano per rendere anonima la notizia, contenuta in un articolo pubblicato nel 2002 e ancora presente sul sito *web*, relativa al suo arresto e al successivo rinvio a giudizio, disposti in relazione ad un reato per il quale era stata assolta. Accogliendo tale richiesta l'editore aveva sostituito le generalità della donna con una più generica locuzione ("nota immobiliarista milanese"); ha tuttavia precisato che la permanenza in Internet dell'articolo in forma non "anonimizzata" era dovuta alla sua pregressa indicizzazione attraverso alcuni motori di ricerca, e che l'articolo doveva pertanto ritenersi tratto non dagli archivi dell'editore, ma da altri basi dati desunte tramite motori di ricerca (*Provv.* 9 novembre 2005 [doc. *web* n. 1200127]; sul tema dei motori di ricerca, si vedano anche i parr. 2.11 e 15.11).

8 Associazioni, movimenti politici e partiti

8.1. *Associazioni*

Istituti di patronato e di assistenza sociale

Sono pervenute all'Autorità nuove segnalazioni e richieste di chiarimenti in ordine alle modalità con cui istituti di patronato e di assistenza sociale raccolgono dati relativi a lavoratori, pensionati, disabili ed altri soggetti aventi diritto a prestazioni in materia di previdenza, assistenza sociale e sanitaria per finalità informative e promozionali. In particolare è emerso che le strutture sanitarie competenti per accertare l'invalidità civile trasmettono regolarmente all'Associazione nazionale mutilati e invalidi civili (Anmic) elenchi nominativi di coloro che fanno istanza per il riconoscimento dell'invalidità, o richiedono a tali persone di manifestare il loro consenso alla trasmissione dei dati che li riguardano. Queste informazioni verrebbero successivamente utilizzate dall'Anmic per sollecitare agli interessati l'adesione all'associazione, senza che ne sia peraltro chiarito il carattere facoltativo.

L'Autorità –che era già intervenuta sull'argomento con precisi rilievi sull'ammissibilità della trasmissione di elenchi nominativi di disabili all'Animic, ad altri patronati e ad associazioni assistenziali e di categoria, fatto salvo l'accesso di tali organismi ai dati anche sensibili degli interessati che abbiano conferito una specifica delega: *cfr.*, *ad es.*, *Nota* 17 settembre 1997 [doc. *web* n. 1055114]– ha avviato ulteriori accertamenti per verificare il rispetto delle disposizioni in materia di trattamento dei dati personali, anche in relazione al nuovo assetto normativo previsto dalla l. 30 marzo 2001, n. 152 (recante "Nuova disciplina per gli istituti di patronato e di assistenza sociale") e dal Codice.

8.2. *Movimenti politici e propaganda elettorale*

Interventi in materia di elezioni e consultazioni politiche

Con riferimento alle attività di partiti e di movimenti politici, il Garante è stato chiamato più volte ad individuare un punto di equilibrio tra iniziative intraprese a fini di propaganda elettorale da tali organismi (inclusi comitati promotori, di sostenitori e singoli candidati), tenendo presente che simili iniziative costituiscono un momento significativo della partecipazione alla vita democratica (art. 49 Cost.) che richiede comunque un'adeguata protezione dei diritti e delle libertà fondamentali delle persone cui si riferiscono informazioni personali utilizzate (art. 2 del Codice).

L'Autorità ha fornito nuovi chiarimenti di ordine generale, anche nel caso segnalato da un cittadino il quale lamentava che, in diversi seggi di un comune durante le consultazioni elettorali del 12 e 13 giugno 2004, i rappresentanti dei gruppi dei candidati presso la sezione detenessero le liste sezionali degli elettori sulle quali venivano riportate le generalità dei cittadini che esercitavano il diritto di voto (*Nota* 24 febbraio 2005).

A tal proposito sono stati richiamati principi già evidenziati nel *provvedimento* generale del 12 febbraio 2004 (*cd.* "decalogo elettorale" [doc. *web* n. 634369]), con cui erano stati individuati, fra l'altro, limiti e prescrizioni per il trattamento di dati personali anche da parte di scrutatori e rappresentanti di lista. Nella medesima cir-

costanza è stato precisato che, in occasione di consultazioni elettorali e di referendum, nonché in sede di verifica della loro regolarità, risulta possibile, in conformità alla legge, raccogliere alcuni dati sensibili degli elettori, in quanto il Codice considera di rilevante interesse pubblico il trattamento di tale categoria di dati per applicare la disciplina in materia di elettorato attivo, passivo e per esperire specifici compiti concernenti, in particolare lo svolgimento di consultazioni elettorali, le richieste di referendum e la verifica delle relative regolarità (artt. 20, 22 e 65). L'Ufficio del Garante ha tuttavia ribadito che scrutatori e rappresentanti di lista, nell'esercizio dei compiti loro affidati o riconosciuti dalla legge, devono osservare particolari cautele in tema di riservatezza in relazione ai dati personali anche di natura sensibile di cui vengono lecitamente a conoscenza. I dati devono essere trattati con ogni opportuna cautela, anche a tutela del principio costituzionale della libertà e segretezza del voto, tanto più in quelle ipotesi (quali referendum abrogativi, o votazioni di ballottaggio) nelle quali l'avvenuta o mancata partecipazione alle operazioni di voto può evidenziare, di per sé, anche una particolare opzione politica dell'elettore. È stata quindi ritenuta illecita la compilazione, effettuata da scrutatori e rappresentanti di lista di elenchi di persone astenutesi dalla partecipazione al voto, ai fini di un successivo utilizzo a fini politici da parte della persona che li ha raccolti o della formazione politica di riferimento (*ad es.*, allo scopo di sollecitare gli elettori rispetto a futuri appuntamenti elettorali).

L'Autorità è intervenuta in materia anche con un provvedimento generale in materia di comunicazioni e di propaganda politica, adottato in previsione sia delle elezioni amministrative di aprile e maggio 2005, sia delle consultazioni referendarie tenutesi nel giugno del medesimo anno (*Provv.* 3 marzo 2005 [doc. *web* n. 1107658], in *G.U.* 18 marzo 2005, n. 64). Con tale provvedimento, nel confermare le prescrizioni del citato "decalogo elettorale" del 12 febbraio 2004, il Garante ha di nuovo evidenziato i casi in cui, in vista delle consultazioni elettorali, partiti, organismi politici, comitati promotori, sostenitori e singoli candidati possono utilizzare dati personali a fini di propaganda politica senza chiedere preventivamente agli interessati uno specifico consenso.

L'Ufficio del Garante ha poi curato l'applicazione di questi principi chiarendo, tra l'altro, ad un cittadino –il quale lamentava la ricezione di messaggi di propaganda elettorale sulla base dell'utilizzo di dati personali ritenuti coincidenti con quelli detenuti presso gli uffici anagrafici e l'ufficio elettorale di un comune– che risulta possibile utilizzare dati personali senza il consenso degli interessati a fini di propaganda elettorale, solo quando i dati siano estratti da fonti "pubbliche" nel senso proprio del termine e siano quindi conoscibili da chiunque senza limitazioni; ciò, fermo restando il diritto dell'interessato di rivolgersi direttamente al candidato che invia messaggi di comunicazione politica, al fine di esercitare i diritti di cui all'art. 7 del Codice e di ottenere l'aggiornamento, la rettificazione, l'integrazione o la cancellazione dei dati (artt. 7, 8, 9 e 10 del Codice) (*Nota* 2 agosto 2005).

I medesimi principi sono stati in seguito applicati rispetto alla segnalazione di un cittadino che lamentava di non aver ricevuto riscontro alla richiesta di accesso ai dati personali rivolta ad una coalizione politica che gli aveva inviato messaggi di propaganda elettorale (*Nota* 17 gennaio 2006). Nella circostanza si è anche ricordato all'interessato che in caso di mancato riscontro da parte del titolare del trattamento può ricorrersi all'autorità giudiziaria o al Garante (art. 145 del Codice).

In questo quadro è stata trattata anche una segnalazione che lamentava una violazione in materia di trattamento dei dati personali riguardo all'invio di messaggi di propaganda elettorale in occasione delle consultazioni elettorali del 3 e 4 aprile 2005, inviati ad un minore da un candidato che ne avrebbe ottenuto il nominativo

dall'ufficio anagrafe di un comune, in qualità di componente del consiglio comunale (*Nota* 3 agosto 2005).

In vista delle consultazioni politiche del 9 e 10 aprile 2006, il Garante è da ultimo intervenuto con un nuovo provvedimento generale sulla propaganda elettorale per chiarire le modalità per utilizzare lecitamente i dati personali dei cittadini (*ad es.*, indirizzo, telefono, *e-mail* ecc.) (*Provv.* 7 settembre 2005 [doc. *web* n. 1165613], in *G.U.* 12 settembre 2005, n. 212). Con il nuovo intervento si è inteso richiamare nuovamente l'attenzione di partiti, organismi politici, comitati promotori e singoli candidati, in termini agevolmente comprensibili ed applicabili, sulle indicazioni a suo tempo fornite nei citati provvedimenti del febbraio 2004 e del marzo 2005. Si è potuto così estenderne l'ambito di applicazione alle selezioni dei candidati effettuate tramite consultazioni primarie.

Il provvedimento ha nuovamente individuato i casi nei quali può non richiedersi il consenso degli elettori per inviare materiale di propaganda. In particolare, si è confermato il principio in base al quale il consenso non è necessario quando si usano dati personali contenuti nelle liste elettorali detenute dai comuni, dati di iscritti ed aderenti a partiti e organismi politici o dati degli abbonati presenti nei nuovi elenchi telefonici accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere, rispettivamente, corrispondenza a domicilio o chiamate telefoniche. L'Autorità ha anche evidenziato che il consenso è invece necessario per particolari modalità di comunicazione elettronica come *Sms, Mms, e-mail*, oltre che per telefonate preregistrate e fax. Sono stati ribaditi, infine, i casi nei quali i cittadini devono essere informati sull'uso delle informazioni personali che li riguardano, anche tramite modalità semplificate (art. 13 del Codice), nonché sui diritti che possono essere esercitati ai sensi dell'art. 7 del Codice.

Va rilevato, a conferma della particolare delicatezza dell'utilizzo dei dati personali in tali contesti, che i principi in questione hanno continuato ad essere oggetto di varie richieste di chiarimenti all'Ufficio del Garante, anche dopo l'adozione del nuovo "decalogo" (*v. Nota* 4 novembre 2005).

Utilizzo delle liste elettorali per finalità di *marketing*

Sempre rispetto alla tematica in esame, va evidenziata una delicata fattispecie all'esame dell'Autorità che riguarda le richieste di rilascio di copia delle liste elettorali rivolte ai comuni da società specializzate in servizi per il *marketing* diretto, le quali intendevano utilizzare le informazioni ivi contenute al fine di effettuare, per conto di propri clienti ed attraverso specifiche banche dati, campagne di propaganda elettorale e di carattere socio-assistenziale, nonché per perseguire interessi collettivi o diffusi.

In tale ambito si è già correttamente pronunciato il Ministero dell'interno, Dipartimento per gli affari interni e territoriali-Direzione centrale dei servizi elettorali, evidenziando che le liste elettorali non possono essere rilasciate in copia a chiunque, potendo essere comunicate solo *"per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso"* (art. 177, comma 5 del Codice, che ha in parte modificato l'art. 51 d.P.R. 20 marzo 1967, n. 223). Il Ministero ha quindi constatato che le finalità che legittimano il rilascio di copia delle liste elettorali, oltre che essere motivate ai sensi di tale art. 51, devono essere riferibili a scopi perseguiti direttamente dal richiedente e, ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività stessa di tale organismo. Pertanto, sempre secondo il Ministero, richieste come quelle in questione non possono essere accolte anche quando le società dichiarino –come nel caso di specie– di annoverare tra i propri clienti soggetti aventi titolo a richiedere le liste elettorali, anche perché l'oggetto dell'attività imprendito-

riale esercitata non esclude la possibilità di un utilizzo dei dati personali contenuti nelle liste elettorali per finalità anche diverse ed ulteriori rispetto quelle di cui al predetto art. 51 d.P.R. n. 223/1967.

Albo degli scrutatori

Ulteriori elementi di approfondimento sono stati rappresentati da una prefettura con riferimento alla liceità del rilascio, da parte dei comuni, di una copia degli albi degli scrutatori di seggio elettorale a partiti politici. L'Ufficio del Garante ha ricordato che la comunicazione di dati personali a privati da parte di un soggetto pubblico è ammessa unicamente quando prevista da norme di legge o di regolamento (art. 19, comma 3, del Codice). Si è così evidenziato che la normativa di riferimento stabilisce che l'albo degli scrutatori debba restare depositato in un periodo determinato, durante il quale ogni cittadino del comune ha diritto di prenderne visione (art. 3, comma 4, l. 8 marzo 1989, n. 95), salve eventuali altre specifiche disposizioni in materia elettorale che prevedano espressamente una comunicazione o permettano, in modo parimenti espresso, di accedere ad altri elenchi in materia, quali ad esempio quelli relativi agli scrutatori nominati dalla commissione elettorale comunale (art. 6 l. n. 95/1989) (*Nota* 28 marzo 2006).

Voto degli italiani all'estero

In materia elettorale l'Autorità è stata interpellata anche dalla Direzione generale per gli italiani all'estero e le politiche migratorie del Ministero degli affari esteri. La Direzione, inoltrando un quesito formulato dal Consolato generale di Francoforte, ha chiesto di conoscere se era possibile estendere il regime di conoscibilità dell'elenco provvisorio dei residenti all'estero aventi diritto al voto, in riferimento a finalità di carattere politico-elettorale connesse a consultazioni comunali in Germania per le quali anche i cittadini italiani ivi residenti godono dei diritti di elettorato attivo e passivo. L'Ufficio ha evidenziato che tale elenco provvisorio è soggetto a un particolare regime di conoscibilità, espressamente vincolato dalla disciplina di riferimento al perseguimento di specifiche finalità. Poiché le limitazioni al relativo utilizzo non derivano dalla normativa in materia di protezione dei dati personali, si è rappresentata al Ministero l'opportunità di valutare se la finalità di carattere politico-elettorale in questione possa essere perseguita mediante l'applicazione di altre diverse disposizioni di settore in vigore (*Nota* 3 marzo 2006).

Documento comune delle autorità di protezione dei dati

In materia di propaganda elettorale occorre, infine, richiamare le conclusioni cui sono giunti i rappresentanti delle autorità di protezione dei dati personali europee e non, riunite in occasione della 27ma Conferenza internazionale sulla protezione dei dati (Montreux -Svizzera-, 14-16 settembre 2005). Su iniziativa dell'Autorità italiana è stata adottata una risoluzione relativa all'utilizzo di dati personali per la comunicazione politica, che ha trovato il sostegno dell'autorità federale svizzera per la protezione dei dati, dell'autorità federale tedesca per la protezione dei dati, dell'Ispettore generale per la protezione dei dati della Polonia e del Commissario per la protezione dei dati della città di Berlino. Si è così evidenziata, in particolare, la necessità di raccogliere e di utilizzare solo dati indispensabili, di informare i cittadini su chi tratta i dati e sull'uso che ne viene fatto, di ottenere, nei casi previsti, il consenso degli interessati quando si usano particolari forme di comunicazione (come messaggi *Sms* o *e-mail*), di raccogliere le informazioni da fonti lecitamente accessibili e di utilizzare i dati solo a fini di propaganda elettorale (*cfr.*, *amplius*, il par. 22).

9 Attività economiche

9.1. *Credito*

Accesso ai dati personali e accesso alla documentazione bancaria

Continuano a pervenire all'Autorità numerose segnalazioni concernenti il rapporto tra diritto di accesso ai dati personali detenuti da istituti di credito, disciplinato dagli artt. 7 e seguenti del Codice, e il diritto di ottenere copia della documentazione bancaria ai sensi dell'art. 119 d.lg. n. 385/1993 (Testo unico in materia bancaria e creditizia), correlato al profilo relativo al rimborso spese chiesto dalle banche ai sensi dello stesso art. 119 per rendere disponibile la documentazione. Nelle risposte inviate dall'Ufficio del Garante è stata ribadita la posizione, già espressa dall'Autorità in una nota inviata alla Banca d'Italia (*Nota* 6 agosto 2004, in *Relazione* 2004, p. 60), con la quale si è precisato il differente ambito di applicazione delle due norme e la conseguente competenza del Garante a pronunciarsi, in termini generali, sulle sole richieste di accesso a dati personali formulate ai sensi del menzionato art. 7 del Codice. Per tale ragione, la richiesta volta a conoscere tali dati personali non può "trasformarsi" in una pretesa del richiedente ad ottenere direttamente, sempre e comunque, copia integrale della documentazione che contenga i dati medesimi.

Rimessa interbancaria diretta

Un altro aspetto, in relazione al quale si sono registrate alcune segnalazioni, ha riguardato il trattamento non autorizzato di dati personali riferiti a clienti (in particolare, delle loro coordinate bancarie). Un cliente ha, ad esempio, contestato l'addebito di una bolletta telefonica tramite rapporti interbancari diretti (R.i.d.), pur non avendo prescelto tale forma di pagamento e non avendo fornito le proprie coordinate bancarie. I titolari del trattamento non hanno fornito prova della circostanza che il cliente fosse stato altresì informato preventivamente dell'utilizzo dei dati con la procedura in esame e sono state fornite alcune prescrizioni a tutela della libertà di scelta del cliente in relazione alle modalità di pagamento.

Trattamenti effettuati nell'ambito dei sistemi di rilevazione creditizia

Dal 1° gennaio 2005 ha trovato applicazione il "codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti" (sottoscritto il 12 novembre 2004 da tutte le associazioni rappresentative del settore e da varie associazioni di consumatori): esso prevede regole specifiche alle quali gli operatori del settore creditizio e finanziario devono attenersi in relazione ai trattamenti di dati personali relativi a contratti di finanziamento.

Come ricordato in precedenti relazioni, per lungo tempo le *cd.* centrali rischi private hanno operato in assenza di un quadro regolamentare. Al di là della conseguente incertezza dal punto di vista dell'operatività di questi sistemi, per ragioni diverse è risultato elevato il contenzioso in materia nei primi anni di applicazione della disciplina di protezione dei dati personali (accentuato dagli effetti negativi che ha sull'accesso al credito l'avvenuta segnalazione in dette centrali). Ciò, in ragione della scarsa trasparenza dei tempi di conservazione dei dati (reputati eccessivamente lunghi, specie in presenza di segnalazioni dovute a meri ritardi nei pagamenti o ad inadempimenti di importo contenuto), a causa della qualità dei dati trattati, non sempre esatti o aggiornati, oltre che per il mancato (o tardivo) riscontro all'esercizio del diritto d'accesso da parte degli interessati.

L'adozione del codice di deontologia e buona condotta da parte degli operatori

del settore (preceduta da una copiosa serie di decisioni su ricorsi proposti *ex* art. 145 del Codice) ha perciò rappresentato una tappa significativa nell'attività svolta dal Garante in questo ambito assai delicato: essa ha determinato l'emersione del fenomeno della referenziazione creditizia, specie grazie alla formulazione di un'informativa chiara agli interessati da parte dei soggetti partecipanti a detti sistemi d'informazione, ed ha determinato una più puntuale attenzione alla qualità delle informazioni trattate ai fini della valutazione del rischio di credito, unitamente alla definizione dei tempi massimi di conservazione delle medesime.

Il codice deontologico ha previsto una serie di misure a carico degli operatori del settore da adottare in fasi successive, nel corso della prima metà del 2005. Tra di esse figuravano la riduzione dei tempi di conservazione dei dati personali relativi ad informazioni creditizie di tipo positivo, la costituzione di un organismo di controllo con la partecipazione di rappresentanti delle associazioni consumeristiche, l'invio al Garante delle informazioni e della documentazione necessaria per consentire il controllo sulla corretta attuazione delle disposizioni contenute nel Codice e l'integrazione dell'informativa fornita agli interessati, contenente le informazioni non comprese nelle informative rese precedentemente.

L'attività svolta nel corso dell'anno dall'Autorità in questo settore ha, quindi, richiesto un attento esame dell'operato dei nuovi sistemi di informazioni creditizie (Sic) allo scopo di valutare sia la progressiva attuazione delle misure previste, sia i primi problemi applicativi. In questa cornice si è svolta, nella seconda parte dell'anno, un'estesa attività di accertamento in loco presso i gestori dei principali sistemi, che ha avuto ad oggetto la verifica della conformità dei trattamenti concretamente posti in essere, rispetto alla disciplina di protezione dei dati personali come integrata dalle disposizioni di natura deontologica. L'attività di accertamento si è protratta presso i gestori di servizi di comunicazione elettronica nei primi mesi del 2006, in vista dei provvedimenti calendarizzati per la prima parte del 2006.

Con riguardo alla tematica dei tempi di conservazione, l'art. 13, comma 4 del codice deontologico prevedeva invece che, in sede di prima applicazione delle disposizioni contenute nell'art. 6 del medesimo codice, i gestori riducessero ad un termine non superiore a trentasei mesi i tempi di conservazione dei dati personali relativi ad informazioni creditizie di tipo "positivo" (relative, cioè, all'avvenuta conclusione positiva del rapporto contrattuale o al diligente adempimento degli obblighi contrattuali in corso). In tempi successivi, l'organo di controllo previsto dall'art. 13, comma 7, del codice deontologico avrebbe valutato, alla luce dell'esperienza maturata, se fosse giustificato il mantenimento del termine più lungo, e il Garante, su richiesta del predetto organismo o di propria iniziativa, avrebbe dovuto indicare il termine da osservare. A questo proposito, con avviso pubblicato in *Gazzetta Ufficiale* 6 marzo 2006, n. 54, il Garante ha infine disposto che i dati personali relativi ad informazioni creditizie di tipo positivo possono continuare ad essere conservati nei sistemi di informazioni creditizie per un termine non superiore a trentasei mesi (anziché per il più breve termine di ventiquattro mesi come prefigurato dall'art. 6, comma 6, del codice deontologico).

Contributo-spese per l'accesso ai dati Sic

Con *deliberazione* n. 15/2004 il Garante aveva riconosciuto, a favore di una società che gestisce un Sic, la possibilità di richiedere contributi-spese in casi ulteriori rispetto a quelli già previsti, in via generale, dalla *deliberazione* n. 14/2004 ([doc. *web* n. 1104892], in *G.U.* 8 marzo 2005, n. 55). La deliberazione era espressamente valida solo per il 2005, con riserva di riesaminare la questione entro lo stesso anno e di confermare, o meno, in tale sede, la previsione di detto contributo.

Alla fine del 2005 la società ha rinnovato la richiesta, unitamente alle analoghe

richieste di altre società che gestiscono sistemi di informazione creditizia. Il Garante ha ritenuto che non sussistessero i presupposti per adottare una deliberazione analoga. Sono risultate, infatti, esaurite le ragioni che avevano condotto a tale determinazione, individuate nell'effettuazione di investimenti di varia natura per semplificare le procedure di riscontro all'esercizio del diritto d'accesso. Il contributo potrà comunque essere richiesto dai titolari nelle misure indicate in via generale dalla deliberazione n. 14/2004 per tutte le categorie di titolari del trattamento.

Sistemi di rilevazione di impronte digitali ed immagini per accesso a banche

Già in passato il Garante ha affrontato in alcuni provvedimenti il tema relativo all'impiego da parte delle banche di sistemi di rilevazione delle impronte digitali in associazione con sistemi di videosorveglianza (*cfr.*, soprattutto, *Provvedimenti* 28 settembre 2001 [doc. *web.* n. 39704] e 29 aprile 2004 [doc. *web.* n. 1003482]). In considerazione delle segnalazioni provenienti da parte di cittadini che, in presenza di talune circostanze, contestavano le modalità di accesso ad istituti bancari e in ragione delle numerose richieste di nuove installazioni provenienti da banche che invocavano una recrudescenza di fenomeni criminali –circostanza rappresentata anche dall'Associazione bancaria italiana–, il Garante è tornato a pronunciarsi in materia.

Con *provvedimento* del 27 ottobre 2005 [doc. *web* n. 1246675] (in *G.U.* 22 marzo 2006, n. 68 ; *cfr.* anche *Provv.* 2 marzo 2006 [doc. *web* n. 1248850], pubblicato nella stessa *G.U.* 22 marzo 2006, n. 68), il Garante, ribadendo il proprio indirizzo –contrario all'uso generalizzato di sistemi che associno immagini e impronte digitali–, ha individuato le misure e gli accorgimenti che, a garanzia degli interessati, devono essere adottati dagli istituti di credito che intendano avvalersi di sistemi di rilevazione dell'impronta digitale in associazione a sistemi di videosorveglianza. Secondo il provvedimento, che ha tenuto conto delle novità sopravvenute con l'entrata in vigore del Codice (in particolare, gli artt. 17, 24, comma 1, lett. *g*) e 154, comma 1, lett. *c*)) e dei principi generali già enunciati nei citati *provvedimenti* del 28 settembre 2001 e 29 aprile 2004, è lecito installare apparecchiature che consentano l'identificazione delle persone attraverso la combinazione di telecamere e di sistemi per la raccolta dell'immagine delle impronte digitali, solo in presenza di condizioni di effettivo rischio (*ad es.*, con riguardo a sportelli siti in aree ad effettiva alta densità criminale, oppure in aree isolate o nella prossimità di "vie di fuga") e per l'esclusiva finalità di incrementare il grado di sicurezza di beni e persone.

Se non sono rispettati i principi di necessità e di proporzionalità il trattamento dei predetti dati non è lecito. Misure articolate devono essere comunque adottate affinché il trattamento sia conforme ai principi di protezione dei dati personali. In particolare:

- la banca, prima che i dati siano rilevati (e, comunque, prima dell'accesso del cliente all'interno della propria sede), deve fornire agli interessati un'informativa sintetica, ma chiara, relativa alla presenza di sistemi di raccolta di impronte digitali e di immagini; informativa che dovrà essere integrata da un'altra, più ampia, informativa esposta all'interno dei locali della banca;
- ai clienti deve essere comunque consentito l'accesso alla banca con modalità alternative, senza apporre le proprie impronte digitali. Ciò, sia disabilitando (temporaneamente) il sistema di rilevazione delle impronte, sia utilizzando accessi alternativi (in tal caso si possono adottare opportune cautele in relazione all'accesso del cliente, quali, ad esempio, la richiesta di esibizione di un suo documento di identificazione);
- le immagini e le impronte digitali devono essere cifrate prima della loro registrazione in un archivio. Il provvedimento ha previsto che il processo crittografico sia garantito dalla figura del "vigilatore dei dati", un soggetto indipendente, anche esterno alla banca, depositario delle chiavi crittografi-

che idonee a decifrare le informazioni conservate. Ai dati "in chiaro" possono accedere soltanto l'autorità giudiziaria e la polizia;

- i dati relativi alle immagini e alle impronte digitali devono essere cancellate automaticamente, salvo quanto disposto per specifici motivi di giustizia o a seguito della richiesta di un interessato, trascorso un periodo non superiore ad una settimana.

Anche al fine di agevolare un'eventuale attività di verifica preliminare, come pure (più in generale) di controllo da parte dell'Autorità, il provvedimento prevede che le banche, le quali intendano intraprendere trattamenti del tipo qui descritto, o che abbiano già installato sistemi di rilevazione dell'immagine e dell'impronta digitale, debbano comunicare detta circostanza al Garante inviando una specifica richiesta per via telematica compilando il modello reso disponibile sul sito *web* dell'Autorità.

Identificazione della clientela presso istituti bancari e postali

Tenendo conto di numerose segnalazioni, il Garante è intervenuto per valutare la conformità, rispetto alla normativa in materia di protezione dei dati personali, della prassi seguita da istituti di credito ed uffici postali che, nell'effettuare operazioni bancarie, finanziarie o postali (*ad es.*, ordinarie operazioni di versamento, pagamenti e altre disposizioni impartite dalla clientela, presentazione per il pagamento di assegni o vaglia postali), identificano clienti mediante richiesta di esibizione di un valido documento di riconoscimento e acquisendone talvolta la relativa copia fotostatica (in particolare, in caso di soggetti non correntisti o comunque non conosciuti dal personale di filiale) (*Provv.* 27 ottobre 2005, [doc. *web* n. 1189435]).

Dopo aver rilevato che le operazioni di identificazione implicano un trattamento di dati personali –che va conformato anch'esso ai principi di liceità, pertinenza e non eccedenza rispetto alle finalità perseguite (art. 11 del Codice)– il Garante ha osservato che è necessario, per valutare la fattispecie, distinguere tra la necessità generale di identificare la persona e le modalità con cui ciò avviene.

L'identificazione del soggetto che effettua una determinata operazione risulta a volte prescritta da una disposizione normativa (si pensi, ad esempio, all'art. 2, comma 14, d.l. 30 settembre 2005, n. 203, a modifica dell'art. 7 d.P.R. 29 settembre 1973, n. 605, oppure all'art. 45 d.P.R. 28 dicembre 2000, n. 445, relativo alle modalità per identificare i cittadini da parte di organi della pubblica amministrazione e di gestori di pubblici servizi o, ancora, alle vigenti disposizioni in materia di riciclaggio), mentre può essere altre volte necessaria per eseguire obblighi derivanti dal contratto o per adempiere a specifiche richieste precontrattuali dell'interessato (art. 24, comma 1, lett. *a*) e *b*), del Codice). In tali ipotesi, fatta salva l'osservanza dell'obbligo di informativa (fornita anche *una tantum* al cliente), non è necessario richiedere il consenso dell'interessato.

Le modalità con le quali avviene l'identificazione, in ossequio al principio di proporzionalità, devono tener conto delle circostanze di fatto: fuori dai casi in cui espresse disposizioni normative stabiliscano precise modalità, la banca o l'ufficio postale ha l'onere di verificare l'identità dell'interessato basandosi su idonei elementi di valutazione, quali, ad esempio, la conoscenza personale, la consultazione di atti e documenti acquisiti in precedenza, anche in sede di instaurazione del rapporto, ovvero l'esibizione di un documento di riconoscimento, provvedendo se del caso ad annotarne gli estremi.

La richiesta di produrre, anche per via telematica, la copia di un documento di riconoscimento e la sua conservazione presso la filiale possono ritenersi giustificate solo quando si rinvenga una disposizione normativa che preveda espressamente l'acquisizione e la conservazione temporanea di tale copia, oppure quando la banca o l'ufficio postale debba poter dimostrare di aver identificato l'interessato con modalità più accurate, tenendo conto del particolare contesto e delle operazioni da

svolgere. In questi ultimi casi può rientrare anche quello del portatore "non conosciuto" di un assegno (o di un vaglia): in tale ipotesi, l'acquisizione del relativo documento è da ritenersi legittima considerata la responsabilità della banca o dell'ufficio postale in relazione ai pagamenti che vanno effettuati, con la necessaria diligenza, solo al creditore (*cfr.* anche l'art. 1189 c.c. e gli artt. 43 e 86 r.d. 21 dicembre 1933, n. 1736).

Il Garante ha affermato conclusivamente che il trattamento delle informazioni raccolte a fini di identificazione risulta lecito, pertinente e non eccedente se effettuato nei termini sopra riassunti, i quali trovano riscontro nelle disposizioni dell'ordinamento che prevedono già la necessità di conservare copia di un documento da esibire. In applicazione del principio della pertinenza e di non eccedenza nel trattamento dei dati occorre altresì evitare di acquisire più volte copie di documenti già disponibili agli atti e, comunque, di utilizzarle ad altri scopi. Infine, gli istituti bancari e gli uffici postali devono assicurare che l'accesso alle informazioni sia consentito unicamente nelle ipotesi indicate e solo da chi ne abbia titolo, evitando, in ciascuna fase, ogni inutile comunicazione di dati personali anche nello svolgimento di operazioni allo sportello.

9.2. *Assicurazioni*

Accesso agli atti assicurativi e protezione dei dati

Nell'ambito del settore assicurativo, si ripropone con accresciuta frequenza il tema dell'accesso alla documentazione del procedimento di liquidazione dei danni ai sensi dell'art. 12-*ter* l. 24 dicembre 1969, n. 990 (introdotto dall'art. 3 l. 5 marzo 2001, n. 57; *v.* oggi l'art. 146 d.lg. 7 settembre 2005, n. 209, recante il Codice delle assicurazioni private). Tale disciplina risponde alla specifica esigenza di garantire al soggetto assicurato un rapporto trasparente con la compagnia assicuratrice, conferendo allo stesso la possibilità di controllare e verificare i singoli passaggi del procedimento di liquidazione, a conclusione dei procedimenti di valutazione, constatazione e liquidazione dei danni.

A fronte di numerose segnalazioni relative alla possibile interferenza tra la citata disciplina di settore e quella sulla protezione dei dati personali, è stato ribadito in più occasioni l'orientamento già espresso in materia dal Garante (*Provv.* 8 maggio 2001 [doc. *web* n. 39284]) secondo cui la disposizione contenuta nel predetto art. 12-*ter* riconosce un particolare diritto d'accesso alla documentazione, distinto rispetto al diritto di accesso ai dati personali previsto dal Codice, confermando la piena compatibilità tra le due discipline. L'Autorità ha nuovamente distinto chiaramente l'esercizio del diritto di accesso ai dati personali (di cui all'art. 7 del Codice), che può essere esercitato –limitatamente ai dati personali relativi all'interessato– in ogni momento, dal diritto degli assicurati e dei danneggiati ad accedere *"agli atti a conclusione dei procedimenti di valutazione, contestazione e liquidazione dei danni che li riguardano"*, per il quale le sopra menzionate disposizioni normative di rango primario in materia assicurativa (cui è stata data attuazione con il d.m. 20 febbraio 2004, n. 74) stabiliscono, parimenti, precisi limiti temporali a garanzia degli interessati.

La diversa qualificazione dell'istanza da parte del soggetto interessato risulta idonea ad individuare la disciplina di volta in volta applicabile in quanto, se la richiesta di accesso concerne dati personali dell'interessato, troveranno applicazione gli artt. 7 e 8 del Codice e la conseguente possibilità, in caso di mancato o inidoneo riscontro da parte del titolare del trattamento, di adire l'autorità giudiziaria ordinaria o di presentare ricorso al Garante ai sensi degli artt. 145 e ss. del Codice. Qualora, invece, l'oggetto dell'accesso riguardi la documentazione relativa al procedimento di liquidazione

del danno, opereranno i limiti ed i presupposti previsti dalla legge n. 57/2001(ora dal Codice delle assicurazioni private) e dal citato regolamento di attuazione.

A questo proposito è opportuno ricordare che, qualora entro sessanta giorni dalla ricezione della richiesta l'assicurato o il danneggiato non sia messo in condizione da parte della compagnia di assicurazione di prendere visione degli atti richiesti, il medesimo può rivolgersi all'Isvap per vedere garantito il proprio diritto (art. 4, comma 4, d.m. 20 febbraio 2004, n. 74).

Il richiamato orientamento del Garante ha trovato ulteriore conferma alla luce del nuovo testo dell'art. 146 del Codice delle assicurazioni private che, nel disciplinare il diritto degli assicurati e dei danneggiati ad accedere agli atti del procedimento di liquidazione, ha chiarito il rapporto con l'esercizio del diritto di accesso ai dati personali dell'interessato, facendo appunto salvo *"quanto previsto per l'accesso ai singoli dati personali dal codice in materia di protezione dei dati personali"* (comma 1). La disposizione in esame ha inoltre stabilito la non gratuità del diritto di accesso agli atti e ai documenti assicurativi (comma 3) ed ha introdotto, altresì, maggiori limitazioni all'esercizio di tale diritto (che "*non è consentito quando abbia ad oggetto atti relativi ad accertamenti che evidenziano indizi o prove di comportamenti fraudolenti*"; la norma prevede, inoltre, la sospensione del diritto in caso di pendenza di controversia giudiziaria tra l'impresa ed il richiedente). Resta salva, nei casi di preclusione del diritto di accesso ai documenti, la facoltà di esercitare l'accesso ai propri dati personali *ex* art. 7 del Codice, nei limiti dell'art. 8, comma 2, lett. *e*).

Dati sensibili e assicurazioni

Sempre in ambito assicurativo, ulteriori prescrizioni hanno riguardato segnalazioni e quesiti relativi all'accesso alle perizie medico-legali, di regola redatte dai medici fiduciari delle compagnie assicurative. In conformità all'opinione già espressa in passato in una pluralità di decisioni (*Provv.* 8 maggio 2001 [doc. *web* n. 39284], e *Provv.* 20 marzo 2002 [doc. *web* n. 1063450]), nel dare riscontro alle numerose segnalazioni che continuano ad essere inviate all'Autorità è stata confermata la possibilità di esercitare in tale ambito i diritti previsti dall'art. 7 del Codice, rivolgendosi direttamente al titolare o al responsabile del trattamento per ottenere l'accesso ai dati, nei limiti stabiliti dall'art. 8, comma 4.

È stato altresì precisato, in conformità con una precedente pronuncia (*cfr. Provv.* 28 dicembre 2000 [doc. *web* n. 40647] in materia di accesso alle informazioni contenute nella documentazione bancaria), che il diritto di accesso comporta l'obbligo per il titolare del trattamento di estrarre i dati riferiti all'interessato e di trasporli, se vi è richiesta, su un supporto cartaceo o informatico; non è invece attribuito all'interessato il diritto di ottenere "copia integrale" della documentazione contenente i dati personali, salvo che risulti particolarmente difficoltosa l'estrazione dei dati dai medesimi atti o documenti e non sia parimenti possibile la loro trasmissione per via telematica.

Maggiori problemi sembra invece comportare il caso della richiesta, rivolta sempre alla compagnia assicuratrice, di copia della perizia medico-legale avente ad oggetto i dati sanitari relativi ad un terzo (*ad es.*, la persona danneggiata da un sinistro): in tale ipotesi, trattandosi di un caso di comunicazione di dati idonei a rivelare lo stato di salute di un terzo, trova applicazione la disciplina prevista dall'art. 26, comma 4, lett. *c*), del Codice –che ammette il trattamento dei dati sensibili senza il consenso dell'interessato, previa autorizzazione del Garante, in presenza dell'esigenza di esercizio del diritto di difesa, purché il diritto che si intenda difendere sia di "rango almeno pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile" (*Provv.* 9 luglio 2003 [doc. *web* n. 29832]).

Nell'ambito dell'attività riguardante il settore assicurativo è stata esaminata una

Contratto di assicurazione sanitaria integrativa del dipendente e protezione dei dati riferiti al coniuge separato

segnalazione relativa al contratto di assicurazione di assistenza sanitaria integrativa stipulato da un datore di lavoro a favore dei propri dirigenti ed estensibile a soggetti appartenenti al nucleo familiare, in qualità di altri beneficiari. Nel caso di specie, il coniuge legalmente separato, sebbene ammesso a fruire delle prestazioni del fondo di assistenza, era tenuto ad inoltrare la propria documentazione sanitaria per il rimborso alla compagnia di assicurazione per il tramite del coniuge assicurato: tale circostanza ha indotto il segnalante, a tutela della propria riservatezza, a chiedere al fondo di poter gestire direttamente ed autonomamente le proprie pratiche.

Il fondo, che in un primo momento aveva negato siffatta possibilità, ostandovi il regolamento di assistenza (approvato tramite accordo collettivo sottoscritto dalle associazioni sindacali), a seguito della richiesta di informazioni da parte dell'Ufficio del Garante volta a chiarire le eventuali ragioni ostative che avrebbero impedito al segnalante, ove legittimato a godere delle prestazioni assicurative, ad inviare direttamente la pertinente documentazione sanitaria all'assicurazione, considerata la delicatezza del caso, si è dichiarato disposto a "derogare" al predetto regolamento (consentendo al segnalante la gestione diretta delle relative pratiche ed impegnandosi a tener in conto di siffatte problematiche connesse con l'esigenza di riservatezza e di protezione dei dati sensibili degli altri beneficiari della polizza, nell'ambito dei negoziati sindacali per la redazione di un nuovo regolamento).

Al di là di questo caso specifico, sono comunque all'esame dell'Autorità le modalità con le quali, nel settore assicurativo, vengono gestiti analoghi contratti, con particolare riferimento alla presenza di possibili modalità individualizzate di trasmissione dei dati (non di rado sanitari) relativi a familiari, potendosi presentare situazioni delicate connesse alla conoscibilità delle informazioni relative alla salute dei congiunti (e destinate ad acuirsi in presenza di particolari circostanze, quali il caso del coniuge separato o di figli, pur maggiorenni, a carico dell'assicurato).

Dati assicurativi e principio di qualità

Altro caso degno di menzione riguarda alcune segnalazioni aventi ad oggetto la ricezione di avvisi di scadenza di polizze assicurative (note di studi legali o di società di recupero crediti), volti a sollecitare pagamenti. Rispetto a tali polizze, per le quali risultava essere stato già esercitato il diritto di recesso da parte degli assicurati (artt. 172 e 177 d.lg. 7 settembre 2005, n. 209) le ulteriori operazioni di trattamento (nella forma della richiesta del pagamento) lasciavano presupporre un mancato aggiornamento dei dati personali relativi agli assicurati.

A seguito dei riscontri forniti e delle successive osservazioni ed integrazioni documentali pervenute dai segnalanti, rispetto ad un caso il procedimento è stato definito senza l'adozione di provvedimenti da parte dell'Autorità, risultando il mancato aggiornamento dei dati imputabile alla pendenza di controversie aventi ad oggetto la regolarità e la tempestività dell'esercizio del diritto di recesso. Nei confronti di un altro gruppo assicurativo, con esclusivo riferimento al trattamento posto in essere da una singola agenzia, è tuttora in corso l'attività istruttoria, attesa la discordanza degli elementi che emergeva dalla documentazione in atti.

9.3. Marketing

Regole per la raccolta del consenso per finalità di *marketing*

Nel 2005 sono state affrontate differenti questioni inerenti al trattamento di dati per finalità di *marketing*, alcune delle quali hanno già formato oggetto di interventi in passato, riferite al trattamento di dati per svolgere attività pubblicitarie e di vendita diretta o per il compimento di ricerche di mercato.

Numerosi, in proposito, sono stati i ricorsi, le segnalazioni e i reclami relativi alla ricezione di lettere, telefonate, fax ed altre comunicazioni, spesso effettuate mediante posta elettronica, relative ad informazioni pubblicitarie non richieste dagli interessati. Si è inoltre esaminato approfonditamente il profilo dei trattamenti di dati personali in occasione di operazioni a premio e, più in generale, in relazione a fenomeni di "fidelizzazione" della clientela (*cfr. Relazione* 2004, p. 70). Hanno formato, altresì, oggetto di trattazione numerose segnalazioni tanto con riguardo ai profili inerenti alle informazioni da rendere agli interessati, quanto in relazione alle modalità di acquisizione del loro consenso –talvolta mediante l'utilizzo di moduli resi disponibili *on-line*– in occasione del compimento di attività di raccolta di dati per il perseguimento della finalità in esame. Se, con riguardo alle informazioni da rendere, si riscontra non di rado che esse sono difettose o comunque non sufficientemente chiare, in relazione al consenso gli operatori economici sembrano prediligere formulazioni generali, tese a ricomprendere più finalità, tra loro diverse e talvolta incompatibili.

Nel 2005, è stata rivolta attenzione anche alle numerose istanze e segnalazioni pervenute in ordine alle modalità prescelte dagli operatori del settore al fine di acquisire, in occasione dell'instaurazione di un rapporto contrattuale, il consenso degli interessati al trattamento dei dati che li riguardano per perseguire finalità di *marketing*.

A questo proposito, con un *provvedimento* del 12 ottobre 2005 [doc. *web* n. 1179604], si è affermato che è non "libero", ma "necessitato" (e, quindi, invalido), il consenso al trattamento dei dati per finalità promozionali reso senza una libera scelta aderendo ad un testo predisposto unilateralmente dalla controparte contrattuale quale condizione per il conseguimento della prestazione principale richiesta. In tal modo, i dati personali raccolti lecitamente dal titolare (e conferiti dall'interessato) per perseguire una finalità determinata (dare esecuzione al rapporto contrattuale, finalità che non richiede il consenso), vengono di fatto piegati ad un utilizzo diverso dallo scopo originario che ne giustifica la raccolta, in violazione del principio di finalità (art. 11, comma 1, lett. *b*), del Codice).

Alla luce di tali considerazioni, pur consentendo che si potesse continuare a perseguire le finalità principali del contratto connesse alla prenotazione, all'acquisto e al recapito di biglietti (art. 24, comma 1, lett. *b*), del Codice), il Garante ha quindi prescritto di adottare alcune necessarie modifiche al modello per la manifestazione del consenso al trattamento dei dati, affinché quest'ultimo risultasse "modulare", ossia prestato dagli interessati distintamente per ciascuna distinta finalità perseguita.

Il consenso *on-line*

L'attività sul tema dell'Autorità ha riguardato anche le modalità di raccolta *on-line* del consenso della clientela. A questo proposito, si è colta l'occasione per ribadire quanto già affermato anche in passato in merito alla necessità che i sistemi informativi dei siti *web* vengano configurati in modo da consentire agli interessati di esplicare pienamente il proprio diritto all'autodeterminazione informativa, prevedendo opzioni di tipo "positivo" (mediante l'inserimento di caselle di scelta, anziché di campi pre-selezionati su una tra le possibili scelte), così da permettere ad essi di esprimere liberamente le proprie scelte in ordine alle finalità legittimamente perseguibili da parte del titolare del trattamento (*cfr.* il già citato *Provv.* 12 ottobre 2005 [doc. *web* n. 1179604]).

In un caso particolare, anche alla luce di quanto sopra rappresentato, è stata ad esempio constatata la non conformità alle norme in materia di protezione dei dati della scelta di raccogliere in un unico contesto (si trattava delle condizioni generali di contratto), sia il "consenso" del cliente per accedere *on-line* ad alcuni servizi, sia il consenso per trattare i dati conferiti per la fruizione di quest'ultimi allo scopo di perse-

guire una finalità diversa, quale quella dell'invio di comunicazioni commerciali in forma elettronica intese a promuovere iniziative proprie o a veicolare iniziative promozionali nell'interesse di terzi. Si è nuovamente ritenuto che un consenso manifestato nei termini appena descritti non può ritenersi valido, atteso che i clienti devono essere messi in condizione di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso –quando questo è necessario– per ciascuna distinta finalità perseguita dal titolare (*Provv.* 3 novembre 2005 [doc. *web* n. 1195215]).

Il Garante ha poi precisato che è possibile basare su un altro presupposto tale trattamento di dati qualora ricorrano le condizioni di cui all'art. 130, comma 4, del Codice, norma in base alla quale il titolare del trattamento che utilizzi le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio ai fini di vendita diretta di propri prodotti o servizi (e sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato), può non richiedere il consenso qualora l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. Affinché in tale ipotesi il trattamento si configuri come legittimo, occorre quindi accordare al cliente la possibilità di opporsi in maniera agevole e gratuitamente all'utilizzo delle coordinate di posta elettronica per finalità di vendita diretta, sin dalla fase di raccolta dei dati ("inizialmente", secondo la prescrizione dell'art. 130, comma 4, del Codice), come pure in occasione dell'invio di ogni comunicazione successiva, possibilità che non veniva accordata all'interessato nel caso esaminato.

Il Garante ha infine evidenziato che la circostanza dell'"assorbimento" del consenso all'utilizzo dei dati per finalità di vendita diretta nelle condizioni generali di contratto (destinate a regolare solo la fornitura dei servizi propriamente intesi), è tra l'altro idonea di per sé a evidenziare una violazione della disposizione richiamata, che intende salvaguardare la facoltà di autodeterminazione dell'interessato, anche nella forma della libera opposizione al trattamento dei dati, in ordine all'utilizzo delle proprie coordinate di posta elettronica al fine di vendita diretta.

Il trattamento dei dati dei minori

Sempre con riguardo al profilo della raccolta del consenso degli interessati, l'Autorità ha affrontato ulteriori aspetti in merito alle operazioni di trattamento di dati personali concernenti minori. In proposito, il Garante ha puntualizzato che la raccolta e le successive operazioni di trattamento sui dati relativi a minori possono essere effettuate lecitamente, una volta resa l'informativa nei termini di cui all'art. 13 del Codice, dopo aver acquisito il consenso espresso dei soggetti titolari della potestà genitoriale (art. 23 del Codice, artt. 316 e ss. c.c.; *v.* anche punto 2.6 del codice di autoregolamentazione Fedma (Federazione europea del *marketing* diretto), rispetto al quale il Gruppo art. 29 si è espresso favorevolmente con parere n. 3/2003 il 13 giugno 2003; *Provv.* 30 novembre 2005 [doc. *web* n. 1212652]).

Operazioni a premio e carte di fidelizzazione

Come anticipato, quello delle carte e dei programmi di "fidelizzazione" della clientela è un fenomeno sempre più diffuso tra la popolazione: interessa in primo luogo il settore della *cd.* grande distribuzione (supermercati), ma anche quello della prestazione di servizi nei trasporti, nel credito, nella telefonia, nell'editoria, nel noleggio, ecc. Preso atto di tale crescente diffusione, conclusi gli accertamenti e la consultazione pubblica avviata sul tema (v. *Relazione* 2004, p. 70), volti ad acquisire gli elementi necessari per verificare la conformità alle norme sulla protezione dei dati personali delle modalità di trattamento di dati personali prescelte dagli operatori di settore, l'Autorità ha fissato alcune prescrizioni per l'uso corretto dei dati dei clienti da parte dei soggetti che rilasciano le *cd.* "carte di fidelizzazione" (*Provv.* 24 febbraio 2005 [doc. *web* n. 1103045]).

Alla luce degli elementi acquisiti il Garante ha constatato che in occasione del rilascio delle carte di fidelizzazione (spesso mediante compilazione di questionari) e della loro successiva utilizzazione (attraverso la registrazione dell'acquisto di beni e servizi) vengono raccolti dati personali dei clienti e, a volte, dei loro familiari (tra i quali, dati anagrafici, titolo di studio, professione, interessi, abitudini di consumo, modalità di acquisto, volumi di spesa effettuata, ecc.), e che tali informazioni sono spesso utilizzate, senza che gli interessati ne abbiano piena conoscenza e possano acconsentire al loro uso, anche per monitorarne in dettaglio i comportamenti o le loro propensioni al consumo; per creare, cioè, "profili" individuali o di gruppo volti a confrontarne le abitudini di consumatori con altri clienti.

Le regole individuate nel provvedimento riguardano pertanto le tre principali finalità per le quali i dati personali degli interessati sono di regola raccolti e trattati: la *cd.* fidelizzazione in senso stretto, che viene realizzata attribuendo vantaggi connessi all'uso della carta (di regola consistenti nella partecipazione ad operazioni a premio), la *cd.* profilazione, volta ad analizzare abitudini e scelte di consumo della clientela, e lo svolgimento di attività di *marketing* diretto.

Il primo obbligo previsto per chi rilascia carte di fedeltà è quello di informare in maniera chiara e completa i clienti sull'uso che verrà fatto dei dati che li riguardano, tenendo conto in maniera differenziata delle diverse finalità perseguite. In base a quanto indicato dall'Autorità, l'informativa al cliente deve essere chiaramente evidenziata all'interno dei moduli di sottoscrizione utilizzati e risultare agevolmente individuabile rispetto alle altre clausole del regolamento. In particolare, deve essere posta in evidenza l'eventuale attività di profilazione e/o quella di *marketing* chiarendo che, per queste ultime due finalità, il conferimento dei dati è libero (e facoltativo rispetto alle ordinarie attività legate alla fidelizzazione in senso stretto) e che il consenso va prestato distintamente per ciascuna di esse.

Il Garante ha poi stabilito che chiunque ponga in essere operazioni a premio (o programmi di fidelizzazione) deve ridurre al minimo l'uso delle informazioni personali e utilizzare solo informazioni pertinenti e non eccedenti (artt. 3 e 11 del Codice). In particolare, per quanto riguarda la fidelizzazione, possono essere trattati senza acquisire il consenso degli interessati solo i dati necessari per attribuire vantaggi connessi all'utilizzo della carta, ovvero i dati correlati all'identificazione dell'intestatario o relativi al volume di spesa globale realizzato, di regola senza riferimento al dettaglio dei singoli prodotti acquistati.

Per l'attività di profilazione, occorre invece il consenso dell'interessato per trattare le informazioni relative agli acquisti effettuati e quelle ulteriori raccolte all'atto dell'adesione del cliente all'iniziativa, ed è necessario adempiere altresì all'obbligo di notificazione (art. 37, comma 1, lett. *d*), del Codice).

Riguardo all'attività di *marketing* possono essere raccolti, sempre con il consenso dell'interessato, i dati necessari all'invio di materiale pubblicitario o di comunicazioni commerciali.

Il Garante ha disposto che. allo stato, la conservazione dei dati personali dei clienti relativi al dettaglio degli acquisti non può superare un anno rispetto alle finalità di profilazione, e due anni per i dati raccolti a fini di *marketing.*

È stato altresì precisato che le carte fedeltà già rilasciate non dovevano essere annullate laddove i dati raccolti venissero utilizzati, sulla base di un'adeguata informativa, ai soli fini di sconti, premi, *bonus,* servizi accessori, facilitazioni di pagamento, sul presupposto che in tali casi non è necessario il consenso degli interessati e che questo resta, invece, necessario quando i dati vengono utilizzati per il perseguimento di altre finalità quali la profilazione e il *marketing* (*Comunicato stampa* 29 luglio 2005).

Per quanto attiene da ultimo all'interconnessione con altre banche dati, va ricordato che il Garante ha adottato un apposito provvedimento in materia di utilizzo a fini di *marketing* e di profilazione degli elenchi "categorici" (*cfr.* par. 15.3), le cui prescrizioni sono ora da coordinare con il disposto dell'art. 19-*bis* l. n. 51/2006 (su cui *v.* par. 1.3).

9.4. *Impresa*

Dati personali e recupero crediti

Ha formato oggetto di esame un numero elevato di segnalazioni relative ai profili di protezione dei dati personali rispetto alle attività di recupero dei crediti. A conclusione dell'istruttoria avviata in tale delicata materia e sulla base dei diversi accertamenti effettuati, il Garante ha constatato l'illecito utilizzo, da parte di diversi operatori, dei dati personali relativi ai debitori.

Si è in particolare riscontrato come, attraverso soggetti incaricati del recupero, venissero poste in essere modalità particolarmente invasive di ricerca, di presa di contatto e di sollecitazione al pagamento delle somme dovute: visite a domicilio o sul posto di lavoro degli interessati, reiterate sollecitazioni al telefono fisso o sul cellulare, utilizzo di sistemi automatizzati di chiamata senza operatore, invio di cartoline o di plichi postali con l'indicazione chiaramente visibile della scritta "recupero crediti" o "preavviso esecuzione notifica" o diciture analoghe, affissione di avvisi di mora sulla porta di casa. Spesso, i dati personali relativi ai componenti di intere famiglie risultavano inoltre inseriti nelle banche dati del soggetto creditore o delle società di recupero crediti.

Il Garante ha conseguentemente adottato un provvedimento a carattere generale con il quale ha prescritto alle società di recupero crediti e a quanti –finanziarie, banche, concessionari di pubblici servizi, compagnie telefoniche– svolgono tale attività direttamente, le misure alle quali attenersi per non incorrere in illeciti e per rispettare i principi posti a tutela dei diritti della persona: fermo restando il diritto del creditore a tutelare le proprie ragioni, il suo esercizio non deve infatti tradursi in abuso, dovendo essere improntato ai generali principi di buona fede e di correttezza contemplati nel nostro ordinamento.

Sono state pertanto considerate illecite tutte le modalità di recupero del credito le quali, ancorché finalizzate all'esercizio di diritti, risultino lesive della sfera personale dei debitori e della loro dignità (*Provv.* 30 novembre 2005 [doc. *web* n. 1213644]).

Non è risultato lecito, in particolare, comunicare ingiustificatamente informazioni relative ai mancati pagamenti a soggetti diversi dall'interessato (*ad es.*, familiari, colleghi di lavoro o vicini di casa) ed esercitare indebite pressioni su quest'ultimo al fine di sollecitare il pagamento di somme dovute. Non è risultato consentito, altresì, ricorrere a telefonate pre-registrate, anche perché attraverso questa modalità persone diverse dal debitore, in assenza di adeguate garanzie, potrebbero venire a conoscenza della sua eventuale inadempienza.

È emersa anche l'illiceità dell'affissione da parte degli incaricati del recupero crediti di avvisi di mora su porte di abitazioni, trattandosi di modalità che rende possibile la diffusione dei dati personali dell'interessato ad una serie indeterminata di soggetti. Non deve inoltre rendersi visibile a persone estranee il contenuto di una comunicazione, come può avvenire ad esempio mediante l'utilizzo di cartoline postali o con l'invio di plichi recanti all'esterno la scritta "recupero crediti" o formule simili. È necessario, invece, che le sollecitazioni di pagamento vengano portate a conoscenza del solo debitore, usando plichi chiusi e senza scritte specifiche.

Gli incaricati delle società non possono poi usare altri dati se non quelli necessari all'esecuzione del mandato (dati anagrafici, codice fiscale, ammontare del credito, recapiti telefonici).

Salvo l'assolvimento di specifici obblighi di legge che può richiedere una conservazione prolungata dei dati raccolti (*ad es.*, per rendere conto delle attività svolte), una volta portato a termine l'incarico i dati non possono formare oggetto di ulteriore trattamento. La loro eventuale conservazione ulteriore deve essere realizzata con modalità tali, comunque, da precluderne agli incaricati del trattamento l'ordinaria consultabilità (adottando opportune misure logiche o provvedendo alla trasposizione dei dati in archivi separati).

Dati personali e servizi radiotaxi

Muovendo da alcune segnalazioni di singoli e di associazioni per la tutela dei diritti dei consumatori, l'Autorità ha valutato la liceità o meno dei trattamenti di dati personali della clientela effettuati da soggetti che forniscono servizi radiotaxi.

Gli accertamenti hanno permesso di constatare che questi ultimi raccolgono, generalmente per via telefonica, richieste di corse taxi nell'interesse dei titolari di licenza (art. 7 l. n. 21/1992). Di regola, le informazioni raccolte si esauriscono nel solo indirizzo di prelievo; in altri casi, invece, formano oggetto di trattamento anche il numero di telefono e il nominativo del cliente (eventualmente associando, in modo automatizzato, il numero telefonico a dati ricavati da elenchi pubblici). In casi limitati, vengono registrate informazioni aggiuntive concernenti comportamenti tenuti dal cliente a seguito della chiamata (*ad es.*, assenza presso l'indirizzo di prelievo o mancato pagamento della corsa).

Con un *provvedimento* del 26 luglio 2005 [doc. *web* n. 1151997], il Garante ha affermato che è lecito utilizzare solo i dati necessari per mettere in contatto il cliente con il taxi indicato per effettuare la corsa, o comunque utili per dare attuazione al relativo rapporto contrattuale (quali l'indirizzo di prelievo, il nominativo, l'eventuale numero telefonico fisso o mobile), agevolando in tal modo l'esatta esecuzione della prestazione (*ad es.*, per segnalare una sostituzione del taxi o per assicurarsi che il servizio venga reso alla persona che lo ha effettivamente richiesto). L'Autorità ha aggiunto che, in base a quanto previsto dall'art. 11, comma 1, lett. *b*), del Codice, non possono essere registrati dati sui percorsi effettuati dai clienti o relativi ad eventuali inadempimenti loro attribuiti, fatta salva l'esigenza di far valere o difendere un diritto in sede giudiziaria; né possono essere conservate informazioni relative all'assenza dei clienti presso l'indirizzo di prelievo indicato oltre il tempo strettamente necessario a rispondere ad eventuali contestazioni, considerato che il loro trattamento ha una finalità del tutto diversa da quella perseguita nel rendere possibile il trasporto della clientela (unica finalità per la quale il gestore del servizio radiotaxi può raccogliere lecitamente i dati).

Al di fuori delle operazioni di raccolta e di successivo trattamento dei dati della clientela preordinati alla ordinaria prestazione del servizio (in relazione alla quale trova applicazione l'art. 24, comma 1, lett. *b*), del Codice), il trattamento delle informazioni relative ai clienti per perseguire scopi ulteriori (*ad es.*, a fini di *marketing* o per compiere ricerche di mercato, o ancora al fine di fornire, anche su registrazione o abbonamento, servizi aggiuntivi rispetto alla singola corsa di volta in volta richiesta) richiede infatti il consenso specifico degli stessi.

È stato altresì precisato che, una volta espletato il servizio, i dati non più necessari devono essere cancellati o trasformati in forma anonima, salva l'osservanza di eventuali e puntuali obblighi di legge che ne legittimino l'ulteriore conservazione; i dati relativi alla clientela possono essere conservati solo per scopi compatibili con il servizio reso (restituzione oggetti smarriti, contestazioni sulla corsa), per un tempo massimo di trenta giorni.

Con riguardo agli ulteriori obblighi previsti dalla normativa contenuta nel Codice, il Garante ha prescritto ai gestori di servizi radiotaxi di informare i propri clienti al momento del contatto (di regola telefonico) circa l'uso che verrà fatto dei dati che li riguardano, con particolare riferimento alle differenti finalità perseguite e alla tipologia dei dati personali utilizzati per ciascuna di esse. Tale informativa può essere resa, previa motivata e specifica richiesta rivolta all'Autorità, in forma semplificata, al telefono –in sede di prenotazione del servizio– e deve essere integrata mediante l'affissione all'interno del taxi di un testo contenente gli elementi menzionati nell'art. 13 del Codice. Al riguardo, l'Autorità ha predisposto un modello di informativa di riferimento per i gestori di servizi radiotaxi cui uniformarsi, allegandolo, a tal fine, al provvedimento sopra citato.

Dati personali e catene alberghiere

A seguito di accertamenti disposti nei confronti di una nota catena alberghiera, l'Autorità si è pronunciata in ordine ai trattamenti di dati raccolti nell'ambito dell'esecuzione della prestazione alberghiera (*Provv.* 9 marzo 2006 [doc. *web* n. 1252220]). Il Garante ha rilevato che, nel modello di informativa reso alla clientela, anche in sede di prenotazione, devono essere in particolare evidenziate le caratteristiche delle attività di profilazione e di promozione commerciale eventualmente svolte. Gli interessati devono essere posti in condizione di esprimere un consenso differenziato, debitamente informato, rispetto a quello manifestato con l'adesione al programma di fidelizzazione. In particolare, nello svolgimento delle operazioni (anche per via telematica) per il rilascio di una carta di fidelizzazione, la società deve specificare la finalità di *marketing* perseguita, precisando nell'informativa che il consenso e, dunque, il conferimento dei dati a tale scopo, è facoltativo ed indipendente rispetto alla finalità di fidelizzazione in senso stretto (art. 23 del Codice).

Il consenso dell'ospite al trattamento dei dati personali a sé riferiti non è in termini generali necessario, sia nella parte in cui si deve adempiere a specifiche disposizioni di legge (ad esempio, per le menzionate finalità di pubblica sicurezza), sia per ciò che attiene all'ordinario servizio di albergo, quando il trattamento dei relativi dati è indispensabile per eseguire obblighi derivanti dal contratto o per adempiere, anche in fase precontrattuale, a specifiche richieste dell'ospite-interessato, ad esempio a seguito dell'adesione ad una operazione a premi (art. 24, comma 1, lett. *a*) e *b*), del Codice).

Ogni altra finalità del trattamento che comporti un'ulteriore conservazione dei dati personali raccolti (*ad es.*, come avvenuto nel caso esaminato, ricerche di mercato, operazioni di *marketing* o profilazioni) necessita, invece, del consenso specifico e informato, espresso distintamente da parte del cliente (art. 23 del Codice). Tale autodeterminazione non è assicurata quando si raccoglie il consenso in modo indifferenziato per perseguire finalità in realtà distinte tra loro, quali la definizione dei profili della clientela e l'invio alla stessa di comunicazioni commerciali (*marketing*), ben potendo essere ciascuna di esse perseguita singolarmente in presenza di autonome valutazioni e determinazioni dell'interessato.

Il Garante è intervenuto anche in ordine al profilo della durata massima di conservazione dei dati raccolti, atteso che nel medesimo caso non era stato stabilito un termine di conservazione dei dati presenti nella banca dati della clientela, accessibili nella loro interezza solo dalle funzioni centrali della società e, limitatamente agli ultimi tre soggiorni di ciascun cliente, anche da parte delle singole strutture alberghiere. In applicazione dei principi di pertinenza e proporzionalità, si è prescritto quindi di identificare i tempi massimi di conservazione dei dati trattati alla luce delle finalità in concreto perseguite dalla società, nonché delle scelte dell'interessato in ordine al trattamento medesimo. In particolare, nell'ipotesi in cui il trattamento dei dati sia preordinato alla realizzazione delle operazioni a premio, la

conservazione non deve protrarsi oltre la scadenza del termine della stessa indicato nel regolamento (o della sua eventuale proroga); con specifico riguardo all'attività di profilazione della clientela il Garante ha poi ribadito il termine massimo di dodici mesi decorrenti dalla registrazione delle informazioni, conformemente a quanto stabilito nel *provvedimento* del 24 febbraio 2005 [doc. *web* n. 1103045].

Per quanto attiene quindi alle finalità di *marketing* e di vendita diretta, si è precisato che resta impregiudicata la facoltà degli interessati di opporsi al trattamento dei dati personali che li riguardano (art. 7, comma 4, lett. *b*), del Codice; *v.* anche, per quanto riguarda le "coordinate di posta elettronica", l'art. 130, comma 4, del Codice).

Da ultimo, nel dichiarare illecito il trattamento dei dati personali della clientela effettuato dalla catena alberghiera in ordine ai profili dell'omessa e incompleta informativa, della mancata acquisizione del consenso per le attività connesse alla definizione dei profili individuali in relazione a scelte e preferenze di consumo e per svolgere operazioni di *marketing* nell'ambito della gestione dell'operazione a premi, nonché dell'omessa notificazione dei trattamenti volti a definire il profilo degli interessati e ad analizzarne abitudini o scelte di consumo, il Garante ha in conclusione vietato, ai sensi dell'art. 154, comma 1, lett. *d*), del Codice, la prosecuzione delle operazioni di trattamento di dati personali effettuate in violazione di legge.

Modalità di voto e delibere assembleari delle società cooperative

Con nota del 10 gennaio 2005, l'Ufficio del Garante si è soffermato sull'utilizzabilità, nell'ambito delle società cooperative a r.l., della modalità di voto a scrutinio segreto ai fini dell'adozione delle relative delibere assembleari.

Muovendo dal rinvio alle disposizioni sulle società per azioni contenuto nell'art. 2519 c.c. in tema di norme applicabili alle società cooperative, è stato rilevato che l'art. 2375 c.c., nella formulazione derivante dalla recente riforma (d.lg. 17 gennaio 2003, n. 6), prevede, in termini generali, la necessità di indicare nel verbale assembleare delle società per azioni modalità e risultati delle votazioni, e di consentire, anche per allegato, l'identificazione dei soci favorevoli, astenuti o dissenzienti. È stato altresì evidenziato l'applicabilità, alle modalità di votazione, dell'art. 2368 c.c., nella parte in cui ammette che l'atto costitutivo possa stabilire norme particolari per la "nomina delle cariche sociali".

Alla luce di tali considerazioni, con riferimento al caso di specie (rispetto al quale la società aveva adottato il sistema di voto a scrutinio palese nelle proprie deliberazioni attraverso l'approvazione di un'autonoma clausola statutaria), l'Autorità si è espressa nel senso che la propria competenza relativa alla liceità e correttezza del trattamento dei dati in relazione al Codice non consente un intervento inibitorio o interdittivo in materia, non disponendo del potere di vincolare l'autonomia contrattuale dei soci di una società a r.l. per introdurre, in deroga al predetto principio civilistico dello scrutinio palese, una clausola statutaria (peraltro controversa in giurisprudenza) che preveda lo scrutinio segreto.

Giochi olimpici invernali

Nel 2005 l'Autorità ha avviato incontri tecnici volti ad esaminare alcune questioni sottoposte all'attenzione dell'Ufficio del Garante dai rappresentanti del Comitato organizzatore dei XX Giochi olimpici invernali, in programma a Torino nel 2006. L'intento perseguito attraverso tale collaborazione è stato quello di garantire, nel corso dello svolgimento di tale manifestazione, il rispetto della riservatezza dei dati concernenti i vari soggetti coinvolti (quali visitatori, dipendenti e atleti), considerata anche l'importanza e la portata dell'evento.

In occasione di tali incontri sono stati affrontati, anche alla luce dei provvedimenti già adottati dal Garante, e in aggiunta ad alcuni profili relativi ai principi generali in materia di trattamento dei dati (quali l'obbligo di rendere l'informativa agli interessati, di notificare i trattamenti al Garante ai sensi dell'art. 37 del Codice e di

designare incaricati ed eventuali responsabili del trattamento), altri più specifici aspetti concernenti l'utilizzazione di sistemi di videosorveglianza, l'attivazione di *call center*, l'adozione di adeguate misure di sicurezza dei dati e le modalità di contatto con la clientela. Inoltre, hanno formato oggetto di esame i nuovi modelli predisposti dal Comitato per informare la clientela, presso i relativi punti vendita, ma anche *on-line* e attraverso il *call center*, all'atto dell'acquisto e/o della prenotazione dei biglietti, nonché per richiedere il suo specifico consenso all'eventuale uso dei dati che la riguardano per compiere operazioni di *marketing*.

9.5. *Trasferimento dei dati personali all'estero*

Autorizzazioni del Garante al trasferimento di dati verso Paesi terzi

Come riportato nella *Relazione* 2004, il Codice (Parte I, Titolo VII) ha disciplinato il trasferimento dei dati all'estero completando il recepimento della direttiva comunitaria 95/46/Ce e ribadendo il principio generale in base al quale il flusso di dati verso un Paese esterno all'Unione europea è autorizzato soltanto quando sussiste il consenso dell'interessato o sulla base di almeno uno degli altri presupposti di liceità (art. 43 del Codice), o se il Paese di destinazione assicura un livello adeguato di protezione.

In quest'ambito l'attività del Garante ha assunto particolare rilievo nel corso del 2005 in corrispondenza all'adozione di alcune decisioni comunitarie concernenti il livello di adeguatezza di protezione di dati personali garantito da Paesi extra-Ue. Il 9 giugno 2005 il Garante ha autorizzato, con due deliberazioni (pubblicate in *G.U.* 25 luglio 2005, n. 171) i trasferimenti dei dati personali dal territorio italiano verso l'Argentina e l'Isola di Man, considerato che, stando alla valutazione svolta dalla Commissione europea nelle decisioni assunte il 30 giugno 2003 (n. 2003/490/Ce) e il 28 aprile 2004 (n. 2004/411/Ce), deve ritenersi che tali Paesi garantiscano nel proprio ordinamento un livello adeguato di protezione dei dati personali (*Autorizzazioni* 9 giugno 2005 [doc. *web* n. 1151846 e n. 1151889]).

Va segnalata, inoltre, la pubblicazione (in *G.U.* 22 luglio 2005, n. 169) della precedente deliberazione n. 6 del 7 settembre 2004 [doc. *web* n. 1139333], con cui il Garante aveva ritenuto parimenti adeguato il livello di protezione dei dati personali nel Baliato di Guernsey, come evidenziato nella decisione della Commissione europea del 21 novembre 2003 n. 2003/821/Ce (*v. Relazione* 2004, pag. 73).

Il Garante ha reso quindi pienamente operative nell'ordinamento interno le tre predette decisioni della Commissione europea che vanno ad affiancarsi alle altre pronunzie in materia, concernenti il livello di adeguatezza di Canada, Svizzera e Ungheria (anteriormentemente al suo ingresso nell'Ue), e rispetto alle quali il Garante ha simmetricamente rilasciato negli anni precedenti apposite autorizzazioni.

L'Autorità, come previsto dai compiti attribuiti dal Codice, si è riservata di svolgere controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti stessi e di adottare, qualora si riveli necessario, eventuali provvedimenti di blocco o di divieto.

Le clausole contrattuali per il trasferimento

Nel corso del 2005 sono state sottoposte all'attenzione dell'Ufficio del Garante alcune iniziative intraprese in relazione alla circolazione di dati personali da parte di una società avente sede negli Stati Uniti, facente parte di un gruppo societario operante a livello internazionale, volte a garantire il rispetto della normativa comunitaria e nazionale nell'ambito delle operazioni di trasferimento di dati personali *infra*-gruppo concernenti differenti tipologie di interessati (quali clienti, dipendenti e fornitori delle società del gruppo).

Al fine di rendere lecite le operazioni sopra menzionate la società interessata ha sottoscritto con altre società controllate e collegate, aventi sede in vari Stati dell'Ue ed in alcuni Paesi terzi, un contratto *cd.* globale volto a regolamentare i flussi transfrontalieri di dati personali all'interno del gruppo.

Sulla base di alcune prime osservazioni formulate dall'Ufficio e da altre autorità di controllo europee interpellate, nell'ambito del rapporto di collaborazione instauratosi, è stato predisposto un nuovo schema di "contratto integrativo" volto a regolamentare specificamente i flussi di dati oggetto di trattamento nel gruppo, dalle società europee alla società americana e alle altre affiliate stabilite al di fuori dell'Ue. Tale schema di contratto, denominato *Eu Addendum*, basato sostanzialmente sulle clausole contrattuali-tipo per trasferire dati a responsabili del trattamento stabiliti in Paesi terzi (di cui all'allegato della decisione del 27 dicembre 2001 della Commissione europea n. 2002/16/Ce, e relativa *autorizzazione* del Garante del 10 aprile 2002 [doc. *web* n. 1065361]), è in corso di valutazione.

Il modello alternativo di clausole contrattuali tipo

Un modello alternativo di clausole contrattuali-tipo (definito "Insieme II"), rispetto a quelle già approvate con la decisione della Commissione europea n. 2001/497/Ce (del 15 giugno 2001), ha formato oggetto della decisione della Commissione del 27 dicembre 2004, n. 2004/915/Ce (pubblicata in *G.U.C.E.* 29 dicembre 2004 L 385/74) che ha in parte modificato la prima decisione ed introdotto l'insieme alternativo predetto di clausole contrattuali-tipo. Tali clausole, secondo la Commissione, costituiscono anch'esse garanzie sufficienti ai fini della tutela della riservatezza, dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi in caso di trasferimento di dati personali verso Paesi terzi a norma della direttiva 95/46/Ce.

Le clausole, elaborate dalla Camera di commercio internazionale (Icc) e da altre organizzazioni commerciali, hanno formato oggetto di un primo parere del Gruppo art. 29 (parere 8/2003, 17 dicembre 2003) il quale aveva suggerito alcune modifiche per rendere il livello di tutela equiparabile a quello delle clausole già approvate dalla Commissione il 15 giugno 2001 e rese operative in Italia con l'*autorizzazione* del Garante del 10 ottobre 2001 [doc. *web* n. 42156].

Le clausole trovano applicazione in caso di trasferimenti di dati effettuati a partire dal territorio dello Stato, da un titolare del trattamento avente sede nella Comunità (soggetto esportatore) ad un diverso titolare del trattamento (soggetto importatore), residente in un Paese terzo che non assicura un livello di protezione adeguato, e possono essere utilizzate alternativamente rispetto alle clausole contrattuali *standard* individuate con la decisione del 2001 (ora definite "Insieme I"). Il Garante ha reso operative tali clausole nell'ordinamento interno con un'*autorizzazione* del 9 giugno 2005 [doc. *web* n. 1151949].

Utilizzo delle *cd.* *binding corporate rules*

Con particolare riferimento ai trasferimenti di dati fra società appartenenti ad uno stesso gruppo multinazionale, il Gruppo art. 29 ha evidenziato l'opportunità di introdurre nell'ambito di tali gruppi, in aggiunta alle clausole-tipo già predisposte, ulteriori garanzie per la protezione dei dati personali, ossia regole di comportamento che avrebbero natura vincolante per tutti i soggetti che ne fanno parte (*Binding Corporate Rules for International Data Transfers*).

Il 14 aprile 2005 il Gruppo ha approvato due documenti (WP 107 e WP 108; *cfr. Newsletter* del 25 aprile-1° maggio 2005), individuando le procedure di verifica attraverso le quali le imprese multinazionali potrebbero vedere riconosciuta in tutti i Paesi dell'Ue la validità delle *cd.* "regole vincolanti nell'impresa" ai fini del trasferimento di dati personali verso Paesi terzi che non garantiscono un livello adeguato di protezione.

Con il primo documento sono stati fissati alcuni aspetti procedurali prevedendo,

come auspicato da soggetti interessati, la designazione di un unico interlocutore, ossia di un'autorità di protezione dati che opererebbe quale "*leader*" della valutazione, alla quale tutte le altre autorità interessate dei Paesi Ue dovrebbero far capo per commenti ed osservazioni. La designazione spetterebbe alla società multinazionale, la quale dovrebbe rifarsi ai criteri indicati nel documento, fra i quali la priorità viene data alla considerazione del Paese ove è situata la capogruppo o la sede centrale europea della multinazionale. Le autorità sono libere di accettare o meno tale designazione, sulla base della documentazione prodotta dalla società, eventualmente formulando una contro-proposta.

La procedura prevede, stabilita l'autorità-*leader*, l'elaborazione di una bozza finale di "regole vincolanti nell'impresa" sottoposta alla valutazione congiunta di tutte le autorità interessate, coordinate dall'autorità-*leader*; l'accettazione di tale bozza finale varrebbe come riconoscimento dell'adeguatezza delle norme in essa contenute e, quindi, come autorizzazione al loro impiego.

Contestualmente all'elaborazione del primo documento citato il Gruppo ha prodotto un ulteriore documento (WP 108) che integra e completa il precedente, fornendo indicazioni specifiche sui contenuti delle regole vincolanti nell'impresa. Rifacendosi ai criteri fissati nel giugno del 2003 (documento WP 74, 3 giugno 2003; *cfr. Newsletter* 2-8 giugno 2003), i Garanti europei hanno elaborato una *checklist* che le imprese potrebbero utilizzare per dimostrare che le rispettive "regole vincolanti nell'impresa" rispondono ai principi fissati nella direttiva 95/46/Ce. Ciò concerne, in particolare, la verifica dell'effettiva vincolatività delle regole –sia all'interno del gruppo (rispetto a controllate, collegate, dipendenti e terzi fornitori), sia all'esterno– soprattutto ai fini dell'esercizio dei diritti riconosciuti agli interessati.

Dati dei passeggeri e vettori aerei

Con riguardo al trasferimento dei dati dei passeggeri europei alle autorità doganali di Paesi non appartenenti all'Unione europea, la Commissione europea, con decisione del 14 maggio 2004, n. 2004/535/Ce (*v. Relazione* 2004, p. 260) aveva ritenuto che l'Ufficio statunitense delle dogane e della protezione delle frontiere (*United States Bureau of Customs and Border Protection*, "Cbp") del Ministero della sicurezza interna (*Department of Homeland Security*) sia in grado di offrire un livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei (*Passenger Name Record*, "Pnr") trasmessi dalla Comunità per quanto riguarda i voli con destinazione o in partenza dagli Stati Uniti, in conformità alla Dichiarazione d'impegno del Ministero della sicurezza interna (*Department for Homeland Security*)-Ufficio delle dogane e della protezione delle frontiere (Cbp) dell'11 maggio 2004, che figura in allegato alla decisione medesima.

Secondo il giudizio della Commissione europea i criteri utilizzati dal Cbp per trattare i dati Pnr dei passeggeri, in conformità alla legislazione statunitense e alla Dichiarazione d'impegno dello stesso Cbp, comprenderebbero elementi fondamentali per assicurare un livello di protezione adeguato delle persone fisiche interessate.

Dovendosi attenere a tale valutazione il Garante, il 14 luglio 2005, ne ha dato attuazione ai sensi del Codice, autorizzando il trasferimento fuori dal territorio dello Stato italiano all'Ufficio statunitense delle dogane e della protezione delle frontiere del Ministero della sicurezza interna, da parte dei vettori aerei che assicurano il trasporto di passeggeri con destinazione o in partenza dagli Stati Uniti, dei dati personali contenuti nelle schede nominative dei passeggeri, nella misura in cui tali dati siano stati raccolti e memorizzati nei relativi sistemi informatici di prenotazione, sulla base dei presupposti e in conformità a quanto previsto dalla decisione della Commissione europea sopra citata e alla Dichiarazione di impegno ivi allegata (*Autorizzazione* 14 luglio 2005 [doc. *web* n. 1149808], in *G.U.* 25 luglio 2005, n. 171).

9.6. *Lavoro*

Informativa per la Borsa continua nazionale del lavoro

Nell'ambito delle attività di approfondimento sui profili di interrelazioni tra le norme contenute nel d.lg. n. 276/2003 e le disposizioni in materia di protezione dei dati personali in ambito lavorativo, sono state fornite alcune indicazioni sul testo di informativa predisposto per gli utenti (lavoratori e imprese) della Borsa continua nazionale del lavoro.

L'esame dell'informativa è stato svolto con la collaborazione di Italia lavoro S.p.A., soggetto deputato a fornire il supporto tecnico e strumentale alla Commissione per il raccordo e il coordinamento permanente tra il livello regionale e quello nazionale della Borsa in qualità di segreteria tecnico-organizzativa della stessa (art. 7, comma 4, d.m. 13 ottobre 2004).

Si è rappresentata, in particolare, l'opportunità di elaborare un'informativa che tenesse conto di una pluralità di circostanze:

- il differente ruolo spettante a ciascun titolare del trattamento nel sistema della Borsa continua nazionale del lavoro;
- la necessità di considerare titolari del trattamento esclusivamente i soggetti indicati dall'art. 6 del predetto decreto interministeriale (cioè, il Ministero del lavoro e delle politiche sociali, le regioni e gli operatori pubblici e privati, ad esclusione degli enti previdenziali ed assistenziali ai quali non compete il ruolo di titolari del trattamento dei dati trattati nella Borsa e che, per la peculiare funzione istituzionale rivestita, non possono essere designati quali responsabili del trattamento da uno dei titolari), specificando il ruolo rivestito da alcuni soggetti preposti al trattamento dei dati in nome e per conto dei titolari e, in tale eventualità, provvedendo (se del caso) a designarli quali responsabili del trattamento e ad identificarli, e fornendo agli interessati l'indirizzo dove reperire l'elenco completo, ovvero consentendo l'accesso a tale elenco mediante un *link* ipertestuale nel sito del Ministero del lavoro e degli altri titolari del trattamento;
- la necessità di esplicitare i diritti degli interessati previsti dall'art. 7 del Codice inserendo opportuni riferimenti (indirizzi di posta elettronica o numeri di telefax o di *call center*), utilizzabili per l'esercizio di tali diritti;
- l'esigenza di chiarire, ferma restando la facoltatività dell'iscrizione alla Borsa, quali dati debbano essere conferiti necessariamente e quali, invece, facoltativamente, ai fini dell'iscrizione, esplicitando anche le conseguenze derivanti dal rifiuto al conferimento di tali dati (ai sensi dell'art. 13, comma 1, lett. *b*) e *c*), del Codice).

L'Autorità ha formulato una riserva in ordine alla possibile espressione, anche ai sensi dell'art. 154, comma 1, lett. *g*), del Codice, di pareri eventualmente chiesti sui profili di protezione dei dati personali emersi in tema di trattamenti effettuati mediante la Borsa, rispetto ai quali si è manifestata la necessità di valutazioni più approfondite con tutti i soggetti interessati al suo funzionamento.

Le agenzie per l'impiego

Nell'ambito della collaborazione richiesta da un'associazione rappresentativa (Assores) di alcuni tra i nuovi operatori privati del mercato del lavoro rientranti tra le agenzie per l'impiego introdotte dalla l. n. 30/2003 (e dal d. lg. n. 276/2003), l'Ufficio del Garante ha fornito alcuni chiarimenti sui profili di protezione dei dati personali dei candidati all'instaurazione di rapporti di lavoro subordinato. Si è ribadito che il consenso dell'interessato, ove prescritto, deve essere reso ai sensi degli artt. 23 e ss. del Codice, dal momento che la disciplina in materia di protezione dei dati non riconosce validità ed efficacia al consenso implicito o manifestato per atti concludenti. È stato altresì sottolineato che il consenso al trattamento dei dati "comuni" non è neces-

sario nei casi di cui all'art. 24, comma 1, del Codice (nel caso di specie, lett. *a*) e *b*)). In tal senso, si è richiamata l'interpretazione già fornita dal Garante con il *provvedimento* in materia di annunci di lavoro del 10 gennaio 2002 [doc. *web* n. 1064553].

Nel confermare, per converso, l'obbligo per i titolari del trattamento di fornire agli interessati un'informativa completa degli elementi prescritti dall'art. 13 del Codice (avvalendosi eventualmente delle formule sintetiche già suggerite dal Garante con il citato provvedimento del 2002), è stato confermato l'impegno a valutare, in sede di adozione del codice di deontologia di cui all'art. 111 del Codice, le modalità attraverso le quali i titolari del trattamento potranno rendere un'informativa semplificata (nei casi eventualmente non già contemplati dall'art. 9 d.lg. n. 276/2003) o potrebbero essere esonerati dal relativo obbligo.

Sono state inoltre fornite indicazioni in materia di notificazione al Garante dei trattamenti che le società rappresentate da Assores potrebbero essere tenute ad effettuare a norma dell'art. 37, comma 1, lett. *d*) ed *e*), del Codice e alla luce del *provvedimento* a carattere generale del Garante del 31 marzo 2004 relativo ai casi sottratti all'obbligo di notificazione [doc. *web* n. 852561].

Navigazione in Internet e controllo sui lavoratori

Il Garante si è pronunciato su un ricorso proposto da un lavoratore che lamentava l'illiceità del controllo effettuato dal datore di lavoro sulle navigazioni in Internet (*Provv.* 2 febbraio 2006 [doc. *web* n. 1229854]).

Il datore di lavoro aveva contestato al dipendente, in seguito licenziato, di aver consultato siti a contenuto religioso, politico e pornografico, fornendone l'elenco dettagliato ed allegando alla contestazione disciplinare notificata al lavoratore numerose pagine dei *file* temporanei e dei *cookie* originati sul suo *computer* dalla navigazione in rete avvenuta durante sessioni di lavoro avviate con la *password* del dipendente. Si trattava di informazioni ricavate da pagine *web*, copiate direttamente dalla *directory* intestata al lavoratore, che la società non avrebbe potuto trattare senza averlo informato preventivamente. In secondo luogo, sebbene i dati fossero stati raccolti nel corso di controlli informatici volti a verificare l'esistenza di un comportamento illecito, le informazioni di natura sensibile, in grado di rivelare ad esempio convinzioni religiose e opinioni sindacali o politiche, potevano essere trattate dal datore di lavoro senza il consenso dell'interessato solo se indispensabili per far valere o difendere un diritto in sede giudiziaria. Tale indispensabilità non è emersa dagli elementi in atti.

È emerso, altresì, un trattamento dei dati relativi allo stato di salute e alla vita sessuale che, a norma del Codice, può essere effettuato senza il consenso dell'interessato solo se necessario per difendere in giudizio un diritto di rango pari a quello dell'interessato della personalità o un altro diritto fondamentale. Anche tale circostanza non è risultata comprovata in atti, dal momento che la società intendeva far valere, invece, diritti legati allo svolgimento del rapporto di lavoro.

L'Autorità ha pertanto vietato alla società l'uso dei dati relativi alla navigazione in Internet del lavoratore, sul presupposto che per contestare l'indebito utilizzo di beni aziendali sarebbe stato proporzionato, nel caso di specie, verificare gli avvenuti accessi a Internet e i tempi di connessione, senza indagare sui contenuti dei siti.

Sistemi di rilevazione biometrica nei luoghi di lavoro

Nel corso dell'anno si è intensificata l'attività dell'Autorità volta alla valutazione della liceità dell'impiego dei sistemi di rilevazione biometrica in specifici contesti e per diverse finalità.

Il Garante ha adottato alcune decisioni a seguito di un formale interpello da parte di alcuni titolari del trattamento, conformemente a quanto stabilito dall'art. 17 del Codice (e dall'art. 20 della direttiva 95/46/Ce). In tale ambito, muovendo dal presupposto che il trattamento di dati biometrici dei lavoratori può risultare in concreto pregiudizievole sul piano del rispetto dei principi di necessità, finalità e proporziona-

lità, sono proseguiti gli approfondimenti iniziati nel 2004 circa l'utilizzo di tecniche di autenticazione biometrica, basate in particolare su impronte digitali.

Un primo caso ha riguardato un'industria di coperture in fibrocemento e metalliche che intendeva implementare un sistema di rilevazione biometrica basato sull'impiego delle impronte digitali dei lavoratori al fine di accertarne la presenza sul luogo di lavoro e di commisurare la retribuzione da corrispondere.

L'impresa intendeva in tal senso prevenire alcune condotte abusive e ovviare allo smarrimento delle tessere magnetiche in uso. Il sistema prevedeva la raccolta dell'impronta di ciascun dipendente e la sua trasformazione in un codice numerico (*template*) poi memorizzato, senza cifratura, nella banca dati aziendale. A ciascun ingresso in azienda i lettori elettronici avrebbero rilevato l'impronta e confrontato il codice da questa ricavato con il *template* previamente memorizzato.

Dall'istruttoria non sono emersi elementi che potessero giustificare la richiesta di introdurre la rilevazione di dati biometrici (come, ad esempio, la necessità di limitare accessi ad aree dell'azienda che richiedono *standard* di sicurezza particolarmente elevati in ragione di specifiche circostanze o attività svolte). Il trattamento è stato pertanto vietato in quanto sproporzionato e non necessario rispetto allo scopo perseguito (*Provv.* 21 luglio 2005 [doc. *web* n. 1150679]). Rispetto alla finalità specifica il Garante ha infatti ritenuto l'uso di dati biometrici eccessivamente invasivo della sfera personale e della libertà individuale dei lavoratori in quanto, pur rientrando il controllo sull'esecuzione della prestazione lavorativa tra le legittime facoltà del datore di lavoro (art. 2094 c.c.), anche attraverso la predisposizione di strumenti di controllo del rispetto dell'orario di lavoro da parte dei lavoratori, per il raggiungimento di tale scopo possono essere adottate altre tecniche più rispettose del principio di proporzionalità ed ugualmente rigorose.

Il trattamento è risultato sproporzionato anche sul piano delle modalità tecniche prefigurate. In luogo della proposta centralizzazione in una banca dati aziendale dei codici identificativi generati dall'esame dell'impronta, il Garante ha osservato che sarebbe stato preferibile una memorizzazione del *template* su un supporto digitale da assegnare al lavoratore e tale da rimanere nella sua esclusiva disponibilità, in modo da prevenire maggiori ripercussioni per i diritti individuali in caso di violazione delle misure di sicurezza, di accesso di persone non autorizzate o comunque di abuso delle informazioni memorizzate.

La stessa informativa predisposta ai sensi dell'art. 13 del Codice è apparsa incompleta rispetto al trattamento ipotizzato: le dichiarazioni rese dalla società circa la libertà accordata ai lavoratori di aderire o meno al sistema di controllo delle presenze basato sull'utilizzo di dati biometrici e all'adozione di strumenti alternativi di rilevazione per i lavoratori impossibilitati, per ragioni fisiche, a registrare le presenze mediante l'impiego del sistema biometrico, non hanno trovato conferma nell'informativa predisposta, secondo la quale il conferimento dei dati, ivi compresi i dati biometrici, avrebbe avuto natura obbligatoria.

Un diverso caso ha riguardato una società fornitrice di tecnologie per la difesa nel settore avionico ed elettronico, che ha presentato all'Autorità una richiesta di verifica preliminare relativa al trattamento di dati biometrici di un numero ristretto di dipendenti al fine di controllarne gli accessi ad un'area aziendale circoscritta. L'impiego delle impronte digitali dei lavoratori interessati era reputato dalla società necessario per identificare in modo certo i soggetti abilitati all'accesso in un'area riservata, nella quale veniva sviluppato un particolare programma avionico rilevante nel settore della difesa, per la cui realizzazione è richiesto un ambiente conforme a *standard* di sicurezza specifici ed elevati richiesti dalla Nato.

Il sistema proposto, basato sulla raccolta di impronte digitali mediante apparecchiature dotate di lettore di impronte digitali e di un apposito *software*, prevedeva che i dati venissero trasformati in un codice numerico (*template*) utilizzato esclusivamente per la raccolta e il successivo trattamento ai fini predetti.

Il trattamento di dati oggetto di verifica preliminare è stato ritenuto lecito alla luce delle specifiche finalità perseguite nel contesto esaminato, degli accorgimenti già adottati dalla società e di talune misure prescritte dal Garante in relazione alle concrete modalità di identificazione biometrica (*Provv.* 23 novembre 2005 [doc. *web* n. 1202254]). I dati trattati sono risultati pertinenti e non eccedenti rispetto alla finalità perseguita in quanto riferiti (non alla generalità dei dipendenti, ma soltanto) ad un numero ridotto di lavoratori (in possesso di nulla osta di sicurezza ed impiegati in attività che comportano la necessità di trattare informazioni rigorosamente riservate).

L'Autorità ha però prescritto alla società di predisporre un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il *template* memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità dei lavoratori interessati, senza creare un archivio centralizzato; ciò dotandosi, ove ritenuto opportuno al fine di identificare con maggiore certezza gli interessati, di un dispositivo idoneo a registrare nel sistema informativo aziendale dedicato all'archiviazione degli accessi all'area riservata altre informazioni personali (anche in forma di codice) necessarie ad identificare univocamente i lavoratori che vi accedono.

Ulteriori casi di impiego di tecniche di rilevazione biometriche nei luoghi di lavoro (attualmente al vaglio dell'Autorità) riguardano, da un lato, la verifica preliminare richiesta da tre società svolgenti attività industriale di carattere molitorio e che intendono porre in essere trattamenti finalizzati alla rilevazione delle presenze e al controllo accessi dei propri dipendenti basato sull'impiego delle loro impronte digitali; dall'altro, la sperimentazione di un sistema di riconoscimento facciale presso l'Aeroporto di Fiumicino "Leonardo da Vinci". A tale proposito, a seguito di segnalazioni provenienti da alcuni interessati, sono stati svolti accertamenti ispettivi che hanno evidenziato come il sistema sia stato installato in via sperimentale per soli 4 mesi presso un varco del *terminal* adibito al transito del personale di *staff*, utilizzato per accedere all'interno di aree sterili dell'aeroporto. I soggetti coinvolti nella sperimentazione (oltre 3.000 operatori aeroportuali) sono stati iscritti al programma su indicazione delle compagnie aeree e delle altre società interessate dalle quali dipendevano. Al fine di consentire la sperimentazione, la società di gestione dell'aeroporto ha messo a disposizione proprio personale addetto alle fasi di registrazione (*enrollment*) dei dati biometrici (avvenuta su *smart-card*, utilizzate come supporto per la memorizzazione della geometria del volto) e di controllo al varco di riconoscimento biometrico.

9.7. *Condomini*

Trattamento dei dati personali nell'amministrazione dei condomini

Il Garante, muovendo dalle problematiche rilevate dall'esame di segnalazioni e quesiti, tenendo conto di provvedimenti adottati in precedenza (in buona parte, in sede di decisione su ricorso) e in vista dell'adozione di un proprio provvedimento, ha avviato una consultazione pubblica in tema di trattamento dei dati nell'ambito delle attività connesse alla gestione dei condomini, chiedendo altresì alle associazioni di categoria interessate (in particolare, associazioni di condomini, amministratori condominiali e conduttori), agli operatori di settore e ai cittadini di far pervenire osservazioni (con riguardo ai profili relativi alla tipologia di dati trattati, alla loro circolazione all'interno del condominio e all'esercizio del diritto d'accesso), e

invitando le medesime associazioni a tenere conto delle considerazioni, di natura generale, idonee a compendiare i precedenti orientamenti sul punto, contenute in un documento di sintesi a tal fine reso disponibile sul sito *web* del Garante.

Sono pervenute all'Autorità 75 comunicazioni di contenuto eterogeneo (richieste di chiarimenti, segnalazioni, quesiti, osservazioni), unitamente a quelle inviate dalle associazioni di categoria.

Tali comunicazioni hanno preso prevalentemente in considerazione i seguenti profili:

- la questione della titolarità del trattamento nell'ambito della gestione condominiale;
- la tipologia dei dati trattati (in particolare, dall'amministratore nello svolgimento del proprio ufficio), tra i quali vengono indicati:
  - i dati inerenti al condominio complessivamente inteso quale ente di gestione (ad esempio, rispetto al conto corrente condominiale, ai contratti per la fornitura di beni e somministrazione di servizi; dati sul consumo ed importi di utenze complessivamente intestate al condominio);
  - i dati personali dei singoli partecipanti al condominio, nei limiti delle informazioni personali raccolte ed utilizzate per le finalità riconducibili alla disciplina civilistica (informazioni relative ai dati anagrafici e ai recapiti degli altri condomini, quote millesimali attribuite a ciascuno di essi, altre informazioni utili a determinare i diritti o gli oneri dei singoli condomini in relazione alle aree comuni);
- il trattamento dei dati relativi a soggetti diversi dai partecipanti al condominio (inquilini, coabitanti e conduttori);
- la circolazione in varie forme, verso terzi, di dati relativi alla gestione condominiale: a) partecipazione all'assemblea da parte di tecnici e professionisti; b) deleghe di voto in assemblea; c) dati conoscibili dal conduttore (anche mediante invio del verbale di assemblea); d) diffusione dei dati (affissione dati personali in bacheche condominiali);
- le problematiche afferenti alle misure di sicurezza;
- trattamento dati personali, sensibili e giudiziari, relativi al rapporto di lavoro con dipendenti e alla disciplina sull'abbattimento delle barriere architettoniche (l. n. 13/1989);
- la gestione della documentazione sanitaria per infortuni in aree condominiali.

10 Libere professioni

10.1. *Attività forense. Ordini e collegi professionali*

Nell'ottica del rafforzamento dell'attenzione del Garante e dell'incidenza della sua azione nel mondo delle libere professioni, con particolare riferimento all'attività forense, e nel variegato ambito di operatività dei concessionari di pubblici servizi, l'Autorità ha istituito con deliberazione del 15 dicembre 2005 un'apposita unità organizzativa di primo livello denominata "Unità attività forense, ordini professionali e pubblici servizi", con decorrenza operativa dal 1° gennaio 2006. A tale unità è stato assegnato il compito di curare l'applicazione del Codice rispetto ai trattamenti di dati personali relativi all'attività degli ordini professionali e all'attività forense, nonché a quelli inerenti ai concessionari di pubblici servizi.

Tra i primi obiettivi che l'Autorità intende raggiungere in proposito a partire dal 2006 vi è quello di riavviare i lavori del codice di deontologia e buona condotta previsto dall'art. 135 del Codice, relativo ai trattamenti di dati personali effettuati da investigatori privati e liberi professionisti, in relazione ad investigazioni difensive e a trattamenti effettuati per far valere o difendere un diritto in giudizio.

11 Concessionari di pubblici servizi

11.1. *Servizi di riscossione tributi*

Dichiarazione stragiudiziale

Negli anni passati, intervenendo a seguito di numerosi quesiti, segnalazioni e ricorsi, l'Autorità aveva giudicato illecita la prassi, propria di alcune società concessionarie del servizio per la riscossione dei tributi, consistente nel richiedere a terzi informazioni personali sul contribuente, in modo da ottenere dichiarazioni stragiudiziali attestanti l'esistenza di crediti del contribuente su cui rivalersi; ciò, in quanto nessuna previsione legislativa o regolamentare attribuiva alle società concessionarie il potere di effettuare questo tipo di trattamento.

La legge finanziaria 2005 ha introdotto, in materia, l'istituto della "dichiarazione stragiudiziale" (art. 1, comma 425, l. n. 311/2004), sulla base della quale il concessionario del servizio di riscossione dei tributi risulta ora legittimato a chiedere ai debitori del soggetto iscritto a ruolo di indicare, per iscritto, le cose e le somme da essi dovute allo stesso soggetto, anche solo in modo generico. Nel più volte richiamato *provvedimento* del 25 maggio 2005 [doc. *web* n. 1131826], il Garante ha affermato al riguardo la necessità di verificare il rispetto del principio di pertinenza e non eccedenza e di assicurare che la competente amministrazione impartisca ai concessionari idonee istruzioni, a norma di legge, per i casi in cui si ritenga di dover ricorrere a tale strumento, prevedendo che il concessionario –oltre ad informare l'interessato sul trattamento dei dati– fornisca allo stesso una comunicazione preventiva della possibilità che, in caso di mancato pagamento, verrà acquisita una dichiarazione stragiudiziale prima di procedere al pignoramento presso terzi, utilizzando tale strumento solo dopo aver documentato l'impossibilità di procedere altrimenti alla riscossione del credito. Dovrà essere altresì verificato su base casistica, anche in relazione all'importo dovuto, se le cose e le somme dovute dai debitori del soggetto iscritto a ruolo debbano essere indicate dal terzo in modo generico oppure puntuale, indicando chiaramente nella richiesta il dettaglio delle informazioni richieste e la facoltatività o meno della risposta.

Relativamente a questo aspetto sarà peraltro necessario prendere in considerazione la riforma in materia di servizio nazionale della riscossione introdotta dalla legge finanziaria per il 2006 (l. n. 266/2005, in *G.U.* 29 dicembre 2005, n. 302, *S.O.* n. 211), che ha previsto la costituzione, da parte dell'Agenzia delle entrate e dell'Inps, della società Riscossione S.p.A.

Tarsu

L'Autorità è intervenuta, a seguito di una segnalazione, per valutare la liceità del trattamento di dati personali previsto ai fini del controllo del pagamento della tassa sui rifiuti solidi urbani (Tarsu). Al riguardo, il Garante ha osservato che la normativa di settore riconosce ai comuni, al fine di accertare e controllare il pagamento della citata tassa, la possibilità di invitare direttamente il contribuente ad esibire o trasmettere atti e documenti e di inviare questionari relativi a dati e notizie di carattere specifico, con invito a restituirli compilati e firmati (art. 11, comma 3, d.lg. 30 dicembre 1992, n. 504; art. 73, comma 1, d.lg. 15 novembre 1993, n. 507). Per lo svolgimento di tale attività, i comuni possono peraltro avvalersi legittimamente, in conformità alle disposizioni in materia di protezione dei dati personali, della collaborazione di soggetti privati (*Nota* 6 dicembre 2005).

12 Rapporto di lavoro e previdenza

12.1. *Rapporti di lavoro in ambito pubblico*

Accesso ai dati personali in ambito lavorativo

L'Autorità è intervenuta in numerose occasioni rispetto all'esercizio del diritto di accesso dei lavoratori ai propri dati personali.

Nell'esaminare due ricorsi concernenti richieste volte a conoscere i dati personali conservati in qualsiasi forma dal datore di lavoro, il Garante ha nuovamente precisato che l'esercizio del diritto di accesso consente all'interessato di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione in forma intelligibile dei dati personali detenuti dal titolare del trattamento; non permette, invece, l'accesso diretto e indiscriminato a documenti ed intere tipologie di atti, ovvero la creazione di documenti inesistenti negli archivi, oppure la loro aggregazione innovativa secondo specifiche modalità prospettate dall'interessato o, ancora, di ottenere, sempre e necessariamente, copia (fotostatica o autenticata) dei documenti detenuti (*Provv.* 16 giugno 2005 [doc. *web* n. 1149999]).

Nel fornire riscontro alla richiesta, il titolare del trattamento deve comunicare solo i dati personali richiesti ed effettivamente detenuti e non è tenuto, invece, a ricercare o raccogliere altri dati che, seppure originariamente trattati, non siano nella propria disponibilità e non siano oggetto in alcuna forma di un attuale trattamento.

In particolare, in uno dei casi sottoposti all'esame del Garante (*Provv.* 21 dicembre 2005 [doc. *web* n. 1217532]), concernente il riscontro a varie istanze di accesso rivolte da una dipendente all'azienda ospedaliera di appartenenza, si è evidenziato che tale riscontro non può avere ad oggetto i dati relativi a terzi, anche di natura sensibile, contenuti nelle richieste di diagnosi e cura sottoscritte dalla ricorrente. Il riscontro può riguardare legittimamente i dati relativi all'interessata consistenti nel suo nome e cognome, nei casi in cui nelle medesime richieste figuri (o vi sia associata) una sottoscrizione intelligibile di quest'ultima, ma non obbliga comunque il titolare del trattamento a fornire copia di tutti i supporti cartacei che li contengano, né tanto meno ad indicare quali e quanti siano tali documenti nel caso in cui i dati siano estrapolati e comunicati nei modi previsti dal Codice (art. 10, comma 4).

Valutazione dei dirigenti

In risposta ad un quesito presentato da un dirigente statale, cui l'amministrazione di appartenenza aveva negato l'accesso ai documenti concernenti la valutazione dei propri colleghi, effettuata ai fini dell'assegnazione del premio di risultato, è stato ribadito che le informazioni di tipo valutativo, ivi compresi i giudizi, le valutazioni e gli altri elementi sui quali si basi eventualmente il giudizio sintetico espresso in occasione della valutazione dei dirigenti, sono dati personali e, in quanto tali, soggetti alla disciplina del Codice (*v.* in particolare, l'art. 8, comma 4, del Codice). Per questo motivo, tali informazioni, ove detenute da una pubblica amministrazione, possono essere rese conoscibili a soggetti privati diversi dalla persona cui si riferiscono, soltanto in base ad una previsione legislativa o regolamentare (art. 19, comma 3, del Codice).

Le disposizioni sull'accesso ai documenti amministrativi, applicabili anche al procedimento di valutazione dei dirigenti per espressa indicazione dell'art. 1, comma 5, d.lg. 30 luglio 1999, n. 286, rappresentano peraltro un'idonea base normativa per la comunicazione a terzi dei dati personali, eventualmente contenuti negli atti cui è rivolta l'istanza di accesso. In questo caso, spetta all'amministrazione destinataria del-

l'istanza di accesso verificare, di volta in volta, l'accoglibilità, o meno, di singole istanze di accesso alla documentazione valutativa, appurando i presupposti legittimanti l'accesso del richiedente, nonché le ragioni in base alle quali tali documenti debbano essere sottratti alla sua conoscibilità (*Nota* 7 febbraio 2005).

Tutela della dignità e riservatezza dei dipendenti

A seguito di una segnalazione il Garante è intervenuto a tutela della dignità e della riservatezza di una lavoratrice i cui dati personali, riguardanti la sua inidoneità al servizio dichiarata da "una commissione medica", erano stati riportati su alcuni atti interni concernenti lo svolgimento di una riunione svoltasi tra alcuni dipendenti, e successivamente affissi all'albo dell'ufficio.

Al riguardo, è stato accertato che le informazioni riportate nel materiale affisso, pur non fornendo alcuna specifica indicazione sui motivi di salute ritenuti all'origine dell'inidoneità della lavoratrice, facevano indirettamente riferimento alle condizioni di salute dell'interessata ed erano perciò da ritenersi "sensibili", in quanto il riscontro dell'inidoneità al servizio era derivato dal pronunciamento di una commissione medica, del quale negli atti affissi si faceva espressa menzione.

L'Autorità ha inoltre rilevato che, nel caso di specie, la diffusione non poteva ritenersi lecita, ponendosi in contrasto con i principi di proporzionalità, indispensabilità, pertinenza e non eccedenza, nonché con le cautele di cui all'art. 22 del Codice. In conformità a tali principi, l'esigenza di rendere noti ai colleghi non presenti alla riunione gli argomenti affrontati avrebbe potuto essere, infatti, utilmente soddisfatta mediante altre modalità di messa a disposizione delle informazioni, maggiormente rispettose della dignità e della riservatezza dell'interessata, come, ad esempio, la consegna in plico chiuso ai colleghi dei documenti affissi all'albo (*Nota* 23 novembre 2005).

Personale delle forze armate e di polizia

Con riferimento al trattamento di dati personali nell'ambito della gestione del personale delle forze armate e di polizia, l'Autorità ha esaminato due casi di opposizione al trattamento posto in essere dalla Guardia di finanza ai fini dell'accertamento della responsabilità disciplinare del personale.

In un primo caso, il Garante ha rilevato che, nell'ambito di tali attività, può essere lecitamente comunicata, ai superiori di un finanziere, la richiesta di archiviazione avanzata da un pubblico ministero in ordine ad una denuncia presentata dall'interessato nei confronti di altri componenti del Corpo, al fine di verificare eventuali violazioni delle disposizioni del regolamento di disciplina militare (in particolare, dell'art. 52, comma 5, lett. *b)*, d.P.R. n. 545/1986, il quale prevede che il militare sia tenuto a comunicare al proprio comando gli "*eventi in cui fosse rimasto coinvolto e che possono avere riflessi sul servizio*") ed avviare, se necessario, il procedimento di contestazione di una infrazione disciplinare (*Provv.* 28 settembre 2005 [doc. *web* n. 1180099]).

In un altro caso è stata ritenuta lecita la comunicazione alle superiori gerarchie del Corpo di vicende riguardanti l'interessato, che lo avevano indotto ad inoltrare una comunicazione di notizia di reato alle competenti autorità giudiziarie militari. Tali informazioni facevano infatti riferimento ad accadimenti di interesse, sia sotto il profilo amministrativo, sia, eventualmente, sotto quello disciplinare, verificatisi nella caserma presso cui l'interessato prestava servizio; non costituivano, nella specie, una violazione delle disposizioni sul segreto nelle indagini preliminari (art. 329 c.p.p.), dal momento che non contenevano alcun riferimento ad atti di indagine (*Provv.* 3 novembre 2005 [doc. *web* n. 1198494]).

Immigrazione

Per quanto riguarda l'attività connessa con l'ingresso e la regolarizzazione dei cittadini extracomunitari, il Garante è intervenuto in riferimento alla predisposizione della modulistica utilizzata per le esigenze dello Sportello unico per l'immigrazione. Il Ministero dell'interno ha chiesto infatti il parere all'Autorità in merito ad un

decreto relativo alla modulistica necessaria al rilascio di provvedimenti di nulla osta in materia di assunzione di lavoratori stranieri o di ricongiungimento familiare.

Il Garante ha evidenziato la necessità di perfezionare l'informativa da rendere all'interessato e di individuare correttamente il titolare di trattamento; è stata inoltre richiamata l'esigenza di rispettare i principi di necessità, pertinenza e non eccedenza nel trattamento dei dati raccolti con la modulistica rispetto alle finalità perseguite, con particolare riguardo ai dati idonei a rivelare lo stato di salute del datore di lavoro in caso di lavoro domestico per assistenza (*Provv.* 25 maggio 2005 [doc. *web* n. 1131847]).

12.2. *Previdenza*

Trasmissione telematica dei certificati di malattia all'Inps

La legge finanziaria 2005 ha stabilito che, a decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante debba trasmettere all'Inps, per via telematica, il certificato di diagnosi sull'inizio e sulla durata presunta della malattia. La definizione delle specifiche tecniche e delle modalità procedurali è demandata ad un apposito decreto interministeriale di iniziativa del Ministero del lavoro e della previdenza sociale (art. 1, comma 149, l. n. 311/2004). Con il più volte richiamato *provvedimento* del 25 maggio 2005 il Garante –che dovrà essere comunque chiamato ad esprimere un parere su tale decreto– ha richiesto preventivamente che vengano individuate in tale sede soluzioni efficaci e rispettose dei principi in materia di protezione dei dati personali.

Accesso dei patronati a banche dati previdenziali

Su specifica richiesta dell'Inps, l'Autorità ha inoltre esaminato uno schema di protocollo volto a consentire ai patronati la consultazione delle posizioni relative agli assicurati contenute nelle banche dati dell'istituto previdenziale e, in particolare, nel Casellario centrale delle posizioni previdenziali (l. 23 agosto 2004, n. 243; d.m. 4 febbraio 2005, in *G.U.* 29 marzo 2005, n. 72).

Le modalità previste nello schema di protocollo sono state ritenute, allo stato, conformi alle disposizioni in materia di protezione dei dati personali, in attesa che vengano stabilite con decreto del Ministro del lavoro e delle politiche sociali le linee-guida per apposite convenzioni da stipularsi tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni, e ferme restando le possibili indicazioni che il Garante potrà impartire nel parere previsto sul medesimo decreto. Il protocollo prevede infatti che i patronati possano accedere alle banche dati dell'istituto, ma nell'ambito del mandato conferito dall'interessato e sulla base del consenso manifestato in relazione a tipi di dati individuati specificamente (art. 116 del Codice).

La circostanza che le disposizioni sul Casellario centrale delle posizioni previdenziali non menzionino espressamente i patronati tra i soggetti legittimati ad accedervi non è stata, peraltro, ritenuta ostativa della possibilità di consentire ai patronati stessi la consultazione delle informazioni contenute nella banca dati, nella misura in cui ciò avvenga alle condizioni e per le sole finalità previste dall'art. 116 del Codice (*Nota* 8 febbraio 2006).

Informativa rilasciata agli assistiti da istituti di patronato

L'Ufficio del Garante ha fornito altresì la propria collaborazione per l'elaborazione, su iniziativa di un gruppo di rappresentanti di alcuni istituti di patronato e di assistenza sociale, di un modello di informativa da fornire agli interessati che decidano di farsi assistere e rappresentare da tali enti nello svolgimento di pratiche relative a prestazioni in materia di previdenza, assistenza sociale e sanitaria.

Prestazioni sociali agevolate

A seguito della segnalazione inoltrata da un'associazione, l'Ufficio si è pronunciato circa il trattamento di dati personali effettuato da un istituto previdenziale, ai fini del riconoscimento di prestazioni sociali agevolate nei confronti di soggetti con

handicap permanente grave e di soggetti ultra-sessantacinquenni non autosufficienti. La normativa di settore demanda ad un apposito decreto del Presidente del Consiglio dei ministri l'individuazione delle informazioni da dichiarare, in modo da evidenziare la situazione economica del solo assistito (art. 3, comma 2-*ter*, d.lg. n. 109/1998). Pur nella persistente mancanza di tale decreto attuativo, su cui l'Autorità dovrà essere chiamata ad esprimere il proprio parere, si è ritenuto che il rispetto dei principi di indispensabilità, pertinenza e non eccedenza dei dati raccolti rispetto alle finalità perseguite, imponga all'istituto di raccogliere soltanto le informazioni personali relative alla situazione economica degli interessati, e non anche quelle relative ai componenti del nucleo familiare di appartenenza (*Nota* 24 marzo 2006).

Incaricati del trattamento di dati previdenziali

L'Autorità è intervenuta in un caso riguardante il trattamento di dati personali relativi all'estratto della posizione contributiva dell'interessato, acquisiti presso gli archivi di un istituto previdenziale e successivamente utilizzati dal coniuge –dipendente di una sede provinciale del medesimo istituto– nel giudizio di separazione legale. In seguito alle lamentele dell'interessato, l'istituto aveva, nel frattempo, oscurato la sua posizione contributiva in modo da evitare ulteriori accessi non autorizzati.

L'Ufficio ha rilevato che spetta all'istituto impartire adeguate istruzioni ai propri dipendenti in merito all'accesso e all'utilizzo delle informazioni da essi conoscibili ed assicurare la corretta applicazione della disciplina sulla protezione e sulla sicurezza dei dati, anche in riferimento a possibili trattamenti illeciti o non conformi alle finalità della raccolta, ascrivibili anche alla condotta di singoli dipendenti (artt. 31-36 del Codice). La sede interessata è stata pertanto invitata a far conoscere le iniziative e gli accorgimenti assunti per rendere il trattamento conforme alle disposizioni sulla sicurezza e per ripristinare, nei casi e nei modi consentiti, l'accesso dell'interessato ai dati personali relativi alla sua posizione contributiva.

Quanto all'utilizzo dei dati dell'interessato nel giudizio di separazione legale è stato precisato che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nei procedimenti giudiziari basati sul trattamento, e quindi anche sulla eventuale raccolta illecita di dati personali, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (art. 11, comma 2, e 160, comma 6, del Codice) (*Nota* 11 novembre 2005).

13 Videosorveglianza

Anche nel corso del 2005, il Garante ha avuto occasione di occuparsi delle tematiche relative all'impianto ed all'utilizzo di sistemi di videosorveglianza.

Abitazioni private

Con riferimento all'installazione di impianti di videosorveglianza presso abitazioni, è stato nuovamente ribadito in una decisione adottata su ricorso che le disposizioni del Codice non risultano applicabili al trattamento di dati effettuato per fini personali, pur restando ferma l'osservanza degli obblighi in materia di sicurezza e di risarcimento dell'eventuale danno, nonché la facoltà dei soggetti che ritengono di aver subito un danno per effetto del trattamento dei dati di far valere i propri diritti in ordine alla liceità e correttezza della raccolta e dell'utilizzazione delle immagini (*Provv.* 27 ottobre 2005 [doc. *web* n. 1193121]).

13.1. *Videosorveglianza in ambito pubblico*

In relazione all'ambito pubblicistico molteplici segnalazioni e quesiti hanno evidenziato come, nonostante i ripetuti interventi del Garante, a due anni dall'adozione del *provvedimento* generale del 29 aprile 2004 [doc. *web* n. 1003482], lo stato di attuazione della disciplina in materia di videosorveglianza non risulti ancora del tutto soddisfacente, essendo emerse situazioni diffuse caratterizzate dall'omessa o inidonea applicazione delle regole fissate. Anche per questo, sono risultate numerose le occasioni per ribadire le indicazioni per un corretto utilizzo di telecamere da parte di soggetti pubblici in specifici settori.

Scuole

Con riferimento all'installazione di sistemi di videosorveglianza presso istituti scolastici l'Autorità ha riaffermato la vigenza delle prescrizioni fornite con il provvedimento generale. In ordine all'attivazione di telecamere all'interno dell'edificio di un istituto anche durante l'orario delle lezioni, è stata ad esempio rappresentata la necessità di limitarla ai casi di stretta indispensabilità, come ad esempio, a causa di ripetuti atti vandalici e comunque al di fuori dell'orario scolastico, quando gli edifici sono chiusi, anche in ragione del fatto che possono essere altrimenti raccolti indebitamente dati riguardanti minori di età e di lavoratori (*Nota* 26 aprile 2005). Nella predetta circostanza l'Ufficio ha invitato l'istituto a produrre ogni documento utile a sostegno delle iniziative assunte al fine di rendere il trattamento dei dati effettuato conforme al quadro di garanzie delineato nel provvedimento generale, ricevendo un riscontro sul quale sono in corso ulteriori accertamenti.

Telecamere mobili

In un diverso ambito il Garante ha fornito riscontro ad una richiesta pervenuta in merito all'utilizzo, da parte di alcuni comuni, di telecamere mobili installate su automezzi e posizionate temporaneamente in siti prestabiliti individuati di volta in volta in base a contingenti esigenze di sicurezza. In proposito, l'Autorità ha ribadito il necessario rispetto del principio di proporzionalità tra i mezzi impiegati e i fini perseguiti; in particolare, secondo tale principio, impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente ritenute insufficienti o inattuabili. Tale valutazione deve essere, poi, effettuata specificamente anche in riferimento alla dislocazione, all'angolo visuale e alle tipologie –fisse o mobili– delle apparecchiature installate. Anche per le telecamere di tipo mobile

restano valide le indicazioni specifiche relative all'installazione di sistemi di videosorveglianza presso, ad esempio, luoghi di culto o di sepoltura o per il controllo di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose (*Nota* 8 novembre 2005).

Presupposti per la videosorveglianza da parte dei comuni

In diverse occasioni sono stati forniti altri chiarimenti circa la possibilità, per i comuni, di attivare sistemi di videosorveglianza. In particolare è stato evidenziato che l'utilizzo di sistemi di videosorveglianza può essere giustificato solo ed esclusivamente dallo svolgimento di funzioni istituzionali che la stessa amministrazione è tenuta ad individuare ed esplicitare con esattezza e di cui essa sia effettivamente titolare in base all'ordinamento di riferimento (*Note* 16 e 22 febbraio 2005, 7 e 22 aprile 2005, 21 ottobre 2005 e 12 dicembre 2005).

È stata richiamata inoltre, in proposito, l'opportuna attenzione sul necessario rispetto di tutte le prescrizioni contenute nel *provvedimento* generale del 29 aprile 2004, ivi comprese la designazione dei responsabili o incaricati del trattamento, la predisposizione dell'informativa da rendere agli interessati (utilizzando eventualmente il modello semplificato messo a disposizione dal Garante in allegato al citato provvedimento) e l'adozione delle misure minime di sicurezza.

Discariche abusive e orario di deposito dei rifiuti urbani

Sono state nuovamente confermate le indicazioni già fornite a proposito dell'utilizzo di sistemi di videosorveglianza presso aree abusivamente impiegate come discariche di materiali, ricordando che tale utilizzo è lecito solo qualora risultino inefficaci o inattuabili altre misure; per converso, non risulta lecito un controllo video al solo scopo di accertare infrazioni amministrative rispetto a disposizioni concernenti le modalità e l'orario di deposito dei sacchetti dei rifiuti dentro gli appositi contenitori (*Note* 29 dicembre 2004 e 22 febbraio 2005). In un caso, a seguito della segnalazione pervenuta da un'associazione di risparmiatori e consumatori, l'Ufficio del Garante ha invitato a conformarsi alle citate prescrizioni un comune che intendeva "monitorare" le operazioni di smaltimento dei rifiuti per verificare il rispetto delle disposizioni sulla raccolta differenziata. L'ente locale ha comunicato di aver disattivato il sistema di registrazione e di aver cancellato tutte le immagini registrate (*cfr. Newsletter* 21-27 febbraio 2005).

Accesso ai centri storici e Ztl

L'Autorità è stata nuovamente interpellata in riferimento all'installazione di sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato. Si è confermato che i comuni devono richiedere una specifica autorizzazione amministrativa e limitare la rilevazione delle immagini ai soli casi di infrazione (art. 3 d.P.R. 22 giugno 1999, n. 250). I dati così trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e per definire il relativo contenzioso; alle informazioni si può accedere solo a fini di polizia giudiziaria o di indagine penale (*Note* 22 febbraio 2005).

Strutture sanitarie

Rigorose e specifiche cautele sono state richiamate anche in relazione all'attivazione di impianti di videosorveglianza in alcune aree di un *campus* ospedaliero e presso gli ingressi di una sede di un'azienda sanitaria (*Note* 22 febbraio 2005 e 12 aprile 2005). In particolare, nel rappresentare che l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria per finalità di sicurezza può evidenziare anche profili inerenti alle condizioni di salute dei pazienti, è stato confermato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (*ad es.*, unità di rianimazione) devono essere limitati a casi di stretta indispensabilità, circoscrivendo le riprese solo a determinati locali e a precise fasce orarie e adottando tutti gli accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate. Nelle stesse occasioni è stato fatto nuovamente presente che possono accedere alle immagini solo i soggetti specificamente autorizzati (*ad es.*, personale

medico ed infermieristico), non potendo le stesse essere visionate da estranei (*ad es.*, visitatori), e che le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale (artt. 22, comma 8, e 167 del Codice).

Luoghi di lavoro

Per quanto riguarda l'installazione di impianti video nei luoghi di lavoro è stato ricordato ad una prefettura e ad una direzione provinciale di un istituto previdenziale, come già rilevato in precedenti provvedimenti dell'Autorità, che detta installazione potrebbe coinvolgere anche i lavoratori dipendenti e configurare pertanto un controllo a distanza nei confronti dei lavoratori. A tale proposito è stata nuovamente richiamata l'attenzione sulle garanzie previste per i rapporti di lavoro anche quando gli impianti sono utilizzati per esigenze organizzative e dei processi produttivi, ovvero sono richiesti per la sicurezza del lavoro, con particolare riferimento al principio contenuto nell'art. 4 dello Statuto dei lavoratori che sancisce il divieto di controllo a distanza dell'attività dei lavoratori (*Note* 8 e 22 febbraio 2005). Non è stata invece rinvenuta lesiva del citato principio la condotta di un ente di ricerca che aveva installato alcune telecamere a tutela della sede di una segreteria ove veniva esplicata una delicata funzione di sicurezza (*Nota* 2 febbraio 2006).

Impianti sportivi

L'Autorità è stata chiamata a pronunciarsi anche a proposito dell'attivazione di sistemi di videosorveglianza presso impianti sportivi di capienza superiore alle diecimila unità, in occasione di competizioni calcistiche.

In particolare, il Garante ha espresso parere riguardo a due schemi di decreto, predisposti dal Ministero dell'interno in attuazione di un decreto-legge (n. 28/2003) che prevede, tra le misure contro la violenza negli stadi, oltre al rilascio di biglietti numerati, anche l'introduzione di telecamere fisse. Al riguardo, l'Autorità ha stabilito che il controllo svolto mediante videosorveglianza, basandosi su un idoneo fondamento normativo, risulta rispettoso del principio di liceità (art. 11, comma 1, lett. *a)*, del Codice) ed è altresì giustificato alla luce del principio di necessità e proporzionalità nel trattamento dei dati, anche in ragione dei reiterati disordini e degli episodi di violenza verificatisi. Sono state poi considerate, in termini generali, proporzionate, alcune disposizioni in materia di conservazione dei dati, di modalità di ripresa e di tipologia di informazioni rilevabili, risultando trattati dati pertinenti e non eccedenti rispetto alle finalità di tutela dell'ordine pubblico e della sicurezza e di accertamento di reati.

Il Garante ha chiesto di limitare l'ambito applicativo ai soli impianti sportivi di capienza superiore alle diecimila unità e ad eventi in occasione di competizioni calcistiche, derivando questi limiti direttamente dalla norma di legge, e di espungere riferimenti ad altri ambiti applicativi non previsti da tale norma (*Parere* 4 maggio 2005 [doc. *web* n. 1120732]).

Accanto a diverse altre indicazioni (deliminazione dell'ambito geografico di alcune riprese alle "immediate vicinanze degli impianti"; registrazioni audio del solo evento calcistico in generale; individuazione del soggetto che dovrebbe prescrivere misure di sicurezza; modalità di previsione dell'obbligo di porre dati e supporti a disposizione dell'autorità o della polizia giudiziaria), il Garante ha affrontato analiticamente la questione della previsione di biglietti nominativi di accesso agli stadi, aggiuntiva rispetto a quella dei biglietti numerati.

L'Autorità ha richiamato l'attenzione sulle misure di controllo di altro tipo introdotte in altri Paesi constatando che il decreto-legge introduce solo l'obbligo di numerare i biglietti e sollecitando quindi una verifica circa la possibilità di introdurre questo ulteriore vincolo con un provvedimento amministrativo. Rilevato poi che la nominatività dei biglietti comporta la creazione di grandi banche dati relative a diverse centinaia di migliaia di interessati, il Garante ha rilevato che a sostegno della richiesta di parere non erano stati allegati specifici elementi che potessero per-

mettergli di ritenere allo stato proporzionata "*una misura delicata di cui, a fronte degli innumerevoli dati personali che dovrebbero essere trattati, dovrà essere valutata attentamente la proporzione e l'effettiva utilità in rapporto alle finalità perseguite e alle più frequenti modalità con cui si svolgono incidenti negli stadi. Ciò, tenendo anche conto che potrebbero essere attivati altri controlli di sicurezza per identificare tifosi violenti ed escluderli dagli stadi...valutando infine la circostanza che i biglietti nominativi non risultano utilizzati diffusamente in altri Paesi dell'Unione europea (a parte i titoli di abbonamento, rilasciati per altre finalità*".

Sulla videosorveglianza in generale, allo scopo di verificare la conformità alle indicazioni contenute nel provvedimento generale sulla videosorveglianza, è stata sviluppata un'intensa attività ispettiva che ha evidenziato in più occasioni un rispetto non ancora rigoroso della disciplina, con particolare riferimento alla liceità dei sistemi installati, all'idoneità della necessaria informativa all'utenza, alle modalità di raccolta dei dati e ai tempi di conservazione delle immagini raccolte.

13.1.1. *Richieste di verifica preliminare*

In casi frequenti, il riscontro alle richieste di chiarimenti in materia di videosorveglianza ha fornito al Garante l'occasione per precisare che l'installazione di sistemi di videosorveglianza non deve essere generalmente sottoposta all'esame preventivo dell'Autorità e che non può per converso desumersi, dal mancato riscontro, alcuna approvazione implicita dalla trasmissione al Garante di comunicazioni o progetti relativi alla intenzione di installare sistemi di videosorveglianza. Non è del resto stabilito alcun termine decorso il quale i progetti sottoposti alla verifica dell'Autorità possano ritenersi dalla stessa autorizzati, non applicandosi neanche il principio del silenzio-assenso; deve ritenersi, invece, che il *provvedimento* 29 aprile 2004 abbia individuato espressamente le specifiche ipotesi in cui i titolari del trattamento sono tenuti a sottoporre alla verifica preliminare i sistemi di videosorveglianza che si intendono attivare.

14 Altre iniziative nel settore pubblico

14.1. *Utilizzo di dati biometrici*

In ambito pubblico sono pervenute numerose segnalazioni, nonché specifiche richieste di parere da parte di comuni, in merito all'utilizzo di sistemi di rilevazione automatica delle presenze mediante il riconoscimento delle impronte digitali. L'Autorità ha avviato nuove istruttorie in merito alla liceità dell'utilizzo di tali sistemi per il controllo dell'accesso al luogo di lavoro da parte dei dipendenti.

14.2. *Ulteriori iniziative dell'Ufficio*

Progetto *"Dove siamo nel mondo"*

L'Unità di crisi del Ministero degli affari esteri ha sottoposto all'esame del Garante un progetto denominato "*Dove siamo nel mondo*" per una valutazione preliminare in ordine alla sua compatibilità con la normativa in materia di protezione dei dati personali. Il progetto, nell'ambito dell'ottimizzazione della gestione di situazioni di crisi internazionali legate a calamità naturali, attentati terroristici ed altre emergenze, è volto a consentire ai cittadini italiani di segnalare al Ministero degli esteri, su base volontaria, i propri recapiti ed itinerari, al fine di facilitare la localizzazione, l'invio di eventuali avvisi o l'intervento di soccorso in caso di emergenze.

L'Ufficio del Garante ha indicato al Ministero le necessarie cautele da adottare nella realizzazione del progetto, con particolare riferimento alle tipologie di dati richiesti, alla loro gestione e conservazione, nonché all'informativa da fornire all'interessato e all'eventuale coinvolgimento di terzi.

La versione definitiva del progetto prevede la creazione di un apposito sito Internet attraverso il quale i cittadini, previa idonea informativa, possono inserire su base volontaria le proprie generalità ed informazioni sul viaggio (*ad es.*, paese di destinazione, date di partenza e di rientro, località di permanenza, dettagli dell'itinerario e recapiti); i dati registrati saranno automaticamente cancellati trascorse quarantotto ore dalla data di rientro. Il titolare del trattamento è il Ministero degli esteri e la banca dati è gestita unicamente dall'Unità di crisi. I dati raccolti sono utilizzati esclusivamente per lo studio e la realizzazione di piani di intervento per la sicurezza degli italiani all'estero in situazioni di crisi e potranno essere comunicati a determinati soggetti terzi al solo fine di assicurare assistenza in caso di emergenza.

15 Reti di comunicazione elettronica

15.1. *Conservazione dei dati di traffico*

Successivamente alle già ricordate modifiche apportate all'art. 132 del Codice dall'art. 3 del d.l. 24 dicembre 2003, n. 354, convertito, con modificazioni, dalla l. 26 febbraio 2004, n. 45 (*v. Relazione* 2004, p. 97), si è assistito, nel 2005, ad un nuovo, significativo intervento normativo, che ha ulteriormente innovato la disciplina della conservazione dei dati di traffico per finalità di accertamento e repressione dei reati (sul quale *v.* par. 1.1).

In tale contesto, il Garante, che aveva già avviato, conformemente alla previsione dell'art. 132, comma 5, del Codice, i lavori necessari per individuare le misure e gli accorgimenti al cui rispetto è subordinato il trattamento per le richiamate finalità di accertamento e repressione dei reati, ha esteso al traffico telematico l'ambito di verifica preliminare dei sistemi attualmente utilizzati dagli operatori, in vista della programmata predisposizione del provvedimento previsto dalla predetta disposizione.

15.2. *I nuovi elenchi telefonici*

Nella *Relazione* 2004 (p. 99) si era dato conto del provvedimento di carattere generale con il quale il Garante, ai sensi dell'art. 129, comma 2, del Codice, nonché in ragione delle modifiche introdotte nella disciplina degli elenchi telefonici, aveva individuato le modalità da osservare per il corretto inserimento e successivo utilizzo dei dati personali relativi ad abbonati (e utilizzatori di schede prepagate) nei nuovi elenchi telefonici (*cfr. Provv.* 15 luglio 2004 [doc. *web* n. 1032381]).

Successivamente all'adozione del provvedimento il Garante ha fornito agli operatori prescrizioni integrative con riferimento ai moduli per l'informativa e la raccolta dei consensi predisposti dagli operatori, ed ha avviato altresì la campagna informativa prevista nel provvedimento stesso. L'Autorità ha, inoltre, avviato direttamente una prima campagna di informazione con un apposito *depliant* messo a disposizione degli operatori e attraverso una conferenza stampa tenutasi presso la sede dell'Autorità il 26 gennaio 2005.

Nel 2005 il Garante ha monitorato con attenzione, anche tramite varie richieste di informazioni agli operatori, il rispetto delle scadenze per l'attuazione della nuova disciplina indicate nel ricordato *provvedimento* del 15 luglio 2004 (*cfr.* l'allegato III del provvedimento).

L'Ufficio, anche in risposta ad alcuni quesiti pervenuti in tema di utilizzabilità dei dati presenti nei nuovi elenchi telefonici da parte di soggetti operanti per finalità non di lucro, ha specificato che la nuova disciplina degli elenchi opera a prescindere dall'eventuale fine di profitto perseguito. Pertanto, ogni uso dei dati presenti nei nuovi elenchi diverso dalla comunicazione interpersonale, quali ad esempio le attività di carattere pubblicitario e promozionale, resta possibile solo con il consenso preventivo degli interessati. Il Garante ha altresì evidenziato come gli enti che perseguono finalità di carattere socio-assistenziale o di interesse collettivo o diffuso continuino, in ogni caso, a disporre di altre modalità per il reperimento dei dati perso-

nali dei potenziali sostenitori, in particolare tramite l'accesso alle liste elettorali (*cfr.* art. 51, d.P.R. n. 223/1967, come modificato dall'art. 177 del Codice).

È stato inoltre rilevato che la nuova disciplina può non operare con riguardo ai dati personali estratti precedentemente dai vecchi elenchi e già effettivamente (e non elusivamente) registrati sempre in precedenza in una banca dati, eventualmente inseriti insieme ad altre informazioni tratte da ulteriori fonti. L'utilizzazione di questi dati è lecita solo se, al momento della loro registrazione, è stata fornita un'idonea informativa agli interessati, instaurando così con gli stessi un "rapporto" nell'ambito del quale il titolare del trattamento è rimasto comunque obbligato a cancellare i dati di chi lo richieda. Se, però, la predetta informativa non è stata resa tempestivamente a norma di legge, il trattamento è stato ed è rimasto illecito; il titolare non può in alcun modo utilizzare i dati e deve necessariamente cancellarli per non incorrere in serie sanzioni. Per quanto concerne il necessario aggiornamento delle informazioni contenute nelle menzionate banche dati, è stato ribadito che lo stesso potrà avvenire soltanto sulla base delle nuove regole sull'uso degli elenchi telefonici.

15.3. *Elenchi telefonici* cd. *"categorici"*

Nel periodo di riferimento, il Garante ha valutato l'opportunità di intervenire in riferimento alla problematica degli elenchi telefonici organizzati per categorie merceologiche/professionali (*cd.* elenchi "categorici"). Tenendo conto del carattere commerciale e promozionale dei menzionati elenchi "categorici", che contengono informazioni relative allo svolgimento delle attività economiche ed equiparate dei soggetti interessati (in particolare aziende, professionisti, esercizi commerciali ed enti), nonché delle specifiche finalità degli stessi non riconducibili esclusivamente alla *"mera ricerca dell'abbonato per comunicazioni interpersonali"*, il Garante ha individuato a favore degli editori di tali elenchi un particolare regime di semplificazione (*Provv.* 14 luglio 2005 [doc. *web* n. 1151640]).

Si è infatti chiarito che, per la formazione degli elenchi in questione, gli editori possono avvalersi della previsione del Codice che permette di prescindere dal consenso degli interessati quando il trattamento riguarda appunto "dati relativi allo svolgimento di attività economiche" (art. 24, comma 1, lett. *d)*, del Codice). Devono essere comunque rispettati gli altri obblighi e diritti in materia di protezione dei dati personali: in particolare, deve essere garantita la completezza dei nominativi degli interessati riportati nelle diverse tipologie di elenchi pubblicati e, nel caso in cui i dati siano attinti dal nuovo "*database* unico", di cui all'allegato II del predetto *provvedimento* del 15 luglio 2004, non possono essere pubblicati gli estremi identificativi di coloro che abbiano eventualmente manifestato la volontà di non comparire negli elenchi telefonici "alfabetici".

L'Autorità, infine, ai sensi dell'art. 13, commi 4 e 5, lett. *c)*, del Codice, ha autorizzato i suddetti titolari del trattamento a fornire a professionisti, esercenti, aziende ecc., che compariranno nell'elenco, un'informativa semplificata tramite la pubblicazione di appositi avvisi su quotidiani, nonché nella parte iniziale dell'elenco "categorico" cartaceo e di quello pubblicato *on-line*.

15.4. Spamming

Anche nel corso del 2005 si è mantenuta elevata l'attenzione dell'Autorità rispetto alla pratica dello *spamming* (invio di messaggi promozionali indesiderati

all'indirizzo di posta elettronica dei destinatari). Sono state, fra l'altro, intensificate le attività di controllo e verifica delle attività svolte da diversi operatori che, direttamente o per mezzo di soggetti specializzati, svolgono campagne pubblicitarie e di *direct marketing* utilizzando tale nuovo mezzo di comunicazione. Risulta, poi, in fase conclusiva l'istruttoria già avviata nei confronti di due importanti società operanti *on-line*, che utilizzano migliaia di indirizzi di posta elettronica per finalità promozionali e commerciali di prodotti e servizi propri e di altre aziende.

Particolare preoccupazione ha destato, tra l'altro, l'incremento delle segnalazioni che lamentano l'invio di *e-mail* riconducibili al fenomeno denominato "*phishing*", consistente nell'uso di messaggi di posta elettronica e nella creazione di pagine *web* progettate per simulare comunicazioni ufficiali da parte soprattutto di istituti di credito, con la finalità di raggirare gli utenti Internet per carpire dati personali o acquisire fraudolentemente informazioni riguardanti la carta di credito o il conto corrente bancario.

In ambito internazionale, nel periodo considerato, l'Autorità ha partecipato attivamente ai lavori del Cnsa (*Contact Network of Spam Authorities*) che si tengono presso la Commissione europea-Direzione generale società dell'informazione e media. Nei vari incontri, cui partecipano le istituzioni di settore di tutti i Paesi membri, si è proceduto a valutare vari strumenti di intervento per intensificare la lotta allo *spam*. È in corso la predisposizione di un documento comune, denominato *London Action Plan*, che definirà le procedure utili a facilitare le indagini sullo *spam* anche attraverso la semplificazione delle modalità di contatto tra le istituzioni partecipanti.

Tra le attività di carattere internazionale finalizzate a contrastare il fenomeno dello *spam* va ricordata anche la *task force* istituita presso l'Ocse, ai cui lavori ha partecipato anche l'Autorità, e che ha redatto nel 2005 una bozza di raccomandazione sulla "cooperazione transfrontaliera nel rafforzamento delle leggi contro lo *spam*" (sul punto, *v.* par. 22.3).

15.5. *Videochiamate*

I nuovi servizi telefonici disponibili attraverso l'impiego di telefoni mobili definiti "di terza generazione", tramite diverse tecnologie di rete, quali *Gprs*, *Edge* o *Umts*, sono stati già oggetto di attenzione da parte dell'Autorità (*cfr. Relazione* 2004, pp. 100-101).

Rispetto al semplice utilizzo dei messaggi del tipo *Sms* e *Mms*, in ordine ai quali il Garante si è più volte pronunciato in passato, i "videotelefono" offrono nuove funzionalità. Questi apparecchi sono dotati di videocamere di dimensioni molto ridotte, orientabili in vario modo, e dispongono di diverse funzioni mediante le quali si possono agevolmente raccogliere, comunicare e diffondere immagini e suoni in tempo reale. Tali applicazioni, utili nell'ordinaria vita di relazione interpersonale, possono essere tuttavia utilizzate in modo da violare, anche involontariamente, i diritti delle persone interessate dalla comunicazione, come pure di terzi inconsapevoli della ripresa.

In ragione dei potenziali pericoli insiti nell'utilizzo di tali nuovi strumenti di telefonia, il Garante, all'esito di una consultazione pubblica attivata al fine di acquisire elementi di valutazione, ha individuato le modalità da osservare per un corretto utilizzo dei medesimi strumenti con riferimento al trattamento dei dati (*Provv.* 20 gennaio 2005 [doc. *web* n. 1089812]). In particolare, nell'evidenziare la generale liceità del loro utilizzo per fini esclusivamente personali, l'Autorità ha sottolineato che il Codice –ferme restando altre norme dell'ordinamento– non si applica se le

immagini rimangono nella disponibilità privata di chi ha effettuato le riprese o circolano solo tra un numero ristretto di persone. Si è indicata comunque la necessità che, anche in questi casi, il soggetto che utilizza l'apparecchio rispetti i diritti dei terzi anche in tema di diritto all'immagine eal ritratto, nonché gli obblighi previsti in materia di sicurezza dei dati, tenendo conto della possibilità di essere chiamati a risarcire eventuali danni anche morali cagionati a terzi.

È stata, poi, sottolineata l'illiceità di un'eventuale comunicazione sistematica attraverso il videotelefono o di una diffusione anche via Internet delle immagini, effettuata senza richiedere, quando è necessario, il consenso preventivo, libero e informato (manifestato per iscritto nel caso siano trattati dati sensibili). L'informativa ed il consenso possono riguardare in tal caso non solo i soggetti che si intende ritrarre direttamente, ma anche eventuali terzi, identificati o identificabili, eventualmente ripresi anch'essi nelle immagini.

Il Garante ha richiamato altresì l'attenzione sull'esigenza di verificare se, in determinati uffici pubblici, luoghi pubblici e privati o aperti la pubblico, l'uso dei videotelefoni sia eventualmente inibito: limiti e cautele (introdotti in alcuni Paesi anche con norme di legge) possono essere infatti prescritti legittimamente da soggetti pubblici e privati e, se non rispettati, possono rendere il trattamento dei dati illecito o non corretto. Garanzie analoghe sono state richiamate anche rispetto all'uso di immagini all'interno di forum *on-line*.

L'Autorità ha, infine, invitato imprese produttrici di apparecchi o impegnate nella realizzazione di *software* di valutare l'opportunità di dotare i cellulari di nuove funzioni, tra cui anche segnali luminosi, per rendere più evidente che il videotelefono è in funzione, come pure di sistemi per il blocco della trasmissione dell'immagine senza che venga interrotta la conversazione.

15.6. *Chiamate in entrata*

Il trattamento dei dati personali relativi alle comunicazioni telefoniche in entrata pone delicate implicazioni per la riservatezza delle persone cui gli stessi si riferiscono: oltre a riguardare gli abbonati o i titolari di una carta prepagata, le chiamate in entrata possono coinvolgere altri soggetti quali familiari, amici, membri di una comunità e dipendenti. Per questi motivi, relativamente a tali dati, il Codice non consente di regola agli interessati di rivolgere al fornitore di un servizio di comunicazione elettronica le istanze di cui all'art. 7. Solo in via di eccezione, le richieste di esercizio dei diritti possono essere presentate e riscontrate positivamente, qualora si comprovi che la risposta da parte del fornitore è necessaria per evitare "un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397" (art. 8, comma 2, lett. *f)*, del Codice).

In tale contesto generale, il Garante (intervenuto già in passato sull'argomento in occasione dell'esame di ricorsi e segnalazioni) ha ritenuto necessario richiamare l'attenzione degli operatori telefonici sui limiti entro i quali i fornitori dei servizi di comunicazione elettronica accessibili al pubblico possono rispondere positivamente ad una richiesta *ex* art. 7 del Codice, impartendo ad essi alcune prescrizioni con un apposito provvedimento di carattere generale (*Provv.* 3 novembre 2005 [doc. *web* n. 1189488]).

All'interno di quest'ultimo, è stato di nuovo posta in rilievo la disposizione codicistica che prevede che l'abbonato o il titolare di una carta prepagata possa conoscere i dati personali relativi al traffico telefonico in entrata, *Sms* ed *Mms* compresi, solo dimostrando l'indispensabilità dell'acquisizione di tali informazioni allo scopo

di tutelare i propri diritti in sede penale, in quanto la mancata conoscenza delle stesse determinerebbe un danno effettivo e concreto al diritto di difesa. I dati in tal modo conosciuti non possono essere utilizzati per altri scopi: a tal fine, il fornitore deve richiedere il rilascio di una dichiarazione, dall'interessato o dall'avvocato cui sia stato conferito mandato, che attesti la veridicità di quanto prospettato e manifesti l'impegno a non utilizzare i dati per altre finalità. Possono essere peraltro prese in considerazione solo le richieste corredate da una motivazione in cui sia specificata l'intenzione di utilizzare i dati nell'ambito di un procedimento penale, risultando pertanto escluse quelle riguardanti controversie civili e di volontaria giurisdizione.

È stato inoltre individuato in capo al fornitore del servizio l'obbligo di accertare con scrupolo l'identità e la legittimazione del richiedente, nonché quello di fornire un riscontro, seppur negativo, entro quindici giorni dal ricevimento dell'istanza. Non vi è, per converso, necessità di un'autorizzazione dell'autorità giudiziaria per comunicare i dati, né occorre che il richiedente documenti anche il numero di repertorio di un procedimento penale, in ragione del fatto che le indagini difensive possono essere avviate lecitamente anche prima di tale procedimento e per l'eventualità che esso sia instaurato (art. 391-*nonies* c.p.p.).

Sono stati infine specificati i dati che il fornitore potrà comunicare: si tratta del numero del chiamante, della data, dell'ora di inizio e della tipologia della comunicazione e della durata.

15.7. *Intercettazioni*

Nel mese di agosto del 2005, il Garante ha avviato un'indagine nei confronti dei principali gestori di telefonia fissa e mobile riguardo alle modalità con le quali essi adempiono alle richieste dell'autorità giudiziaria in materia di intercettazioni.

Gli accertamenti hanno messo in luce che i gestori, pur non venendo a conoscenza dei contenuti delle intercettazioni, raccolgono, selezionano, elaborano ed utilizzano una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali questi comunicano. Si tratta di dati personali particolarmente delicati che riguardano l'identità dei soggetti sottoposti ad intercettazione e l'arco temporale di svolgimento dell'intercettazione nonché i dati di traffico telefonico o telematico. In alcuni casi, tali dati sono integrati da informazioni aggiuntive relative alle chiamate in ingresso, ai tentativi di chiamata e alla localizzazione geografica dell'utenza intercettata.

È emerso, inoltre, che gli ulteriori servizi svolti dai fornitori a supporto dell'attività investigativa possono riguardare anche aspetti diversi dalle intercettazioni e comprendere interrogazioni anagrafiche, localizzazione dell'utenza, tracciamento e sospensione dei servizi agli utenti, documentazione del traffico storico. A differenza di quanto avviene con le conversazioni intercettate, i gestori hanno la possibilità di conoscere le informazioni derivanti dall'attivazione di questi servizi, essendo essi stessi ad estrarre i dati, a selezionarli secondo i criteri richiesti dall'autorità giudiziaria e ad organizzarli in tabulati. Infine, anche i servizi *Sms* ed *Mms* sono risultati compresi nell'attività di intercettazione.

All'esito dell'istruttoria e sulla base della documentazione pervenuta, l'Autorità ha prescritto ai gestori (*Provv.* 15 dicembre 2005 [doc. *web* n. 1203890]) di adottare alcuni accorgimenti e misure ulteriori nel proteggere i dati allorché adempiano alle menzionate richieste dell'autorità giudiziaria. Le misure riguardano sia gli aspetti organizzativi, sia la sicurezza dei flussi informativi diretti verso l'autorità giudiziaria, sia la protezione dei dati trattati a scopo di giustizia.

I diversi accorgimenti prescritti dal Garante ai fornitori (ai quali è stato assegnato un termine di centottanta giorni per l'adeguamento) riguardano in particolare: l'individuazione più selettiva del ristretto numero di incaricati designati a trattare i dati; la separazione tra i dati di carattere contabile e i dati documentali prodotti nel corso delle attività svolte su richiesta dell'autorità giudiziaria; l'adozione di procedure di autenticazione robuste per l'accesso informatico da parte del personale incaricato ai dati trattati, con il ricorso anche a caratteristiche biometriche; l'adozione di sistemi di comunicazione con l'autorità giudiziaria basati su aggiornati strumenti telematici e tecniche di firma digitale, evitando l'uso di sistemi meno sicuri (*ad es.*, il fax); la protezione dei dati, per il periodo di presenza nelle banche dati dei gestori, con strumenti avanzati di cifratura; la cancellazione immediata dei dati dopo la loro comunicazione all'autorità giudiziaria.

15.8. *Servizi telefonici non richiesti*

Anche nell'anno di riferimento sono pervenuti al Garante numerosi reclami, segnalazioni e quesiti con i quali sono state lamentate ripetute violazioni del diritto al corretto e lecito utilizzo dei dati personali nella prestazione di alcuni servizi di comunicazione elettronica da parte, oltre che dei fornitori di servizi, anche dei rivenditori dislocati sul territorio. In particolare sono state evidenziate violazioni connesse all'indebita attivazione di contratti, schede o servizi telefonici non richiesti dagli interessati; in alcuni casi, soggetti cui erano state intestate falsamente schede di telefonia mobile senza consenso si sono trovati addirittura coinvolti in indagini penali.

Le segnalazioni pervenute hanno riguardato anche ulteriori problematiche legate alla selezione automatica dell'operatore e all'attivazione di servizi non richiesti, tra i quali segreterie telefoniche e collegamenti Internet a banda larga.

L'ampia portata del fenomeno risulta, peraltro, anche dalla trattazione di diversi ricorsi presentati all'Autorità, la quale da tempo si occupa della tematica, avendo svolto negli anni passati (*v. Relazione* 2003, pp. 87 e 140), anche impegnativi accertamenti di carattere ispettivo.

Sulla base delle informazioni acquisite, anche in occasione di nuovi accertamenti ispettivi effettuati presso alcuni tra i maggiori operatori telefonici, il Garante ha effettuato un'apposita istruttoria al fine di intervenire sul fenomeno con un provvedimento di carattere generale volto ad individuare un quadro di garanzie che assicuri il rispetto dei diritti e delle libertà fondamentali dei cittadini.

Nel *provvedimento* adottato il 16 febbraio 2006 ([doc. *web* n. 1242592], in *G.U.* 6 marzo 2006, n. 54), il Garante ha quindi imposto agli operatori telefonici la predisposizione di procedure che consentano di rilevare tempestivamente le intestazioni multiple di schede telefoniche prepagate ad una medesima persona. In particolare, quando le intestazioni siano superiori a 4 (per le persone fisiche) e a 7 utenze (per le società) l'operatore dovrà chiederne espressa conferma all'intestatario. Resta vietato attivare servizi senza aver acquisito l'espresso consenso preventivo degli interessati; inoltre, le persone vanno contattate per finalità pubblicitarie o promozionali solo se hanno manifestato uno specifico e preventivo consenso a ricevere a tal fine chiamate e comunicazioni. Gli addetti ai *call center* devono, al momento del contatto, spiegare agli interessati da dove siano stati estratti i dati che li riguardano. Deve essere, inoltre, registrata immediatamente e rispettata la volontà di non ricevere il servizio, nonché l'eventuale contrarietà espressa in relazione all'uso dei dati.

Il Garante ha inoltre imposto ad operatori telefonici, di comunicazione elettronica e *call center* di verificare attentamente, anche attraverso controlli a campione,

l'attività di rivenditori e incaricati, allo scopo di rintracciare immediatamente chi materialmente abbia effettuato eventuali attivazioni indebite.

15.9. *Informativa con modalità diverse da quelle ordinarie*

Nel mese di dicembre dell'anno di riferimento l'Autorità ha ricevuto la richiesta di un operatore telefonico volta a consentire di informare gli interessati in modo diverso da quello ordinario ai sensi dell'art. 13 del Codice.

La richiesta riguardava un progetto di fusione per incorporazione (avvenuta poi nei primi mesi del 2006) tra la società istante ed un altro operatore, del quale la prima ha acquisito il complesso aziendale con tutti i rapporti giuridici attivi e passivi in atto, assumendo di conseguenza la qualità di titolare del trattamento dei dati personali dei relativi interessati. All'esito dell'istruttoria sono state individuate modalità di informazione sostitutive di quelle rivolte, caso per caso, a ciascun interessato, con particolare riguardo alle caratteristiche, anche comunicative, del contenuto dell'avviso da pubblicare sugli organi di stampa.

15.10. *Il codice deontologico*

La prossima definizione del codice deontologico per gli operatori Internet consentirà di introdurre, in un settore in continua evoluzione, specifiche garanzie al cui rispetto sarà subordinata la liceità e la correttezza dei diversi trattamenti di dati personali (art. 12, comma 3, del Codice). L'obiettivo principale è indicare soluzioni effettive, adeguate e dinamiche ad alcune questioni relative al trattamento dei dati personali *on-line* che possano, da un lato, sensibilizzare maggiormente gli utenti in rete sui rischi in materia correlati all'uso di Internet, offrendo loro ulteriori opportunità di tutela e, dall'altro, indicare ai diversi operatori interessati concreti strumenti per adempiere agli obblighi di legge (anche per quanto riguarda i principi di cui all'art. 11 del Codice) assicurando un più elevato livello di rispetto della normativa sulla protezione dei dati personali.

In questa prospettiva sono proseguiti nel 2005 gli incontri nel tavolo di lavoro composto dagli operatori del settore –rappresentati dalle relative organizzazioni di categoria– e dalle associazioni dei consumatori che hanno entrambi aderito all'invito a parteciparvi rivolto dall'Autorità.

In tale ambito sono state affrontate diverse esigenze fra le quali quelle relative: all'obbligo di informare adeguatamente gli utenti circa i possibili trattamenti, impliciti o espliciti, che possono riguardarli; al consenso da manifestare espressamente e liberamente; ai presupposti e ai limiti entro i quali è legittimo l'uso di marcatori o dispositivi analoghi *on-line*; alle modalità semplificate per esercitare i diritti di cui all'art. 7 del Codice; ai trattamenti che possono presentare rischi specifici per la sicurezza degli utenti in rete, come nel caso del *phishing*; allo *spamming*, con particolare riferimento alla possibilità di individuare misure di filtraggio a tutela degli interessati. Il gruppo di lavoro ha poi riscontrato l'opportunità di affrontare altri temi impegnativi quali quello del trattamento dati rispetto ai nomi a dominio, al diritto all'oblìo in rete e, quindi, alle garanzie rispetto ai motori di ricerca.

Alla luce dei vari contributi e delle riflessioni svolte, il tavolo redigerà una prima bozza di codice deontologico che sarà pubblicata sul sito Internet dell'Autorità per una consultazione pubblica. Sulla base delle osservazioni e proposte che perverranno, il tavolo apporterà le eventuali modifiche al testo che, sottoposto all'esame

dell'Autorità e da questa "certificato" in conformità alle procedure in tema di codici deontologici in fase di generale formalizzazione, verrà trasmesso al Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* e la sua allegazione al Codice sulla protezione dei dati personali.

15.11. *Motori di ricerca e diritto all'oblìo*

La problematica relativa al *cd.* "diritto all'oblìo", ossia il diritto ad "essere dimenticato" nella dimensione pubblica o, comunque, non più privata, precedentemente acquisita, presenta profili di particolare complessità laddove le informazioni personali che si intendano cancellare siano state diffuse in Internet. Inserendo nei motori di ricerca più comuni alcune parole chiave è infatti particolarmente agevole risalire in tempo reale ad un numero considerevole di informazioni di carattere personale riguardanti una stessa persona e riferite ad epoche assai diverse.

Questa efficiente profilazione generalizzata può porsi in conflitto con il diritto di un soggetto interessato a veder delimitata nel tempo la diffusione indifferenziata di molte informazioni che lo riguardano, che può non essere più giustificata alla luce delle finalità e delle circostanze originarie; ciò, senza considerare i casi nei quali le informazioni pubblicate risultino sin dall'inizio non corrette o, comunque, incomplete o non aggiornate.

In questo quadro diversi interessati contestano spesso la circostanza che le copie *cache* (e le relative sintesi) –attraverso le quali i motori di ricerca mettono a disposizione degli utenti le pagine *web* indicizzate contenenti le parole chiave utilizzate nelle ricerche– non riportano automaticamente le modifiche già intervenute nelle pagine *web* dei "siti sorgente", anche quando queste ultime siano state modificate o cancellate da diverso tempo. I motori di ricerca non procedono infatti ad una revisione automatica ed immediata dei propri indici a fronte della modifica dei siti richiamati, bensì effettuano aggiornamenti periodici degli stessi attraverso l'utilizzo di un *software* (*cd. crawler*).

Sul ruolo dei motori di ricerca, è stata pertanto avviata una specifica riflessione da parte dell'Autorità, anche alla luce dei numerosi ricorsi e segnalazioni pervenuti.

Fra questi ultimi merita menzione almeno un ricorso proposto nei confronti di Google Italy S.r.l.. In tale occasione, il Garante, con una decisione intervenuta poi di recente, ha infine riconosciuto in capo al motore di ricerca un'autonoma titolarità del trattamento, consistente nella creazione e nella conservazione di cosiddette copie *cache* di pagine *web* pubblicate sul sito sorgente. Tuttavia, non risultando provato che il trattamento contestato fosse effettuato da un soggetto stabilito sul territorio dello Stato, l'Autorità si è riservata di esaminare, nell'ambito di una distinta attività, le questioni relative alla tutelabilità dei diritti dell'interessata in rapporto a titolari situati all'estero (nella specie, Google Inc. avente sede negli Stati Uniti). A tal fine, è stata sollecitata una fattiva collaborazione con tale società, per individuare nel breve periodo soluzioni concrete che permettano di garantire pienamente sul territorio italiano i diritti e le libertà fondamentali degli interessati, anche quando gli strumenti utilizzati per il trattamento siano situati in Paesi non appartenenti all'Unione europea (*cfr. Comunicato stampa* 13 aprile 2006; sulla tematica, *v.* anche quanto riportato al par. 18.3).

15.12. *Televisione digitale: i servizi interattivi*

Nel 2005 l'Autorità ha adottato un provvedimento generale (*Provv.* 3 febbraio 2005 [doc. *web* n. 1109503]) con il quale ha prescritto ai fornitori dei servizi televisivi interattivi di adottare misure necessarie per conformare i loro trattamenti alle disposizioni in materia di protezione dei dati personali. Il provvedimento si è reso necessario per evitare eventuali forme invasive di controllo sulle abitudini delle persone ed operazioni illecite di profilazione, oltre che per garantire ad utenti ed abbonati una piena consapevolezza sui trattamenti di dati personali che li riguardano, anche al fine di esercitare liberamente le loro scelte ed i loro diritti, senza essere pregiudicati nella fruizione di servizi e di opportunità.

La circostanza che la televisione digitale interattiva trovi usuale utilizzo in un ambito segnatamente "privato", quale quello familiare, richiedeva particolare attenzione da parte del Garante. In tali contesti, l'utente nutre la ragionevole aspettativa di essere al riparo da forme di controllo; spesso, poi, ad uno stesso apparecchio televisivo possono corrispondere più fruitori differenziati (appartenenti o estranei al nucleo familiare dell'abbonato), i quali debbono essere messi tutti in grado di compiere liberamente le loro scelte, senza che ciò comporti schedature o profilazioni.

Nello scorso anno si è registrato un aumento sensibile del numero degli utenti e degli operatori del settore (a prescindere dalla tecnica di trasmissione impiegata, che può implicare l'utilizzo del satellite, del cavo o del digitale terrestre), unitamente a novità tecnologiche che possono presentare nuovi rischi o, comunque, profili di interesse per la sfera privata degli interessati.

Nel richiamato provvedimento l'Autorità ha pertanto prescritto agli operatori del settore le misure di carattere generale volte a garantire il rispetto dei principi di necessità, liceità, correttezza e proporzionalità. In primo luogo, occorre ridurre al minimo l'utilizzo delle informazioni relative ad abbonati e utenti identificabili, privilegiando l'uso di dati anonimi (come schede prepagate). In questo caso, anche l'acquirente del *decoder* digitale terrestre deve essere anonimo, ferma restando la necessità di prender nota del nome al solo fine di evitare un'attribuzione multipla del relativo contributo statale. Si prefigura diversamente, invece, il caso del rapporto contrattuale che debba intercorrere necessariamente con un abbonato identificato. Resta poi ferma l'illiceità di eventuali banche dati di titolari di antenne televisive o satellitari (il cosiddetto "catasto delle antenne").

Profilazione

Quanto, poi, alla profilazione attraverso la tv interattiva, il Garante ha stabilito che non è lecito trattare dati personali quali quelli relativi a tempi di connessione, visioni di programmi ed eventi, nonché ad analisi del comportamento in presenza di spazi pubblicitari, a meno che l'interessato, debitamente informato, non abbia prestato il proprio consenso libero e specifico. In tal caso, i dati di dettaglio su acquisti e servizi possono essere tuttavia conservati per un periodo comunque non superiore a dodici mesi dalla loro registrazione, salva la loro trasformazione in forma anonima. Le eventuali intenzioni di trattare i dati oltre tali termini possono essere attuate solo previa valutazione preliminare dell'Autorità ai sensi dell'art. 17 del Codice.

Sondaggi e ricerche di mercato

Con riguardo ai sondaggi, alle ricerche di mercato e alle altre ricerche campionarie, il fornitore deve adottare una tecnica che separi il voto espresso dal nominativo di chi ha partecipato al sondaggio; laddove la commistione risulti tecnicamente inevitabile, deve rendere le risposte realmente anonime subito dopo la loro raccolta, escludendo a maggior ragione ogni eventuale comunicazione a terzi o diffusione dei dati personali.

Non è di regola ammesso il trattamento di dati sensibili, né per l'ordinaria pre-

stazione di servizi televisivi, né per eventuali finalità di profilazione o fidelizzazione della clientela, a meno che tale trattamento sia realmente indispensabile in rapporto ad uno specifico bene o servizio richiesto e sia altresì autorizzato dal Garante, oltre che consentito dall'interessato in forma scritta o telematica equiparabile allo scritto.

Informativa

L'Autorità ha, poi, prescritto ai gestori di servizi televisivi l'obbligo di fornire informative più chiare e complete, prevedendo anche l'inserimento, prima di ogni acquisto o altro tipo di rapporto interattivo, di un'apposita schermata-video. Il consenso può essere manifestato anche elettronicamente attraverso il telecomando e deve essere libero da qualsiasi condizionamento. In caso di fatturazione degli acquisti (*ad es.* di partite o film), l'abbonato deve avere la possibilità di non ricevere una fatturazione dettagliata. Gli acquisti devono essere indicati per importo totale, data e costo, mentre vanno forniti i "titoli" specifici solo su richiesta.

L'Autorità ha poi imposto agli operatori di indicare nell'informativa il termine di conservazione dei dati dopo la cessazione del rapporto (termine che non può essere comunque superiore ad un trimestre, salvi eventuali obblighi di legge specifici sulla conservazione di documentazione contabile), nonché di predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi ai quali gli stessi siano stati eventualmente comunicati.

Verifica preliminare

Il Garante ha inoltre previsto in capo ai fornitori dei servizi televisivi interattivi l'obbligo di richiedere la verifica preliminare ai sensi dell'art. 17 del Codice laddove il trattamento di dati consista nella "*richiesta –rivolta dal fornitore ai singoli utenti– di identificarsi nominativamente al momento in cui essi inviano informazioni attraverso il canale di ritorno*". Ciò, al fine di poter prescrivere specifici accorgimenti e misure a garanzia degli interessati, nei casi in cui all'utente (persona fisica eventualmente diversa dall'abbonato) sia richiesto di essere individuato specificamente nel momento in cui compia un'operazione diversa da quelle effettuabili "ordinariamente" nel quadro del comune svolgimento di un rapporto. A tale riguardo sono già pervenute all'Autorità alcune richieste di valutazione preliminari sulle quali il Garante è in procinto di pronunciarsi caso per caso.

È stata infine avviata una complessa attività ispettiva volta a verificare il corretto e completo adeguamento degli operatori alle prescrizioni impartite dall'Autorità in materia.

15.13. Pornosquatting

Sono pervenute a questa Autorità diverse segnalazioni con le quali è stata lamentata la violazione del diritto all'immagine, al nome ed alla professionalità, commessa presso alcuni siti Internet a contenuto pornografico. I segnalanti lamentano in particolare che, digitando il loro nome su un qualsiasi motore di ricerca, compaiono, fra i risultati, anche alcuni indirizzi di siti pornografici che associano al loro nome contenuti osceni e denigratori della reputazione.

Da alcune ricerche preliminari curate da questa Autorità, si è potuto verificare che i casi di specie rientrano nel fenomeno, diffuso in Internet, meglio noto come "*pornosquatting*" che consiste nell'inserire nomi di personaggi famosi, o di noti marchi, tra le parole chiave riscontrabili nei *cd.* "*meta-tag*" (stringhe ipertestuali) della pagina *web*, che dovrebbero descrivere essenzialmente il contenuto del sito.

Tale pratica risulta piuttosto lesiva degli interessati in quanto la tecnologia dei motori di ricerca imposta le ricerche proprio in base alle parole contenute in tali stringhe ipertestuali. Di conseguenza, se si cercano in rete notizie relative ad un

determinato soggetto e il suo nome è contenuto nei "*meta-tag*" di un sito *web*, l'indirizzo di quest'ultimo verrà sicuramente presentato tra i risultati dal motore di ricerca interrogato.

La circostanza che i titolari dei siti pornografici utilizzino nomi di personaggi noti per rendere maggiormente "reperibili" gli indirizzi dei siti stessi può peraltro essere considerata alla stregua di uno sfruttamento illegittimo della notorietà delle persone coinvolte, oltre che un'induzione in errore degli utenti.

L'Autorità sta ultimando, anche avvalendosi della collaborazione della Guardia di finanza, i necessari accertamenti preliminari.

15.14. Rfid

In un *provvedimento* del 9 marzo 2005 [doc. *web* n. 1109493] il Garante ha impartito prescrizioni specifiche per chi intenda produrre ed utilizzare le cosiddette "etichette intelligenti", minuscoli *chip* a radiofrequenza (*Radio Frequency Identification-Rfid*) attivati da lettori ottici, che hanno iniziato a trovare applicazione anzitutto nell'ambito di aziende, esercizi commerciali e della grande distribuzione per ottenere alcuni vantaggi, a volte anche per il consumatore (migliore gestione di prodotti aziendali, maggiore rapidità di operazioni commerciali, agevole rintracciabilità dell'origine di particolari prodotti e controllo degli accessi a luoghi riservati).

Alcuni utilizzi di questa tecnologia –che non si limitino a tracciare un prodotto per garantire l'efficienza del processo di produzione industriale– possono comportare anche una violazione del diritto alla protezione dei dati personali e determinare forme di controllo sulle persone. Con l'uso di *Rfid* si potrebbero, infatti, raccogliere innumerevoli dati sulle abitudini dei consumatori a fini di profilazione ed essere in grado di tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usano, indossano o trasportano.

I sistemi *Rfid* possono essere impiegati da soggetti pubblici o privati anche ad altri scopi quali l'identificazione personale o la tutela della salute. Alcuni particolari usi come l'impianto di *microchip* sottopelle hanno già sollevato problematiche di grande delicatezza. Ulteriori pericoli possono derivare dall'adozione di *standard* comuni in materia, tali da favorire la possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (*ad es.*, mediante la loro riscrittura). I rischi possono accrescersi nel caso in cui si integrino le tecniche *Rfid* con infrastrutture di rete avvalendosi della telefonia e di Internet, e sulla base dello stesso sviluppo tecnologico che, potenziando i sistemi, potrebbe consentire una "lettura" delle etichette a distanze sempre maggiori.

Il provvedimento generale si collega a quello varato nello stesso periodo dal Gruppo art. 29, allo scopo di stabilire alcune misure per rendere conformi l'impiego dei sistemi *Rfid* alle norme sulla *privacy* nei casi in cui si trattino dati personali relativi a persone identificate o identificabili, e tutelare la loro dignità e la libertà.

Informativa

In particolare, l'Autorità ha prescritto che gli interessati siano adeguatamente informati dell'utilizzo di sistemi *Rfid,* così come dell'esistenza dei lettori ottici che attivino l'etichetta. La presenza di avvisi nei luoghi nei quali le tecniche *Rfid* sono utilizzate non esime, peraltro, dall'apporre un'informativa più specifica in relazione agli stessi oggetti e prodotti che recano le etichette intelligenti.

L'uso di etichette intelligenti deve risultare proporzionato agli scopi che si intendono perseguire. I dati possono essere utilizzati solo per le finalità per le quali sono stati raccolti e devono essere conservati per il tempo strettamente necessario.

L'utilizzo delle *Rfid* che comporta un trattamento di dati personali può avvenire

solo con il consenso espresso e specifico degli interessati, a meno che ricorra uno degli altri presupposti di legge; il consenso non è valido se ottenuto con pressioni o condizionamenti sull'interessato.

Rfid e profilazione

Se le etichette intelligenti sono associate all'utilizzo di carte di fedeltà, e si trattano dati a fini di profilazione dei consumatori, occorre informare ed acquisire il consenso degli interessati; il consenso non è invece necessario quando le etichette intelligenti sono adoperate solo per modalità di pagamento e tale impiego non comporti alcuna riconducibilità dei prodotti ad acquirenti identificati o identificabili.

Deve comunque essere garantito comunque il diritto di asportare, disattivare o interrompere gratuitamente ed in maniera agevole il funzionamento delle *Rfid* al momento dell'acquisto del prodotto sui cui è apposta l'etichetta. Le etichette devono essere posizionate in modo tale da risultare facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto (*ad es.*, collocate solo sulla confezione); non è, di regola, lecita l'installazione di *Rfid* destinate a rimanere attive oltre la barriera-cassa dell'esercizio commerciale.

Nei casi di impiego delle *Rfid* per la verifica di accessi a determinati luoghi riservati devono essere predisposte idonee cautele per i diritti e le libertà delle persone; in particolare, per i luoghi di lavoro, va rispettato quanto previsto dallo Statuto dei lavoratori relativamente al divieto di utilizzo di impianti per controlli a distanza di dipendenti. Per l'accesso occasionale di terzi a determinati luoghi occorre predisporre un meccanismo che, nel caso di indisponibilità ad usare *Rfid* da parte dell'interessato, permetta comunque l'ingresso.

L'avvio di trattamenti di dati che indichino la posizione geografica di persone o oggetti mediante reti di comunicazione elettronica o che siano effettuati allo scopo di costruire profili o personalità di un individuo deve essere, inoltre, comunicato preventivamente al Garante.

Impianto di *microchip* sottopelle

Il Garante ha inoltre ritenuto che l'impianto di *microchip* sottopelle debba essere in via di principio escluso in quanto contrastante con i diritti, le libertà fondamentali e la dignità della persona. Tali impianti sono limitatamente ammissibili, in casi eccezionali, per comprovate e giustificate esigenze di tutela della salute delle persone. L'interessato, comunque, deve poter ottenere la rimozione del *microchip* e l'interruzione del relativo trattamento dei dati che lo riguardano; si devono inoltre prevedere modalità di impianto che garantiscano la riservatezza circa la presenza delle etichette nel corpo dell'interessato. Il Garante ha stabilito infine che i soggetti che intendono utilizzare tali *microchip* devono sottoporre i relativi sistemi alla verifica preliminare dell'Autorità.

16 La sicurezza dei dati e dei sistemi

Anche nel corso del 2005 sono pervenute numerose richieste di chiarimenti circa la disciplina in materia di "misure minime" di sicurezza introdotta dal Codice.

Documento programmatico sulla sicurezza

Il Garante ha in numerose occasioni confermato le indicazioni già fornite agli operatori con una *nota* di carattere generale del 22 marzo 2004 [doc. *web* n. 771307] con riguardo alla natura del documento programmatico sulla sicurezza (d.p.s.). In particolare, si è precisato che: la redazione e/o l'aggiornamento del d.p.s. rientra tra le misure minime di sicurezza; di esso deve dotarsi qualsiasi titolare che effettui un trattamento di dati sensibili e/o giudiziari con strumenti elettronici; è sostenibile affermare che il d.p.s. sia una "nuova" misura minima, con la conseguenza che anche a questo adempimento è applicabile la disciplina transitoria (art. 180, comma 1, del Codice); deve essere conservato dal titolare presso la propria struttura, essendone doverosa l'esibizione o l'invio al Garante in caso di accertamenti ispettivi o su richiesta dell'Autorità (art. 34, comma 1, lett. *g)*, del Codice e regola 19 dell'Allegato B) al Codice).

I principi già affermati dall'Autorità con la citata *nota* del 22 marzo 2004 sono stati, da ultimo, ribaditi nella risposta ad un quesito della Confederazione nazionale dell'artigianato e delle piccole e medie imprese (Cna). Richiamandosi ai contributi già resi dall'Autorità in materia, con specifico riguardo alla redazione di una guida operativa disponibile sul sito del Garante [doc. *web* n. 1007740], volta ad agevolare la stesura e l'aggiornamento di un d.p.s. ancor più semplificato e impostato per le esigenze peculiari delle piccole e medie imprese, l'Ufficio del Garante si è reso disponibile a fornire ulteriori contributi alla categoria, precisando che eventuali provvedimenti di esonero o di deroga non rientrano tra i poteri attribuiti al Garante dal Codice (*Nota* 1 marzo 2005). Si è pertanto sviluppata una proficua collaborazione con la Confederazione che ha portato allo studio e alla definizione di modalità operative semplificate di stesura del d.p.s. reputate dal Cna maggiormente idonee a rappresentare le istanze e le caratteristiche dei piccoli e medi operatori del mercato.

Utilizzo di credenziali biometriche

Un ultimo caso interessante, a riprova del crescente interesse all'impiego di tecniche di autenticazione biometrica, ha riguardato il quesito di una multinazionale operante nel settore della promozione e vendita di prodotti farmaceutici, riguardo al progetto di attivazione di un sistema di credenziali di autenticazione dei propri agenti ed informatori scientifici basato sull'impiego delle loro impronte digitali.

In base alla dettagliata descrizione fornita dalla società è risultato che gli agenti (tutti incaricati del trattamento dei dati del proprio pacchetto clienti) ricevono in dotazione dalla società un *computer* portatile che contiene, come dotazione *standard*, un dispositivo per la rilevazione delle impronte digitali gestito da un *software* installato sul *computer*. Il dispositivo di riconoscimento e il relativo *software*, presenti su ciascun *computer*, sono attivabili solo dall'agente che voglia avvalersene. L'immagine dell'impronta viene registrata esclusivamente su un'area protetta del disco fisso del *computer* stesso ed associata ad una *password* scelta dall'utente e solo dallo stesso modificabile successivamente, senza alcuna centralizzazione in archivi aziendali o possibilità di accesso da parte della società al dato biometrico (anche in caso di malfunzionamento, il *computer* viene reso alla direzione informatica della

società che formatta il disco cancellando l'impronta registrata), il quale resta nell'esclusivo controllo dell'utente-incaricato che può cancellarlo in qualsiasi momento.

Nel caso di specie non è apparsa necessaria la valutazione preventiva del Garante tenuto conto delle caratteristiche del tutto peculiari del progetto e, soprattutto, della finalità di autenticazione informatica perseguita. L'adozione di un sistema di autenticazione informatica (mediante il quale gli incaricati dotati di apposite credenziali possono effettuare specifici trattamenti di dati personali), conforme ai requisiti tecnici indicati dalle regole 1.11. dell'Allegato B) al Codice, costituisce infatti una misura minima di sicurezza che il titolare, il responsabile (ove designato) e l'incaricato sono tenuti ad utilizzare (art. 34, comma 1, lett. *a)*, del Codice). Tali credenziali di autenticazione, come nel caso di specie, possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o a una parola chiave.

17 Registro dei trattamenti

Il registro dei trattamenti previsto dall'art. 37 del Codice ha consolidato la propria veste nel corso del 2005, nella nuova connotazione informatica che ha fornito esiti ancora più positivi in termini di efficienza, efficacia, economicità e rapidità nel monitoraggio.

Nel registro confluiscono come è noto le notificazioni del trattamento di dati personali, le quali pervengono al Garante secondo le procedure previste dall'art. 38. L'intera notificazione (compresa la firma) avviene telematicamente. Il registro è pubblico e chiunque può consultarlo, tramite il sito dell'Autorità, mediante un apposito motore di ricerca.

I contenuti della notificazione sono limitati alle informazioni essenziali sui trattamenti effettuati; rendono però possibile effettuare ampi controlli, estrazioni di dati ed elaborazioni statistiche. Il registro viene pertanto utilizzato dall'Autorità a fini di monitoraggio, controllo e orientamento delle attività ispettive in determinati settori.

Gli obiettivi posti con il nuovo sistema di notificazione (flessibilità del sistema; contenimento delle notizie da richiedere e ai titolari; semplificazione della procedura; pubblicità completa del registro dei trattamenti), la filosofia e il modello posti alla base della procedura, sono stati in seguito tenuti presenti per altre attività legate ai trattamenti che presentano rischi specifici *ex* art. 17 del Codice (verifica preliminare del Garante).

Preme evidenziare, rispetto all'esperienza di applicazione relativa all'anno precedente, il fattivo ausilio offerto all'utenza che ha avuto occasione di sollecitare ed ottenere chiarimenti dal dipartimento dell'Ufficio che vi è preposto.

Tra i momenti istituzionali di contatto con l'utenza si segnala la possibilità, offerta al notificante, di sospendere la notificazione in qualsiasi momento e di continuarla successivamente, utilizzando un codice numerico che viene spedito automaticamente dall'Ufficio, con due vantaggi immediati:

- l'utente può indicare il motivo della sospensione; il dipartimento è messo in grado di intervenire tempestivamente nel caso in cui l'utente stia effettuando una notificazione non dovuta, sia in difficoltà o non abbia compreso alcuni elementi, ovvero semplicemente intenda essere "guidato" o agevolato nella compilazione;
- viene così reso noto all'utente l'indirizzo *e-mail* dell'Ufficio, in seguito utilizzato frequentemente per altre richieste e segnalazioni.

Le difficoltà incontrate dagli utenti nella compilazione della notificazione (trattasi di un fenomeno comunque assai marginale) attengono –salvo quanto si dirà di seguito– quasi esclusivamente all'apposizione della firma digitale (possesso di un certificato scaduto, mancata lettura delle istruzioni, ecc.).

A questi elementi, deve aggiungersi l'esperienza che il dipartimento può continuare ad offrire rispetto ad alcuni dubbi interpretativi emersi nell'individuazione dei soggetti obbligati alla notificazione, anche dopo il provvedimento di esonero del Garante del 2004 e le connesse delucidazioni fornite con una risposta di ordine generale a quesiti (*Provv.* n. 1 del 31 marzo 2004 [doc. *web* n. 852561]; *Nota* 23 aprile 2004 [doc. *web* n. 993385]; *v.* anche *Nota* 26 aprile 2004 [doc. *web* n. 996680], visto che l'art. 37 del Codice descrive il suo ambito di applicazione con una disciplina

generale senza entrare in innumerevoli dettagli legati alle migliaia di diversi titolari del trattamento e di banche dati.

Nel 2005, a parte i picchi registratisi in occasione della scadenza di taluni termini per l'adempimento ad obblighi previsti dal Codice (a volte erroneamente associati all'obbligo di notificazione, come è avvenuto per la redazione del documento programmatico sulla sicurezza), il numero di notificazioni giornaliere ha oscillato tra le sei e le sette.

Le tabelle statistiche riportate in altra parte della presente relazione forniscono altri elementi utili per valutare come il registro si evolve. Ad esempio, dalle tabelle relative alle singole tipologie di trattamenti notificati, si riscontra una netta prevalenza di quelli riferiti alla salute, alla profilazione e alla solvibilità economica rispetto ad altri trattamenti.

Il versamento dei diritti di segreteria (euro 150,00 per ciascuna notificazione) resta possibile utilizzando *on-line* una carta di credito (circa il 22% dei casi) o con altri sistemi quali il bonifico bancario (30 %) o il conto corrente postale (48 %).

Sono stati poi previsti particolari accorgimenti sul piano della sicurezza: un messaggio di avvenuta ricezione della notificazione viene spedito dal dipartimento al notificante, unitamente ad un codice segreto (codice univoco del notificante, Cun) che permette l'eventuale modifica della precedente notificazione o la sua cessazione. Tale aspetto è monitorato costantemente ed eventuali anomalie sono segnalate ad altri dipartimenti dell'Ufficio.

Per agevolare il compito di apposizione della firma digitale, l'Autorità continua inoltre a dare applicazioni ad alcune convenzioni con Poste italiane S.p.A., Unappa (Unione nazionale professionisti pratiche amministrative), Alar (Associazione lavoratori autonomi riuniti) e Comune di Livorno, per permettere la notificazione, tramite l'ausilio di intermediari qualificati, anche a chi non voglia o non possa dotarsi del *kit* di firma digitale. Altri tentativi intrapresi dall'Autorità per estendere le convenzioni ad altri soggetti (banche, comuni, camere di commercio) non hanno per ora riscontrato l'interesse degli interlocutori.

Il notificante può inoltre rivolgersi a soggetti di fiducia (commercialisti, avvocati, notai, conoscenti, purché in possesso di chiave per la firma digitale), senza limitazioni. Il costo del servizio reso dall'intermediario convenzionato, consistente nella stampa della notificazione, nell'apposizione della firma digitale, nell'inserimento di eventuali riferimenti ai diritti di segreteria e nell'invio del *file* è pari ad un massimo di euro 25,00 che l'utente paga direttamente all'intermediario.

Alla data del 31 dicembre 2005, risultavano inoltrate 6.439 notificazioni tramite gli intermediari convenzionati, con prevalenza dell'utilizzo di Poste italiane S.p.A.

Va operato un cenno alla possibilità, consentita dal sistema in uso, di monitorare il flusso dei dati in arrivo e di compiere ricerche ed elaborazioni di statistiche, anche al fine di riscontrare richieste dei dipartimenti dell'Ufficio operanti nel settore giuridico, in particolare allo scopo di coadiuvare l'attività ispettiva. Risultano in particolare interessanti le interrogazioni volte ad estrarre, all'interno delle tabelle descrittive dei trattamenti, le categorie di dati, di interessati, le finalità e le modalità del trattamento, l'eventuale comunicazione dei dati e l'utilizzazione, per il trattamento dei dati, di un sito *web*.

A titolo sperimentale, il dipartimento ha assunto infine l'iniziativa di inviare automaticamente un messaggio di posta elettronica ad alcuni dipartimenti interni (compreso quello ispettivo), segnalando volta per volta l'avvenuta notificazione di trattamenti più significativi (*ad es.*, il trattamento di dati genetici trasferiti all'estero).

18 La trattazione dei ricorsi

18.1. *Considerazioni generali*

Uno strumento di tutela agile e "multiuso": questa definizione, nella sua sinteticità, sembra fotografare efficacemente il ruolo e la funzione che il ricorso, ai sensi degli artt. 145 e ss. del Codice, è venuto ad assumere nel quadro più generale della tutela dei dati personali. L'analisi del numero e della tipologia dei ricorsi proposti nel 2005 attesta la veridicità della definizione a conferma di un *trend* chiaramente emerso già negli ultimi anni. L'esame dell'ampia casistica affrontata in questi mesi dal Garante sottolinea, poi, l'utile funzione di "antenna" di questo strumento di tutela che segnala tempestivamente nuove frontiere della protezione dei dati e, al tempo stesso, evidenzia settori di maggiore "utilizzo" delle opportunità di tutela che il Codice offre.

In questo senso, lo sguardo agli ultimi due anni mette in luce un'autentica "esplosione" dei ricorsi relativi al trattamento di dati effettuato da banche e società finanziarie, con particolare riferimento alla comunicazione e conservazione delle informazioni negli archivi dei Sic (sistemi di informazioni creditizie), già comunemente noti come "centrali rischi private". La vicenda è significativa e rappresenta un interessante esempio di intreccio fra la dinamica sociale ed economica (la crescita esponenziale del credito al consumo in connessione con una fase di limitata disponibilità reddituale delle famiglie) e lo sforzo di disciplina di un settore che era privo di una normativa organica di riferimento.

In questo quadro sono emerse con forza le esigenze di tutela dei dati personali dei consumatori (esattezza dei dati, tempestività degli aggiornamenti, chiarezza informativa dei meccanismi di segnalazione nei citati Sic, definizione dei tempi di conservazione delle posizioni, ecc.) che, in equilibrato contemperamento con le esigenze di garanzia e stabilità degli operatori finanziari, hanno ispirato la disciplina ora affidata, essenzialmente, all'apposito codice di deontologia e di buona condotta di settore (*Provv.* n. 8 del 16 novembre 2004 [doc. *web* n. 1070713] e connesso provvedimento sul bilanciamento di interessi, *Provv.* n. 9 del 16 novembre 2004 [doc. *web* n. 1070779]).

Anche ricorsi presentati in altri campi hanno, parimenti, permesso di far emergere aspetti nuovi. Ne sono testimonianza diverse decisioni che hanno avuto a tema i trattamenti in Internet, così come l'utilizzo dei dati personali da parte degli operatori telefonici o le nuove forme che può assumere, nel quadro tecnologico attuale, il controllo sui lavoratori (*v.* par. 18.3).

18.2. *Profili procedurali*

Venendo in primo luogo a profili più strettamente procedurali, è possibile rilevare alcune linee di tendenza ormai consolidate.

Il ricorso, specie se proposto con l'assistenza di un legale, appare sempre più spesso utilizzato come "tassello" di una più ampia strategia difensiva: diventa, cioè, il veicolo privilegiato per acquisire le informazioni indispensabili alla tutela della posizione di un soggetto o per contestare, sotto lo specifico profilo della protezione

dei dati, operazioni poste in essere, ad esempio, nell'ambito di un rapporto contrattuale. In questo quadro, acquisisce rilievo l'intero "catalogo" dei diritti previsti dall'art. 7 del Codice per la cui tutela il ricorso viene proposto. Lo stesso, quindi, non è più funzionale solamente alla tutela del diritto di accesso ai dati, ma viene frequentemente e consapevolmente utilizzato per accertare l'origine dei dati personali, le finalità o le modalità di uno specifico trattamento o per sollecitare, in caso di violazione di legge, la cancellazione dei dati stessi.

La più ampia conoscenza dei diritti di cui all'art. 7 del Codice e della loro tutelabilità con lo strumento del ricorso ha fatto poi sviluppare, negli ultimi mesi, l'attività di terzi (talvolta associazioni di consumatori, in altri casi soggetti operanti in veste professionale di delegato) che hanno promosso numerose richieste volte ad accedere ai dati e ad ottenere successivamente la loro cancellazione, con particolare riferimento alle informazioni conservate negli archivi dei già citati Sic.

In alcuni casi, peraltro, la procedura del ricorso è dovuta passare attraverso una necessaria fase di regolarizzazione, secondo il disposto dell'art. 148, comma 2, del Codice, in quanto –ad esempio– le procure rilasciate ai soggetti incaricati di presentare ricorso in nome dell'interessato non erano accompagnate dalla necessaria firma autenticata dello stesso. In altri casi, la presentazione del ricorso è avvenuta senza essere stata preceduta dalla doverosa presentazione di un'istanza formulata ai sensi del citato art. 7 del Codice, allegando solamente l'esistenza di generici motivi di urgenza.

Al riguardo, il Garante è pervenuto a declaratorie di inammissibilità (*ad es.*, *Provv.* 14 luglio 2005 [doc. *web* n. 1157708]), ricordando che la presentazione in via di urgenza del ricorso è possibile, ai sensi dell'art. 146, comma 1, del Codice, solo fornendo prova del pregiudizio imminente e irreparabile che avrebbe impedito di procedere all'invio dell'interpello preventivo e di attendere il decorso dei quindici giorni previsti dalle citate disposizioni del Codice.

È stata altresì richiamata più volte l'attenzione degli interessati sul disposto dell'art. 5, comma 3, del Codice secondo il quale "il trattamento dei dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del (...) Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione". Ciò ha reso inammissibile la presentazione di ricorsi incentrati su ipotesi di trattamento di dati relativi, ad esempio, a controversie fra vicini per installare impianti di sorveglianza (*Provv.* 19 ottobre 2005 [doc. *web* n. 1191132]), ferma restando l'applicazione del Codice quando il trattamento è risultato effettuato nell'ambito di un'attività professionale ed economica (*Provv.* 27 ottobre 2005 [doc. *web* n. 1195275]).

Infine, qualche breve annotazione statistica: nel corso dell'anno solare 2005, come evidenziato anche nelle tabelle riportate in altra parte della presente *Relazione*, il Garante ha definito la trattazione di 634 ricorsi.

18.3. *Brevi cenni sulla casistica*

Come in passato, si offre in questo paragrafo una succinta sintesi sui principali temi affrontati con le decisioni in materia di ricorsi, rimandando alle altre parti della relazione per l'ulteriore esame di alcune problematiche sottese alle decisioni stesse.

Diffusione di dati personali tramite siti Internet istituzionali

Meritano anzitutto di essere ricordate due vicende che hanno riguardato la diffusione di dati personali tramite i siti Internet di due autorità amministrative indipendenti.

Nel primo caso (*Provv.* 10 novembre 2004 [doc. *web* n. 1116068]; *cfr.* anche *Newsletter* 21-27 marzo 2005), il ricorso concerneva l'opposizione per motivi legittimi

al trattamento di dati personali contenuti in alcune decisioni (una delle quali risalente nel tempo) adottate dall'Autorità garante della concorrenza e del mercato pubblicate, tra l'altro, sul sito Internet della medesima autorità. Tali decisioni erano state correttamente pubblicate, in adempimento di specifici obblighi normativi, in relazione all'attività di un operatore economico sanzionato per pubblicità ingannevole.

Il provvedimento del Garante ha esaminato le implicazioni della conoscibilità via Internet di tali provvedimenti (specie in relazione alla possibilità di rinvenire agevolmente tali informazioni tramite l'utilizzo di motori di ricerca). Tale forma di diffusione dei dati può comportare infatti un sacrificio sproporzionato dei diritti dell'interessato, specie quando si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le finalità perseguite.

La questione affrontata nel caso di specie è risultata particolarmente delicata, richiedendo il contemperamento fra il dovere di informazione da parte di organi pubblici sulla propria attività, il diritto degli utenti e dei consumatori di conoscere l'esito di determinati provvedimenti sanzionatori e le non convergenti aspettative dei soggetti cui si riferiscono i dati "sanzionatori" diffusi. Con la decisione adottata, il Garante ha tra l'altro riconosciuto il pieno diritto-dovere dell'Antitrust di continuare a pubblicare i propri provvedimenti sul relativo sito *web*, modulando però nel tempo il periodo entro il quale le decisioni del tipo di quella in questione potranno essere direttamente individuabili nel sito Internet dell'Autorità tramite motori di ricerca esterni al sito stesso (non è stato posto in discussione un sistema di ricerca rapida delle decisioni all'interno del medesimo sito).

In un diverso caso, esaminato con decisione del 19 maggio 2005 [doc. *web* n. 1151205], l'Autorità ha invece constatato come non fosse giustificata da un idoneo presupposto normativo la diffusione indifferenziata, tramite il sito Internet dell'Autorità per la vigilanza sui lavori pubblici, di alcune specifiche informazioni contenute nel "Casellario informatico delle imprese qualificate". Per espressa limitazione derivante dalla specifica disciplina applicabile al caso di specie, tali dati devono essere resi agevolmente disponibili, ma solo alle stazioni appaltanti, e non possono essere invece oggetto di una diffusione indifferenziata in rete (*v. amplius* par. 2.5).

Le citate fattispecie, venute ad evidenza in conseguenza delle straordinarie potenzialità diffusive della rete Internet e dei meccanismi di "navigazione" nella stessa, hanno così fatto emergere prepotentemente e il tema del "diritto all'oblìo" e della sua declinazione nel presente quadro tecnologico.

Altri trattamenti svolti da soggetti pubblici

Vari, e molto differenziati tra loro, sono risultati i ricorsi che hanno riguardato trattamenti effettuati da pubbliche amministrazioni. Fra le principali problematiche emerse si può ricordare la decisione del 3 novembre 2005 [doc. *web* n. 1198422] con la quale il Garante ha riconosciuto come lecite e conformi alle disposizioni del Codice le modalità di acquisizione (tramite le liste elettorali) e di successivo utilizzo dei dati personali impiegati per inviare una pubblicazione istituzionale curata dal Ministero della salute.

Con altre decisioni (in particolare, quelle del 16 giugno 2005 [doc. *web* n. 1149999] e del 21 dicembre 2005 [doc. *web* n. 1217532]), sono stati esaminati nuovamente i profili concernenti l'accesso ai dati personali di dipendenti di pubbliche amministrazioni; ciò, richiamando le corrette modalità di riscontro a tali istanze delineate dall'art. 10 del Codice e le linee differenziali rispetto al diritto di accesso ad atti e documenti amministrativi disciplinato dalla l. n. 241/1990.

Sempre con riferimento a problematiche concernenti impiegati pubblici va ricordato il *provvedimento* del 30 novembre 2005 [doc. *web* n. 1215256] con cui è stata esaminata una vicenda relativa alla lamentata diffusione di dati personali sensibili a seguito dell'affissione di una determinazione dirigenziale all'albo pretorio di un

Comune. Con *provvedimento* del 21 dicembre 2005 [doc. *web* n. 1219054] l'attenzione è stata invece rivolta allo svolgimento di un procedimento disciplinare, sempre nell'ambito di un'amministrazione comunale.

I casi in cui i dati personali degli interessati sono stati oggetto di comunicazione ad altri soggetti pubblici o a privati, nonché le ipotesi di diffusione dei medesimi dati (a mezzo affissione all'albo pretorio, pubblicazione a stampa, divulgazione tramite la rete Internet, ecc.), sono stati, quindi, le principali ipotesi che hanno formato oggetto del contenzioso dinanzi all'Autorità in relazione all'attività degli enti pubblici. Ciò, a conferma della particolare sensibilità degli interessati per quelle operazioni di trattamento (comunicazione e diffusione appunto) che moltiplicano le potenzialità lesive di un eventuale uso illecito dei dati.

Trattamenti svolti presso sistemi di informazioni creditizie

Come già ricordato, il settore rispetto al quale si è registrato il maggior numero di ricorsi è stato quello dei Sic. Il 2005 ha rappresentato il primo anno di applicazione delle nuove disposizioni introdotte con il codice deontologico di settore e le decisioni adottate in proposito sono state l'occasione per una verifica del livello di conoscenza e di applicazione delle stesse. Forse in ragione di una non perfetta conoscenza del predetto codice deontologico e del connesso provvedimento di bilanciamento degli interessi, sono pervenuti molti ricorsi incentrati su richieste di "cancellazione totale" delle posizioni riferite ad un interessato, senza che sussistessero, però, i presupposti per un loro accoglimento: ciò, pur in presenza di ritardi o di altre patologie nei rimborsi dei finanziamenti o in ragione di regolarizzazioni molto recenti e destinate quindi a rimanere annotate negli archivi in questione per il lasso temporale previsto dal predetto codice deontologico.

I ricorsi proposti nei confronti dei gestori dei Sic hanno dato luogo spesso a decisioni molto articolate, soprattutto in presenza di numerose posizioni segnalate nelle relative banche dati dei Sic, riferite a prestiti, mutui, carte di credito a saldo o rateali, ecc.

Occorre infatti discernere fra posizioni "positive" (relative a finanziamenti regolari di cui è possibile chiedere la cancellazione previa revoca del consenso al trattamento dei relativi dati) e "negative" (per le quali opera il già richiamato provvedimento sul bilanciamento degli interessi e che possono essere conservate negli archivi dei Sic nel rispetto dell'articolata tempistica che il codice deontologico ha delineato).

Altri archivi contenenti dati relativi ad attività economiche e finanziarie

Numerosi ricorsi sono stati rivolti nei confronti di altri archivi di dati e relativi ad attività economiche.

L'esigenza di assicurare un ordinato svolgimento dei rapporti economici, di permettere una rilevazione puntuale dei rischi creditizi, di garantire la stabilità del sistema finanziario e di prevenire fenomeni di sovraindebitamento ha portato negli ultimi anni sia ad un'estensione del tipo di operazioni e/o di "patologie" finanziarie oggetto di monitoraggio, sia ad un rapido adeguamento alle procedure informatiche dei sistemi di rilevazione, al fine di garantire un maggior livello di affidabilità e trasparenza di questi ultimi.

Il soggetto più antico operante nel settore è, come noto, la "centrale rischi" gestita dalla Banca d'Italia, istituita già nel 1964 per raccogliere le segnalazioni relative ai finanziamenti di importo pari o superiore attualmente a euro 75.000 e ai crediti in "sofferenza". Nei confronti di tale soggetto (art. 8, comma 2, lett. *d)*, del Codice), non è però esperibile il ricorso *ex* art. 145 del Codice, pur rimanendo la possibilità di proporre una segnalazione all'Autorità. Ciò spiega perché alcuni ricorsi pervenuti in ordine a tali trattamenti siano stati dichiarati inammissibili.

Le istanze rivolte *ex* art. 7, e gli eventuali, successivi ricorsi, possono essere invece proposti nei confronti dei trattamenti effettuati presso "la centrale rischi di

importo contenuto" gestita, in conformità alle istruzioni della Banca d'Italia, da S.i.a. S.p.A. cui possono essere rivolte le istanze citate.

Con riferimento ai finanziamenti di più limitato importo ricadenti prevalentemente nel novero del credito al consumo operano, infine, le già indicate disposizioni sui Sic, soggetti rispetto ai quali, come detto, si è concentrato in maggior misura il contenzioso su ricorso del 2005.

Tipologicamente diverso è invece il fenomeno (oggetto di attenzione in numerosi ricorsi) della conservazione in appositi archivi distinti da quelli relativi ai Sic, di altri tipi di informazioni quali dati personali tratti dai registri immobiliari e dagli archivi delle ex-conservatorie, ai quali si applica quindi il disposto dell'art. 24, comma 1, lett. *c)*, del Codice.

A tale riguardo (nei numerosi casi che hanno riguardato richieste di cancellazione rivolte a Crif S.p.A.) l'Autorità ha preso atto della già avvenuta sospensione della loro visualizzazione nella banca dati, anche in relazione alle intervenute modifiche legislative concernenti i nuovi presupposti (oggetto peraltro di ampio contenzioso giudiziario) per la riutilizzazione commerciale di tali dati di cui all'art. 1, commi 368/371, l. n. 311/2004, nonché all'art. 1, comma 5, d.l. 10 gennaio 2006, n. 2, convertito con l. 11 marzo 2006, n. 81.

19 Contenzioso giurisdizionale

19.1. *Considerazioni generali*

Come già osservato nella *Relazione* 2004 (p. 118), l'art. 152 del Codice ha introdotto nel sistema processuale italiano un procedimento a cognizione ordinaria, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali e connotato da una procedura snella, capace di fornire al diritto alla riservatezza una tutela specifica e tempestiva.

L'opportunità di tale impianto normativo ha avuto riscontro nel numero delle azioni proposte direttamente avanti all'autorità giudiziaria, in via alternativa al ricorso presentato in sede amministrativa al Garante. Nel corso del 2005 si è registrata la notifica al Garante, secondo quanto prescritto dal comma 7 dell'art. 152 del Codice, di un numero di ricorsi all'autorità giudiziaria, non coinvolgenti direttamente pronunce dell'Autorità, significativamente superiore a quello registrato nell'anno precedente: a fronte di trentadue controversie introdotte nel 2004, infatti, nel 2005 sono stati notificati al Garante settantaquattro ricorsi, con un incremento quantitativo superiore al 120%.

La crescita dei ricorsi avanti l'autorità giudiziaria, e delle relative decisioni, attribuiscono sicuro rilievo a due novità introdotte dal Codice. L'obbligo imposto dal citato comma 7 di notificare al Garante i ricorsi presentati all'autorità giudiziaria concernenti tutte le controversie relative all'applicazione del Codice (non solo di quelle in cui sia proposta opposizione avverso i provvedimenti dell'Autorità), unitamente alla trasmissione, a cura delle cancellerie, di copia dei provvedimenti emessi a definizione dei relativi giudizi o in materia di criminalità informatica (art. 154, comma 6), consentono al Garante, oltre che di intervenire nelle controversie in cui, pur non essendo direttamente coinvolto, sono in discussione profili di carattere generale, di avere un'ampia informazione sull'evoluzione della giurisprudenza nella materia. Ciò anche al fine di adottare eventuali provvedimenti amministrativi e di segnalare al Parlamento e al Governo gli interventi normativi opportuni per tutelare i diritti e le libertà fondamentali correlati alla protezione dei dati (art. 154, comma 1, lett. *f)*, del Codice).

19.2. *Profili procedurali*

L'art. 152 del Codice ha ribadito che tutte le controversie riguardanti l'applicazione del Codice sono devolute all'autorità giudiziaria ordinaria, precisando che l'azione deve proporsi con ricorso da depositarsi "nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento" (comma 2): nel 2005 si sono però registrati ancora alcuni casi di mancato rispetto del dettato normativo.

Controversie instaurate erroneamente dinanzi al giudice amministrativo

Si è rivolta al Tribunale amministrativo del Lazio una società operante nel settore del *direct marketing* chiedendo l'annullamento, previa sospensione, del *provvedimento* del Garante del 15 luglio 2004 [doc. *web* n. 1032381] concernente l'individuazione delle modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi telefonici cartacei o elettronici. Costituitasi in giudizio, l'Autorità ha eccepito il difetto di giurisdizione del giudice amministrativo, alla luce della ricordata chiara dizione normativa. Con ordinanza del 25 maggio 2005, il

Tribunale ha respinto la domanda di sospensione presentata dai ricorrenti, rimettendo ogni decisione, anche in ordine alla questione della giurisdizione, alla fase di merito.

Foro competente

In ordine al foro competente non sono mancate decisioni con le quali, in accoglimento di eccezioni fondate sul luogo di residenza del titolare del trattamento, i giudizi sono stati rimessi al tribunale competente per territorio. In tal senso si sono pronunciati, fra gli altri, il Tribunale di Roma (sentenza del 10 gennaio 2006) e quello di Viterbo (sentenza n. 767 del 7 settembre 2005). Con analoga decisione il Tribunale di Napoli (sentenza n. 11727 del 25 novembre 2005) ha ribadito la natura esclusiva ed inderogabile del foro stabilito dall'art. 152, dichiarando manifestamente infondata la questione di legittimità costituzionale in ordine alla scelta effettuata dal legislatore ed escludendo, in particolare, che in materia del trattamento dei dati personali possa farsi applicazione alternativa del foro del consumatore di cui all'art. 1469-*bis*, comma 3, c.c., disposizione ora abrogata dal d.lg. 6 settembre 2005, n. 206 (in *G.U.* 8 ottobre 2005, n. 235, *S.O.* n. 162/L) che ha stabilito (art. 63) il foro del consumatore nel luogo di residenza o di domicilio di questi, se ubicato nel territorio dello Stato.

Incompetenza del giudice di pace

Infine, il Garante si è costituito in vari giudizi (introdotti, in particolare, nel 2005 avanti al Giudice di pace di Taranto) al fine di far valere il rispetto della competenza del tribunale ordinario nella materia della protezione dei dati personali.

19.3. *Profili di merito*

Giova in primo luogo ricordare due casi particolarmente significativi, costituiti da decisioni assunte in sede di opposizione a provvedimenti del Garante, che hanno confermato orientamenti di merito sempre sostenuti dall'Autorità.

Con riferimento alle vicende (che hanno dato origine in passato a decisioni contrastanti dell'autorità giudiziaria) relative alla riconducibilità delle valutazioni alla nozione di "dato personale" fornita dalla l. n. 675/1996 e ribadita dal Codice, il Tribunale di Roma, facendo seguito ad una sua precedente analoga decisione, e confermando il provvedimento con cui il Garante aveva ordinato ad una compagnia di assicurazioni di comunicare all'interessato i dati personali, anche di natura valutativa, contenuti in una perizia medico-legale finalizzata alla quantificazione del risarcimento del danno, ha riconosciuto che l'interessato può esercitare il diritto di accesso ai dati personali che lo riguardano anche con riferimento a dati valutativi e, in particolare, alle valutazioni espresse in perizie medico-legali (sentenza n. 1832 del 25 gennaio 2006).

Merita di essere sottolineato che alla questione della riconducibilità dei dati valutativi alla nozione di "dato personale" il legislatore ha dedicato, dopo l'iniziale contenzioso sorto, una specifica disciplina attraverso la soluzione adottata nell'art. 8, comma 4, del Codice.

In altra fattispecie, concernente l'opposizione al provvedimento con cui il Garante, facendo seguito a precedenti decisioni di analogo tenore, ha vietato alla società editrice di un quotidiano l'ulteriore diffusione di fotografie di persone sottoposte a misure restrittive della libertà personale, il Tribunale di Milano, con sentenza n. 12746 del 9 novembre 2004 ha statuito che le foto segnaletiche rientrano nelle immagini indicative e riproduttive dello stato di detenzione del soggetto, quindi non pubblicabili perché idonee a lederne la dignità.

Infine, deve segnalarsi che, con la sentenza n. 14390 del 2005, la Corte di Cassazione ha riaffermato la necessità per i soggetti pubblici di adottare, nei casi previsti dall'art. 20, comma 2, del Codice, gli atti di natura regolamentare che specifichino i tipi di dati sensibili e le operazioni eseguibili, per procedere lecitamente al trattamento dei dati sensibili.

19.4. *Opposizione ai provvedimenti del Garante*

Il 2005 ha registrato quindici opposizioni ad altrettanti provvedimenti del Garante, quattordici delle quali hanno riguardato decisioni adottate su ricorso. In un caso, l'opposizione è stata proposta nei confronti della pronuncia dell'Autorità avente ad oggetto la disciplina dei nuovi elenchi telefonici. L'Autorità si è sempre costituita in questi giudizi.

Quattro opposizioni, di identico tenore, sono state proposte da due società che svolgono attività nel settore della riutilizzazione a fini commerciali dei dati acquisiti dagli archivi catastali o dai pubblici registri immobiliari, tenuti dagli uffici dell'Agenzia del territorio. La materia è stata innovata dalla l. n. 311/2004 (legge finanziaria 2005), che al comma 371 dell'art. 1 ha vietato tale riutilizzazione –precedentemente libera–, salva la stipula di apposite convenzioni con l'Agenzia. In conseguenza di detta innovazione il Garante, nelle more dell'adozione del codice deontologico per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (art. 61 del Codice), cui le convenzioni dovranno ispirarsi, ha accolto i ricorsi con i quali gli interessati avevano chiesto la cancellazione delle informazioni che li riguardavano, conservate presso dette società.

Si deve rilevare che la nuova normativa non ha ancora ricevuto univoca interpretazione da parte della giurisprudenza. Le due opposizioni finora definite hanno infatti registrato esiti contraddittori; nel primo caso il provvedimento del Garante è stato confermato, mentre nell'altro è stato annullato.

Per quanto riguarda le altre opposizioni presentate nel 2005 e quelle relative anche ad anni precedenti, della cui pendenza si è dato conto nella *Relazione* 2004 (p. 121), le decisioni dell'autorità giudiziaria hanno tutte confermato le pronunce dell'Autorità.

In particolare, è stato confermata la validità delle determinazioni adottate con il provvedimento del Garante di divieto all'Inail del trattamento di dati contenuti nei certificati medici, acquisiti dall'Istituto al di fuori delle ipotesi normativamente consentite, nell'ambito della procedura avviata dall'assicurata per il riconoscimento di malattia professionale (Tribunale di Genova, sentenza n. 4982 del 22 dicembre 2005).

In tre occasioni, hanno trovato conferma i provvedimenti con i quali l'Autorità ha ordinato ad alcuni istituti di credito di comunicare i dati richiesti, negati perché relativi a rapporti bancari intrattenuti da persone defunte di cui gli interessati erano eredi o perché subordinati al pagamento di una somma di denaro richiesta ai sensi dell'art. 119 d.lg. n. 385/1993. In questa seconda decisione è stato ribadito, in particolare, che l'esercizio dei diritti attribuiti dal Codice in materia di dati personali è gratuito e non può essere confuso con il diverso diritto di ottenere copia della documentazione bancaria, condizionato al rispetto delle norme poste dal citato d.lg. n. 385/1993.

Sono state parimenti respinte due opposizioni, presentate da altrettante amministrazioni locali, nei confronti di decisioni con le quali il Garante ha censurato, in termini di mancato rispetto del principio di pertinenza, la pubblicazione nell'albo pretorio di deliberazioni contenenti dati anche sensibili degli interessati.

Ancora in senso favorevole all'Autorità, oltre alle già citate opposizioni in materia di diffusione di fotografie di persone sottoposte a misure restrittive della libertà personale e in tema di accesso ai dati valutativi, si è conclusa l'opposizione proposta dall'amministratore di una società il quale aveva chiesto il blocco dei dati del casellario giudiziale che lo riguardavano, acquisiti da un ente pubblico, che in base ad essi aveva escluso la società da una gara d'appalto (Tribunale di Padova, sentenza n. 2454 del 16 settembre 2004). Nei confronti della sentenza è stato proposto ricorso in Cassazione.

È giunto a positiva conclusione per il Garante anche il giudizio introdotto dal ricorso presentato dinanzi al giudice ordinario da Rai S.p.A. e dall'Agenzia delle entrate contro il *provvedimento* adottato il 5 dicembre 2001 [doc. *web* n. 40405] in materia di canone televisivo. Con tale decisione, confermata dal Tribunale di Roma con sentenza n. 10802 del 29 aprile 2005, l'Autorità ha segnalato a Rai S.p.A., individuata quale responsabile del trattamento per conto dell'amministrazione finanziaria, la necessità di interrompere la raccolta, e di astenersi da ogni ulteriore trattamento dei dati personali degli acquirenti in carenza di presupposti giuridici idonei a legittimare la raccolta e il successivo trattamento dei dati stessi.

Infine, va ricordata la già menzionata ordinanza del 25 maggio 2005 con cui il Tribunale amministrativo del Lazio ha respinto la domanda di sospensione del *provvedimento* del Garante del 15 luglio 2004 concernente l'individuazione delle modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi telefonici cartacei o elettronici.

19.5. *Intervento del Garante in giudizi relativi all'applicazione del Codice*

Come già riferito, nel 2005 si è registrata la notifica al Garante di settantaquattro ricorsi all'autorità giudiziaria, non coinvolgenti direttamente pronunce dell'Autorità (art. 152, comma 7, del Codice).

A tale proposito occorre evidenziare che il Garante, conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato –che si è pronunciata in termini favorevoli alla costituzione in giudizio del Garante, ritenendo essenziale che l'Autorità possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni–, ha deciso di delimitare la propria presenza attiva in giudizio ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto. Ciò, pur continuando a seguire con attenzione tutti i contenziosi.

In questo quadro, l'Autorità, laddove non ha ritenuto opportuno intervenire, ha pregato i competenti uffici dell'Avvocatura generale dello Stato di seguire periodicamente le vicende processuali.

Per sei ricorsi che le sono stati notificati l'Autorità ha ritenuto opportuno costituirsi. In particolare, si è trattato di tre casi –cui si è fatto già riferimento– nei quali è stato adito il Giudice di pace di Taranto. Si è ritenuto che la questione investisse un aspetto generale relativo alla corretta applicazione del Codice, con particolare riferimento alla individuazione nel tribunale ordinario del giudice competente a trattare la materia.

Uno dei casi di costituzione si è avuto in una causa nella quale il ricorrente ha esposto di essere raggiunto sul proprio telefono portatile da messaggi pubblicitari per la cui ricezione non aveva fornito il preventivo assenso. In questo caso l'Autorità ha inteso ribadire i principi già affermati nel proprio *provvedimento* di carattere generale adottato in tema di invio di *Sms* pubblicitari promozionali il 10 giugno 2003 [doc. *web* n. 29836], con il quale ha inteso fornire agli operatori indicazioni necessarie per conformare il trattamento dei dati personali alla disciplina vigente.

Al fine di ribadire principi più volte espressi, il Garante ha ritenuto necessario costituirsi in due giudizi nei quali si verte in tema di accesso, rispettivamente dell'erede (ai dati relativi a rapporti bancari del *de cuius*) e dell'infortunato (alle informazioni di natura valutativa che lo riguardano contenute in una perizia medico-legale).

20 Attività ispettive e applicazione di sanzioni amministrative

20.1. *Il potenziamento del dispositivo di controllo*

Nel 2005 si è registrato un importante incremento delle attività ispettive (+130% rispetto al 2004) in conseguenza di un complesso di decisioni rientranti nel processo di potenziamento delle attività di controllo dell'Autorità.

Anno	*2002*	*2003*	*2004*	*2005*
Ispezioni	40	69	100	230

Il Garante, per svolgere al meglio i compiti di garanzia dei cittadini e per evitare che, nell'esercizio dell'attività di impresa, soggetti poco virtuosi acquisiscano rendite illecite sulla base di trattamenti di dati personali effettuati in contrasto con la legge, a danno delle altre imprese, ha investito nuovamente in modo significativo sull'attività ispettiva attraverso:

- una revisione e un potenziamento organizzativo del Dipartimento che cura tale attività;
- la firma di un nuovo protocollo di intesa con la Guardia di finanza;
- l'introduzione di una nuova procedura di programmazione delle attività ispettive tesa ad intensificare ulteriormente il controllo su determinati settori di volta in volta individuati in ragione di una più specifica attività di analisi.

Per quanto riguarda il profilo organizzativo, l'esperienza degli anni precedenti ha evidenziato la necessità di accorpare organizzativamente funzioni afferenti all'espletamento dell'attività ispettiva e alla contestazione e all'applicazione delle sanzioni amministrative (spesso connesse all'attività ispettiva stessa), oltre che a diversi rapporti con l'autorità giudiziaria, al fine di orientare in una nuova unità organizzativa istituita internamente all'Ufficio del Garante (Dipartimento attività ispettive e sanzioni) la cura del controllo dell'Autorità di tipo ispettivo nei confronti dei settori che hanno evidenziato, anche a seguito delle sanzioni contestate, il più alto coefficiente di inadempimento, nonché di rendere più spedito il procedimento relativo alle contestazioni delle sanzioni che coinvolge l'operato di più unità organizzative.

Alla medesima, nuova unità organizzativa è stata quindi attribuita la competenza di provvedere alla procedura per il *cd.* "ravvedimento operoso" in relazione all'omessa adozione delle misure minime di sicurezza, punita con una sanzione penale dall'art. 169, comma 2. Trattasi della procedura in base alla quale, una volta accertata la mancata adozione di quelle misure di sicurezza considerate come "minime" e previste dal disciplinare tecnico costituente l'Allegato B) al Codice, il Garante impartisce all'autore del reato le prescrizioni per ripristinare il livello minimo di sicurezza previsto dalla legge. La verifica della congruità dell'adempimento apre la strada per la definizione del procedimento attraverso il pagamento del quarto del massimo dell'ammenda prevista dalla legge, estinguendo così il reato.

Altro elemento determinante per lo sviluppo delle attività ispettive è stato rappresentato dalla firma di un nuovo protocollo di intesa con la Guardia di finanza. Il nuovo accordo, siglato presso il Comando generale l'11 novembre 2005, muove dalla considerazione dell'eccellente livello di collaborazione nell'attività di controllo

raggiunto a seguito del protocollo del 2002 e dell'accresciuta capacità operativa del Corpo conseguente all'istituzione del Nucleo funzione pubblica e *privacy*, reparto specializzato nell'attività di vigilanza in materia di protezione dei dati personali.

In relazione a quanto stabilito nel nuovo protocollo la Guardia di finanza, oltre ad assicurare al Garante la collaborazione nell'attività ispettiva, si impegna a rilevare e a segnalare all'Autorità tutte le situazioni rilevanti sotto il profilo dell'applicazione della legge di cui sia venuta a conoscenza nell'ambito dello svolgimento di attività di controllo, constatate anche con altre finalità (ad esempio, nell'ambito dei controlli tributari).

Altro elemento qualificante dell'attività ispettiva svolta nel 2005 è stato il potenziamento dell'attività di prevenzione attraverso accertamenti *cd.* di iniziativa, ovvero avviati *motu proprio* dall'Autorità anche in assenza di atti di impulso di cittadini (segnalazioni, reclami o ricorsi), i quali hanno costituito la parte più consistente dell'intera attività di controllo (circa il 70%).

A partire dal mese di settembre 2005 è stata messa a punto una procedura di programmazione attraverso la quale il collegio del Garante, con cadenza semestrale, tenuto conto delle risorse disponibili, detta le linee di indirizzo dell'attività ispettiva di iniziativa, individuando i settori e gli ambiti delle ispezioni e determinando il numero delle attività di controllo da effettuarsi in relazione ai diversi settori.

Le linee generali degli indirizzi stabiliti con la programmazione dell'attività ispettiva vengono di volta in volta rese pubbliche.

Questa nuova impostazione dell'attività di controllo consente, attraverso verifiche effettuate nei confronti di più soggetti operanti nello stesso settore o che effettuano tipologie omogenee di trattamento, di acquisire importanti elementi di valutazione in ordine:

- al grado di adeguamento al Codice degli operatori appartenenti ad un determinato settore (*ad es.*, società di selezione e collocamento del personale) o che utilizzano i dati personali per particolari finalità (*ad es.*, profilazione dei clienti attraverso l'uso di tessere di fidelizzazione);
- a fenomeni di ampia portata che possono costituire presupposto per l'adozione di provvedimenti generali (diretti, cioè, ad un insieme indeterminato di operatori);
- alla verifica dell'impatto dei provvedimenti adottati.

Ne deriva una valorizzazione dell'attività di controllo come strumento di governo del sistema in un'ottica non solo repressiva, ma anche conoscitiva e di indirizzo.

20.2. *La collaborazione con la Guardia di finanza*

Anche nel 2005 è risultato determinante, nel settore ispettivo, il rapporto con la Guardia di finanza, che ha consentito all'Autorità di poter disporre di risorse qualificate per espletare l'attività di controllo affidata dalla legge.

Il perfezionamento del nuovo protocollo di intesa consente al Garante di avvalersi del Corpo attraverso:

- la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- l'assistenza nei rapporti con l'autorità giudiziaria;
- lo sviluppo di attività ispettive delegate o *sub*-delegate per l'accertamento delle violazioni;
- la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;

- l'esecuzione di indagini conoscitive sullo stato di attuazione del Codice in determinati settori;
- la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

In pratica il Garante, ogni qualvolta ritenga necessario avvalersi della collaborazione del Corpo, attiva il Nucleo speciale funzione pubblica e *privacy* che, disponendo di personale specializzato, provvede direttamente ad effettuare gli accertamenti avvalendosi anche dei reparti del Corpo territorialmente competenti.

Le informazioni e i documenti acquisiti nell'ambito degli accertamenti vengono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei principi previsti dalla legge. Quando nell'ispezione emergono violazioni penali o amministrative la Guardia di finanza procede direttamente ad inoltrare la notizia di reato all'autorità giudiziaria e a contestare la violazione amministrativa.

Una delle novità più rilevanti del nuovo protocollo consiste nel maggior coinvolgimento nell'attività di controllo della componente territoriale della Guardia di finanza (nuclei di polizia tributaria, compagnie e tenenze). L'obiettivo è di disporre di un dispositivo di controllo flessibile ed articolato che consenta, in funzione della complessità degli accertamenti, di effettuarli direttamente a cura del Dipartimento attività ispettive e sanzioni dell'Ufficio del Garante, ovvero attraverso il Nucleo speciale, oppure, nel caso di accertamenti di non elevata complessità che concernono ad esempio la verifica di singoli adempimenti, delegando anche i reparti territoriali della Guardia di finanza.

Al fine di implementare le competenze in materia di protezione dei dati personali, è stato avviato, con il supporto dell'Autorità, già nel mese di dicembre 2005, un complesso piano di formazione del personale appartenente ai comandi territoriali a cui partecipano 120 tra ufficiali e ispettori.

Altro elemento qualificante del nuovo accordo di collaborazione riguarda il supporto che il Corpo si è impegnato ad offrire al Garante per la diffusione delle informazioni sull'applicazione delle norme in materia di protezione dei dati personali, attraverso una stretta interazione tra gli Uffici relazioni con il pubblico. Grazie a questo accordo gli Uffici relazioni con il pubblico della Guardia di finanza potranno costituire, per i cittadini, punti di contatto attraverso i quali ricevere informazioni di prima necessità sulla legge e sui principali adempimenti e reperire materiali esplicativi editi dall'Autorità.

Anche in questo ambito è stato avviato un idoneo percorso formativo per il personale della Guardia di finanza impiegato nel settore delle relazioni con il pubblico.

20.3. *Settori oggetto dei controlli e casi più rilevanti*

I principali settori nei quali sono stati effettuati controlli sono stati:

- aziende sanitarie locali (43);
- società di ricerca e selezione del personale (40);
- società di gestione di alberghi (21);
- società che effettuano sondaggi di opinione (18);
- palestre e centri benessere (12);
- laboratori di analisi che effettuano anche trattamenti di dati genetici (10);
- società che utilizzano tessere di fidelizzazione (10);
- società che utilizzano sistemi di videosorveglianza in luoghi aperti al pubblico (tra cui servizi di trasporto ferroviario, metropolitano e aeroportuale) (7);
- società ed enti che effettuano trattamenti di dati biometrici (5);

- società che gestiscono sistemi di informazione creditizia, *cd.* centrali rischi private (4);
- società che forniscono nuovi servizi televisivi (digitale terrestre e *web* TV) (2);
- operatori telefonici, con riguardo alla *data retention* dei dati di traffico telefonico e telematico (2).

Oltre alle ispezioni di iniziativa di cui sopra, sono state effettuati ulteriori cinquantasei accertamenti in relazione a segnalazioni, reclami e ricorsi pervenuti al Garante o comunque necessari per definire procedimenti aperti dall'Autorità nei confronti di titolari.

I controlli effettuati nei confronti delle aziende sanitarie sono stati volti a verificare l'esatto adempimento alle disposizioni relative alla notificazione al Garante del trattamento di dati genetici e di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria (ai sensi dell'art. 37 del Codice).

Anche se le ispezioni hanno evidenziato un elevato numero di violazioni si è avuto comunque modo di rilevare che alcune realtà hanno avviato interessanti progetti per implementare la protezione dei dati personali attraverso non solo il corretto adempimento degli obblighi di legge, ma anche mediante un'opera di sensibilizzazione e formazione del personale sanitario e amministrativo degli enti, tesa ad accrescere la cultura della *privacy*.

Per quanto riguarda i controlli nei confronti delle società di selezione del personale, sono emerse alcune violazioni relative all'omessa notificazione con riferimento all'art. 37, comma 1, lett. *d)* del Codice –dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato– e alla lett. *e)* del medesimo comma –dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi–.

In generale, si è riscontrato un utilizzo di informative sul trattamento dei dati dei candidati alle selezioni non sempre in linea con i principi del Codice, nonché la diffusione di prassi che non trovano supporto nel dettato normativo, come quella dell'inserimento della locuzione "*autorizzo il trattamento dei miei dati ai sensi del* d.lg. *n. 196/2003*" nell'ambito di *curricula*.

Alcuni accertamenti ispettivi sono stati effettuati a seguito di segnalazioni concernenti accessi illeciti a dati anagrafici detenuti presso il Comune di Roma, al fine di verificare anche il rispetto delle misure di sicurezza nel trattamento dei dati in correlazione a casi di falsa sottoscrizione di candidature alle elezioni regionali del 3 e 4 aprile 2005. L'esito degli accertamenti, effettuati anche nell'esercizio di funzioni di polizia giudiziaria, è stato comunicato alla competente autorità giudiziaria.

Il caso riguardava in particolare accessi effettuati, per finalità e con modalità non consentite, tramite Laziomatica S.p.A. (società per azioni a prevalente capitale regionale istituita dalla Regione Lazio, che le ha affidato la gestione del Sistema informativo regionale), ad una banca dati anagrafica del Comune di Roma che la regione era stata autorizzata a consultare solo per alcune finalità sanitarie, sulla base di un protocollo di intesa. Gli accessi, effettuati in singolari circostanze (utilizzo di *password* altrui; consultazioni in orari non di servizio, notturni e festivi; asseriti interventi di manutenzione straordinaria che hanno determinato la cancellazione di dati di tracciamento di accessi), hanno permesso di consultare ed utilizzare illecitamente vari dati personali inerenti anche a documenti di identità, per finalità diverse da quelle per le quali i dati anagrafici erano stati resi accessibili alla regione (*v.*

amplius par. 2.6). Gli accertamenti effettuati dal Garante sono stati estesi alla sicurezza dei dati presso le banche dati anagrafiche del Comune, ove è emerso il mancato rispetto di alcune misure minime di sicurezza tra le quali l'omesso aggiornamento del documento programmatico sulla sicurezza dei dati, unitamente a talune inosservanze della disciplina applicabile alla gestione dell'anagrafe della popolazione residente. Rispetto ai profili relativi alle misure minime di sicurezza sono stati avviati autonomi procedimenti nei confronti dei responsabili.

Parallelamente a questa vicenda sono stati effettuati accertamenti in relazione a segnalazioni, pervenute nel medesimo periodo, che evidenziavano la possibile utilizzazione illecita, per scopi elettorali, di dati relativi a dipendenti di un ente pubblico e di un'azienda municipale. All'esito dell'attività ispettiva è stata in effetti rilevata la mancata adozione delle misure minime di sicurezza da parte dell'ente pubblico ispezionato e si è proceduto, anche in questo caso, alla segnalazione del reato di cui all'art. 169 del Codice all'autorità giudiziaria competente.

20.4. *L'attività sanzionatoria del Garante*

Le sanzioni amministrative contestate hanno riguardato: l'omessa notificazione al Garante (61); l'omessa o inidonea informativa all'interessato (24); l'omessa risposta alle richieste di informazione del Garante (8) e la mancata acquisizione del consenso preventivo del consumatore per l'utilizzo di sistemi del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax prevista dall'art. 12 del d.lg n. 185/1999 (*v.* ora art. 62 d.lg. 6 settembre 2005, n. 206, recante il Codice del consumo) (1).

A fronte delle sanzioni contestate, sono state riscossi euro 644.000 da parte di enti e società sanzionate che hanno acceduto alla procedura *cd.* di "definizione in via breve", versando il doppio del minimo previsto per la sanzione contestata.

20.5. *Alcuni riferimenti statistici*

Delle 230 attività ispettive effettuate nel 2005, 22 sono state curate direttamente dal Dipartimento attività ispettive e sanzioni del Garante e 208 sono state effettuate su delega dalla Guardia di finanza.

Gli accertamenti hanno riguardato sia l'ambito pubblico (53), sia quello privato (179) e sono stati volti a verificare il rispetto dei principali adempimenti previsti dalla normativa.

Le attività ispettive avviate dal Garante *motu proprio* sono state 169, quelle effettuate nell'ambito di procedimenti conseguenti a segnalazioni pervenute dai cittadini sono state 46; 15 accertamenti sono stati effettuati in relazione ad elementi emersi a seguito di ricorsi, o sono stati tesi a verificare il corretto adempimento dei provvedimenti del Garante.

Con riferimento all'ambito territoriale la ripartizione è stata la seguente:

- nord (97);
- centro (62);
- sud (71).

L'incidenza delle violazioni penali e amministrative riscontrate è stato pari a circa al 44% sul totale delle ispezioni effettuate.

Le violazioni penali segnalate all'autorità giudiziaria riguardano ipotesi di trattamento illecito di dati personali (1), omessa adozione di misure di sicurezza (4), inos-

servanza dei provvedimenti del Garante e false dichiarazioni al Garante (2) e hanno comportato la segnalazione di 10 persone all'autorità giudiziaria.

Undici sono stati i procedimenti connessi al *cd.* "ravvedimento operoso" in materia di misure minime di sicurezza, previsto dall'art. 168, comma 2, del Codice, in relazione ai quali sono state impartite dodici prescrizioni, in relazione alle quali sono state ammesse al pagamento del quarto del massimo dell'ammenda prevista dalla legge, in quanto responsabili della violazione, n. 16 persone, per un totale di sanzioni applicate pari a euro 189.145.

Il Dipartimento attività ispettive e sanzioni ha inoltre provveduto, tramite il Nucleo speciale della Guardia di finanza, alla notifica di 70 atti tra proroghe e decisioni di ricorsi e, in generale, provvedimenti dell'Autorità.

21 Relazioni istituzionali

21.1. *L'Autorità e le attività di sindacato ispettivo e di indirizzo del Parlamento*

Anche nel 2005 l'Autorità ha svolto un ruolo consultivo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo del Parlamento in relazione ad aspetti di specifico interesse in materia di protezione dei dati personali; ha fornito altresì al Governo, ove richiesta, chiarimenti ed indicazioni necessari.

Nell'ambito di tale collaborazione sono stati inoltrati al Governo elementi di valutazione in relazione ad alcuni atti di sindacato ispettivo fra i quali si ricordano, in particolare:

- un'interrogazione a risposta scritta dell'on. Cortiana (n. 4-01434) concernente la diffusione su organi di stampa della vicenda di una ragazza dichiarata adottabile nonostante l'assoluzione del padre dall'accusa di violenza nei suoi confronti (*Nota* 2 agosto 2005). L'Autorità ha richiamato, in proposito, l'applicazione delle disposizioni del Codice (art. 50) e sul processo penale a carico di imputati minorenni (art. 13 d.P.R. 22 settembre 1988, n. 448), che prevedono limiti alla diffusione di notizie e di immagini relative a minori di età o che comunque consentano l'identificazione di minorenni coinvolti in un procedimento giudiziario, anche in materie diverse da quella penale;
- un'interrogazione a risposta orale dell'on. Perrotta (n. 3-3617) concernente l'intestazione ad un utente di più schede telefoniche prepagate, attivate illecitamente a nome e all'insaputa del ricorrente (*Nota* 2 agosto 2005). L'Autorità ha evidenziato di essersi occupata, in più occasioni, dell'attivazione di servizi di telefonia mobile e fissa non richiesti, ivi comprese le schede telefoniche "prepagate", anche in relazione alla vicenda cui si riferiva l'interrogazione, già oggetto di un ricorso presentato all'Autorità per i connessi profili riguardanti la protezione dei dati personali.

21.2. *L'attività consultiva del Garante sugli atti del Governo*

L'articolo 154, comma 4, del Codice prevede che il Presidente del Consiglio dei ministri e ciascun Ministro consultino il Garante all'atto della predisposizione di norme regolamentari e di atti amministrativi suscettibili di incidere sulla protezione dei dati personali, nell'interesse pubblico e dei cittadini, al fine di prevenire problemi applicativi e in un quadro di collaborazione istituzionale del quale, più volte, vari ministeri hanno riconosciuto l'importanza e l'utilità.

Nel 2005, il Garante ha espresso in questa chiave diversi pareri i quali hanno riguardato, in particolare:

- uno schema di provvedimento dell'Agenzia delle entrate con cui sono state stabilite le specifiche tecniche per l'invio delle richieste e delle risposte in modalità telematica in materia di indagini finanziarie, in attuazione dell'art. 32, comma 3, d.P.R. n. 600/1973 e dell'art. 51, comma 4, d.P.R. n. 633/1972 (*Parere* 21 dicembre 2005 [doc. *web* n. 1210095]). Il provvedimento individua, quale modalità di comunicazione, la posta elet-

tronica certificata, la cui casella è accessibile tramite *password* ed è utilizzabile solo dai titolari degli accertamenti (provvedimento Agenzia delle entrate 22 dicembre 2005, in *G.U.* 10 gennaio 2006, n. 7, *S.O.* n. 6);

- uno schema di regolamento che istituisce presso il Dipartimento per lo sviluppo delle economie territoriali della Presidenza del Consiglio dei ministri una banca di dati informatica denominata "Guida agli investimenti locali" (*Parere* 21 dicembre 2005 [doc. *web* n. 1212504]);
- uno schema di regolamento del Ministro del lavoro e delle politiche sociali, di concerto con il Ministro della salute, concernente gli accertamenti di assenza di tossicodipendenza sui lavoratori destinati a mansioni che comportano rischi per la sicurezza, l'incolumità e la salute dei terzi, adottato ai sensi dell'art. 125 d.P.R. 9 ottobre 1990, n. 309, e successive modificazioni (*Parere* 15 dicembre 2005 [doc. *web* n. 1209068]). Nel parere, dopo aver segnalato che gli esami per accertare l'assenza di tossicodipendenza nell'ambito di particolari categorie di lavoratori devono essere compiuti nel rispetto della dignità e della riservatezza delle persone coinvolte, l'Autorità ha sottolineato la necessità che il regolamento eviti formulazioni generiche o non rispettose del principio di proporzionalità rispetto alle finalità di tali esami. È stato richiesto, in particolare, di specificare la previsione che impone gli esami complementari tossicologici; in considerazione della loro invasività, è stato richiesto di precisare che questo tipo di esami (successivi alla visita medica) vanno eseguiti soltanto quando ci si trovi in presenza di sintomi di una "dipendenza" da sostanze stupefacenti e non solo di un loro uso, magari occasionale. Il Garante ha poi chiesto di individuare con precisione i casi di incidente sul lavoro che possono imporre tali accertamenti e i conseguenti trattamenti di dati, dovendosi fare riferimento solo a quelli che, per le loro caratteristiche e in relazione ai comportamenti dei lavoratori coinvolti, possano derivare da una tossicodipendenza;
- uno schema di decreto del Presidente della Repubblica recante modifiche alla disciplina concernente il sistema matricolare del Corpo della Guardia di finanza, adottato ai sensi dell'art. 5 l. 5 novembre 1962, n. 1695 (*Parere* 19 ottobre 2005 [doc. *web* n. 1185148]);
- uno schema di decreto del Ministro dell'interno, di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, concernente le misure che i titolari o gestori di esercizi pubblici e circoli privati che pongono a disposizione del pubblico apparecchi terminali utilizzabili per comunicazioni, anche telematiche (*cd.* Internet *point*), devono osservare per rispettare l'obbligo di monitorare le operazioni degli utenti e di archiviare i relativi dati, ai sensi dell'articolo 7, comma 4, d.l. n. 144/2005 (decreto *cd.* "antiterrorismo", sul quale *v. amplius* par. 1.1.) (*Parere* 11 agosto 2005 [doc. *web* n. 1170246]). Il decreto adottato ha recepito le osservazioni del Garante (d.m. 16 agosto 2005, in *G.U.* 17 agosto 2005, n. 190);
- uno schema di decreto del Ministro degli affari esteri, per l'istituzione di un nuovo modello di passaporto ordinario atto a contenere dati biometrici (*cd.* passaporto elettronico), in linea con quanto previsto in sede comunitaria (regolamento del Consiglio n. 2252/2004 e decisione della Commissione n. 409/2005) (*Parere* 26 luglio 2005 [doc. *web* n. 1153396]). Il decreto ha recepito le osservazioni del Garante prevedendo, in particolare, che i dati biometrici possano essere utilizzati solo per finalità di verifica dell'identità del titolare e non debbano essere registrati in banche di dati (d.m. 29 novembre 2005, in *G.U.* 17 gennaio 2006, n. 13);

- uno schema di decreto interministeriale, trasmesso dal Ministero dell'interno, per individuare i dati e le informazioni da registrare nell'archivio informatizzato dello Sportello unico per l'immigrazione, ai sensi dell'art. 30-*quater*, comma 3, d.P.R. n. 394/1999, introdotto dal d.P.R. n. 334/2004 (*Parere* 26 luglio 2005 [doc. *web* n. 1152007]);
- uno schema di decreto del Ministro della salute, relativo all'istituzione del registro nazionale delle strutture autorizzate all'applicazione delle tecniche della procreazione medicalmente assistita, degli embrioni formati e dei nati a seguito dell'applicazione delle tecniche medesime, previsto dall'art. 11, comma 1, l. n. 40/2004 (*Parere* 26 luglio 2005 [doc. *web* n. 1151435]; *v.* par. 3.1.4). Il decreto ha recepito le indicazioni del Garante prevedendo che nel registro possano essere inseriti solo dati in forma anonima, anche aggregata, relativi alle coppie che accedono alle predette tecniche, agli embrioni e ai nati (d.m. 7 ottobre 2005, in *G.U.* 3 dicembre 2005, n. 282);
- uno schema di provvedimento del Ministero dell'economia e delle finanze relativo alla trasmissione al Ministero della salute e alle regioni, con modalità telematiche, dei dati relativi alle ricette mediche, ai sensi dell'art. 50, comma 10, d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, dalla l. n. 326/2003 (*Parere* 21 luglio 2005 [doc. *web* n. 1151167]). Il provvedimento è stato adottato in data 9 marzo 2006 ed è stato pubblicato nella *G.U.* 20 marzo 2006, n. 66;
- uno schema di decreto del Ministro dell'interno concernente la modulistica relativa ai procedimenti per l'assunzione di lavoratori stranieri e per il ricongiungimento familiare, di competenza dello Sportello unico per l'immigrazione, ai sensi dell'art. 30-*bis* d.P.R. n. 394/1999 (*Parere* 25 maggio 2005 [doc. *web* n. 1131847]);
- tre schemi di regolamento del Ministro dell'economia e delle finanze concernenti gli obblighi antiriciclaggio per intermediari abilitati, altri operatori non finanziari e alcuni professionisti, in attuazione degli articoli 3, comma 2, e 8, comma 4, d.lg. n. 56/2004 (*Parere* 12 maggio 2005 [doc. *web* n. 1131800]);
- due schemi di decreto del Ministro dell'interno in materia di registrazione di immagini e di titoli di accesso negli stadi, adottati in attuazione dell'art. 1-*quater* d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla l. 2 aprile 2003 n. 88 (*Parere* 4 maggio 2005 [doc. *web* n. 1120732]; *v.* par. 13.1). I decreti prevedono l'utilizzo di strumenti di videosorveglianza presso gli impianti sportivi di capienza superiore alle diecimila unità e l'obbligo di accedere nei medesimi stadi muniti di biglietti nominativi (dd.mm. 6 giugno 2005, in *G.U.* 30 giugno 2005, n. 150);
- uno schema di decreto dirigenziale del Ministero della giustizia, di attuazione in via parziale e transitoria dell'art. 33 d.P.R. 14 novembre 2002, n. 313, concernente il rilascio all'interessato della visura, non avente valore di certificato, dei dati registrati nel casellario giudiziale (*Nota* 6 aprile 2005). Il decreto è stato adottato il 1° agosto 2005 ed è stato pubblicato nella *G.U.* 10 ottobre 2005, n. 185;
- due schemi di decreto del Ministro dell'istruzione, recanti l'individuazione delle modalità e dei contenuti delle prove di ammissione ad alcuni corsi di laurea programmati a livello nazionale (*Nota* 5 aprile 2005; *v.* par. 2.7.1);
- uno schema di convenzione fra il Ministero dell'interno e l'Agenzia del territorio ai sensi dell'art. 54 del Codice, per l'accesso degli organi di polizia agli archivi informatici del catasto terreni, del catasto edilizio urbano e del catasto geometrico, ai fini della consultazione degli atti (*Nota* 4 aprile 2005);

- uno schema di regolamento del Dipartimento per le pari opportunità della Presidenza del Consiglio dei ministri, recante modifiche ed integrazioni al regolamento sulla costituzione e il funzionamento della commissione per le adozioni internazionali (d.P.R. 1° dicembre 1999, n. 492) (*Nota* 4 aprile 2005);
- due schemi di decreti (trasmessi dal Ministero delle attività produttive), concernenti l'utilizzo di strumenti di controllo nel settore dei trasporti su strada (tachigrafi digitali), adottati ai sensi dell'art. 3, commi 7 e 8, d.m. n. 361/2003 (*Nota* 18 febbraio 2005). Le indicazioni fornite dal Garante sono state recepite nei decreti adottati (d.m. 11 marzo 2005, in *G.U.* 11 maggio 2005, n. 108; d.m. 23 giugno 2005, in *G.U.* 26 luglio 2005, n. 172).

L'Autorità, inoltre, nel quadro di una proficua collaborazione istituzionale, ha fornito osservazioni ed elementi di valutazione sugli aspetti di protezione dei dati personali in ordine ad alcuni schemi di decreti legislativi, alle amministrazioni che ne hanno fatto richiesta, con particolare riferimento al codice dell'amministrazione digitale, al sistema pubblico di connettività e all'utilizzo di dati pubblici (*v. amplius* par. 1.4).

A fronte dei pareri espressi sopra menzionati, deve segnalarsi che –anche se in misura ridotta rispetto al 2004– continuano a registrarsi casi di mancata consultazione dell'Autorità. Si riportano le fattispecie più significative:

- decreto del Ministro della salute 30 dicembre 2004 (*"Norme procedurali per l'effettuazione dei controlli antidoping e per la tutela della salute, ai sensi dell'art. 3, comma 1, della legge 14 dicembre 2000, n. 376"*) (*G.U.* 17 febbraio 2005, n. 39);
- provvedimento dell'Agenzia delle entrate 10 marzo 2005 (*"Trasmissione telematica di comunicazioni all'anagrafe tributaria"*) (*G.U.* 21 marzo 2005, n. 66);
- provvedimento dell'Agenzia delle entrate 16 marzo 2005 (*"Comunicazione all'anagrafe tributaria dei dati catastali identificativi degli immobili presso cui sono attivate utenze di energia elettrica, di servizi idrici e del gas"*)(*G.U.* 23 marzo 2005, n. 68);
- decreto del Ministro del lavoro e delle politiche sociali 4 febbraio 2005 (*"Istituzione del Casellario centrale delle posizioni previdenziali attive, presso l'Istituto nazionale della previdenza"*) (*G.U.* 29 marzo 2005, n. 72);
- decreto del Ministro della salute 3 marzo 2005 (*"Protocolli per l'accertamento della idoneità del donatori di sangue di emocomponenti"*) (*G.U.* 13 aprile 2005, n. 85);
- decreto del Ministro della salute 3 marzo 2005 (*"Caratteristiche e modalità per la donazione del sangue e di emocomponenti"*)(*G.U.* 13 aprile 2005, n. 85);
- decreto del Ministro dell'interno 2 agosto 2005 (*"Modificazioni al d.m. 19 luglio 2000, recante: «Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici»*) (*G.U.* 12 agosto 2005, n. 187);
- decreto del Ministro dell'interno 2 agosto 2005 (*"Regole tecniche e di sicurezza per la redazione dei piani di sicurezza comunali per la gestione delle postazioni di emissione Cie, in attuazione del comma 2 dell'art. 7*-vicies ter *della legge 31 marzo 2005, n. 43"*)(*G.U.* 19 settembre 2005, n. 218);
- decreto del Ministro dell'economia e delle finanze 4 agosto 2005 (*"Modalità di attuazione del progetto Pc ai giovani"*) (*G.U.* 27 settembre 2005, n. 225).

21.3. *Altra collaborazione con la Presidenza del Consiglio dei ministri*

L'Autorità ha proseguito, nel 2005, l'attività consultiva sollecitata dalla Presidenza del Consiglio dei ministri sul contenuto di alcune leggi regionali, rispetto agli aspetti riconducibili alla materia della protezione dei dati personali, al fine di segnalare questioni eventualmente rilevanti in sede di conflitto di attribuzioni tra Stato e regioni.

In alcuni casi non si sono ravvisati profili di illegittimità costituzionale; in altri, sono stati invece rilevati aspetti problematici, come avvenuto nel caso della legge della Regione Toscana 15 dicembre 2004, n. 63, recante "*Norme contro le discriminazioni determinate dall'orientamento sessuale o dall'identità di genere*", di cui si è già riferito nella *Relazione* 2004 (p. 136).

In particolare, l'esame degli articoli 7 e 8 di tale legge –che individuano il soggetto competente ad esprimere il consenso ad un determinato trattamento terapeutico per conto di chi si trovi in condizione di incapacità e grave pericolo per la salute o l'integrità fisica– ha evidenziato questioni di legittimità costituzionale attinenti al profilo della potestà legislativa dello Stato in materia di protezione di dati personali, con specifico riferimento alle disposizioni del Codice sull'acquisizione del consenso informato al trattamento dei dati, sulle garanzie a tutela della riservatezza dei pazienti e sulla necessità e proporzionalità della raccolta di informazioni in banche di dati. L'Autorità ha segnalato tali aspetti alla Presidenza del Consiglio dei ministri (*Nota* 11 gennaio 2005) che ha, in seguito, impugnato la legge davanti alla Corte costituzionale.

Di particolare interesse si sono inoltre rivelate le ulteriori vicende della legge della Regione Emilia-Romagna 24 maggio 2004, n. 11 (*Sviluppo regionale della società dell'informazione*). Come riportato nella precedente *Relazione* (p. 135), l'Autorità aveva rilevato importanti profili di illegittimità costituzionale di tale legge, che sono stati poi dedotti dalla Presidenza del Consiglio dei ministri nel contestarne la legittimità dinanzi alla Consulta.

Con sentenza 7 luglio 2005, n. 271, la Corte costituzionale ha sostanzialmente accolto le argomentazioni contenute nel ricorso presentato dalla Presidenza del Consiglio dei ministri, dichiarando incostituzionali gli artt. 12, 13 e 14 della legge regionale in relazione all'art. 117, secondo comma, lettere *l*), *m*) ed *r*), e sesto comma, Cost., e in riferimento ai principi della legislazione statale in materia di protezione dei dati personali.

La Corte ha rilevato che, alla luce del riparto delle potestà legislative di cui al nuovo art. 117 Cost., al legislatore regionale va riconosciuta una limitata competenza *"a disciplinare procedure o strutture organizzative che prevedono il trattamento di dati personali"*, e solo *"nell'integrale rispetto della legislazione statale sulla loro protezione"*; di qui la dichiarazione di illegittimità costituzionale sia dell'art. 12 della legge (che, pur affermando il rispetto delle norme a tutela della riservatezza e delle forme di segreto, risultava in concreto contraddire sotto molteplici profili la legislazione statale vigente in materia di protezione dei dati personali, nonché le stesse direttive europee che ne sono all'origine), sia dell'art. 13, comma 1, della medesima legge (nella parte in cui non richiamava la legislazione statale in materia di protezione dei dati personali).

In seguito alla dichiarazione di incostituzionalità, la Regione Emilia-Romagna, con la legge regionale 22 dicembre 2005, n. 22, ha modificato il testo degli articoli 12 e 13 della predetta l.r. n. 11/2004. L'Autorità ha rilevato che le nuove disposizioni approvate da tale Regione possono ritenersi nel loro complesso sostanzialmente rispondenti ai principi affermati dalla Corte. Il Garante si è peraltro soffer-

mato in particolare su una disposizione (il nuovo comma 7 del citato articolo 12), che intende promuovere la comunicazione alla regione e agli altri soggetti pubblici dei dati personali contenuti nei sistemi informativi dei soggetti privati che operano in ambito regionale svolgendo "attività di interesse pubblico", precisando che ritiene possibile interpretarla –conformemente alla prospettiva indicata dalla Corte– nel senso che la regione potrà promuovere la predetta comunicazione di dati relativamente alle sole informazioni pertinenti e non eccedenti rispetto alle attribuzioni regionali. L'Autorità ha rilevato, altresì, che in sintonia con questa interpretazione dovrebbe essere letta anche l'ulteriore previsione, prevista dalla l.r. n. 11/2004, di intese fra la regione stessa e gli enti locali, in relazione alle rispettive attribuzioni dei diversi enti, necessarie per assicurare il rispetto del principio di finalità nel trattamento (*Nota* 10 febbraio 2006).

22 Relazioni internazionali

Lo stato di recepimento delle direttive comunitarie negli Stati membri dell'Unione europea

Non vi sono particolari novità da segnalare per quanto riguarda il recepimento della direttiva generale in materia di protezione dei dati personali (direttiva n. 95/46/Ce), poiché tutti gli Stati membri hanno già adottato disposizioni attuative nel diritto interno e non sussistono attualmente, né sono state avviate procedure di infrazione dalla Commissione europea.

Occorre invece menzionare brevemente alcuni sviluppi intercorsi nel 2005 in rapporto alla direttiva "*e-Privacy*" (direttiva n. 2002/58/Ce). Come riferito nella *Relazione* 2004 (p. 141), la Commissione europea aveva adito la Corte di giustizia nei confronti di alcuni Paesi (Belgio, Grecia, Lussemburgo) per omessa segnalazione delle misure nazionali di recepimento della direttiva n. 2002/58/Ce. Successivamente, Belgio e Lussemburgo hanno notificato l'adozione dei provvedimenti che recepiscono le disposizioni della direttiva e il procedimento avviato nei loro confronti si è quindi concluso. Viceversa, la Grecia non risulta aver notificato le norme nazionali di trasposizione e risulta altresì essere l'unico Stato membro dell'Ue nei cui confronti è aperto un procedimento dinanzi alla Corte per mancato recepimento della direttiva stessa.

Sono tuttavia in corso altre procedure di infrazione aperte nei confronti di Repubblica Ceca, Germania, Lettonia e Slovacchia per imperfetta trasposizione delle disposizioni contenute nella medesima direttiva. In particolare, Repubblica Ceca, Lettonia e Slovacchia non avrebbero attuato correttamente le norme comunitarie in materia di comunicazioni commerciali indesiderate (art. 13 dir. n. 2002/58/Ce), mentre la Slovacchia non avrebbe introdotto l'obbligo di informare gli utenti della presenza e dei meccanismi di funzionamento dei *cookie*. Rispetto alla Germania, i servizi della Commissione stanno inoltre valutando la trasposizione delle norme concernenti i dati relativi all'ubicazione (art. 9), che non sarebbero pienamente recepite nel diritto interno. Infine, è da segnalare che la Commissione europea ha inviato un "parere motivato" al Regno Unito (il secondo passo nella procedura di infrazione, che fa seguito all'invio di una lettera di "messa in mora") per non aver notificato alcuna misura di attuazione relativa al territorio di Gibilterra, cui si applicano le norme comunitarie ai sensi del Trattato di adesione del Regno Unito alle Comunità europee.

Conferenze delle autorità di protezione dei dati a livello europeo

Dal 1991, le autorità di protezione dati europee si incontrano tutti gli anni in primavera in un'occasione divenuta ormai istituzionale, la *cd. Spring Conference*. Nel 2005, la Conferenza di primavera si è svolta il 25 e 26 aprile a Cracovia ed è stata dedicata in particolare alla valutazione dell'impatto della direttiva n. 95/46/Ce, a dieci anni dalla sua approvazione. Fra gli altri temi all'ordine del giorno meritano di essere menzionati il trasferimento di dati verso Paesi "non adeguati", con particolare riferimento alle "regole vincolanti nell'impresa" (*Binding Corporate Rules*), alla figura dell'incaricato per la *privacy* (*privacy officer*) e alle modalità di regolazione nazionale del diritto di accesso da parte dell'interessato ai propri dati personali.

Il dibattito che ha caratterizzato maggiormente la Conferenza, dando luogo ad una Dichiarazione e ad una presa di posizione ufficiali delle autorità di protezione dati, ha riguardato il tema dei flussi di dati nelle attività giudiziarie e di polizia, anche in previsione dell'adozione da parte della Commissione europea di uno stru-

mento che fissi le garanzie da applicare al trattamento dei dati personali nel *cd.* "Terzo pilastro". Nel documento comune, le autorità, dando atto che le attività di lotta al terrorismo e al crimine organizzato comportano un rafforzamento dello scambio di dati personali, hanno chiesto che tale scambio avvenga apprestando previamente un sistema di garanzie adeguato per la protezione dei dati personali.

Le autorità hanno ribadito che gli *standard* fissati nella direttiva n. 95/46/Ce restano validi anche per il trattamento di dati per le predette finalità, ed hanno rilevato in particolare che la proporzionalità del trattamento deve essere utilizzata come criterio per valutare la necessità delle misure che prevedono uno scambio di informazioni nel Terzo pilastro. Ciò significa che dovrà essere garantito il controllo a livello nazionale e comunitario da parte delle autorità indipendenti, con il coinvolgimento degli Stati membri.

Successivamente alla presentazione da parte della Commissione europea, in data 11 ottobre 2005, di una proposta di decisione-quadro per introdurre principi armonizzati di protezione dati nei trattamenti di dati per finalità di giustizia e polizia (2005/0202/Cns), le autorità garanti hanno inoltre adottato un parere nel quale, oltre a richiamare le linee esposte nella dichiarazione, hanno sviluppato una serie di osservazioni puntuali sul testo.

Conferenze delle autorità su scala internazionale

La 27ma Conferenza internazionale dei Garanti si è tenuta in Svizzera, a Montreux, dal 14 al 16 settembre 2005, ed ha riunito le autorità di 45 Paesi. Durante la Conferenza sono state poste al centro dell'attenzione le tematiche relative alla tutela delle libertà fondamentali –in particolare della *privacy*– nell'attuale contesto geopolitico, delle applicazioni biometriche, dello sviluppo di tecnologie invasive, del *marketing* politico e della creazione e gestione delle biobanche.

A quest'ultimo tema è stata dedicata una intera sessione, presieduta dal presidente del Garante prof. Francesco Pizzetti, il quale ha affrontato i delicati problemi posti dalle strutture che conservano a scopi sanitari o di ricerca i campioni biologici, con particolare riguardo alla necessità di determinare quali soggetti possano trattare dati relativi a campioni biologici, alle modalità di controllo del loro utilizzo e al rischio di sovrapposizione dei compiti delle autorità di garanzia e dei comitati etici.

Nell'ambito dei lavori della Conferenza, il segretario generale dell'Autorità dott. Giovanni Buttarelli è intervenuto sul tema della comunicazione politica, soffermandosi sull'analisi dei principi guida dettati dal *provvedimento* del 7 settembre 2005 [doc. *web* n. 1165613] per una propaganda elettorale rispettosa dei cittadini, e auspicando l'adozione di un codice deontologico che disciplini in modo organico il *marketing* politico, nonché l'individuazione di principi generali in cui tutte le autorità nazionali possano riconoscersi.

Al termine della Conferenza sono stati adottati tre importanti documenti. Nella Dichiarazione su "La protezione dei dati personali e della *privacy* in un mondo globalizzato: un diritto universale che rispetta le diversità", i Garanti hanno ribadito l'impegno a collaborare con i governi e con gli organismi internazionali e sopranazionali, al fine di mettere a punto una "convenzione universale" per la protezione delle persone fisiche rispetto al trattamento di dati personali. A tal fine le autorità hanno rivolto un invito alle Nazioni unite affinché preparino uno strumento giuridico vincolante, un'esortazione a tutti i governi del mondo affinché promuovano l'adozione di strumenti in materia di protezione dei dati e della *privacy* conformi ai principi fondamentali (fra cui rientra il principio del controllo indipendente e dell'esistenza di sanzioni) e un appello al Consiglio d'Europa affinché inviti anche gli Stati non membri ad aderire alla Convenzione n. 108/1981 e al suo Protocollo addizionale.

Nella stessa Dichiarazione sono stati inoltre sollecitati:

- gli organismi internazionali, ad istituire al proprio interno autorità di vigilanza indipendenti dotate di poteri di controllo;
- le organizzazioni non governative internazionali, a mettere a punto *standard* basati sui principi fondamentali della protezione dati;
- i produttori di *hardware* e *software*, a sviluppare prodotti e sistemi che incorporino tecnologie idonee a potenziare la *privacy*.

Nella "Risoluzione sull'utilizzo della biometria in passaporti, carte di identità e titoli di viaggio"[doc. *web* n. 1170552], le autorità, dopo aver rilevato l'impiego crescente dei dati biometrici sia nel settore pubblico, sia in quello privato, nonché i rischi connessi alla possibilità di raccogliere tali dati all'insaputa dell'interessato e di utilizzarli come identificatori univoci a livello globale, hanno richiesto:

- che l'impiego delle tecnologie biometriche preveda garanzie efficaci al fine di limitare i rischi connessi alla loro natura;
- che si tengano rigidamente distinti i dati biometrici raccolti e memorizzati per finalità di natura pubblica in base ad obblighi di legge (ad esempio, i controlli alle frontiere) e quelli raccolti e memorizzati per finalità contrattuali sulla base del consenso;
- che si limiti tecnicamente l'impiego della biometria nei passaporti e nelle carte d'identità alle finalità di verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal titolare all'atto della presentazione del documento stesso.

Infine, nella "Risoluzione sull'utilizzo di dati personali per la comunicazione politica" [doc. *web* n. 1170546], predisposta e presentata dal Garante, è stato ribadito che ogni attività di comunicazione politica che comporti il trattamento di dati personali deve rispettare i diritti e le libertà fondamentali degli interessati, fra cui rientra il diritto alla protezione dei dati personali.

Nel documento, i principi di *data protection* consolidati vengono declinati con riferimento alla comunicazione politica. In particolare, si stabilisce che i dati personali devono essere trattati solo se necessari per il raggiungimento delle finalità di comunicazione politica; devono essere raccolti attraverso fonti accessibili lecitamente, accurati, pertinenti, non eccedenti e aggiornati. I dati raccolti da fonti, istituzioni o associazioni pubbliche o private possono essere utilizzati per scopi di comunicazione politica solo se il trattamento ulteriore è compatibile con le finalità per le quali sono stati raccolti e gli interessati sono stati informati. L'informativa deve precedere la raccolta dei dati e specificare l'identità del titolare e le tipologie di flussi, mentre il trattamento deve essere fondato sul consenso dell'interessato o su un altro presupposto legittimo previsto dalla legge. I titolari del trattamento, siano essi forze politiche o singoli candidati, devono adottare tutte le misure di sicurezza necessarie a tutelare l'integrità delle informazioni e a prevenire la perdita e/o l'utilizzo abusivo dei dati. Devono inoltre essere riconosciuti agli interessati il diritto di accesso, rettifica, blocco e/o cancellazione, nonché il diritto di opporsi alle comunicazioni indesiderate e il diritto di chiedere, gratuitamente e con modalità semplici, di non ricevere ulteriori messaggi. L'esistenza di tali diritti deve essere menzionata nell'informativa e in caso di violazione devono essere previsti adeguati rimedi giuridici e sanzioni.

22.1. *La cooperazione tra autorità garanti nell'Ue: il Gruppo art. 29*

Nel 2005 è stato avviato un più intenso rapporto di collaborazione del con la Commissione e, in particolare, con il nuovo commissario italiano on. Frattini, vice

presidente e responsabile del settore Libertà, sicurezza e giustizia, per garantire il pieno rispetto del diritto alla protezione dei dati personali e favorire un dialogo più intenso tra le autorità indipendenti e le istituzioni comunitarie.

Per sottolineare questo impegno, in gennaio il Commissario ha incontrato il Gruppo riaffermando le linee di azione e gli impegni già presi in materia dalla nuova Commissione e annunciati sia nel primo contatto con il Parlamento europeo, sia nella precedente riunione di dicembre con le autorità comuni di controllo.

Proprietà intellettuale

L'incremento della circolazione delle informazioni legato allo sviluppo di Internet pone il delicato problema del controllo delle informazioni protette dal diritto d'autore, in particolar modo con riferimento ai diritti e agli obblighi dei soggetti che hanno interessi rispetto alle informazioni protette dal *copyright* e dei soggetti che sono coinvolti nel *digital rights management*. Il Gruppo art. 29 si è occupato del rapporto tra diritti di proprietà intellettuale e protezione dati in un documento di lavoro adottato il 18 gennaio 2005 (WP 104). Il documento è rivolto ai soggetti coinvolti a vario titolo nella gestione del *copyright* (titolari, produttori, fornitori di servizi e utenti).

Con riferimento alla tutela preventiva del diritto d'autore, nel documento sono state analizzate le tecnologie usate più frequentemente per il trattamento di dati personali. In alcuni casi viene chiesto all'utente di identificarsi per poter accedere a determinati contenuti, e viene associato al contenuto scaricato da Internet un identificatore univoco, che lega inscindibilmente l'utente a quel contenuto. In altri casi vengono impiegate tecniche di tracciamento finalizzate ad individuare gli utenti che scaricano documenti o altro materiale protetto senza averne il diritto: in questi casi i legittimi titolari del diritto d'autore ricorrono solitamente all'indirizzo *Ip* dell'utente, oppure impongono ai fornitori di servizi Internet di comunicare i dati in loro possesso, ovvero confrontano tali informazioni con i dati contenuti nei registri *Whois*. Il Gruppo, rispetto ai casi appena descritti, ha ricordato la necessità di rispettare alcuni principi fondamentali in materia di protezione dati, e in particolare la possibilità di mantenere l'anonimato nelle operazioni che avvengono in Internet, l'impiego di identificatori univoci solo se disciplinato da specifiche norme nazionali secondo quanto previsto dalla direttiva n. 95/46/Ce, lo sviluppo di ausili tecnologici che consentano di ridurre l'ambito dei dati personali utilizzati in rapporto alle singole operazioni (*Privacy Enhancing Technologies-Pet*), l'obbligo di fornire agli interessati un'informativa adeguata e preventiva, il rispetto del principio di finalità e la necessità di delimitare il tempo di conservazione dei dati.

Con riferimento alla tutela *ex post*, finalizzata a individuare i soggetti sospettati di avere violato la normativa sul diritto d'autore, sono stati parimenti ribaditi alcuni principi. I dati contenuti nel registro *Whois* non devono essere utilizzati per finalità incompatibili con quelle per cui sono stati raccolti, e gli *Internet Service Provider* (Isp) non sono tenuti a fornire a soggetti privati, titolari di diritti d'autore, le informazioni in loro possesso, raccolte per la fornitura dei servizi di tlc (diverso è il caso in cui la richiesta provenga da autorità giudiziarie o di polizia, sulla base di specifiche disposizioni di legge). Con riferimento al tempo di conservazione dei dati, gli Isp non sono tenuti a conservare a tempo indeterminato tutti i dati di traffico relativi a informazioni tutelate dal diritto d'autore. La conservazione di dati giudiziari può avvenire solo nel rispetto di rigide disposizioni adottate dai singoli Stati membri, i quali devono prevedere anche adeguate garanzie per gli interessati.

Rfid

L'utilizzo delle tecnologie *Rfid* (*Radio Frequency Identification*) pone diverse problematiche da analizzare per il pieno rispetto dei diritti degli interessati. La tecnologia *Rfid* è utilizzata in un numero crescente di settori, fra i quali si possono ricordare

il settore dei trasporti, della distribuzione, dell'aviazione, della sanità, del controllo degli accessi, della vendita al dettaglio; pur caratterizzata da evidenti vantaggi da un punto di vista economico –anche in considerazione dei costi relativamente contenuti– se non correttamente utilizzata la *Rfid* può infatti consentire indebite intrusioni nella sfera privata. Attraverso questi dispositivi è infatti possibile raccogliere surrettiziamente differenti categorie di dati: ad esempio, profilare i clienti, monitorando i loro comportamenti, i capi di abbigliamento, gli accessori o le medicine utilizzate.

Il Gruppo art. 29 ha approvato un documento di lavoro (WP 105, 19 gennaio 2005), rivolto agli utilizzatori di queste tecnologie e ai produttori ed organismi che si occupano di standardizzazione, chiamati a cooperare per orientare queste tecnologie in termini più rispettosi della *privacy*.

Dopo aver richiamato l'attenzione sulla necessità di applicare tutti i principi contenuti nelle direttive europee in materia di protezione dei dati laddove si trattino informazioni relative ad un individuo identificato o identificabile, il Gruppo ha sottolineato la possibilità di utilizzare dispositivi tecnologici e accorgimenti di varia natura al fine di dare effettiva attuazione a tali principi. Esistono, infatti, strumenti che, a vari livelli, permettono di sviluppare i principi di protezione dati già all'interno di dispositivi come quelli basati sulle tecnologie *Rfid*.

Fra le indicazioni specifiche fornite dal Gruppo di lavoro si evidenziano in particolare:

a) il riconoscimento del diritto degli interessati ad essere informati, sia sulla presenza di dispositivi *Rfid*, sia sulla loro attivazione (*ad es.*, attraverso pittogrammi, o segnalazioni luminose);

b) la possibilità di esercitare il diritto di accesso, rettifica, cancellazione ecc. (viene consigliato l'utilizzo di linguaggi *standard* come l'*Xml* o di dispositivi per la disattivazione permanente o temporanea);

c) la necessità che il trattamento di dati personali attraverso la tecnologia *Rfid* sia comunque basato sul consenso dell'interessato e, laddove sia possibile ritirare il consenso, che siano utilizzati dispositivi in grado di disattivare facilmente il *tag Rfid* (*tag disabler*);

d) la necessità di proteggere i dati personali contenuti nei *tag Rfid* attraverso misure di sicurezza proporzionali alla natura del trattamento effettuato (cifratura e autenticazione del lettore *Rfid*, impiego di protocolli *standard* di autenticazione secondo norme Iso, impiego di metodi di autenticazione crittografica ecc.).

Il documento è stato sottoposto ad una consultazione pubblica, conclusasi il 31 marzo 2005, a cui hanno partecipato soggetti pubblici e privati. Sulla base dell'analisi delle risposte è stato preparato un documento di sintesi che non esprime considerazioni di merito e si limita a evidenziare alcune questioni maggiormente controverse:

- non necessità di integrare la direttiva n. 95/46/Ce con norme specifiche per la *Rfid*. Tale opportunità non risulta condivisa dalle imprese, secondo le quali una regolamentazione troppo dettagliata potrebbe avere ripercussioni negative in termini di concorrenza rispetto ad altre aree del mondo;
- richiesta al Gruppo art. 29 di fornire ulteriori indicazioni riferite specificamente a determinate applicazioni (*ad es.*, uso di dispositivi *Rfid* nelle attività commerciali, nei passaporti, nei trasporti pubblici);
- necessità di approfondire la natura dei trattamenti effettuati attraverso dispositivi *Rfid*, con particolare riguardo all'esistenza di un trattamento effettivo di dati personali e al concetto di dato personale, che a giudizio di alcuni commentatori è interpretato in modo eccessivamente estensivo dal Gruppo art. 29;

A seguito di queste riflessioni il Gruppo art. 29 ha ritenuto di dover costituire un sottogruppo che approfondisca il concetto di "dato personale" con particolare riguardo alle applicazioni *Rfid*.

Dati relativi all'ubicazione

La possibilità di ricavare informazioni sulla localizzazione via satellite e la maggiore diffusione della telefonia mobile hanno determinato un aumento enorme dell'uso di dati relativi all'ubicazione nell'offerta di beni e servizi.

Il Gruppo art. 29, in un parere sul tema dell'uso di dati relativi all'ubicazione al fine della fornitura di servizi a valore aggiunto (WP 115, 25 novembre 2005), ha ricordato che a tale settore vanno applicate le disposizioni delle direttive comunitarie in materia di protezione dati. Con riferimento al diritto nazionale applicabile è stato evidenziato il principio secondo cui il trattamento di dati relativi all'ubicazione è soggetto al diritto dello Stato membro in cui è stabilito il responsabile del trattamento, anziché a quello dello Stato membro di cui è cittadino la persona interessata. Quando il responsabile non è stabilito in uno Stato membro, il trasferimento di dati può avvenire solo alle condizioni previste dal capo IV della direttiva n. 95/46/Ce.

Per quanto riguarda l'informativa, il documento ribadisce l'obbligo di renderla a carico del fornitore del servizio a valore aggiunto ovvero, se quest'ultimo non ha contatti diretti con la persona interessata, dell'operatore delle comunicazioni elettroniche. L'informativa può essere fornita o direttamente ogni volta che il servizio viene utilizzato, oppure nelle condizioni generali del servizio, purché in quest'ultime caso le informazioni siano consultabili in qualsiasi momento e in maniera semplice.

Il Gruppo si è soffermato anche sul tema del consenso, escludendo che questo possa essere prestato nel quadro dell'accettazione delle condizioni generali del servizio offerto. I fornitori di servizi sono chiamati a predisporre misure adeguate per garantire che la persona che ha manifestato il consenso sia effettivamente quella cui i dati si riferiscono, e rappresenti l'effettivo utilizzatore dell'apparecchiatura terminale. Pertanto, è stata richiamata l'attenzione degli operatori sulla necessità di introdurre misure efficaci per la verifica e l'autenticazione delle richieste di accesso ai dati di ubicazione. Il consenso deve poter essere revocato in qualsiasi momento, anche in via temporanea, mediante una funzione semplice e gratuita. I dati relativi all'ubicazione possono essere trattati solo per la durata necessaria alla fornitura di un servizio a valore aggiunto, e con tutte le precauzioni relative alle misure di sicurezza finalizzate a garantire la riservatezza e l'integrità dei dati.

La seconda parte del documento è dedicata a due casi che sollevano problemi più delicati con riferimento al trattamento dei dati personali: il trattamento di dati di localizzazione riferiti a minori e a lavoratori dipendenti.

Per quanto riguarda i minori, il Gruppo art. 29 ha ricordato che la Convenzione internazionale sui diritti del fanciullo prevede già che qualsiasi decisione concernente i minori debba essere presa tenendo in considerazione, in primo luogo, il migliore interesse del fanciullo, e che nessun fanciullo possa essere oggetto di interferenze arbitrarie o illegali nella vita privata. I fornitori di servizi devono pertanto introdurre procedure adeguate per identificare le persone che si registrano come "genitori" e limitare solo ad esse l'accesso.

In riferimento alla localizzazione di lavoratori dipendenti il Gruppo ha sottolineato che la liceità del trattamento dei dati relativi all'ubicazione non deve basarsi esclusivamente sul consenso del lavoratore (il quale, peraltro, rappresenta il "soggetto debole" del rapporto), ma deve essere affrontata in una prospettiva più ampia anche attraverso accordi collettivi. Il trattamento deve inoltre corrispondere ad un'esigenza specifica dell'impresa. Il Gruppo ha poi richiamato l'attenzione sulla necessità di rispettare tutti gli altri principi di protezione dei dati e in particolare i limiti

al periodo di conservazione (che non dovrebbe superare due mesi) nonché le misure di sicurezza, al fine di evitare che soggetti non autorizzati accedano ai dati relativi all'ubicazione dei lavoratori dipendenti.

Rapporto sulla notificazione

All'esito delle attività di cui si era già riferito nella *Relazione* 2004 (p. 142), il Gruppo ha reso pubblico un rapporto (WP 106, 18 gennaio 2005), con il quale ha fornito ai Paesi membri indicazioni rispetto alla notificazione dei trattamenti di dati personali. Il rapporto si accompagna ad un *Vademecum* (messo a punto sotto il coordinamento del Garante italiano nel 2004 e perfezionato durante il 2005) sulla disciplina della notificazione vigente nei 25 Paesi Ue, in modo da consentire, a chiunque lo desideri (titolari di trattamento e/o interessati), di poter conoscere come si articoli e si diversifichi il sistema della notificazione in ambito Ue, e quali siano i passi da compiere per notificare un trattamento nei diversi Stati membri.

Nel rapporto, è stato osservato che la notificazione resta un adempimento necessario, in particolare nei Paesi di recente adesione all'Ue, laddove riveste anche la funzione generalpreventiva di richiamare l'attenzione sull'esistenza di particolari obblighi connessi alla legislazione sulla protezione dei dati; tuttavia, essa non deve mai costituire un puro appesantimento di stampo burocratico. Per questo motivo, nell'ottica di semplificazione degli obblighi amministrativi già indicata come obiettivo dalla Commissione europea (*v. Relazione* 2004, p. 142), il Gruppo ha segnalato la possibilità di razionalizzare e semplificare i meccanismi di notificazione:

- promuovendo forme di notificazione *on-line* o comunque basate in massima parte su strumenti elettronici (moduli scaricabili o compilabili via Internet, utilizzo della firma digitale);
- invitando il legislatore nazionale a riflettere sull'opportunità di introdurre la figura dei *cd.* "*privacy officer*" (soggetti che all'interno di un'azienda o di un ente siano incaricati di vigilare sul rispetto della normativa in materia di *privacy* e di censire tutti i trattamenti di dati personali effettuati, con conseguente esenzione dall'obbligo di notificazione all'autorità nazionale di protezione dei dati);
- avvalendosi di tutte le soluzioni di esenzione dall'obbligo di notifica praticabili alla luce della direttiva n. 95/46/Ce;
- avviando una riflessione a livello nazionale sull'effettiva necessità della richiesta di alcuni elementi attualmente previsti nei modelli di notificazione, che vadano al di là di un "nucleo comune" di informazioni (periodo di conservazione dei dati, origine dei dati, meccanismi per l'esercizio dei diritti riconosciuti agli interessati), rispetto agli elementi "minimi" obbligatori ai sensi dell'art. 19, comma 3, della direttiva. La scelta del *common core* sembra costituire un'opzione ragionevole e sul quale la maggioranza dei Paesi Ue risulta concordare;
- valutando la necessità di conferire maggiori poteri alle autorità di protezione dati nella scelta dell'approccio più indicato ed efficace in termini di notificazione.

Il rapporto propone, infine, un meccanismo di notificazione semplificata per i soggetti stabiliti in più Stati membri, che prevederebbe la presentazione di una notificazione "completa" in un solo Paese (tendenzialmente quello in cui ha sede, ad esempio, l'impresa capogruppo), contestualmente ad una sorta di notificazione "ridotta" da presentare negli altri Paesi in cui il soggetto in questione risulti stabilito. Su quest'ultimo punto, la discussione nel Gruppo è ancora aperta.

Pnr - Canada

Il Gruppo art. 29 si è pronunciato favorevolmente, con il parere n. 1/2005 (WP 103, 19 gennaio 2005), sul livello di adeguatezza in materia di protezione dati offerto dal Canada con riferimento alla trasmissione da parte delle compagnie aeree

dei dati di identificazione dei passeggeri (Pnr) e di informazioni anticipate sui viaggiatori (Apis). Il Gruppo si era già pronunciato su tale argomento nel 2004 (parere n. 3/2004), sollevando una serie di critiche al sistema messo in piedi con riferimento ai principi di protezione dati, e invitando la Commissione a proseguire i negoziati con il Canada.

I negoziati successivi hanno portato il Canada a rivedere il sistema d'informazione sui passeggeri, e in particolare a modificare i seguenti aspetti:

- il sistema è stato configurato per ricevere i dati Apis/Pnr dalle compagnie aeree attraverso il sistema "*push*";
- è stato identificato un elenco chiaro e limitato dei reati gravi direttamente connessi con il terrorismo;
- le tipologie di dati da trasferire sono state ridotte da 38 a 25, con l'esclusione dei dati sensibili e dei campi "testo aperto" o "osservazioni generali";
- il tempo di conservazione dei dati è stato ridotto da 6 anni a 3 anni;
- la comunicazione dei dati sui passeggeri ad altre autorità è stata circoscritta, e il trasferimento è stato limitato ai Paesi di cui sia stata accertata l'adeguatezza;
- è stato indicato l'obbligo di fornire un'adeguata informativa da parte del *Canada Border Service Agency*, così come l'impegno a garantire i diritti di accesso, rettifica e opposizione non solo alle persone interessate presenti in Canada;
- è stata infine prevista una verifica congiunta dell'attuazione degli impegni assunti.

Cd. Binding Corporate Rules

Il Gruppo art. 29 ha approvato nel corso del 2005 due documenti (WP 107, 14 aprile 2005 e WP 108, 14 aprile 2005) riguardanti le "regole vincolanti nell'impresa" (*Binding Corporate Rules*-Bcr). Le imprese, soprattutto multinazionali, hanno chiesto con riferimento all'autorizzazione al trasferimento dei dati, di poter dialogare con un solo interlocutore, anziché di volta in volta con le singole 25 autorità nazionali. Le Bcr sono uno degli strumenti attraverso i quali le imprese multinazionali potranno trasferire dati personali da Paesi Ue verso Paesi terzi non adeguati; esse potranno consentire alle autorità di protezione dati di svolgere una valutazione comparata nella prospettiva di garanzie auspicabilmente più uniformi e nel rispetto delle prerogative di ciascuna.

Il Gruppo ha definito gli aspetti procedurali nel documento WP 107, che prevede la designazione di un'autorità di protezione dati quale *leader* della valutazione, alla quale tutte le altre autorità interessate dovrebbero far capo per commenti e osservazioni. La designazione spetta alla società multinazionale, che dovrà rifarsi ai criteri indicati nel documento, fra i quali viene data priorità alla considerazione del Paese ove è situata la capogruppo o la sede centrale europea della multinazionale. Le autorità sono libere di accettare o meno tale designazione sulla base della documentazione prodotta dalla società, formulando eventualmente una controproposta. La procedura prevede, stabilita l'autorità-*leader*, l'elaborazione di una bozza finale di "regole vincolanti nell'impresa" da sottoporre alla valutazione congiunta di tutte le autorità interessate, coordinate dall'autorità-*leader*; l'accettazione della bozza è da intendersi come riconoscimento dell'adeguatezza delle norme in essa contenute e, quindi, come autorizzazione al loro impiego.

Il WP 108 integra e completa il documento precedente, fornendo indicazioni specifiche sui contenuti delle regole vincolanti nell'impresa. Il Gruppo ha elaborato una sorta di "*checklist*" che le imprese devono utilizzare per verificare che le rispettive Bcr rispondano ai principi fissati nella direttiva n. 95/46/Ce. In particolare, deve essere dimostrata l'effettiva vincolatività delle norme, sia rispetto all'interno del

gruppo (controllate, collegate, dipendenti, terzi fornitori), sia rispetto all'esterno, soprattutto ai fini dell'esercizio dei diritti riconosciuti agli interessati.

Interpretazione dell'art. 26 (1) della direttiva n. 95/46/Ce

Il Gruppo art. 29 ha adottato un documento di lavoro (WP 114, 25 novembre 2005) sul tema del trasferimento dei dati personali verso Paesi che non garantiscono un livello di protezione adeguato, al fine di fornire un'interpretazione che consenta un'applicazione uniforme negli Stati Ue dell'art. 26 (1) della direttiva n. 95/46/Ce, che prevede deroghe rispetto al principio di adeguatezza della destinazione enunciato nell'art. 25.

Il Gruppo ha sottolineato, in particolare, che le disposizioni dell'art. 26 (1) devono essere interpretate in modo restrittivo, e che le deroghe possono essere utilizzate solo nei casi in cui i rischi per l'interessato siano ridotti, o in cui si può ritenere che altri interessi prevalgano sul diritto dell'interessato alla riservatezza. Nel documento vengono inoltre formulate diverse raccomandazioni volte ad incoraggiare i responsabili del trattamento a garantire, nella maggior parte dei casi, l'uso "fisiologico" dell'art. 25; viene svolta poi un'analisi dei concetti di "consenso" e di "esecuzione di un contratto", deroghe sulle quali i responsabili del trattamento tendono a basarsi più di frequente.

Sistema Vis

Il Gruppo art. 29 ha adottato un parere (WP 110, 23 giugno 2005) sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione sui visti e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (sistema Vis). Secondo la proposta, l'archivio Vis verrebbe costituito da una banca dati centrale e da interfacce nazionali; sarebbe accessibile da sistemi nazionali collegati con i consolati e i posti di frontiera di ciascun paese partecipante; l'archivio conterrebbe i dati identificativi di tutte le persone che richiederanno visti di ingresso trimestrali per uno dei Paesi aderenti all'Accordo di Schengen. Oltre ai dati alfanumerici, sarebbero registrati anche i dati biometrici, in particolare la foto digitalizzata del richiedente e le sue impronte digitali.

Il Gruppo ha ritenuto che la raccolta massiccia di dati personali e biometrici in una banca dati centralizzata, in concomitanza con uno scambio di dati effettuato su larga scala e riguardante un enorme numero di persone, risulti gravemente rischiosa con riferimento alla garanzia dei principi fondamentali della protezione dati.

Per tale ragione, il Gruppo ha chiesto:

- che vengano specificate chiaramente ed esaustivamente le finalità del trattamento dei dati contenuti nel Vis, in rapporto alla politica comune sui visti che ne costituisce il fondamento giuridico;
- che siano stabiliti tempi di conservazione dei dati limitati e proporzionati;
- che siano definite con precisione le autorità abilitate ad introdurre dati nel Vis, così come a modificarli e a cancellarli, anche su richiesta dell'interessato.

Nel parere viene infine ribadita la necessità di individuare gli organismi che possono accedere al sistema (con particolare riguardo per le previste interconnessioni con il Sistema informativo Schengen), nonché di specificare meglio le funzioni di controllo e supervisione rimesse alla competenza delle autorità nazionali per la protezione dei dati personali.

Biometria nei passaporti

Dopo l'adozione della Decisione della Commissione sulle specifiche tecniche relative alle caratteristiche di sicurezza e agli elementi biometrici nei passaporti, il Gruppo art. 29 si è pronunciato (WP 112, 30 giugno 2005) sull'attuazione del regolamento comunitario relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri.

Il Gruppo, dopo aver ribadito i principi enunciati nel parere precedente e confermato le segnalazioni inviate al riguardo al Parlamento europeo, ha richiamato i

rischi legati all'acquisizione presso i cittadini europei di dati biometrici in forma digitalizzata, che potranno essere memorizzati in banche di dati centralizzate e resi disponibili per tutta una serie di scopi non tutti previsti. Per tale ragione, il Gruppo ha espresso ampie riserve riguardo alla costituzione di una banca dati centralizzata, sia europea, sia nazionale, di informazioni biometriche, la quale violerebbe il principio basilare della proporzionalità nel trattamento di dati personali.

Secondo il Gruppo, l'impiego della biometria va limitato ai soli scopi di verifica, allo scopo della comparazione dei dati inclusi nel documento, con i dati riscontrabili direttamente presso il detentore all'atto della presentazione del documento. Il Gruppo ha inoltre chiesto che possano avere accesso ai dati memorizzati nel *chip* solo le *"autorità competenti"* e che venga istituito un registro esaustivo delle medesime autorità e degli organismi autorizzati al trattamento.

Riguardo agli aspetti tecnici, il Gruppo art. 29 ha espresso forti perplessità sulla possibilità di garantire la sicurezza attraverso l'introduzione di *chip* "senza contatto" (*ad es.*, *tag Rfid*), nonché sull'opportunità dell'inserimento di caratteristiche biometriche direttamente nel *chip*. A questo proposito, il Gruppo si è invece espresso in favore dell'istituzione di un'infrastruttura globale a chiave pubblica (*Pki*).

Sis II

Il Gruppo art. 29 ha adottato un parere (WP 116, 25 novembre 2005), predisposto sotto il coordinamento della delegazione italiana, relativo alle proposte presentate dalla Commissione europea che definiscono l'istituzione di un nuovo sistema informativo (Sis II) destinato a sostituire l'attuale Sistema informativo Schengen (Sis). Il Sis è previsto e disciplinato dalla Convenzione Schengen e rappresenta uno strumento fondamentale per lo scambio di dati ai fini della non ammissione di stranieri segnalati nei Paesi aderenti alla Convenzione, nonché per favorire la cooperazione nelle attività di polizia.

Le nuove norme proposte prevedono per il futuro Sis II un ampliamento di natura funzionale e strutturale, oltre che in termini di contenuti. Le principali novità riguardano infatti: l'articolazione della banca dati centralizzata, unitamente alle nuove funzioni di tipo dinamico che si vogliono introdurre (in particolare, la possibilità di interconnessioni fra segnalazioni inserite per finalità diverse nel Sis II); le modalità di consultazione dei dati da parte delle autorità nazionali e degli organismi sopranazionali (Europol, Eurojust); la possibilità di inserire nuove categorie di dati compresi quelli di natura biometrica (immagine digitale del volto e impronte digitali); l'esercizio dei diritti riconosciuti agli interessati; i tempi di conservazione dei dati.

Il Gruppo ha evidenziato alcuni aspetti critici che si accompagnano alle proposte della Commissione, da armonizzare meglio ai principi di protezione dati sanciti dalla direttiva n. 95/46/Ce, ed ha segnalato, rispetto a ciascuno di tali punti, emendamenti da apportare.

Per quanto attiene alle finalità del Sis II e all'individuazione dei soggetti autorizzati ad accedervi, i Garanti ritengono che, allo stato, non sia possibile consentire l'accesso ad organismi quali Europol ed Eurojust, perché ciò contrasterebbe con le finalità del sistema come attualmente configurate. Con riferimento alla possibilità di interconnessioni fra i dati relativi alle segnalazioni inserite per finalità diverse, il Gruppo ha rilevato che occorrono norme più dettagliate sull'utilizzo di tale meccanismo e sui soggetti autorizzati ad accedere alle informazioni.

Il Gruppo ha altresì segnalato che l'utilizzo di dati biometrici per finalità identificative non può avvenire su base sistematica, dovendo essere previsto soltanto "caso per caso" e se realmente indispensabile. Per quanto attiene alla salvaguardia dell'effettivo esercizio dei diritti riconosciuti agli interessati, si è ritenuto peraltro necessario garantire un'informazione adeguata sulle possibilità di opporsi alla decisione

dello Stato sull'inserimento di segnalazione nel Sis. Infine, con riferimento alla durata della conservazione dei dati inseriti nel sistema, il Gruppo ha chiesto di mantenere il termine di tre anni attualmente previsto nella Convenzione Schengen.

Conservazione dei dati di traffico *"Data Retention"*

La conservazione preventiva e generalizzata dei dati di traffico interferisce con il diritto fondamentale alla riservatezza delle comunicazioni; per questo motivo, in linea generale, il Gruppo art. 29 ha sempre ritenuto che il ricorso a tale misura debba essere riservato solo a casi eccezionali e per motivate e pressanti esigenze sociali, nonché sulla base di adeguate e specifiche garanzie previste per legge.

Nel 2005 il Gruppo ha adottato un parere (WP 113, 21 novembre 2005) coordinato dal Garante in merito alla proposta di direttiva sulla conservazione dei dati presentata dalla Commissione europea nel mese di settembre (Com(2005)438; ora direttiva n. 2006/24/Ce), come parte di un "pacchetto" di misure messe a punto nel quadro della lotta contro il terrorismo e la criminalità organizzata. Il Gruppo, come già in varie occasioni dopo gli eventi del settembre 2001, ha voluto sottolineare la propria consapevolezza e condivisione rispetto alle sfide poste dal terrorismo e alla necessità di farvi fronte in modo efficace; tuttavia, ha precisato che ciò deve avvenire senza minare i principi e diritti fondamentali (ivi compreso il diritto alla *privacy*) che formano la base delle società democratiche.

La proposta di direttiva ha previsto un obbligo generalizzato per tutti i fornitori di servizi di comunicazione di conservare i dati di traffico per finalità non connesse alla fatturazione, bensì per scopi investigativi. Pur prendendo atto con favore dell'intento di armonizzare il quadro normativo europeo in questo campo, in cui sussistono numerose diversità, il Gruppo non ha ritenuto che le motivazioni addotte dalle competenti autorità dei Paesi membri a sostegno della conservazione obbligatoria dei dati fossero sufficientemente solide, in particolare rispetto al periodo massimo di conservazione previsto nella proposta.

In questo contesto, i Garanti hanno chiesto alla Commissione ed al Parlamento (chiamato a decidere congiuntamente sull'adozione della direttiva) di prevedere alcune garanzie essenziali, anche alla luce di altri strumenti internazionali come la Convenzione europea dei diritti umani:

- specificare chiaramente le finalità della conservazione dei dati, che devono essere connesse alla lotta contro il terrorismo e la criminalità organizzata, anziché contro generiche forme di "grave criminalità";
- indicare chiaramente a quali condizioni le autorità competenti potrebbero accedere ai dati in oggetto ed utilizzarli per combattere la minaccia del terrorismo;
- limitare al massimo il periodo di eventuale conservazione, chiarendo che esso rappresenta il tetto massimo applicabile dagli Stati membri (che però dovrebbero poter prevedere periodi più brevi);
- dare massima pubblicità alle misure introdotte;
- prevedere un riesame periodico delle motivazioni alla base delle misure di conservazione obbligatoria dei dati (almeno ogni 2-3 anni);
- prevedere che, in ogni caso, si tratti di misure ad applicazione limitata nel tempo (3 anni) proprio per la natura circostanziale delle motivazioni che stanno alla base della proposta della Commissione.

I Garanti hanno richiamato queste ed altre specifiche garanzie in forma sintetica in un elenco finale recante venti prescrizioni. Tra esse vanno citati almeno: il divieto di trattamenti ulteriori dei dati conservati (se non in presenza di rigide e specifiche garanzie); l'opportunità di autorizzare l'accesso caso per caso attraverso decisioni dell'autorità giudiziaria o, comunque, delle autorità competenti; la predisposizione di misure concernenti la sicurezza e la separazione logica dei dati che i fornitori di

servizi devono adottare; la definizione precisa delle categorie di dati da conservare e la previsione di meccanismi di revisione di tali categorie; la necessità di escludere in ogni caso i dati relativi ai contenuti delle comunicazioni.

22.2. *Cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Il 2005 ha visto un'accelerazione delle iniziative legislative proposte dalla Commissione per rafforzare la cooperazione tra le autorità nazionali di polizia e giudiziarie.

Tra le più importanti, si segnalano le proposte per una nuova base legale del Sistema informativo Schengen e per la creazione del Sis II, presentate dalla Commissione il 31 maggio 2005, la bozza e la direttiva in materia di conservazione dei dati di traffico telefonico e telematico a fini di repressione dei reati. Altra proposta ufficialmente presentata dalla Commissione e da tempo auspicata ed attesa dai Garanti europei è quella relativa ai principi in materia di protezione dei dati nel Terzo pilastro.

L'attività del Garante nell'Autorità di controllo comune Schengen

Il Garante continua ad esercitare le funzioni di autorità nazionale per il controllo indipendente dell'archivio della sezione italiana del Sis e per verificare che l'elaborazione e l'utilizzazione dei dati inseriti non leda i diritti della persona interessata, ai sensi dell'art. 114 della Convenzione; in tale veste, fa parte dell'Autorità di controllo comune (Acc).

Fra le attività di maggior rilievo dell'Acc, alle cui riunioni il Garante ha partecipato fin dall'inizio nella persona del segretario generale, prima vice presidente poi, nel biennio 2002-2003, presidente dell'Autorità, va ricordata quella di verifica e controllo del funzionamento della parte centrale del Sis e di vigilanza sulla corretta applicazione delle disposizioni della Convenzione, attività che viene svolta anche attraverso l'indicazione, ove necessario, degli aggiustamenti e delle prassi corrette da adottare. Considerato che ad una persona può essere rifiutato l'accesso al territorio Schengen (non più solo al territorio nazionale) sulla base di informazioni contenute nel sistema, resta di immediata ed ovvia importanza assicurare che le informazioni siano ad esempio accurate ed aggiornate.

Gran parte dell'attività dell'Acc ha continuato ad essere concentrata sui problemi legati allo sviluppo del Sistema informativo Schengen, il *cd.* Sis II. Il passaggio dall'attuale al nuovo sistema determinerà l'introduzione di nuove funzioni e di ulteriori dati tra cui, in particolare, dati biometrici (foto digitalizzate ed impronte digitali). È inoltre prevista l'interoperabilità tra Sis, Vis ed Eurodac per creare una sinergia tra grandi *data-base* europei e l'estensione delle possibilità di accesso al sistema per Europol ed Eurojust.

Le nuove categorie di informazioni e i nuovi tipi di dati, l'accesso al Sis e l'uso dei dati nel sistema, inclusa la possibilità di una loro trasmissione a Paesi terzi, sembrano volte a trasformare il Sis in un sistema di indagine e non più solo di informazione, mutandone quindi sensibilmente le finalità rispetto a quelle definite dalla Convenzione del 1990.

L'Autorità ha adottato un lungo ed articolato parere sulle proposte presentate dalla Commissione nel mese di settembre, ribadendo le preoccupazione espresse nei precedenti pareri e offrendo anche formulazioni diverse per la discussione sul testo.

Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso

L'Autorità comune di controllo Europol ha proseguito la sua attività esprimendo, in particolare, un parere sul trasferimento di dati verso l'Australia.

Come già indicato nella precedente *Relazione*, si è svolta la consueta ispezione

annuale degli archivi che, come deliberato dall'Acc, si è concentrata sull'esame dei dati di natura personale trasmessi nell'ambito dell'accordo e sulla qualità dei dati trattati.

La conduzione d'ispezioni *in loco* delle attività dell'Europol costituisce peraltro uno dei modi adottati dall'autorità di controllo comune per ottemperare al suo mandato. L'Acc ha al riguardo definito gli obiettivi ed i criteri che guideranno le ispezioni future (di regola annuali), anche alla luce della considerazione che il ruolo dell'Europol si sta sviluppando rapidamente, con un numero sempre maggiore di dati trattati. Il comitato ricorsi ha deciso in merito a due ricorsi.

Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune

Come si è ricordato nelle precedenti *Relazioni*, a seguito della ratifica ed entrata in vigore della Convenzione sull'uso dell'informatica nel settore doganale, è stato creato un sistema informativo automatizzato comune ai Paesi membri dell'Ue (Sistema informativo doganale-Sid). Il sistema consiste in una base di dati centrale cui si può accedere tramite terminali in ogni Stato membro. La Commissione europea provvede alla gestione tecnica dell'infrastruttura del Sid.

La vigilanza sul corretto funziamento del Sid è affidata ad una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati. L'Autorità si è riunita una volta nel 2005.

Permangono i temi problematici già presentati nella scorsa *Relazione*, legati alla mancanza di risorse proprie per costituire il *team* di esperti che dovrebbe svolgere la prima ispezione al Sid, nonché allo scarso utilizzo del sistema da parte delle autorità doganali, che preferiscono in genere utilizzare canali bilaterali per gli scambi di informazioni.

Eurodac

Per quanto concerne Eurodac, la grande base di dati europei che contiene le impronte digitali dei richiedenti asilo e delle persone fermate dalla autorità di frontiera in posizione irregolare è attualmente affidata al Garante europeo per la protezione dei dati personali (Gepd). Nel 2005 il Gepd ha organizzato una riunione di coordinamento con le autorità nazionali di protezione dei dati per iniziare una collaborazione e verificare sulla base della comune esperienza la liceità dei trattamenti effettuati.

22.3. *Partecipazione ad altri comitati e gruppi di lavoro*

Circa Complaint

Gli incontri previsti nell'ambito della rete istituita fra le autorità europee per la protezione dei dati ai fini dello scambio di informazioni sulle casistiche nazionali e sul contenzioso si sono tenuti nel corso dell'anno a Budapest (10-11 marzo 2005) e a Parigi (17-18 novembre 2005).

Facendo seguito alle indicazioni emerse dal precedente *workshop* di Praga (novembre 2004), a partire dall'incontro di Budapest si è sperimentata una nuova formula di organizzazione, in base alla quale si prevede di dedicare una mezza giornata di riunione alla trattazione approfondita di un tema di interesse, attraverso sessioni parallele.

Tale approccio si è dimostrato efficace ed è stato quindi formalizzato in occasione della *Spring Conference* di Cracovia, che ha stabilito anche la nuova denominazione dei seminari, ora ribattezzati "*Case Handling Workshops*" (seminari sulla trattazione della casistica nazionale), per sottolineare anche l'ampliamento dell'ambito di discussione, non più limitato ai soli "ricorsi", ma riguardante l'intera gamma delle attività condotte dalle autorità nazionali sulle quali si ritenga necessario confrontarsi.

In tale sede è stata ribadita, inoltre, l'opportunità di concretizzare i risultati dei *workshop* sotto forma di documenti o proposte da sottoporre ai soggetti competenti

(in primo luogo, la *Spring Conference*, ma anche il Gruppo art. 29) nell'ottica di favorire la diffusione e l'elaborazione di *best practice*.

I temi affrontati nel corso del 2005 hanno riguardato, in particolare:

- le attività di ispezione e controllo svolte dalle autorità nazionali e le relative modalità esecutive. In proposito, l'autorità italiana ha formulato la proposta di istituire una lista di punti di contatto in materia di ispezioni e controlli, per facilitare lo scambio di informazioni e la rapida definizione di questioni controverse che investano più Paesi, così da redigere una possibile lista di "buone pratiche", basate sull'esperienza sinora formatasi in materia di controlli ed ispezioni, da utilizzare quale strumento per potenziare l'efficacia delle attività nei Paesi che già le hanno avviate, nonché come possibile impulso per i Paesi che ne stanno impostando le linee direttrici;
- i problemi connessi alla creazione di *black list* per la telefonia mobile, anche alla luce dell'assenza di norme specifiche nella maggioranza dei Paesi Ue;
- il trattamento di dati sanitari, con particolare riguardo alle istanze di accesso degli interessati ai dati relativi alla salute detenuti da strutture sanitarie, società di assicurazione e datori di lavoro, nonché al funzionamento dei sistemi nazionali basati sull'istituzione di "cartelle cliniche elettroniche" con tutti i problemi connessi;
- il trattamento dei dati nel settore bancario, soprattutto a seguito dell'adozione degli accordi "Basilea II" (in materia di lotta al riciclaggio e alla frode);
- il rapporto con i *media* e le opportunità di sensibilizzazione pubblica da ciò derivanti, con riguardo alla necessità di curare i rapporti con la stampa ed i *media* attraverso personale specializzato, e di elaborare strategie di *marketing* (in senso lato) che consentano di massimizzare la presenza delle autorità di protezione dei dati in tutti i settori della società;
- altri temi di attualità. Tra di essi, si segnalano le problematiche connesse alla legge Sarbanes-Oxley (che impone la comunicazione ad autorità Usa di dati relativi all'affidabilità di consulenti e revisori in materia contabile) e al correlato fenomeno del "*whistleblowing*" (segnalazioni anonime effettuate da dipendenti di un'azienda attraverso linee dedicate, cosiddette "*integrity lines*"); la raccolta di dati connessi all'origine razziale ed etnica per finalità antidiscriminatorie o per la tutela delle pari opportunità; la tutela della proprietà intellettuale in Internet; il rapporto fra comunicazione politica e diritto alla *privacy*.

Su tali punti, le autorità hanno convenuto di proseguire la discussione nei prossimi mesi.

Consiglio d'Europa

I temi più importanti, affrontati dal Comitato consultivo della Convenzione n. 108/1981 (T-Pd) nel corso del 2005, hanno riguardato l'applicazione dei principi di protezione dati alle reti telematiche e l'applicazione dei principi della Convenzione del Consiglio d'Europa alla raccolta e al trattamento dei dati biometrici.

Sul primo punto, uno studio commissionato dal Consiglio d'Europa ad esperti esterni ha evidenziato alcune problematiche legate a recenti sviluppi che sembrerebbero indicare l'opportunità della ridefinizione del concetto di identità, profondamente mutato nella direzione di una frammentazione crescente dell'identità personale e di una crescente difficoltà, per l'utente Internet, di veder garantiti i propri diritti.

Lo studio in esame ha affrontato in modo specifico il concetto di autodeterminazione informativa nel contesto di Internet, evidenziando i rischi connessi ai trattamenti di dati "invisibili" e la necessità di promuovere un approccio tecnologico alla tutela dei dati personali, intervenendo nella fase di configurazione dei sistemi

informativi. Fra i rischi legati all'impiego delle nuove tecnologie, l'attenzione del Consiglio d'Europa si è focalizzata, in particolare, sui temi della profilazione e dell'effettività del consenso.

In materia di trattamento di dati biometrici, è stato pubblicato un rapporto sullo stato di avanzamento dell'analisi dell'applicazione dei principi della Convenzione al trattamento di tali dati. Tale rapporto intende rappresentare "lo stato dell'arte", in particolare al fine di contribuire al dibattito internazionale, che in più sedi (*ad es.*, Ocse, Ue) ha posto al centro dell'attenzione le molte tematiche connesse alle tecnologie biometriche.

Avendo descritto le specificità della biometria e dei sistemi che utilizzano indicatori biometrici, con particolare riguardo all'architettura centralizzata o decentralizzata di tali sistemi e alle rispettive implicazioni in termini di protezione dei dati, il rapporto esamina in particolare l'applicazione delle singole disposizioni della Convenzione a questa costellazione di trattamenti. Pur senza giungere a conclusioni definitive, il T-Pd segnala che i principi della Convenzione sono idonei a mantenere la propria validità anche rispetto ai trattamenti legati all'impiego di sistemi biometrici, risultando opportuna, prima del ricorso a tali sistemi, la verifica da parte del titolare del trattamento relativa all'esistenza e alla praticabilità di opzioni meno invasive. Infatti, attraverso il ricorso a identificatori biometrici viene incrementata la possibilità di ledere la dignità delle persone, anche in base alla circostanza per cui i dati risultano direttamente "prelevati" dal corpo umano e possono restare inalterti nel corso della vita.

Fra le altre iniziative sviluppate dal T-Pd merita almeno un cenno la proposta di istituire una "giornata europea della protezione dei dati", alla quale potrebbero associarsi iniziative a livello nazionale per sensibilizzare i cittadini rispetto ai loro diritti e alle attività delle autorità nazionali.

Ocse

Il Garante ha partecipato anche nel 2005 ai lavori del gruppo che in seno all'Ocse si occupa dei temi legati alla *privacy*. Il *Working Party on Information Security and Privacy* (Wpisp) ha proseguito il suo impegno sul tema della sicurezza, già considerato come tema prioritario a partire dal 2001, e si è concentrato in particolare sull'attuazione delle linee-guida. Grazie al lavoro di sintesi condotto dal segretariato sulla base delle risposte ad un questionario inoltrato alle delegazioni nazionali, è emersa l'indicazione di quattro settori prioritari ai quali dedicare l'attenzione del gruppo nel prossimo futuro: incentivazione dell'attività di sensibilizzazione rispetto al tema della sicurezza, soprattutto nei confronti delle amministrazioni locali e degli utenti finali; censimento condotto a livello nazionale con riferimento ai *Computer Emergency Response Team* (Cert), e sviluppo delle relative potenzialità attraverso la raccolta degli eventi più significativi che si verificano in rete; incremento della protezione delle infrastrutture critiche e analisi di dettaglio sui temi della sicurezza legati all'*e-Government*; sviluppo di indicatori attendibili in grado di misurare le spese pubbliche e private dedicate alla sicurezza.

Fra gli altri temi discussi nell'ambito del Wpisp in riferimento alla sicurezza nell'uso delle nuove tecnologie, meritano di essere menzionati almeno quelli legati ai sistemi di autenticazione elettronica e all'*Rfid*. Con riferimento al primo tema, la discussione si è soffermata sulla necessità di rendere più coerenti i differenti approcci nazionali, di sviluppare adeguati strumenti che agevolino l'interoperabilità, di censire le *best practice* in tema di autenticazione, di promuovere la conoscenza dei benefici che derivano dall'autenticazione, di stabilire un dialogo fra le differenti giurisdizioni nazionali nell'utilizzo dell'autenticazione e di approfondire lo studio delle possibili vie per gestire i problemi connessi all'identità digitale.

Per quanto riguarda l'*Rfid*, l'Ocse ha organizzato nel mese di ottobre 2005 un

forum dedicato al tema, nell'ambito del quale si sono confrontati soggetti pubblici, esponenti del mondo dell'industria, dell'università e della società civile. Numerosi interventi hanno evidenziato l'ampia gamma di applicazioni di questa tecnologia, confrontandoli con i rischi emersi in riferimento alla sicurezza e alla *privacy*.

Più in generale, vale la pena ricordare i lavori avviati sui modelli di informativa e sulla cooperazione nelle attività di implementazione della normativa in materia di *privacy*.

Rispetto all'elaborazione di modelli di informativa, occorre ricordare che il Gruppo art. 29 aveva già indicato la strada di un approccio "stratificato" nella redazione delle informative *on-line*, attraverso un documento pubblicato al termine del 2004 del quale si è riferito nella *Relazione* 2004 (p. 142). Nell'approccio del Gruppo, la "soluzione in prima battuta" dovrebbe essere rappresentata dalla versione sintetica dell'informativa, con la possibilità di spostarsi agevolmente ai livelli successivi (caratterizzati da più ampi dettagli e indicazioni), qualora l'interessato ritenga necessario approfondire il quadro relativo al trattamento.

In questa stessa prospettiva, si situa la riflessione condotta in ambito Ocse sulla *cd. Multilayered Information Notice*, al fine di ottenere informative "facili da leggere", complete nei contenuti ed omogenee. Secondo l'Ocse, gli strumenti comunicativi utilizzabili a tale scopo sono riconducibili, sostanzialmente, a tre modelli: un'informativa molto breve, quando lo spazio è molto limitato; un'informativa "concentrata", che consenta comunque di far presente gli elementi essenziali (titolare del trattamento, tipo di dati, modalità e finalità del trattamento, natura obbligatoria o facoltativa, recapito per contattare l'organizzazione); un'informativa completa ed approfondita, disponibile su richiesta dell'interessato. E' stato perciò proposto di elaborare un documento-guida per l'elaborazione di modelli idonei di informativa da parte delle imprese e dei governi.

Il Wpisp ha inoltre ritenuto di occuparsi nuovamente del flusso transfrontaliero dei dati, partendo dalla considerazione che la globalizzazione pone nuove sfide che non potevano essere state previste dalle linee-guida Ocse del 1980.

In particolare, si è fatto esplicito riferimento alla diffusione crescente di documenti di identità che contengono dati biometrici, all'impiego sempre più diffuso di forme di *outsourcing* nella gestione dei dati, alle tracce lasciate dall'impiego di tutte le nuove tecnologie e alla raccolta senza precedenti di dati personali da parte delle autorità pubbliche, connessa a motivi di sicurezza e lotta al terrorismo. Questi fenomeni comportano una crescita esponenziale della circolazione transfrontaliera di dati che diventa più rischiosa quando i dati personali vengono trattati in Paesi nei quali la tutela non è sufficiente, soprattutto con riferimento alla possibilità di esercizio dei diritti di accesso e di rettifica. Per tali ragioni è necessario stabilire procedure condivise che facilitino l'assistenza reciproca in ambito applicativo quando si affrontano questioni che coinvolgono una pluralità di Stati. É stato così proposto di condividere le rispettive conoscenze ed esperienze soprattutto nel settore dell'applicazione transfrontaliera delle norme di legge. A tale riguardo l'esperienza del Gruppo art. 29 nel settore dell'*enforcement* è stata segnalata come esempio virtuoso cui ispirarsi nel trovare soluzioni a problemi comuni.

Il punto di partenza di questa riflessione potrebbe essere rinvenuto nei principi già presenti nelle linee-guida Ocse del 1980. Per questi motivi è stata avviata una riflessione che resta suscettibile di portare all'adozione di nuove linee-guida, ovvero di un protocollo addizionale alle linee-guida, che affrontino il tema di cooperazione transfrontaliera in materia di *enforcement*.

In particolare si ritiene necessario:

- garantire che i cittadini e i residenti di altri Paesi possano esercitare i loro

diritti rispetto alle informazioni che li riguardano, anche nei confronti di enti ed organismi governativi situati in altri Paesi;

- condividere, anche attraverso accordi bilaterali o multilaterali, le informazioni acquisite su problemi comuni rispetto ai flussi transfrontalieri, ivi comprese eventuali indagini o elementi probatori utilizzabili per attività di *enforcement*;
- realizzare verifiche congiunte rispetto agli enti che trasferiscono dati all'estero per stabilire se le informazioni siano utilizzate e tutelate in modo adeguato;
- collaborare alla messa a punto di linee-guida in materia di sicurezza rispetto a questi flussi;
- valutare modalità di riconoscimento ed esecuzione rispetto a sentenze o altri dispositivi provenienti da un altro Stato.

Taiex

Nel corso del 2005 il Garante ha partecipato al Programma Taiex, finanziato dalla Commissione europea per i Paesi candidati all'ingresso nell'Ue nel 2007.

In particolare, il Garante ha contribuito ad un progetto di formazione proposto dall'Autorità rumena per la protezione dei dati personali, con l'obiettivo di acquisire conoscenze specifiche in materia di attività ispettive. L'attività legata al progetto ha comportato l'invio di due esperti italiani presso la sede dell'Autorità rumena stessa, e la tenuta di un corso *in loco* al quale hanno partecipato tutti i funzionari locali. Successivamente si è instaurata una collaborazione regolare con l'Autorità rumena, che ha condotto a numerosi scambi di documentazione ed esperienze nel corso del 2005, nonché ad una visita da parte di alcuni funzionari presso il Garante, al fine di raccogliere indicazioni pratiche e di natura organizzativa sulle concrete attività svolte in Italia.

23 Attività di ricerca, comunicazione e formazione

23.1. *La comunicazione del Garante: profili generali*

L'attività di informazione e comunicazione svolta nel 2005 è stata caratterizzata dall'impulso del nuovo collegio nella direzione della previsione di specifiche garanzie, con provvedimenti a carattere generale, in settori di particolare delicatezza ed interesse specifico per i cittadini, come pure del potenziamento nell'azione di accertamento e verifica del rispetto delle norme.

Grande rilievo ha assunto, in particolare, l'iniziativa promossa nei confronti della pubblica amministrazione, che ha consentito il recupero da parte di alcuni soggetti pubblici del ritardo accumulato nella predisposizione dei regolamenti sul trattamento dati sensibili e giudiziari, e l'avvio di un nuovo rapporto dei soggetti pubblici stessi con i cittadini, basato sull'acquisizione della cultura di protezione dati come base dell'intervento amministrativo.

Nell'ambito comunicativo, se da una parte si è riscontrato che l'attenzione del Garante è stata concentrata su alcuni grandi temi rilevanti per la tutela dei diritti delle persone, tra i quali la *data retention*, le intercettazioni, la creazione di grandi banche dati, la messa in sicurezza dei dati e il diritto di cronaca, dall'altra si rileva che l'Autorità ha dedicato particolare impegno rispetto alle enormi possibilità offerte dalle nuove tecnologie di raccolta e conservazione di dati personali, al ricorso crescente e spesso sproporzionato ai dati biometrici e genetici, così come al potenziale uso indiscriminato delle informazioni più delicate relative alle persone.

Un rilevante sforzo è stato assunto rispetto all'analisi di ampi settori della vita sociale ed economica: credito al consumo, nuovi elenchi telefonici, propaganda elettorale, grande distribuzione, catene alberghiere, sanità, scuola, controllo dei lavoratori, vita condominiale. Non è mancata una decisa azione di promozione della *privacy* come "valore aggiunto" per le imprese, al fine di instaurare un rapporto nuovo con utenti e consumatori sulla base delle innovative funzioni che la protezione dei dati può svolgere nell'economia del mercato globale.

Tra i primari obiettivi che l'Autorità si è posta, in questa fase, risalta l'esigenza di una ancor più decisa azione di informazione, volta a far crescere ulteriormente la consapevolezza di cittadini, istituzioni, imprese, liberi professionisti riguardo al valore dei dati personali, degli interessi in gioco, dei diritti da tutelare per porre in essere un'effettiva protezione dei dati personali.

L'Autorità ha perciò privilegiato ancora un'informazione ed una comunicazione tanto più divulgativa, quanto più attenta all'impiego di un linguaggio rigoroso. Nel dar conto della propria attività e delle tematiche all'ordine del giorno, si è richiamata l'attenzione di istituzioni, pubbliche amministrazioni, mondo dell'impresa e in generale degli utilizzatori di dati personali, sugli obblighi da attuare, sui rischi di violazione e sul valore sociale e culturale del diritto alla *privacy*.

La tipologia dei prodotti informativi ed editoriali dell'Autorità è risultata, così, ampia, differenziata e connotata da una forte caratterizzazione, favorita peraltro da una consolidata *corporate identity* e da una strategia integrata di comunicazione, nella quale spicca anche un aumentato utilizzo di *mass-media* tradizionali, come radio e tv, ma anche di *media on-line* e prodotti multimediali.

Alcune cifre

La presenza sui *media* delle tematiche riguardanti la protezione dei dati personali, ed in particolare l'attività del Garante, si è mantenuta costantemente alta. Nel periodo dal 1° gennaio 2005 al 31 dicembre 2005 sono stati selezionati oltre 12.500 articoli di interesse dell'Autorità. Sulla base della rassegna stampa prodotta ad uso interno, è risultato che le pagine dei maggiori quotidiani e periodici nazionali ed internazionali e dai dei media *on-line* che hanno offerto spazio alle questioni legate generalmente alla *privacy* sono state circa 3.700, delle quali circa 2.400 sono state dedicate specificamente all'attività dell'Autorità anche con l'impulso del nuovo collegio. Le prime pagine dedicate ai temi della protezione dei dati personali sono state circa 350 (di cui oltre 220 riguardanti la sola Autorità). Numerose sono state le interviste pubblicate, gli interventi e le dichiarazioni (160) sulla carta stampata (160), su tv e radio nazionali e locali (135), e anche su pubblicazioni *on-line*.

23.2. *Prodotti informativi*

Newsletter

L'Autorità, nel 2005, ha diffuso 72 comunicati stampa e 29 *Newsletter*. La *Newsletter* settimanale, giunta al suo settimo anno di pubblicazione (per un totale complessivo di 268 numeri), privilegia un'informazione approfondita, anche a carattere internazionale. La possibilità di una sua consultazione *on-line* e il suo invio telematico ad un numero sempre maggiore di abbonati (istituzioni, privati cittadini, imprese, liberi professionisti) ne hanno ulteriormente facilitato la diffusione, contribuendo all'apprezzamento crescente del pubblico.

Cd-rom* e *Bollettino

Nel 2005, il *Cd-rom* dell'Autorità ha cambiato denominazione, per assumere quella di "Il Garante e la protezione dei dati personali". Giunto alla sua XIV edizione, il *Cd-rom* contiene, in forma integrale e nell'originale veste editoriale, i provvedimenti del Garante, la documentazione relativa alla normativa nazionale ed internazionale di riferimento e le pubblicazioni realizzate. L'archivio digitale ipertestuale, che consente la consultazione con funzioni di ricerca "*full-text*", rappresenta uno strumento ormai conosciuto e costantemente richiesto da parte di amministrazioni pubbliche, imprese, liberi professionisti e cittadini.

Rispetto alle precedenti edizioni, peraltro, il *Cd-rom* offre oggi una presentazione multimediale su compiti, funzioni e organizzazione dell'Autorità e sui temi di maggiore interesse affrontati nel corso della sua attività.

Tra le pubblicazioni curate dall'Autorità va inoltre annoverato il *Bollettino*, attualmente consultabile *on-line* per quanto attiene ai periodi più recenti, che raccoglie i provvedimenti adottati dal Garante.

***Depliant* illustrativi**

L'impegno per una comunicazione agile e diretta in primo luogo al cittadino ha trovato concreta attuazione nella realizzazione di *depliant* divulgativi in grado di illustrare i diversi aspetti connessi alla protezione dei dati. I primi cinque pieghevoli sono stati dedicati rispettivamente: all'esercizio dei diritti riconosciuti dalla normativa; all'attività e al ruolo del Garante; alla difesa della *privacy* su Internet; alle telecomunicazioni; ai nuovi elenchi telefonici. Il più recente è stato dedicato al tema della videosorveglianza.

23.3. *Prodotti editoriali*

Il notiziario bimestrale "*Garanteprivacy.it*" è giunto al suo terzo anno di pubblicazione e al diciottesimo numero. Il bimestrale è una pubblicazione destinata a personalità del mondo imprenditoriale ed istituzionale, caratterizzata da una comuni-

cazione mirata ed essenziale, in grado di sottolineare l'attività dell'Autorità nei diversi settori di intervento, con particolare attenzione anche al panorama internazionale. Il bimestrale presenta in ogni numero un editoriale a firma di uno dei quattro componenti del collegio del Garante su temi all'ordine del giorno.

Allo scopo di contribuire in maniera fattiva all'approfondimento dei temi legati alla *privacy* e ai principi posti dalla normativa nazionale e comunitaria, il Garante ha inoltre dato vita, da alcuni anni, ad un nuovo prodotto editoriale, la collana "*Contributi*", nella quale sono pubblicati testi di approfondimento sulle problematiche riguardanti la protezione dei dati personali e la tutela della dignità della persona. Nel 2005 è stato pubblicato il quarto volume, "*Innovazioni tecnologiche e* privacy", curato da Gaetano Rasi, nel quale sono affrontati i complessi rapporti che legano sviluppo economico, progresso civile e tutela della identità, della dignità e della libertà della persona. Il volume raccoglie i contributi di autorevoli studiosi ed esperti italiani e stranieri che si sono espressi nel corso di una conferenza internazionale organizzata dal Garante svoltasi a Roma, presso la sede dell'Autorità, nel giugno 2004.

23.4. *Incontri internazionali*

L'Autorità italiana ha partecipato con il suo presidente, prof. Francesco Pizzetti, e con il segretario generale, dott. Giovanni Buttarelli, all'annuale Conferenza di primavera (*Spring Conference*) delle autorità europee per la protezione dei dati, svoltasi a Cracovia il 25 e 26 aprile 2005, appuntamento che ha rivestito particolare significato, come già descritto, in quanto legato al decimo anniversario dall'approvazione della direttiva n. 95/46/Ce.

Le sessioni di lavoro nelle quali si è articolata la Conferenza hanno affrontato diversi temi: l'impatto della direttiva sul livello di protezione dei dati nell'Ue e nei Paesi terzi; la valutazione delle disposizioni della direttiva in rapporto ai principali problemi applicativi; le problematiche connesse al trasferimento di dati verso Paesi terzi, con particolare riguardo ai nuovi strumenti giuridici elaborati di recente dalla Commissione europea quali le "regole vincolanti nell'impresa" (*cd. Binding Corporate Rules*); le modalità operative e dei possibili benefici connessi all'introduzione dei *privacy officer* (soggetti indipendenti designati dal titolare a vigilare sulla conformità e liceità dei trattamenti svolti) secondo l'esperienza raccolta dai Paesi nei quali essi sono stati previsti (Svezia, Germania, Paesi Bassi, Lussemburgo e, di recente, Francia); le disposizioni nazionali che regolamentano il diritto di accesso da parte degli interessati ai propri dati personali (anche in termini di tempi e costi); le attività di sensibilizzazione ed educazione alla "cultura della *privacy*"; il necessario, contemperamento fra protezione dei dati ed esigenze di sicurezza, in particolare nell'ambito del Terzo pilastro (*v.* anche parr. 22.1 e 22.2). Al prof. Stefano Rodotà, in qualità di ex-presidente del Gruppo art. 29, è stato affidato il compito di aprire i lavori con una relazione introduttiva.

Sempre nel quadro della collaborazione internazionale in materia di protezione dei dati personali, il presidente del Garante, prof. Francesco Pizzetti, ha avviato nel giugno del 2005 una serie di incontri con i propri omologhi europei al fine di una ricognizione sulle problematiche comuni e sulle "questioni in agenda", incontrando a Madrid il direttore dell'Autorità spagnola per la protezione dei dati (*Agencia española de Proteccion de datos*), José Luis Piñar Mañas, e a Parigi il presidente della Cnil (*Commission Nationale de l' Informatique e des Libertés*), Alex Türk.

L'Autorità ha partecipato anche all'annuale Conferenza internazionale delle autorità garanti per la protezione dei dati personali svoltasi a Montreux, in Svizzera,

dal 14 al 16 settembre 2005. I lavori della Conferenza hanno ruotato attorno ad alcune questioni fondamentali, come le biobanche, la globalizzazione, la lotta al terrorismo, le problematiche legate alla possibilità di un'unica normativa sulla tutela dei dati personali in contesti sociali, economici, culturali spesso profondamente diversi, l'adeguatezza dei principi di protezione dati alle sfide di Internet, la possibilità di una semplificazione di norme e procedure per venire incontro alle esigenze del mondo economico, che lamenta una eccessiva diversità normativa nei diversi Paesie e, infine, la comunicazione politica (*v.* anche par. 22.1).

Nell'ambito della Conferenza, il prof. Francesco Pizzetti ha presieduto il 15 settembre la sessione dedicata al tema delle biobanche, tenendo la relazione introduttiva. É stato anche sviluppato il dibattito sull'ipotesi di elaborare un codice deontologico per la comunicazione politica –questione sulla quale è intervenuto, il giorno 15 settembre, il segretario generale del Garante, dott. Giovanni Buttarelli–, e sui metodi per conciliare l'esigenza della lotta al terrorismo e le garanzie per i diritti fondamentali dei cittadini europei.

Il 14 dicembre 2005, il vicepresidente del Garante, dott. Giuseppe Chiaravalloti, ha partecipato al Seminario europeo organizzato a Madrid in occasione del Premio istituito per le migliori esperienze europee nel settore pubblico in tema di protezione dei dati personali, svolgendo un intervento dedicato all'analisi dell'esperienza italiana.

23.5. *Il sito Internet dell'Autorità*

Gestione del *web*, nuove funzioni di ricerca e usabilità

Il sito dell'Autorità si è rinnovato con la previsione di ulteriori funzioni di ricerca e reperimento della documentazione. É stata rinnovata e semplificata l'interfaccia del motore di ricerca, grazie all'introduzione di operatori logici nell'interrogazione e all'accentuato uso della classificazione per tematiche e tipologie di atto. Risulta più rapida la ricerca dell'identificativo numerico di ogni documento (doc. *web* n.), adesso disponibile già dall'*Home Page*. É stata introdotta anche la funzione "*Archivio*" per ripercorrere agevolmente e visualizzare quanto pubblicato negli ultimi tre anni nelle aree *Primo piano*, *Novità* e *In evidenza* dell'*Home page*. In tema di accessibilità del sito è attualmente disponibile anche la "versione solo testo", che consente –eliminando la visualizzazione delle immagini– un caricamento più rapido delle sole informazioni, pur mantenendo il rigore organizzativo proprio del portale.

La *Intranet*

Da tempo in progettazione, è disponibile ora un portale ad esclusivo uso interno che modificherà i flussi comunicativi dell'Ufficio, consentendo una condivisione più ampia di informazioni, attività e documentazione. L'interfaccia *web*, chiara e semplice, vuole rappresentare una piattaforma unica di lavoro condiviso dove reperire ogni riferimento, risorsa di rete o procedura utile allo svolgimento delle operatività quotidiane.

Stato di attuazione del progetto di *e-Government* *"NormeInRete"*

Il progetto, avviato nel settembre del 2004 grazie alla collaborazione nata con il Cirsfid (Centro interdipartimentale di ricerca in storia del diritto, filosofia, sociologia del diritto e informatica giuridica) dell'Università di Bologna, ha prodotto dapprima un approfondito esame tecnico-giuridico sulle diverse tipologie di atti che il Garante può emanare, partendo dal momento della sua costituzione, per proseguire con l'analisi di tutta la banca dati dei provvedimenti.

NormeInRete prevede la marcatura con il *Dtd* approvato dal Cnipa, in linguaggio *Xml*. Il compito del gruppo di lavoro così costituito è stato quello di studiare e proporre modifiche ed integrazioni ai metadati del *Dtd standard* –costruito per la normativa– per l'applicazione a provvedimenti amministrativi; lavoro culminato nel giugno 2005 con l'approvazione Cnipa del *Dtd*. Da quel momento è stato possibile portare

a compimento la marcatura sia di tutta la normativa di interesse in una catena temporale (dalla l. n. 675/1996 al Codice), sia delle fonti comunitarie. Parallelamente, i ricercatori Cirsfid assegnati al progetto hanno avviato la marcatura dei provvedimenti dell'Autorità. Non appena sarà terminata l'integrazione della piattaforma tecnologica del sito, la documentazione così marcata sarà resa disponibile.

I *"numeri"* del portale

Nel 2005, il sito dell'Autorità ha registrato la presenza di 32.000.000 utenti, che hanno consultato una media di 15 documenti ciascuno, per un totale poco inferiore a 500.000.000 di documenti diffusi, a cui si aggiungono le 75.000 *e-mail* indirizzate alla sola Redazione del sito.

La cura editoriale profusa per ciascun documento e area del portale mira a favorire una nuova modalità più dinamica di comunicazione tra amministrazione e cittadino in grado di soddisfare i crescenti bisogni di una società sempre più sensibile ai temi della riservatezza e della dignità della persona e che cerca, semplicemente, informazioni chiare, giuridicamente corrette e tra loro collegate, prontamente disponibili. Un successo che, per crescere e migliorare, richiederà concreti sostegni in termini di strumenti e risorse umane, differenziate e caratterizzate professionalmente in modo trasversale (giuridico, editoriale, informatico).

Prossimi obiettivi

Accrescere il bacino di utenti del portale. Raggiungere la totale usabilità ed accessibilità. Rendere ancora più armonica la struttura del portale, prendendo anche spunto dai suggerimenti contenuti nella corrispondenza elettronica. Produrre la versione inglese del sito e migliorare la *performance* del motore di ricerca. Offrire l'intera catena normativa "*privacy*" in forma consolidata vigente sensibile al contesto. Ogni *link* proporrà il testo in vigore alla data del documento individuato, mentre tutte le altre fonti citate, condurranno a *NormeInRete.it* che –presentando la lista dei siti delle amministrazioni aderenti– proporrà il testo della fonte. Analogamente, ogni citazione in tema trattamento dei dati personali, presente in documenti pubblicati su altri siti istituzionali trattati con il *Dtd* in *Xml*, presenterà la nostra documentazione.

23.6. *Ufficio per le relazioni con il pubblico*

Profili di carattere generale

Il rapporto diretto con la società civile riveste un'importanza fondamentale per l'Autorità che, fin dall'inizio della sua attività, ha inteso presentarsi come istituzione vicina ai cittadini, attenta alle nuove frontiere della protezione dei dati personali e ai nuovi diritti della persona.

Il quotidiano richiamo alla *privacy*, evocato in tutti gli aspetti della vita sociale, spesso alimentato da appassionati dibattiti in ragione dell'importanza e della delicatezza degli argomenti trattati ha svolto, senz'altro, un ruolo determinante per lo sviluppo del Garante. Questo sviluppo è stato ulteriormente arricchito dalla comunicazione che l'Autorità ha saputo fornire nello svolgimento delle proprie funzioni istituzionali, anche attraverso l'utilizzo di tutti i canali di divulgazione pubblica (sito *web*, *media*, iniziative di formazione, convegni, pubblicazioni), così da far registrare fin dal suo esordio, a partire dall'inizio del 2003, una crescita progressiva delle esigenze di informazione, assistenza, consulenza da parte dell'utenza, che si riscontra sempre più qualificata.

L'attività dell'Ufficio relazioni con il pubblico

Rispetto alle principali funzioni dell'Ufficio relazioni con il pubblico, si è rilevata, anche nel corso del 2005, una crescita costante dell'attività.

Tali significativi incrementi, registrati nel corso dell'anno rispetto al precedente periodo, hanno stimolato la ricerca di nuove e più mirate risposte per favorire il dialogo con i cittadini, che si sostanzia attualmente nell'attività di *back office*, caratte-

rizzata dalla ricezione di quesiti e richieste di documentazione per *e-mail* (14.500), nonché in maniera diretta mediante un'impegnativa, quanto essenziale, attività di *front office* svolta attraverso il *call center* (18.100 telefonate pervenute) e il ricevimento diretto del pubblico presso l'Ufficio (1.550 visitatori).

In proposito, oltre al consolidamento di tale positiva tendenza, è stato riscontrato un più alto profilo delle richieste di intervento da parte di un'utenza eterogenea (singoli cittadini, operatori economici, pubbliche amministrazioni, professionisti e consulenti). L'Urp, nel corso del periodo in esame, ha dovuto quindi confrontarsi con siffatte aumentate aspettative da parte di una utenza attenta, desiderosa di trovare nei tempi più brevi qualificate soluzioni, alle quali ha provveduto attraverso l'impegno crescente da parte degli operatori e il miglioramento dell'efficienza delle procedure in vigore.

Allo scopo di corrispondere alle più qualificate attese dell'utenza, che si prevedono ulteriormente crescenti in futuro, si è potenziato l'Urp secondo un modello organizzativo di tipo dipartimentale, più rispondente ai dettami della normativa in materia e con l'ampliamento delle relative competenze, tra le quali rientra, adesso, l'istruzione di risposte a taluni quesiti di interesse generale (nel 2005 ne sono stati evasi circa 1.000), nonché delle istanze d'accesso informale agli atti amministrativi, in attuazione della l. n. 241/1990 e successive modificazioni.

In applicazione del nuovo Protocollo d'intesa con la Guardia di finanza, siglato il 10 novembre 2005, sono stati avviati preliminari contatti con l'Ufficio relazioni con il pubblico del Corpo, diretti a sviluppare forme di collaborazione nell'area della formazione. Tale potenziamento, unitamente all'organizzazione più razionale dei compiti, consente di predisporre nuove e più mirate metodologie di lavoro capaci di offrire un prodotto di maggior spessore e più elevata qualità che, oltre a soddisfare le richieste avanzate, possa al tempo stesso permettere un monitoraggio delle medesime, così da poter costantemente misurare i nuovi bisogni del pubblico ed assumere le opportune iniziative con intuibili riflessi positivi.

Il nuovo modello organizzativo dell'Urp risulta, pertanto, strumentale alla sua speciale posizione di "osservatorio privilegiato" dell'Autorità, attraverso il quale raccogliere, catalogare ed elaborare speditamente le diverse istanze, mettendo in campo interventi e servizi dedicati e differenziati per ciascuna fascia di pubblico (cittadini, operatori economici, P.a.), suscettibili di riflessi positivi in termini di soddisfazione dell'utenza.

Tematiche di interesse

Anche il 2005 è stato caratterizzato dalla richiesta di approfondimento di alcune specifiche tematiche di particolare ed urgente interesse per il pubblico, sia in relazione ai termini di applicazione di singole disposizioni del Codice, sia rispetto all'emergere di questioni di rilevanza sociale.

In particolare è stata riscontrata una cospicua affluenza del pubblico presso la sede dell'Ufficio in prossimità delle varie scadenze correlate agli adempimenti previsti dal Codice. Al riguardo sono pervenute diverse richieste di chiarimenti nei periodi antecedenti alla scadenza dei termini per l'adozione delle "nuove" misure minime di sicurezza, determinandosi in corrispondenza degli stessi una sensibile intensificazione dell'attività dell'ufficio.

Analogo impegno è stato richiesto per far fronte ai numerosi quesiti provenienti da pubbliche amministrazioni interessate all'adozione di regolamenti per il trattamento dei dati sensibili e giudiziari. Inoltre, in previsione delle consultazioni elettorali sono state prese in esame numerose segnalazioni dei cittadini in materia di propaganda elettorale, a testimonianza di una maturata sensibilità sui temi di competenza dell'Autorità.

23.7. *Manifestazioni e conferenze*

L'attività dell'Autorità collegata a seminari, convegni e ad altre iniziative ha riscontrato, nel 2005, la conferma di un elevato interesse da parte del pubblico. In linea con l'obiettivo di promuovere la conoscenza della legge e di diffonderla presso cittadini ed operatori pubblici e privati, il Garante ha confermato la sua presenza in importanti manifestazioni con il proprio *stand* e con la partecipazione dei suoi rappresentanti a dibattiti e convegni.

La XVI edizione del *Forum P.A.*, svoltasi a Roma dal 9 al 13 maggio 2005, ha offerto l'occasione per una presentazione al pubblico del nuovo collegio del Garante e per un primo incontro con i giornalisti. Il 9 maggio 2005, inoltre, il segretario generale dell'Autorità, dott. Giovanni Buttarelli, ha partecipato, quale relatore, alla sessione antimeridiana del convegno "*Identificazione, dati personali e* privacy".

Nei cinque giorni di *Forum*, i visitatori complessivi sono stati 51.800 circa contro i 51.000 dello scorso anno. Sono stati 54.700 i visitatori del sito del Forum; lo *stand* dell'Autorità ha visto un considerevole afflusso di pubblico, con una media giornaliera di circa 300 visitatori.

L'Autorità è stata presente anche al *Com-P.A.* 2005, Salone della comunicazione pubblica, svoltosi a Bologna dal 3 al 5 novembre 2005. In tale occasione, i vertici dell'Autorità hanno partecipato ad alcuni dei convegni in programma: il 4 novembre il presidente del Garante, prof. Francesco Pizzetti, ha concluso i lavori del convegno "*Accesso,* privacy *e sicurezza nelle comunicazioni*"; nella stessa giornata, il vicepresidente, dott. Giuseppe Chiaravalloti, è intervenuto a chiusura del convegno "*Sicurezza e protezione: prima regola, comunicare*". Nella mattinata del 4 novembre, dallo *stand* delle Forze armate, il presidente Pizzetti ha inoltre avuto l'opportunità di dialogare in diretta via satellite con esponenti dei contingenti militari italiani all'estero.

Sulla base dei dati forniti dagli organizzatori, la manifestazione ha visto complessivamente la presenza di 300 espositori, 550 giornalisti accreditati, 721 relazioni presentate e 28.100 visitatori, a conferma della costante, continua crescita di interesse da parte del pubblico. Anche in questa occasione, lo *stand* dell'Autorità ha riscontrato un considerevole afflusso di pubblico, con una media giornaliera di circa 500 visitatori.

23.8. *L'attività di studio, ricerca e documentazione*

L'attività di ricerca e documentazione dell'Ufficio è stata profondamente rinnovata e potenziata nel corso del 2005, al fine dell'acquisizione di un adeguato bagaglio conoscitivo sia rispetto all'attività svolta dal Garante in base a ricorsi, reclami o segnalazioni provenienti dai cittadini, sia in riferimento alle iniziative intraprese d'ufficio dell'Autorità e collegate ai molteplici eventi normativi, scientifici e tecnologici, che si ripercuotono sulla materia della protezione dei dati.

In questa prospettiva, sono state affrontate, tra le altre, le tematiche legate al nuovo assetto della legislazione sul diritto di accesso (con riferimento agli aspetti procedurali, sostanziali ed alla collaborazione istituzionale tra autorità preposte a diverse competenze in merito), alle questioni emergenti in materia di giornalismo, all'istituzione, regolazione e gestione delle biobanche genetiche in prospettiva comparatistica, al *cd. pornosquatting* come trattamento abusivo di dati personali, alla casistica europea in tema di valutazione dei sistemi biometrici sotto il profilo della legittimità del trattamento di dati personali da essi implicato, all'informatizzazione

delle pubbliche amministrazioni, alla condizione di transessuali e *transgender* nonché al carattere super-sensibile delle relative informazioni personali, alla rilevanza crescente dei *blog* nel quadro della libertà di manifestazione del pensiero, alla prescrizione e somministrazione di particolari trattamenti sanitari nella prospettiva del diritto all'autodeterminazione nelle scelte sessuali e procreative.

Nella medesima ottica di lavoro è proseguito l'impegno di approfondimento sulle carte biometriche (anche rispetto alle esperienze in corso di maturazione in altri ordinamenti), sullo sviluppo dei sistemi *Rfid*, nonché sulle apparecchiature "portatili" per il controllo a distanza delle prestazioni lavorative dei dipendenti. Attraverso l'analisi di questi casi di studio si è cercato di fornire un quadro di insieme sulle tecnologie in questione, nonché di prospettare possibili soluzioni e proposte sui relativi profili di applicazione del Codice, anche in vista dell'elaborazione di provvedimenti generali dell'Autorità.

Le finalità di diffusione di strumenti di documentazione e di aggiornamento del personale sono state poste al centro dell'attenzione, e perseguite attraverso la diffusione di un esteso repertorio mensile, nonché attraverso l'invio di *newsletter* interne quindicinali, nelle quali si sono raccolte e commentate le principali novità normative e giurisprudenziali rilevanti per il lavoro dell'Autorità, nonché le elaborazioni della dottrina in merito alle tematiche legate alla protezione dei dati e, più in generale, dei diritti delle persone. In tal quadro sono stati evidenziati e divulgati, ad esempio, i profili emergenti in ambito nazionale ed internazionale, in relazione alle misure di filtraggio dei contenuti illeciti sulla Rete, all'oscuramento dell'identità delle parti nelle sentenze, ai confini del segreto bancario, alla valutazione del *cd.* danno all'immagine delle amministrazioni pubbliche, alla giurisprudenza sul diritto d'accesso ai documenti amministrativi.

Sempre attraverso la *newsletter* interna sono stati inoltre diffusi diversi approfondimenti tematici, talvolta resi in occasione della pubblicazione di sentenze, provenienti anche dall'estero, o emesse dagli organi giudiziari europei e comunitari.

Particolare attenzione è stata dedicata, in tale ambito, tra l'altro, alla riforma del regime delle intercettazioni ambientali in Germania, alla tematica delle violazioni del *copyright* attraverso strumenti *on-line* e motori di ricerca, alla pubblicità effettuata per via telefonica, all'intercettazione e all'accesso ai contenuti di *e-mail* del lavoratore, al trattamento di dati personali svolto nelle attività investigative, al carattere di riservatezza proprio dei colloqui tra detenuti ed avvocati o familiari, al diritto all'anonimato riconosciuto alla madre biologica nel bilanciamento con l'interesse dell'adottato a conoscere le proprie origini, alla riforma della normativa tedesca sull'analisi per identificazione genetica nei procedimenti penali e al trattamento di dati personali effettuato nelle scuole ed università anche in prospettiva comparatistica.

PAGINA BIANCA

L'UFFICIO DEL GARANTE

PAGINA BIANCA

III - L'Ufficio del Garante

24 La gestione amministrativa dell'Ufficio

24.1. *Il bilancio e gli impegni di spesa*

La gestione delle risorse finanziarie affluite al Garante nel corso del 2005 è stata finalizzata al raggiungimento degli obiettivi fissati dal documento programmatico presentato in allegato al bilancio di previsione nel rispetto dei canoni di trasparenza delle procedure e della flessibilità ed efficienza dell'azione amministrativa.

L'esercizio 2005 ha visto acuirsi i problemi connessi con l'erosione delle risorse che lo Stato ha destinato all'attività dell'Autorità; per l'esercizio appena concluso, infatti, le risorse finanziarie a disposizione del Garante si sono ancora ridotte, essendo passate da euro 9.618.000,00 a euro 9.540.653,00. La legge finanziaria 2005 (l. n. 311/2004) prevedeva in tabella C euro 9.177.000,00; durante l'esercizio, per effetto di due provvedimenti di cui uno normativo (d.l. n. 106/2005 convertito con modificazioni nella l. n. 156/2005) che ha imposto una riduzione dello stanziamento, e uno amministrativo (d.m. del Ministero dell'economia e delle finanze n. 77390/2005) di aumento dello stanziamento, le risorse attribuite e effettivamente trasferite nell'esercizio all'Autorità sono state pari a euro 9.540.653,00.

L'anno concluso è stato quindi condizionato finanziariamente dalla riduzione del contributo dello Stato, nonché da entrate proprie che, pur incrementatesi rispetto alle previsioni, sono tornate nell'alveo della normalità.

Obiettivo dell'esercizio 2005 è stato, ancora una volta, il massimo contenimento delle spese dirette di gestione e delle spese per investimenti. Il bilancio di previsione 2005, con le modifiche apportate dai provvedimenti richiamati, si era assestato prevedendo un utilizzo dell'avanzo di amministrazione pari a euro 5.576.193,00. A consuntivo, nonostante la diminuzione delle risorse già richiamata, l'utilizzo effettivo dell'avanzo di amministrazione è stato di euro 4.107.707,77 – inferiore di circa euro 1.500.000,00 a quello preventivato.

La tabella allegata (par. 25.1, n. 23) riassume sinteticamente per gli anni di attività del Garante, dal 1997 al 2005, le risorse finanziarie che lo Stato ha previsto e trasferito all'Autorità per la sua attività, nonché le somme riscosse e le somme pagate ogni anno.

La gestione si è uniformata alle indicazioni contenute nel documento programmatico approvato dal Garante. Si è dovuta scontrare, però, con le ristrettezze del bilancio imposte dalla legge finanziaria e con il fatto che le entrate proprie effettivamente incassate sono passate da euro 3.000.000,00 nel 2004 a meno di euro 1.500.000,00 nel 2005. Tale diminuzione ha riguardato principalmente i minori introiti provenienti dai diritti dovuti per le notificazioni, per i quali non si è ripetuto l'effetto *una tantum* veri-

ficatosi nel precedente esercizio finanziario. Per contro, le uscite effettive hanno subito un balzo di quasi 3 milioni di euro, principalmente dovuto agli aumenti retributivi del personale scaturiti dagli accordi sottoscritti con le organizzazioni sindacali il 10 dicembre 2004, e in minor misura, dall'insediamento del nuovo collegio. Al capitolo relativo alle sanzioni pecuniarie, per il quale era stata prevista una entrata pari a euro 50.000,00, l'accertamento riscontrato è stato pari a euro 240.000,00, grazie ad un più capillare intervento del settore ispettivo dell'Autorità con la fattiva collaborazione del Nucleo apposito della Guardia di finanza.

La gestione è stata indirizzata, come per gli anni passati, al miglioramento della funzionalità complessiva dell'Ufficio ed al potenziamento dei dipartimenti e servizi in particolare giuridici, avvenuto con l'immissione all'inizio del 2005 del personale assunto con l'ultimo concorso espletato nel 2004, considerando l'aggravio di lavoro conseguente all'avvicinarsi delle scadenze imposte dal Codice, nonché a soddisfare le necessità tecnico-logistiche delle segreterie del nuovo collegio che si è insediato ad aprile del 2005, per consentirne la pronta operatività.

24.2. *L'attività contrattuale*

Dal punto di vista normativo, non vi sono da segnalare novità normative di rilievo ed idonee ad incidere sulle procedure contrattuali seguite negli anni passati, dal momento che l'atteso nuovo Codice dei contratti pubblici relativi a lavori, servizi e forniture, attuativo delle direttive n. 2004/17/Ce e n. 2004/18/Ce, rimasto in fase preparatoria durante tutto il 2005, è stato approvato dal Consiglio dei ministri solo il 23 marzo 2006 (d.lg. 12 aprile 2006, n. 163, in *G.U.* 2 maggio 2006, n. 100, *S.O.*).

La prospettiva del nuovo quadro normativo ha però indotto l'Autorità a considerare, già prima dell'approvazione del Codice dei contratti pubblici, l'opportunità di adeguare il limite previsto per la trattativa privata dal proprio regolamento di contabilità del 2000, al fine di assicurare la necessaria snellezza nelle procedure che si svolgano al di sotto della "soglia comunitaria".

L'attività contrattuale dell'anno in esame, al pari di quella dell'anno precedente, ha avuto come obiettivo principale la razionalizzazione dei fabbisogni relativi all'acquisizione di beni o servizi e il contenimento della relativa spesa, imposto dalla gravosità dei vincoli di bilancio.

In particolare, anche al fine di contemperare il perseguimento della contrapposta esigenza di efficienza ed efficacia dell'azione amministrativa e di garanzia delle migliori condizioni tecniche ed economiche di esercizio, si è provveduto ad una puntuale programmazione delle acquisizioni di beni e servizi al fine di realizzare economie di scala, nonché a un'attenta verifica delle disponibilità interne dell'ufficio e all'eventuale individuazione delle più idonee procedure di acquisto.

Nel senso prospettato, merita di essere menzionata anche la decisione di rinviare di un anno, dopo un'attenta e articolata riflessione, la stipula del contratto di assistenza sistemistica per le strutture informatiche, al fine di provvedere alla relativa richiesta con una gara unica, anziché con una pluralità di contratti separati che non avrebbero garantito, al contempo, omogeneità nell'erogazione del servizio e contrazione della spesa.

Nel corso dell'anno si è poi provveduto, con la collaborazione del *broker* prescelto, a preparare gli atti della gara europea per i servizi assicurativi (incendio, *all risk* elettronica, responsabilità civile sia verso terzi e prestatori d'opera, sia patrimoniale, premorienza).

Come già registrato nelle precedenti edizioni della *Relazione*, in ragione dell'importo relativamente contenuto e dello stato ormai consolidato della struttura, i contratti sono stati stipulati sulla base di una trattativa privata preceduta da una ricerca di mercato, in ottemperanza all'art. 25 reg. n. 3/2000 (tra essi si citano, a titolo di mero esempio, il contratto avente ad oggetto l'allestimento e la conservazione dello *stand* dell'Autorità e quello relativo alla fornitura del *Cd-rom* istituzionale del Garante nella versione aggiornata).

24.3. *Le novità legislative e regolamentari e l'organizzazione dell'Ufficio*

Nella prima parte del 2005 sono state adottate alcune significative, seppure circoscritte modifiche regolamentari per rendere l'assetto organizzativo dell'Autorità più rispondente ai nuovi compiti demandati al Garante dal Codice in materia di protezione dei dati personali e, più in generale, alle esigenze istituzionali.

In particolare sono state rideterminate le competenze del dipartimento "vigilanza e controllo", il quale ha assunto la nuova denominazione "attività ispettive e sanzioni", in considerazione dei nuovi compiti ad esso affidati connessi all'attuazione del protocollo sottoscritto con la Guardia di finanza e alla crescente attività relativa alla contestazione delle sanzioni amministrative e ai correlativi procedimenti, nonché alla collaborazione con l'autorità giudiziaria, specie in ambito penale per l'accertamento degli illeciti previsti dal Codice.

Analogamente, al fine di potenziare e qualificare le attività di informazione e di consulenza rese ai cittadini, alle amministrazioni pubbliche e alle imprese, l'Ufficio per le relazioni con il pubblico è stato trasformato in unità organizzativa di primo livello.

Nel quadro delle iniziative in corso per migliorare la capacità di risposta dell'Autorità, è stata prevista inoltre la possibilità di istituire articolazioni organizzative anche di livello generale, nonché di nominare uno o più vice segretari generali.

In tema di trattamento giuridico ed economico del personale, nel periodo considerato è stata data attuazione ad alcune circoscritte modifiche regolamentari, adottate alla fine del 2004 e finalizzate al riequilibrio del trattamento economico dei diversi segmenti di personale di cui si compone l'Ufficio del Garante, nonché all'adeguamento di alcuni profili della disciplina dell'orario di lavoro e dei contratti a tempo determinato alle novità legislative intervenute. Questi ultimi sono stati rimodellati, in conformità alla normativa comunitaria e interna, riducendo ad un anno la durata dei contratti di specializzazione (destinati a giovani laureati), e allungando quella dei contratti a tempo determinato sino a tre anni (con possibilità di rinnovo per non più di due volte), ferma restando la previsione che a tale tipologia contrattuale è possibile ricorrere solo in presenza di particolari esigenze organizzative e funzionali.

Parallelamente, l'adeguamento dello stanziamento dell'Autorità previsto dalla legge finanziaria 2006 ha consentito di proseguire l'attività per potenziare il peraltro esiguo organico dell'Autorità con la decisione di bandire due nuovi concorsi, come si dirà in seguito. Ciò ha comportato una rimodulazione della dotazione organica delle aree direttiva (particolarmente carente in relazione ai nuovi e delicati compiti connessi all'attuazione del Codice), operativa ed esecutiva. Con deliberazione del Garante (pubblicata nella *G.U.* 27 gennaio 2006, n. 22), la pianta organica è stata modificata incrementando di n. 4 posti la dotazione organica dell'area direttiva (la quale ora ammonta a 49 posti), con una corrispondente riduzione della consistenza organica delle aree operativa ed esecutiva per rispettivi n. 2 posti.

24.4. *Il personale e i collaboratori esterni*

Agli inizi del 2005 si sono concluse le procedure dei due concorsi pubblici banditi nel febbraio del 2004, di cui uno a nove posti di funzionario e l'altro a quattro posti di impiegato operativo, con l'immissione in servizio dei vincitori. Tali concorsi prevedevano una riserva del trenta per cento dei posti per il personale non di ruolo, in conformità all'art. 182, comma 1, lett. *b*), del Codice, riserva rimasta inutilizzata per mancanza di candidati riservatari risultati idonei. Dei tredici posti complessivamente banditi ne sono stati coperti solo dieci (n. 7 posti di funzionario e n. 3 di impiegato operativo). Sono state poi inquadrate nel ruolo organico n. 9 unità.

Il processo di consolidamento dell'Autorità è proseguito, nel periodo considerato, con la decisione di bandire due nuovi concorsi pubblici, di cui uno per quattro posti di funzionario e, l'altro, per tre posti di impiegato operativo. Contestualmente, sono stati riaperti i termini della selezione per il reclutamento di (sino a) 3 giovani laureati con contratto di specializzazione a tempo determinato, bandita nel febbraio del 2004, ed è stata indetta una selezione per la frequenza di periodi di tirocinio presso l'Autorità, unitamente ad una procedura selettiva a tre posti di funzionario riservata al personale interno, in attuazione di una disposizione del regolamento concernente il trattamento giuridico ed economico del personale. I relativi bandi ed avvisi sono stati pubblicati nella *Gazzetta Ufficiale*, IV serie speciale, 31 gennaio 2006, n. 8. A conclusione delle predette procedure l'organico dell'Autorità risulterà coperto al 95%.

Al 31 dicembre 2005 l'Ufficio poteva contare su un organico, a diverso titolo, di n. 96 unità, di cui 91 effettivamente in servizio (*cfr.* prospetto al par. 25.1). Il 77% ca. del personale appartiene al ruolo organico, mentre l'8% ca. presta servizio presso l'Autorità in posizione di fuori ruolo da altre amministrazioni o enti pubblici e il 15% ca. a contratto.

Consulenze, incarichi professionali, convenzioni

Allo stato l'Autorità non si avvale della collaborazione di consulenti. Nel periodo considerato si è reso peraltro necessario ricorrere ad un numero circoscritto di incarichi professionali occasionali per acquisire competenze qualificate in materia informatica per le problematiche concernenti il sistema informativo interno e il sito *web* del Garante, nonché per la verifica, la manutenzione e il necessario aggiornamento del registro informatico dei trattamenti e per alcune attività di supporto ai dipartimenti giuridici.

Nel corso del 2005, nell'ottica della formazione rivolta a giovani laureati, si sono svolti alcuni *stage* in collaborazione con diverse università.

Avvalendosi delle convenzioni Consip, sono state inoltre conferite in *insourcing* alcune attività di natura esecutiva che non richiedono un apporto lavorativo di elevato contenuto professionale (*ad es.*, per l'attività di portineria e per compiti ausiliari).

L'Autorità si avvale, altresì, di un servizio di controllo interno presieduto da un dirigente della Ragioneria generale dello Stato e composto da un magistrato della Corte dei conti e da un dirigente generale in quiescenza della medesima Ragioneria generale.

24.5. *Il settore informatico e tecnologico*

Attività nel settore informatico e tecnologico

Il ruolo del Dipartimento risorse tecnologiche si è andato ulteriormente caratterizzando nel 2005 sulla base delle necessità dell'Autorità e dell'attività effettivamente svolta, con duplice valenza di servizio per lo sviluppo e la gestione dei sistemi informativi e di unità per la consulenza interna in grado di supportare i dipartimenti giuridici e ogni altra articolazione dell'Autorità stessa, nell'elaborazione di provvedimenti o in altri ambiti dell'attività amministrativa in cui sia richiesta l'analisi di aspetti informatici e tecnologici.

Nell'impegno per soddisfare alle esigenze dell'Ufficio, il dipartimento ha compiuto ogni possibile sforzo per rendere disponibili quando necessario le competenze richieste, anche non riferibili a quelle formalmente assegnate alla struttura sulla base dei regolamenti interni. Il mutato carico di lavoro e l'innalzamento del livello di approfondimento e analisi reso necessario dalla ricorrente applicazione a problematiche derivanti da trattamenti informatici, rende opportuno un potenziamento della struttura al fine di assolvere più efficacemente ai compiti in materia di sistemi informativi e di analisi, studio e consulenza nell'ambito dell'attività "di merito" dell'Autorità nel suo complesso, e di supporto all'attività ispettiva, mantenendo al suo interno l'unità delle competenze e la condivisione delle esperienze.

Sviluppo dei sistemi informativi

Nel 2005, gli investimenti in tecnologie e in servizi informatici sono andati incontro a una temporanea contrazione, mentre è stata continua l'attività di gestione interna e di progettazione di nuovi servizi.

Tra le realizzazioni compiute è stata particolarmente significativa quella relativa alla procedura *on-line* per la trasmissione di richieste di verifica preliminare ai sensi dell'art. 17 del Codice, progettata e implementata nell'ultimo bimestre del 2005 con il riscorso prevalente a sistemi *open source*. Tale procedura, che affianca quella di notificazione telematica, consente di ricevere le richieste di verifica preliminare per via telematica, con garanzie di sicurezza e autenticità fornite dal ricorso alle certificazioni digitali e alla firma digitale, integrandosi con i sistemi di protocollo e di *workflow* documentale.

Per quanto attiene ai servizi *web* e *Intranet* si è fornito supporto al progetto di documentazione giuridica relativo ai provvedimenti e agli atti normativi inerenti la protezione dei dati personali, nell'ambito del progetto nazionale "*NormeInRete*", approntando le opportune tecnologie e adattando i sistemi esistenti per la gestione del formato di marcatura *Xml*.

È stato dettagliatamente progettato il sistema informatico per la gestione dell'attività ispettiva e sanzionatoria, che verrà sviluppato nel 2006 e che sarà basato su strumenti *open source*.

Sono stati messi a punto strumenti di reportistica per il rilevamento di indici di prestazione utili alla gestione dell'Ufficio, integrandoli nei sistemi informativi e sviluppandoli come applicazioni esterne che interagiscono con le basi di dati.

Dal punto di vista delle infrastrutture è stato avviato il consolidamento delle risorse *hardware* con l'adozione di un'architettura di tipo *blade* e di un sistema di *storage* a tecnologia fibre *channel* che consentirà, a regime, di concentrare tutti i servizi erogati dal Drt su un'unica piattaforma tecnologica, garantendo così una più agevole realizzazione di procedure di *disaster recovery* e di continuità operativa.

Insieme alle attività di progettazione e gestione dei sistemi informativi è stata svolta continuamente attività di *help-desk* interno, di assistenza tecnica per l'intero sistema tecnologico e di supporto per le esigenze informatiche dell'Autorità.

Impegno per la sicurezza dell'Ufficio

Un grande attenzione è stata rivolta alla stesura del documento programmatico sulla sicurezza (d.p.s.) secondo le disposizioni del Codice, che è stato poi costantemente aggiornato sulla base dell'evoluzione dei sistemi e dell'organizzazione dell'Ufficio.

I livelli di protezione sono stati monitorati costantemente grazie agli strumenti di *intrusion detection* e alle architetture di protezione perimetrale. Particolarmente importante è stata la conduzione periodica di *security assessment* che ha consentito di verificare l'efficacia delle misure di sicurezza messe in atto in rapporto al rischio attuale e previsto.

Nel 2005, come negli anni precedenti, nessun *virus* informatico è penetrato sulla rete interna tramite posta elettronica né per altre vie, grazie all'adozione di più livelli

di filtraggio che hanno sempre assicurato una copertura totale anche nei momenti di maggior recrudescenza dei fenomeni di diffusione di *malware* tramite la rete Internet e nonostante il sempre crescente utilizzo della rete per comunicazioni di ogni tipo nell'ambito dell'attività dell'Ufficio.

Attività di consulenza e cooperazione interna

È cresciuto notevolmente il coinvolgimento nell'attività amministrativa propria dell'Autorità, compresa l'attività ispettiva. Il dipartimento ha fornito supporto per l'analisi tecnica richiesta nell'ambito di procedimenti di ricorso o di altri tipo curati dai dipartimenti giuridici, ha svolto consulenza interna extra-procedimentale e ha curato l'approfondimento di argomenti a contenuto informatico-tecnologico, anche in relazione a esigenze specifiche dell'Autorità.

Tra le attività più significative sono comprese quelle svolte in relazione ai procedimenti di *prior checking* connessi all'implementazione di sistemi biometrici da parte di soggetti pubblici e privati, al trattamento dei dati di traffico telefonico e telematico, alle intercettazioni telefoniche per scopi di giustizia, ai ricorsi relativi a trattamenti di dati personali tramite la rete Internet o tecnologie informatiche nell'ambito lavorativo, ai provvedimenti relativi ai motori di ricerca e al loro rapporto con il diritto all'oblìo, alla videosorveglianza, ai sistemi di informazioni creditizie, ai pareri su atti normativi in materia di immigrazione, visti, permessi di soggiorno e passaporti. Intenso è stato poi il lavoro, tuttora in corso, in riferimento al codice deontologico per i servizi Internet. Analogo impegno è stato riservato alla trattazione dei regolamenti per i dati sensibili nelle pubbliche amministrazioni, con particolare riferimento ai trattamenti in ambito sanitario. Il dipartimento ha inoltre contribuito allo svolgimento di ispezioni e accertamenti svolti nell'ambito della programmazione stabilità dall'Autorità; ha partecipato all'attività internazionale nell'ambito del Gruppo art. 29, contribuendo attivamente ai lavori della *Internet Task Force* (Itf) e nell'ambito dell'Ocse (Wpisp); in ambito Itf, ha contribuito alla definizione dei documenti adottati dal Gruppo art. 29 in materia di *data retention*, servizi di posta elettronica, geolocalizzazione; ha partecipato inoltre al gruppo di lavoro Cnipa che ha elaborato le linee guida sulla biometria nella pubblica amministrazione.

24.6. *Il monitoraggio dell'efficacia e dell'efficienza e il supporto al controllo interno*

L'esigenza di monitorare l'andamento delle diverse attività dell'Ufficio per l'efficace ed efficiente impiego delle risorse è stato assicurato attraverso *report* periodici elaborati, nell'ambito della segreteria generale, sulla base delle informazioni provenienti dai sistemi informativi del protocollo, amministrativo-contabile e del personale.

Il livello di informatizzazione raggiunto dall'Ufficio consente di sostenere l'esecuzione di programmi ordinari e straordinari fornendo al segretario generale e alle unità organizzative coinvolte flussi tempestivi di dati sui risultati che si stanno conseguendo, sulle risorse impiegate e sugli eventuali scostamenti, in modo da avviare per tempo le necessarie azioni correttive.

Si tratta di una funzione di rilievo in una gestione tesa al costante miglioramento dei livelli di efficacia, di efficienza e di economicità delle azioni amministrative e alla qualità dei servizi resi ai cittadini e che, inoltre, è in grado di garantire al Servizio di controllo interno le informazioni necessarie a svolgere le analisi e le valutazioni di sua competenza.

Per tali motivi, alla fine del 2005 il Garante ha deciso di istituire un'apposita articolazione denominata "Unità raccolta dati, flussi informativi e supporto al controllo interno", alla quale è stato preposto un dirigente con pregresse esperienze nel settore della valutazione strategica e del controllo di gestione.

25 Dati statistici

25.1. *Tabelle e grafici*

1. Principali attività dell'Autorità

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali [1]	724
Ricorsi	634
Altri provvedimenti collegiali sul trattamento dei dati personali	45
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154 del Codice)	22
Autorizzazioni al trasferimento dati all'estero	4
Autorizzazioni anche generali al trattamento di dati sensibili e giudiziari	9
Notificazioni pervenute	11.905
Sanzioni amministrative contestate dal Garante	94
Denunce del Garante all'autorità giudiziaria	7 [2]
Riscontri a segnalazioni e reclami	906
Risposte a quesiti	200
Accertamenti e controlli effettuati direttamente presso i titolari del trattamento	230
Altre richieste ai sensi dell'art.157 del Codice	84
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	11
Verifiche preliminari per trattamenti che presentano rischi specifici	4
Comunicazioni al Garante su flussi di dati tra P.a. o in tema di ricerca (*ex* art. 39 del Codice)	45
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	16
Altri pareri	1

2. Altre attività

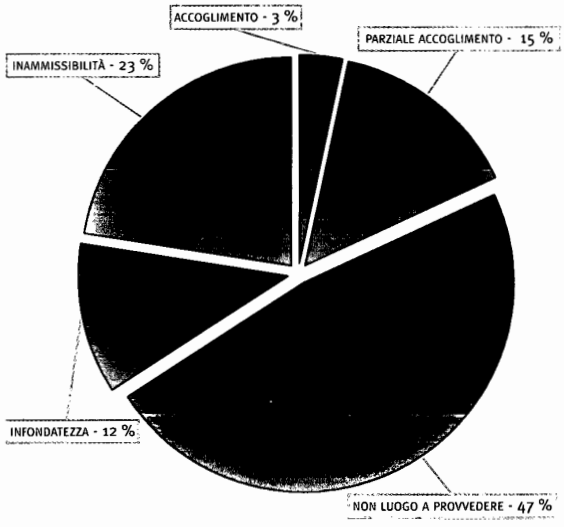
Altre attività dell'Autorità	
Comunicati stampa	72
Newsletter	29
Cd-rom pubblicati	2
Volumi pubblicati	1
Incontri di formazione per soggetti pubblici e privati	1
Presenze internazionali e comunitarie in comitati e gruppi di lavoro	59
Conferenze internazionali	9

(1) Escluse deliberazioni di rilievo interno sull'attività dell'Autorità e sull'organizzazione e il funzionamento dell'Ufficio

(2) Relative a n. 10 soggetti denunciati

3. Tipologia delle decisioni su ricorsi (tabella e grafico)

Decisioni su ricorsi	
tipi di decisione [1]	**numero ricorsi**
Accoglimento	21
Parziale accoglimento	93
Non luogo a provvedere [2]	303
Infondatezza	74
Inamissibilità	143
Totale	634

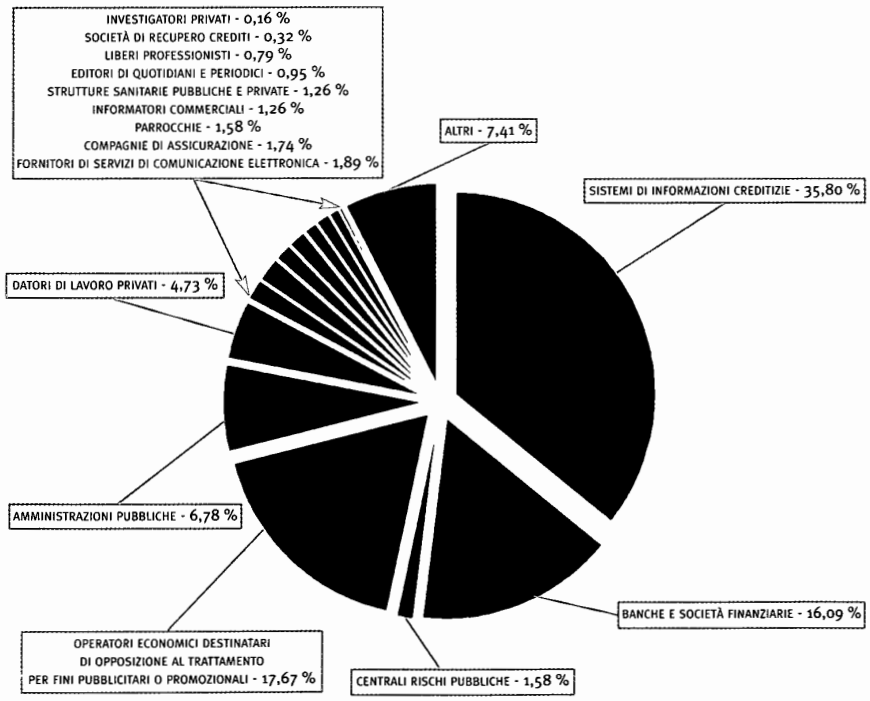


(1) Le decisioni sui ricorsi possono contenere più statuizioni: la statistica si basa sulla statuizione più "favorevole" per il ricorrente

(2) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

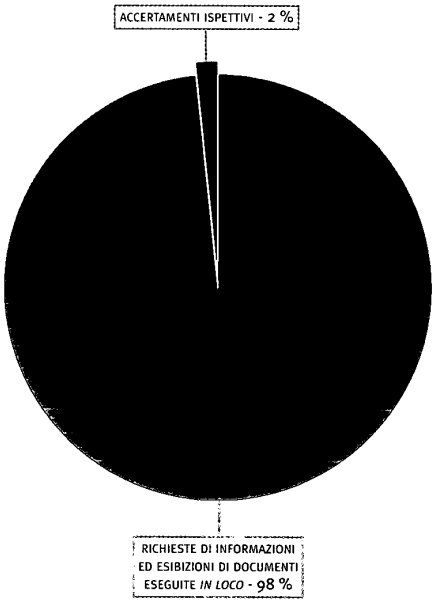
Categorie di titolari	Numero ricorsi
Sistemi di informazioni creditizie	227
Banche e società finanziarie	102
Centrali rischi pubbliche	10
Operatori economici destinatari di opposizione al trattamento per fini pubblicitari o promozionali	112
Amministrazioni pubbliche	43
Datori di lavoro privati	30
Fornitori di servizi di comunicazione elettronica	12
Compagnie di assicurazione	11
Parrocchie	10
Informatori commerciali	8
Strutture sanitarie pubbliche e private	8
Editori di quotidiani e periodici	6
Liberi professionisti	5
Società di recupero crediti	2
Investigatori privati	1
Altri	47
Totale	**634**

4. Suddivisione dei ricorsi in relazione alla categorie di titolari del trattamento (tabella e grafico)



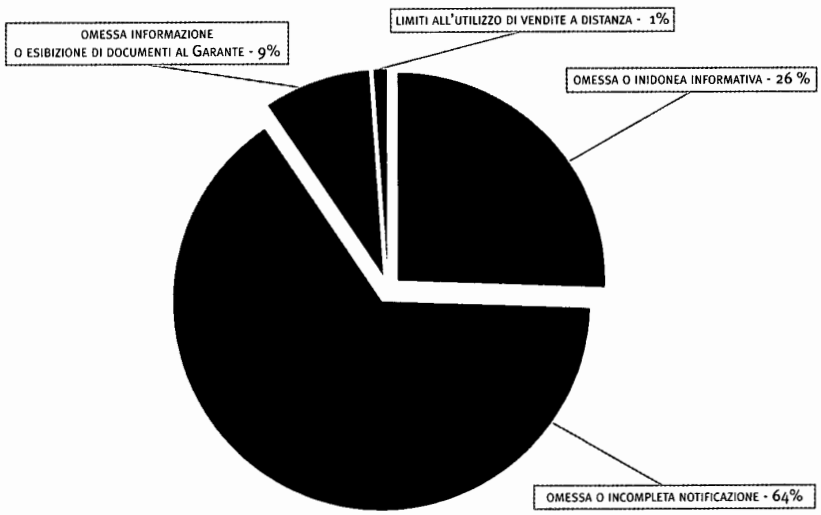
5. Accertamenti e controlli eseguiti (tabella e grafico)

Accertamenti e controlli eseguiti direttamente presso titolari del trattamento	
Richieste di informazioni ed esibizioni di documenti, eseguite *in loco* (art. 157 del Codice)	226
Accertamenti ispettivi (art. 158 del Codice)	4
Totale	**230**



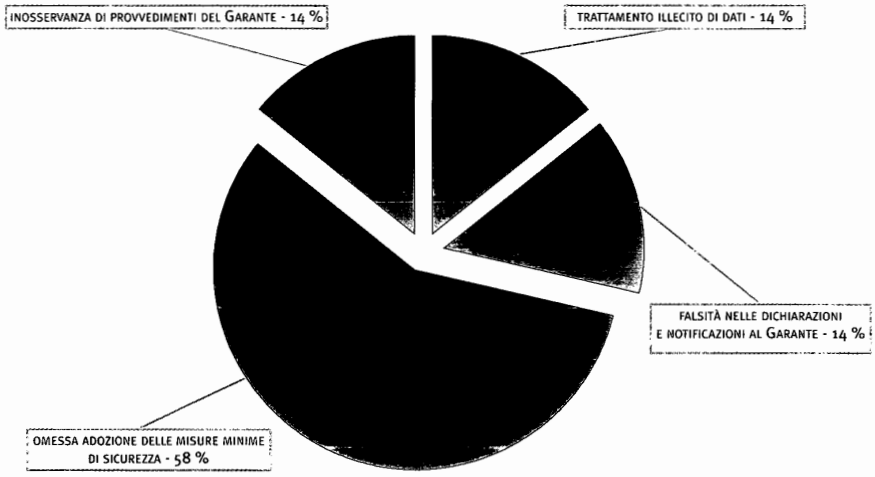
6. Sanzioni contestate dal Garante (tabella e grafico)

Sanzioni amministrative contestate dal Garante	
Omessa o inidonea informativa (art. 161 del Codice)	24
Omessa o incompleta notificazione (art. 163 del Codice)	61
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	8
Limiti all'utilizzo di vendite a distanza (art. 12 d.lg. 185/1999; *v.* ora art. 62, commi 1 e 3, d.lg. n. 206/2005)	1
Totale	**94**



7. Denunce all'autorità giudiziaria (tabella e grafico)

Denunce del Garante all'autorità giudiziaria		
	denunce	denunciati
Trattamento illecito di dati (art. 167 del Codice)	1	1
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168 del Codice)	1	1
Omessa adozione delle misure minime di sicurezza (art. 169 del Codice)	4	7
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	1	1
Totale	**7**	**10**



8. Pareri

Pareri [1] (art.154, comma 4, del Codice)		
temi	pervenuti nell'anno	riscontri resi nell'anno[2]
altro		1
carte identificative, codice fiscale e numeri di identificazione personale	1	1
controllo spesa sanitaria	2	1
dati (e fascicoli) personali di dipendenti	2	2
giustizia	2	2
informatizzazione e banche dati P.a.	1	1
Internet	2	3
monitoraggi sanitari	3	2
rilevazioni biometriche	1	1
riservatezza della corrispondenza	1	1
sanità	3	1
telefonia	1	1
trasparenza	1	1
tributi	2	1
videosorveglianza (finalità di prevenzione e repressione illeciti)	1	1
videosorveglianza (finalità di sicurezza pubblica)	1	2
Totale	**24**	**22**

9. Quesiti

Quesiti [1]		
temi	pervenuti nell'anno	riscontri resi nell'anno [2]
altro	17	
anagrafe e stato civile	21	8
carte identificative, codice fiscale e numeri di identificazione personale	3	
dati (e fascicoli) personali di dipendenti	36	19
esteri (elenco aventi diritto al voto)		1
giornalismo (dati contenuti in sentenze)	1	1
giornalismo (altre questioni)	1	
giornalismo (informazioni raccolte mediante telecamere nascoste)		1
giornalismo (trasmissioni radiofoniche e televisive)	1	1
giustizia (casellario giudiziario e carichi pendenti)		1
giustizia (altre questioni)	6	4
giustizia (modalità per notifiche e comunicazioni)	2	
giustizia (prove nel processo)	4	
giustizia (pubblicità dei provvedimenti)	1	
giustizia (raccolta di dati per finalità di difesa)	4	2
indicatori di condizioni economiche	4	
informatizzazione della P.a.	1	
Internet (foto in Internet)	2	1
Internet (altre questioni)	16	8
Internet (*spamming*)	1	
lavoro (controlli sul lavoro)	5	5
leva e liste elettorali	20	3
licenze e autorizzazioni	1	1
polizia municipale	1	1
pubblicità esiti scolastici		1

(segue)

(1) Dati riferiti ai fascicoli istituiti presso l'Ufficio e non ai singoli documenti (criterio adottato invece nella *Relazione* 2004)
(2) Inerenti anche affari pervenuti anteriormente al 2005

(segue)

raccolte dati in ambito assicurativo e banca dati Isvap	1	1
recapito pubblicità non gradita		1
rilevazioni biometriche	14	7
riservatezza della corrispondenza	2	1
sanità (cartelle cliniche)	5	6
sanità (certificazioni di invalidità)	6	3
sanità (certificazioni mediche)	4	
sanità (Hiv)	1	
sanità (altre questioni)	21	17
sanità (monitoraggi sanitari)	13	3
servizi di assistenza sociale	1	
smaltimento rifiuti	2	3
sms istituzionali	1	1
telefonia (elenchi telefonici)	3	1
telefonia (fatturazione dettagliata)	1	1
telefonia (fax indesiderati)	1	1
telefonia (altre questioni)	5	2
trasparenza (attività organi collegiali)	6	4
trasparenza (altro)	17	12
trasparenza (legge n. 241/1990)	9	5
tributi banche dati fiscali		1
tributi	3	
uffici tributi locali	3	
videosorveglianza (finalità di monitoraggio e controllo del traffico)	2	2
videosorveglianza (finalità di prevenzione e repressione illeciti)	18	13
videosorveglianza (finalità di rispetto disposizioni smaltimento rifiuti)	1	5
videosorveglianza (finalità di sicurezza pubblica)	23	12
videosorveglianza (finalità di tutela patrimonio edilizio ed artistico)	1	2
videosorveglianza (da parte di privati)	20	17
videosorveglianza (altre questioni)	6	19
zone a traffico limitato e parcheggi riservati	2	2
Totale	**340**	**200**

10. Segnalazioni/Reclami

Segnalazioni e reclami [1]		
temi	pervenuti nell'anno	riscontri resi nell'anno [2]
altro	3	
anagrafe e stato civile	9	5
carte identificative, codice fiscale e numeri di identificazione personale	25	14
certificazioni	1	
dati (e fascicoli) personali di dipendenti	114	43
giornalismo (cronache giudiziarie)	5	13
giornalismo (dati contenuti in sentenze)	4	2
giornalismo (foto segnaletiche e di persone arrestate)	4	4
giornalismo (altre questioni)	68	49
giornalismo (indagati)	11	8
giornalismo (informazioni raccolte mediante telecamere nascoste)	1	2
giornalismo (minori)	14	17
giornalismo (pubblicazioni occasionali)	1	2

(1) Dati riferiti ai fascicoli istituiti presso l'Ufficio e non ai singoli documenti (criterio adottato invece nella *Relazione* 2004)
(2) Inerenti anche affari pervenuti anteriormente al 2005

(segue)

(segue)

giornalismo (trasmissioni radiofoniche e televisive)	13	20
giornalismo (vittime di reato)	3	1
giustizia (altre questioni)	21	6
giustizia (indagini del pubblico ministero)	1	
giustizia (modalità per notifiche e comunicazioni)	7	1
giustizia (prove nel processo)	5	2
giustizia (pubblicità dei provvedimenti)	7	3
giustizia (raccolta dei dati per finalità di difesa)	5	2
indicatori di condizioni economiche	3	2
Internet (Enum)	1	
Internet (foto in Internet)	6	3
Internet (in generale)	73	29
Internet (*newsgroup*)	1	
Internet (*spamming*)	28	24
lavoro (controlli sul lavoro)	18	9
leva e liste elettorali	4	2
mense e trasporti	1	
monitoraggi sanitari	9	5
notificazione in busta aperta	11	4
polizia municipale	15	5
pubblicità esiti scolastici		1
raccolte dati in ambito assicurativo e banca dati Isvap		1
recapito pubblicità non gradita	73	35
registro dei protesti	8	8
ricerca e selezione del personale		1
rilevazioni biometriche	14	2
riservatezza della corrispondenza	35	15
sanità (cartelle cliniche)	29	20
sanità (certificazioni di invalidità)	8	3
sanità (certificazioni mediche)	29	22
controllo spesa sanitaria	1	1
sanità (Hiv)	5	3
sanità (altre questioni)	37	30
servizi di assistenza sociale	1	1
smaltimento rifiuti	2	17
sms istituzionali	3	
sms pubblicitari	17	8
telefonia (chiamate di disturbo)	17	12
telefonia (elenchi telefonici)	19	15
telefonia (errata ricarica schede telefoniche)	1	
telefonia (fatturazione dettagliata)	35	199
telefonia (fax indesiderati)	13	10
telefonia (altre questioni)	109	62
telefonia (localizzazione geografica)		2

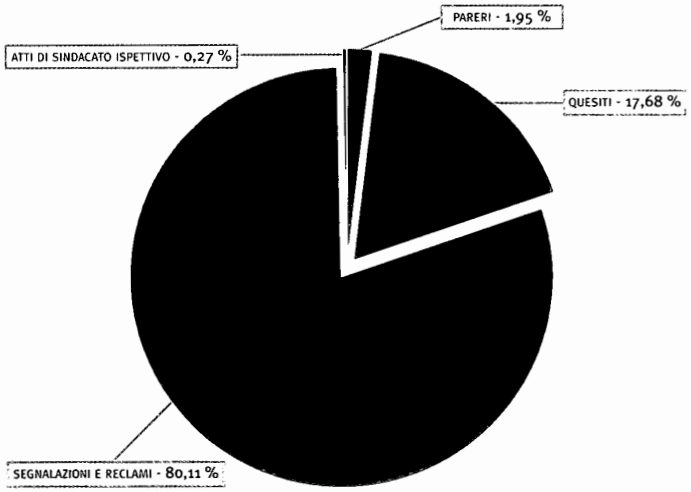
(segue)

telefonia (numeri riservati)	54	37
telefonia (servizi non richiesti)	61	34
telefonia (899)		2
telefonia (*sms* anonimi)	2	1
trasparenza	4	5
trasparenza (legge n. 241/1990)	7	5
tributi (canone Rai)	80	16
tributi (contenuto delle dichiarazioni dei redditi)	1	2
tributi (altre questioni)	1	1
uffici (tributi locali)	12	1
videosorveglianza (finalità di monitoraggio e controllo del traffico)	9	2
videosorveglianza (finalità di prevenzione e repressione illeciti)	22	7
videosorveglianza (finalità di sicurezza pubblica)	8	1
videosorveglianza (finalità di tutela patrimonio edilizio ed artistico)	1	
videosorveglianza (da parte di privati)	51	40
videosorveglianza (altre questioni)	4	5
zone a traffico limitato e parcheggi riservati	4	2
Totale	**1.269**	**906**

11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo [1]		
temi	pervenuti nell'anno	riscontri resi nell'anno[2]
dati (e fascicoli) personali di dipendenti	1	
giornalismo (minori)		1
Internet (*spamming*)	1	1
telefonia (servizi non richiesti)	1	1
Totale	**3**	**3**

12. Tipologie dei riscontri resi a interessati e richiedenti



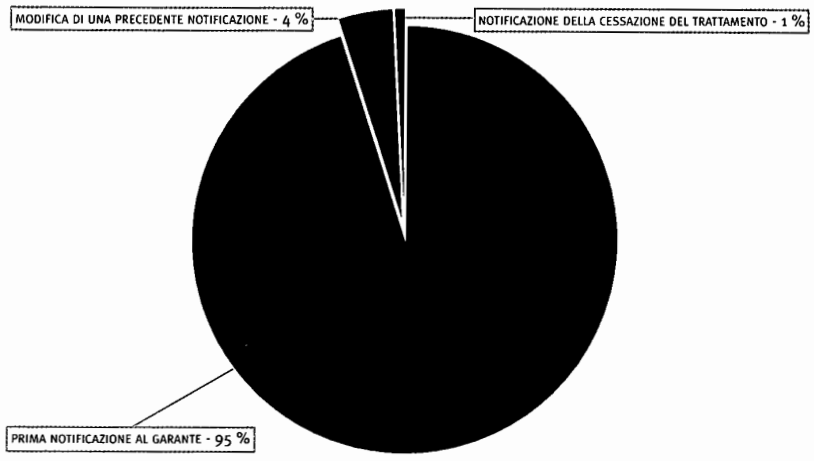
(1) Dati riferiti ai fascicoli istituiti presso l'Ufficio e non ai singoli documenti (criterio adottato invece nella *Relazione* 2004)
(2) Inerenti anche affari pervenuti anteriormente al 2005

Autorizzazioni al trattamento di dati sensibili e giudiziari	
Autorizzazioni generali	7
Autorizzazioni a singoli titolari del trattamento	2
Totale	**9**
Autorizzazioni al trasferimento dei dati all'estero	4

13. Autorizzazioni

tipologia	da soggetti pubblici	da soggetti privati	totale pervenute [1]
Prima notificazione al Garante	878	10.437	11.315
Modifica di una precedente notificazione	20	470	490
Notificazione della cessazione del trattamento	---	100	100
Totale notificazioni[1]	**898**	**11.007**	**11.905**

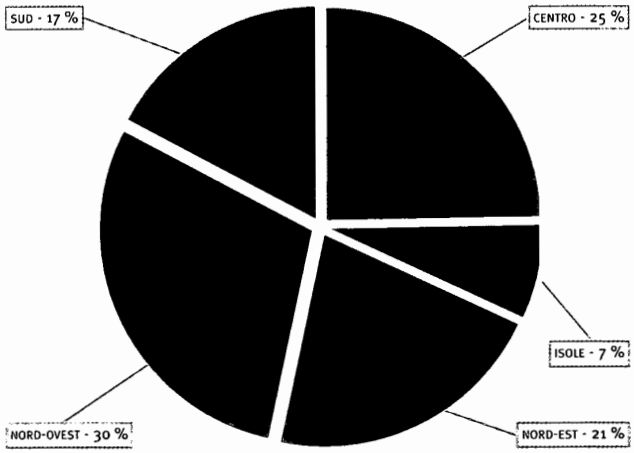
14. Tipologie di notificazioni (tabella e grafico)



(1) Situazione alla data del 31 dicembre 2005. Alla data del 31 dicembre 2004, il totale delle notificazioni al Garante era di 9.997

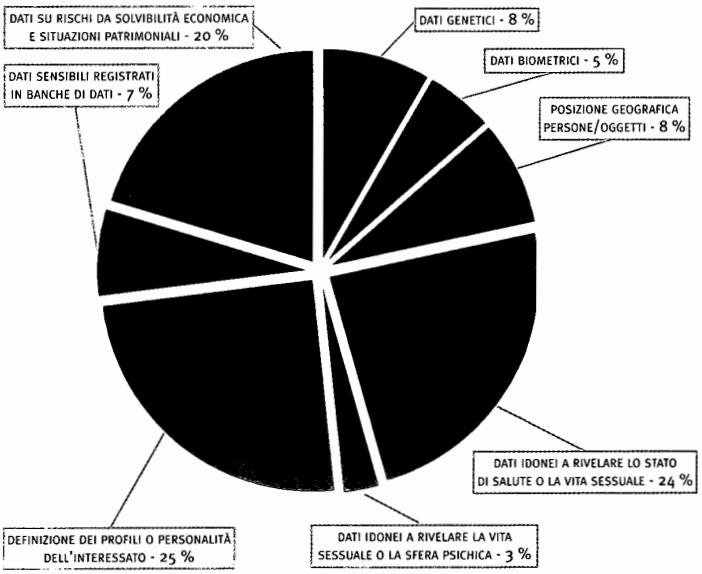
15. Provenienza geografica delle notificazioni nel 2005 (tabella e grafico)

Italia	
zone geografiche	pervenute
Centro	464
Isole	136
Nord-Est	401
Nord-Ovest	552
Sud	324
Totale	**1.877**



16. Suddivisione delle notificazioni per tipologia di trattamento svolto (tabella e grafico)

tabelle di notifica compilate [1]	
Tabella 1 - Trattamento di dati genetici	1.477
Tabella 2 - Trattamento di dati biometrici	964
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	1.408
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	4.255
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	520
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	4.362
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	1.196
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	3.621
Totale	**17.803**



(1) Situazione alla data del 31 dicembre 2005

17. Modalità di inoltro delle notificazioni

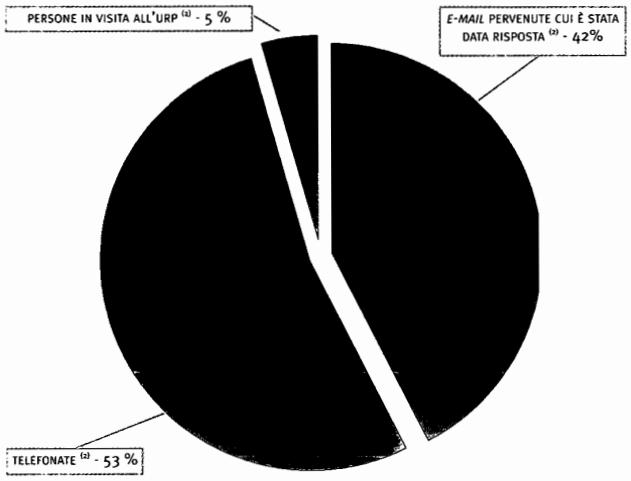
Modalità di inoltro delle notificazioni	pervenute nel 2005
attraverso intermediari	1.047
direttamente a cura dei titolari	838
Totale	**1.885**

18. Modalità di versamento utilizzate

Modalità di versamento utilizzate[1]		
tipo movimento	numero	totale euro
versamento mediante bollettino postale	5.745	861.750
versamento mediante bonifico bancario	3.560	534.000
versamento mediante carta di credito	2.577	386.550
Totale	**11.882**	**1.782.300**

19. Prospetto delle attività dell'Ufficio relazioni con il pubblico 2004/2005 (tabella e grafico)

Ufficio relazioni con il pubblico			
	2004	2005	**Totale**
e-mail esaminate	13.000	14.500	**27.500**
contatti telefonici	10.000	18.100	**28.100**
persone in visita all'Urp	2.400	1.550	**3.950**
Totale	**25.400**	**34.150**	



20. Sito Internet del Garante

Sito Internet del Garante *www.garanteprivacy.it* [3]	
tipologia	totale
utenti (alcuni sono *proxy server*)	32.000.000
documenti consultati in media da ogni utente	16
documenti distribuiti	512.000.000
e-mail pervenute	75.000

(1) Situazione alla data del 31 dicembre 2005

(2) Dati riferiti alla sola attività dell'Urp

(3) Valori rappresentati con arrotondamenti per difetto

21. Organico del Garante

Posti previsti in organico	
area	unità di personale
dirigenti	26
funzionari	45
operativi	26
esecutivi	3
Totale	**100**
personale a contratto	20

22. Personale in servizio presso il Garante

Personale in servizio[1]				
area	in ruolo (a)	collocato fuori ruolo (b)	comandato presso altre amministrazioni o in aspettativa (c)	impiegato dall'Ufficio (a+b-c)
dirigenti	16	4	2	18
funzionari	37	3	2	38
operativi	21	1	1	21
esecutivi	---	---	---	---
Totali	**74**	**8**	**5**	77
a contratto				14

23. Risorse finanziarie

anno	trasferimenti da parte dello Stato		somme riscosse compreso il contributo dello Stato		somme pagate	
	lire	euro	lire	euro	lire	euro
1997	8.029.000.000	4.146.632,44	8.029.000.000	4.146.632,44	1.372.350.430	708.759,85
1998	12.045.000.000	6.220.723,35	12.045.000.000	6.220.723,35	5.491.467.960	2.836.106,51
1999	22.045.000.000	11.385.292,34	27.045.000.000	13.967.576,84	8.725.548.850	4.506.369,90
2000	22.045.000.000	11.385.292,34	22.293.735.850	11.513.753,69	14.235.888.830	7.352.223,00
2001	22.000.000.000	11.362.051,78	24.285.004.432	12.542.158,08	20.019.011.761	10.338.956,74
2002		10.849.996,00		12.186.883,99		11.510.285,48
2003		10.252.000,00		11.244.455,31		13.102.960,92
2004		9.618.000,00		12.694.621,09		12.618.901,26
2005		9.540.653,00		11.011.616,26		15.603.768,31

(1) Situazione alla data del 31 dicembre 2005

PAGINA BIANCA

DOCUMENTAZIONE

PAGINA BIANCA

Provvedimenti del Garante

26 Autorizzazione n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. *d*), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del Codice;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di diciotto mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1 [doc. *web* n. 1203930 vers. EN n. 1208632]

minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato nell'ambito dei rapporti di lavoro;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il prof. Francesco Pizzetti;

Autorizza

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, finalizzato alla gestione dei rapporti di lavoro, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata:

a) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e agli organismi che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lettere b) e c);

b) ad organismi paritetici o che gestiscono osservatori in materia di lavoro, previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi anche aziendali;

l'autorizzazione riguarda anche l'attività svolta:

c) dal medico competente in materia di igiene e di sicurezza del lavoro, in qualità di libero professionista o di dipendente dei soggetti di cui alla lettera a) o di strutture convenzionate;

d) da associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro, al solo fine di perseguire le finalità di cui al punto 3), lettera h).

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) a lavoratori subordinati, anche se parti di un contratto di apprendistato, o di formazione e lavoro, o di inserimento, o di lavoro ripartito, o di lavoro intermittente o a chiamata, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione, o in rapporto di tirocinio, ovvero ad associati anche in compartecipazione e, se necessario in base ai punti 3) e 4), ai relativi familiari e conviventi;

b) a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatari;
c) a soggetti che effettuano prestazioni coordinate e continuative, anche nella modalità di lavoro a progetto, o ad altri lavoratori autonomi in rapporto di collaborazione, anche sotto forma di prestazioni di lavoro accessorio, con i soggetti di cui al punto 1);
d)a candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti;
e) a persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto 1);
f) a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui alle precedenti lettere.

3) Finalità del trattamento

Il trattamento dei dati sensibili deve essere indispensabile:
a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi anche aziendali, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica;
b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;
d) per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
e) per esercitare il diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;
f) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
g) per garantire le pari opportunità;
h) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

4) Categorie di dati

Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e in particolare:
a) nell'ambito dei dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, i dati concernenti la fruizione di permessi e festività religiose o di servizi di mensa, nonché la manifestazione, nei casi previsti dalla legge, dell'obiezione di coscienza;
b) nell'ambito dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale, i dati concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali (sempre che il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pubbliche ini-

ziative, nonché i dati inerenti alle trattenute per il versamento delle quote di servizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;

c) nell'ambito dei dati idonei a rivelare lo stato di salute, i dati raccolti e ulteriormente trattati in riferimento a invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psicofisica a svolgere determinate mansioni, all'appartenenza a determinate categorie protette, nonché i dati contenuti nella certificazione sanitaria attestante lo stato di malattia, anche professionale dell'interessato, o comunque relativi anche all'indicazione della malattia come specifica causa di assenza del lavoratore.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Restano inoltre fermi gli obblighi di informare l'interessato e, ove necessario, di acquisirne il consenso scritto, in conformità a quanto previsto dagli articoli 13, 23 e 26 del Codice.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lettera *e*), del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto 3), ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e, ove necessario, diffusi, nei limiti strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), a soggetti pubblici o privati, ivi compresi organismi sanitari, casse e fondi di previdenza ed assistenza sanitaria integrativa anche aziendale, istituti di patronato e di assistenza sociale, centri di assistenza fiscale, agenzie per il lavoro, associazioni ed organizzazioni sindacali di datori di lavoro e di prestatori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

Ai sensi dell'art. 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla

data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità dalle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute:

a) nell'art. 8 della legge 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

b) nell'art. 6 della legge 5 giugno 1990, n. 135, che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività;

c) nelle norme in materia di pari opportunità o volte a prevenire discriminazioni;

d) fermo restando quanto disposto dall'art. 8 della legge 20 maggio 1970, n. 300, nell'art. 10 del decreto legislativo 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'*handicap*, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute e ad eventuali controversie con i precedenti datori di lavoro, nonché di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

27 Autorizzazione n. 2/2005 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto l'art. 76 del Codice, secondo cui gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85 del medesimo Codice, possono trattare i dati personali idonei a rivelare lo stato di salute anche senza il consenso dell'interessato, previa autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica di un terzo o della collettività;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sin ora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di diciotto mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice, principi valutati anche sulla base delle raccomandazioni adottate in materia di dati sanitari dal Consiglio d'Europa ed in particolare dalla Raccomandazione N. R (97)5, in base alla quale i dati sanitari devono essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza e di efficacia pari a quelle previste in tale ambito;

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1
[doc. *web* n. 1203946 vers. EN n. 1208647]

Considerato che un elevato numero di trattamenti idonei a rivelare lo stato di salute e la vita sessuale è effettuato per finalità di prevenzione o di cura, per la gestione di servizi socio-sanitari, per ricerche scientifiche o per la fornitura all'interessato di prestazioni, beni o servizi;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il prof. Francesco Pizzetti;

Autorizza

a) gli esercenti le professioni sanitarie a trattare i dati idonei a rivelare lo stato di salute, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica o la salute di un terzo o della collettività, e il consenso non sia prestato o non possa essere prestato per effettiva irreperibilità;
b) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare con il consenso i dati idonei a rivelare lo stato di salute e la vita sessuale;
c) gli organismi sanitari pubblici, istituiti anche presso università, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute, qualora ricorrano contemporaneamente le seguenti condizioni:
   1. il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;
   2. manchi il consenso (articolo 76, comma 1, lett. *b*), del Codice), in quanto non sia prestato o non possa essere prestato per effettiva irreperibilità;
   3. non si tratti di attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione ai sensi dell'art. 85, commi 1 e 2, del Codice;
d) anche soggetti diversi da quelli di cui alle lettere a), b) e c) a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora il trattamento sia necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato.

Per l'informativa e, ove previsto, il consenso si osservano anche le disposizioni di cui agli articoli 13, 23, 26 e da 75 a 82 del Codice.

1) Ambito di applicazione e finalità del trattamento

1.1. L'autorizzazione è rilasciata:
   a) ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;
   b) al personale sanitario infermieristico, tecnico e della riabilitazione che esercita l'attività in regime di libera professione;

c) alle istituzioni e agli organismi sanitari privati, anche quando non operino in rapporto con il servizio sanitario nazionale.

In tali casi, l'autorizzazione è rilasciata anche per consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, dalla normativa comunitaria o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni, di diagnosi e cura, ivi compresi i trapianti di organi e tessuti, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di profilassi delle malattie infettive e diffusive, di tutela della salute mentale, di assistenza farmaceutica, di medicina scolastica e di assistenza sanitaria alle attività sportive o di accertamento, in conformità alla legge, degli illeciti previsti dall'ordinamento sportivo. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario, ovvero di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini appena indicati.

Qualora il perseguimento di tali fini richieda l'espletamento di compiti di organizzazione o di gestione amministrativa, i destinatari della presente autorizzazione devono esigere che i responsabili e gli incaricati del trattamento preposti a tali compiti osservino le stesse regole di segretezza alle quali sono sottoposti i medesimi destinatari della presente autorizzazione, nel rispetto di quanto previsto anche dall'art. 83, comma 1, del Codice.

1.2. L'autorizzazione è rilasciata, altresì, ai seguenti soggetti:

a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle relazioni tra i fattori di rischio e la salute umana, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. In tali casi occorre acquisire il consenso (in conformità a quanto previsto dagli articoli 106, 107 e 110 del Codice), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima. Resta fermo quanto previsto dall'art. 98 del Codice;

b) alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;

c) alle comunità di recupero e di accoglienza, alle case di cura e di riposo, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie;

d) agli enti, alle associazioni e alle organizzazioni religiose riconosciute, relativamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi nei limiti di quanto stabilito dall'art. 26, comma 4, lettera *a)*, del Codice, fermo restando quanto previsto per le confessioni religiose dagli articoli 26, comma 3, lett. *a*), e 181, comma 6, del Codice e dell'autorizzazione n. 3/2005;

e) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati, ove necessario attinenti anche alla vita sessuale, e alle operazioni indispensabili per adempiere agli obblighi, anche precontrattuali, derivanti da un rapporto di fornitura all'interessato di beni, di prestazioni o di servizi.

Se il rapporto intercorre con istituti di credito, imprese assicurative o riguarda valori mobiliari, devono considerarsi indispensabili i soli dati ed operazioni necessari per fornire specifici prodotti o servizi richiesti dall'interessato. Il rapporto può riguardare anche la fornitura di strumenti di ausilio per la vista, per l'udito o per la deambulazione;

f) alle persone fisiche e giuridiche, agli enti, alle associazioni e agli altri organismi che gestiscono impianti o strutture sportive, limitatamente ai dati e alle

operazioni indispensabili per accertare l'idoneità fisica alla partecipazione ad attività sportive o agonistiche;

g) alle persone fisiche e giuridiche e ad altri organismi, limitatamente ai dati dei beneficiari e dei donatori e alle operazioni indispensabili per effettuare trapianti di organi e tessuti, nonché donazioni di sangue.

1.3. La presente autorizzazione è rilasciata, altresì, quando il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale sia necessario per:

a) lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che il diritto sia di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile, e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario per il loro perseguimento;

b) adempiere o esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi per la gestione del rapporto di lavoro, nonché della normativa in materia di previdenza e assistenza o in materia di igiene e sicurezza del lavoro o della popolazione, nei limiti previsti dalla autorizzazione generale del Garante n. 1/2005 e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111 del Codice.

1.4. Fino alla data in cui sarà efficace l'apposita autorizzazione per il trattamento dei dati genetici prevista dall'art. 90 del Codice, restano autorizzati i trattamenti di dati genetici nei soli limiti e alle condizioni individuate al punto 2, lettera b), dell'autorizzazione n. 2/2002.

2) Categorie di dati oggetto di trattamento

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e può comprendere le informazioni relative a stati di salute pregressi.

Devono essere considerate sottoposte all'ambito di applicazione della presente autorizzazione anche le informazioni relative ai nascituri, che devono essere trattate alla stregua dei dati personali in conformità a quanto previsto dalla citata raccomandazione N. R (97) 5 del Consiglio d'Europa.

3) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Per le informazioni relative ai nascituri, il consenso è prestato dalla gestante. Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario (art. 82, comma 4, del Codice).

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice, i dati possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti sopra indicati, ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

5) Comunicazione e diffusione dei dati

I dati idonei a rivelare lo stato di salute, esclusi i dati genetici, possono essere comunicati, nei limiti strettamente pertinenti agli obblighi, ai compiti e alle finalità di cui al punto 1), a soggetti pubblici e privati, ivi compresi i fondi e le casse di assistenza sanitaria integrativa, le aziende che svolgono attività strettamente correlate all'esercizio di professioni sanitarie o alla fornitura all'interessato di beni, di prestazioni o di servizi, gli istituti di credito e le imprese assicurative, le associazioni od organizzazioni di volontariato e i familiari dell'interessato.

Ai sensi degli artt. 22, comma 8, e 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

I dati idonei a rivelare la vita sessuale non possono essere diffusi, salvo il caso in cui la diffusione riguardi dati resi manifestamente pubblici dall'interessato e per i quali l'interessato stesso non abbia manifestato successivamente la sua opposizione per motivi legittimi.

6) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione, relative, ad esempio, al caso in cui la raccolta del consenso comporti un impiego di mezzi manifestamente sproporzionato in ragione, in particolare, del numero di persone interessate.

7) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dall'art. 5, comma 2, della legge 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, secondo cui la rilevazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona;

b) dall'art. 11 della legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento

di interruzione di gravidanza devono inviare al medico provinciale competente per territorio una dichiarazione che non faccia menzione dell'identità della donna;

c) dall'art. 734-*bis* del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal Codice di deontologia medica adottato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati e di includerli, in particolare, nelle pubblicazioni a contenuto scientifico o finalizzate all'educazione, alla prevenzione o all'informazione di carattere sanitario.

8) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

28 Autorizzazione n. 3/2005 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto altresì il comma 4, lett. *a*), del citato art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, "quando il trattamento è effettuato da associazioni, enti ed organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinanti e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13";

Visto il comma 3, lettere *a*) e *b*), del predetto art. 26, il quale stabilisce che la disciplina di cui al relativo comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni; b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria;

Rilevato che le confessioni di cui alla lettera a) devono determinare, ai sensi del medesimo art. 26, comma 3, lett. *a*), idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

Visto l'art. 181, comma 6, del Codice secondo cui le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui al predetto art. 26, comma 3, lett. *a*), possono proseguire l'attività di trattamento nel rispetto delle medesime;

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1
[doc. *web* n. 1203934 vers. EN n. 1208661]

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di diciotto mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da enti ed organizzazioni di tipo associativo e da fondazioni, per la realizzazione di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice, recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il dott. Mauro Paissan;

Autorizza

il trattamento dei dati sensibili di cui art. 4, comma 1, lett. *d*), del Codice da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata:

a) alle associazioni anche non riconosciute, ai partiti e ai movimenti politici, alle asso-

ciazioni e alle organizzazioni sindacali, ai patronati e alle associazioni di categoria, alle casse di previdenza, alle organizzazioni assistenziali o di volontariato, nonché alle federazioni e confederazioni nelle quali tali soggetti sono riuniti in conformità, ove esistenti, allo statuto, all'atto costitutivo o ad un contratto collettivo;

b) alle fondazioni, ai comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, ivi comprese le organizzazioni non lucrative di utilità sociale (Onlus);

c) alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818.

L'autorizzazione è rilasciata altresì agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per l'applicazione dell'articolo 310 del decreto legislativo 16 aprile 1994, n. 297 e degli artt. 3 e 10 del decreto legislativo 19 febbraio 2004, n. 59.

Resta fermo l'obbligo per le confessioni religiose di determinare, ai sensi dell'art. 26, comma 3, lett. *a*), del Codice, idonee garanzie relativamente ai trattamenti effettuati nel rispetto dei principi indicati con la presente autorizzazione.

Ai sensi dell'art. 181, comma 6, del Codice, le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'art. 26, comma 3, lett. *a*), del Codice possono proseguire l'attività di trattamento effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, nel rispetto delle medesime.

2) Finalità del trattamento

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi.

La presente autorizzazione è rilasciata per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.

Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro o di liberi professionisti per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi, persone giuridiche o liberi professionisti.

I soggetti di cui alle lettere a), b) e c) possono comunicare alle persone giuridiche e agli organismi con scopo di lucro titolari di un autonomo trattamento, i soli dati sensibili strettamente indispensabili per le attività di effettivo ausilio alle predette finalità, con particolare riferimento alle generalità degli interessati e ad indirizzari, sulla base di un atto scritto che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo, le particolari misure di sicurezza, nonché, ove previsto, le idonee garanzie determinate. La dichiarazione scritta di consenso degli interessati deve porre tale circostanza in particolare

evidenza e deve recare la precisa menzione dei titolari del trattamento e delle finalità da essi perseguite. Le persone giuridiche e gli organismi con scopo di lucro, oltre a quanto previsto nei punti 4) e 6) in tema di pertinenza, non eccedenza e indispensabilità dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

3) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili attinenti:

a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;

b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l'associazione, la fondazione o il diverso organismo;

c) ai soggetti che ricoprono cariche sociali o onorifiche;

d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall'associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all'atto costitutivo, ove esistenti, o comunque a coloro nell'interesse dei quali i soggetti menzionati al punto 1) possono operare in base ad una previsione normativa;

e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;

f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

4) Categorie di dati oggetto di trattamento

L'autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l'autorizzazione generale n. 2/2005.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 4, comma 1, lett. *d*), del Codice, 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.

Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, che non possano essere perseguiti o adempiuti, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto ai predetti obblighi e finalità, in particolare per quanto riguarda i dati che rivelano le opinioni e le intime convinzioni, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, e dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità, agli scopi e agli obblighi di cui al punto 2).

I dati sono raccolti, di regola, presso l'interessato.

Fermo restando quanto previsto ai punti 2) e 7) della presente autorizzazione, se è indi-

spensabile, in conformità al medesimo punto 7), comunicare o diffondere dati all'esterno dell'associazione, della fondazione, del comitato o del diverso organismo, il consenso scritto è acquisito previa idonea informativa resa agli interessati ai sensi dell'art. 13 del Codice, la quale deve precisare le specifiche modalità di utilizzo dei dati tenuto conto delle idonee garanzie adottate relativamente ai trattamenti effettuati.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità e gli scopi di cui al punto 2), ovvero per adempiere agli obblighi ivi menzionati.

Le verifiche di cui al punto 4) devono riguardare anche la pertinenza, non eccedenza e indispensabilità dei dati rispetto all'attività svolta dall'interessato o al rapporto che intercorre tra l'interessato e i soggetti di cui al punto 1), tenendo presente il genere di prestazione, di beneficio o di servizio offerto all'interessato e la posizione di quest'ultimo rispetto ai soggetti stessi.

7) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati a soggetti pubblici o privati, e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi di cui al punto 2) e tenendo presenti le altre prescrizioni sopraindicate.

I dati sensibili possono essere comunicati alle autorità competenti se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

8) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

9) Norme finali

Restano fermi gli obblighi previsti dalla normativa comunitaria, da norme di legge o di regolamento che stabiliscono divieti o limiti in materia di trattamento di dati personali.

Restano inoltre ferme le norme volte a prevenire discriminazioni, e in particolare le disposizioni contenute nel decreto-legge 26 aprile 1993, n. 122, convertito, con modificazioni, dalla legge 25 giugno 1993, n. 205, in materia di discriminazione per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio, nel decreto legislativo 9 luglio 2003, n. 215 di attuazione della direttiva 2000/43/Ce per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica e nel decreto legislativo 9 luglio 2003, n. 216, di attuazione della direttiva 2000/78/Ce per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

29 Autorizzazione n. 4/2005 al trattamento dei dati sensibili da parte dei liberi professionisti 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. *c*), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario ai fini dello svolgimento delle investigazioni difensive ai sensi della legge 7 dicembre 2000, n. 397 o, comunque per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, e che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale il diritto sia di rango pari a quello dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di diciotto mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da liberi professionisti iscritti in albi o elenchi professionali per l'espletamento delle rispettive attività professionali;

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1
[doc. *web* n. 1203954 vers. EN n. 1208675]

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il dott. Giuseppe Chiaravalloti;

Autorizza

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta, ai liberi professionisti tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96, o alle norme di attuazione dell'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza.

Sono equiparati ai liberi professionisti i soggetti iscritti nei corrispondenti albi o elenchi speciali istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato.

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, ai praticanti e ai tirocinanti presso il libero professionista, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

Il presente provvedimento non si applica al trattamento dei dati sensibili effettuato:

a) dagli esercenti la professione sanitaria e dagli psicologi, dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/2005;
b) per la gestione delle prestazioni di lavoro o di collaborazione di cui si avvale il libero professionista o taluno dei soggetti sopra indicati, alla quale si riferisce l'autorizzazione generale n. 1/2005;
c) da soggetti privati che svolgono attività investigative, dai giornalisti, dai pubblicisti e dai praticanti giornalisti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69.

2) Interessati ai quali i dati si riferiscono e categorie di dati

Il trattamento può riguardare i dati sensibili relativi ai clienti.

I dati sensibili relativi ai terzi possono essere trattati ove ciò sia strettamente indispensabile per l'esecuzione di specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

In ogni caso, i dati devono essere strettamente pertinenti e non eccedenti rispetto ad incarichi conferiti che non possano essere svolti mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato anche nel rispetto della citata autorizzazione generale n. 2/2005.

3) Finalità del trattamento

Il trattamento dei dati sensibili può essere effettuato ai soli fini dell'espletamento di un incarico che rientri tra quelli che il libero professionista può eseguire in base al proprio ordinamento professionale, e in particolare:

a) per curare gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro;

b) ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, anche a mezzo di sostituti e di consulenti tecnici, o, comunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

c) per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia, salvo quanto previsto dall'art. 60 del Codice in relazione ai dati sullo stato di salute e sulla vita sessuale.

4) Modalità di trattamento

Il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto all'incarico conferito dal cliente.

Restano fermi gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice.

Restano inoltre fermi gli obblighi di informare l'interessato ai sensi dell'art. 13, commi 1, 4 e 5, del Codice, anche quando i dati sono raccolti presso terzi, e di acquisire, ove necessario, il consenso scritto.

Se i dati sono raccolti per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive (punto 3), lettera b), l'informativa relativa ai dati raccolti presso terzi, e il consenso scritto, sono necessari solo se i dati sono trattati per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità, oppure per altre finalità con esse non incompatibili.

Le informative devono permettere all'interessato di comprendere agevolmente se il titolare del trattamento è un singolo professionista o un'associazione di professionisti, ovvero se ricorre un'ipotesi di contitolarità tra più liberi professionisti o di esercizio della professione in forma societaria ai sensi del decreto legislativo 2 febbraio 2001, n. 96.

Resta ferma la facoltà del libero professionista di designare quali responsabili o incaricati del trattamento i sostituti, gli ausiliari, i tirocinanti e i praticanti presso il libero professionista, i quali, in tal caso, possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Analoga cautela deve essere adottata in riferimento agli incaricati del trattamento preposti all'espletamento di compiti amministrativi.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice, i dati sensibili possono essere conservati, per il periodo di tempo previsto dalla normativa comunitaria, da leggi, o da regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine, anche mediante controlli periodici, deve essere verificata la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto agli incarichi in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

I dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti, non eccedenti e indispensabili rispetto a successivi incarichi.

6) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati e ove necessario diffusi, a soggetti pubblici o privati, nei limiti strettamente pertinenti all'espletamento dell'incarico conferito e nel rispetto, in ogni caso, del segreto professionale.

I dati idonei a rivelare lo stato di salute possono essere comunicati solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle leggi 20 maggio 1970, n. 300, e 5 giugno 1990, n. 135, come modificata dall'art. 178 del Codice, nonché dalle norme volte a prevenire discriminazioni.

Restano fermi, altresì, gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici o di buona condotta relativi alle singole figure professionali.

9) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

30 Autorizzazione n. 5/2005 al trattamento dei dati sensibili da parte di diverse categorie di titolari 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di diciotto mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da parte di soggetti operanti in diversi settori di attività economiche di seguito individuate;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice, recanti norme e regole sulle misure di sicurezza;

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1 [doc. *web* n. 1203938 vers. EN n. 1208769]

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il dott. Giuseppe Fortunato;

Autorizza

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, fatta eccezione dei dati idonei a rivelare la vita sessuale, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

CAPO I - ATTIVITÀ BANCARIE, CREDITIZIE, ASSICURATIVE, DI GESTIONE DI FONDI, DEL SETTORE TURISTICO, DEL TRASPORTO ED ALTRE ATTIVITÀ AUTORIZZATE

1) Soggetti ai quali è rilasciata l'autorizzazione:

a) imprese autorizzate all'esercizio dell'attività bancaria e creditizia o assicurativa ed organismi che le riuniscono, anche se in stato di liquidazione coatta amministrativa;
b) società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;
c) società ed altri organismi di intermediazione finanziaria, in particolare per la gestione o l'intermediazione di fondi comuni di investimento o di valori mobiliari;
d) società ed altri organismi che emettono carte di credito o altri mezzi di pagamento, o che ne gestiscono le relative operazioni;
e) imprese che svolgono autonome attività strettamente connesse e strumentali a quelle indicate nelle precedenti lettere, e relative alla rilevazione dei rischi, al recupero dei crediti, a lavorazioni massive di documenti, alla trasmissione dati, all'imbustamento o allo smistamento della corrispondenza, nonché alla gestione di esattorie o tesorerie;
f) imprese che operano nel settore turistico o alberghiero o del trasporto, agenzie di viaggio e operatori turistici;
g) operatori economici autorizzati a svolgere la propria attività in base ad autorizzazione comunque resa ai sensi delle norme contenute nel regio decreto 18 giugno 1931, n. 773 (T.u.l.p.s.) o nel decreto legislativo 31 marzo 1998, n. 112.

2) Finalità del trattamento

La presente autorizzazione è rilasciata, anche senza richiesta, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti di cui al punto 1) assumono, nel proprio settore di attività, al fine di fornire specifici beni, prestazioni o servizi richiesti dall'interessato.

L'autorizzazione è rilasciata anche per adempiere o per esigere l'adempimento ad obblighi previsti, anche in materia fiscale e contabile, dalla normativa comunitaria, dalla legge, dai regolamenti, o dai contratti collettivi, o prescritti da autorità od organi di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.

Il trattamento avente tali finalità può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

3) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che, ove necessario, abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

4) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati, nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società controllate e collegate ai sensi dell'art. 2359 del codice civile, nonché, ove necessario, ai familiari dell'interessato.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lettera *c*), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

I dati sensibili non possono essere diffusi.

CAPO II - SONDAGGI E RICERCHE

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

Imprese, società, istituti ed altri organismi o soggetti privati, ai soli fini del compimento di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il sondaggio o la ricerca devono essere effettuati per scopi puntualmente determinati e legittimi, noti all'interessato.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati attinenti ai soggetti che abbiano manifestato il proprio consenso informato e che abbiano risposto a questionari o ad interviste effettuate nell'ambito di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il consenso deve essere manifestato in ogni caso per iscritto.

I dati personali di natura sensibile possono essere trattati solo se il trattamento di dati anonimi non permette al sondaggio o alla ricerca di raggiungere i suoi scopi.

3) Conservazione dei dati

Il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente, mediante un riferimento ad una qualsiasi altra informazione.

I dati personali, individuali o aggregati, devono essere distrutti o resi anonimi subito dopo la raccolta, e comunque non oltre la fase contestuale alla registrazione dei campioni raccolti. La registrazione deve essere effettuata senza ritardo anche nel caso in cui i campioni siano stati raccolti in numero elevato.

Entro tale ambito temporale, resta ferma la possibilità per il titolare della raccolta, nonché per i suoi responsabili o incaricati, di utilizzare i dati personali al fine di verificare presso gli interessati la veridicità o l'esattezza dei campioni.

4) Comunicazione dei dati

I dati sensibili non possono essere né comunicati, né diffusi.

I campioni del sondaggio o della ricerca possono essere comunicati o diffusi in forma

individuale o aggregata, sempre che non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili.

CAPO III - ATTIVITÀ DI ELABORAZIONE DI DATI

1) Soggetti ai quali è rilasciata l'autorizzazione

Imprese, società, istituti ed altri organismi o soggetti privati, titolari autonomi di un'attività svolta nell'interesse di altri soggetti, e che presuppone l'elaborazione di dati ed altre operazioni di trattamento eseguite in materia di lavoro, ovvero a fini contabili, retributivi, previdenziali, assistenziali e fiscali.

2) Prescrizioni applicabili

Il trattamento è regolato dalle autorizzazioni:

a) n. 1/2005, rilasciata il 21 dicembre 2005, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione;

b) n. 4/2005, rilasciata il 21 dicembre 2005, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati, qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

CAPO IV - ATTIVITÀ DI SELEZIONE DEL PERSONALE

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento

La presente autorizzazione è rilasciata, anche senza richiesta, alle agenzie per il lavoro e agli altri soggetti che, in conformità alla legge, svolgono, nell'interesse di terzi, attività di intermediazione, ricerca e selezione del personale o supporto alla ricollocazione professionale.

2) Interessati ai quali i dati si riferiscono e categorie di dati trattati

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la loro raccolta è giustificata da scopi determinati e legittimi ed è strettamente indispensabile per instaurare tale rapporto.

Il trattamento dei dati idonei a rivelare lo stato di salute dei familiari o dei conviventi dei candidati è consentito con il consenso scritto degli interessati e qualora sia finalizzato al riconoscimento di uno specifico beneficio in favore dei candidati, in particolare ai fini di un'assunzione obbligatoria o del riconoscimento di un titolo derivante da invalidità o infermità, da eventi bellici o da ragioni di servizio.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Il trattamento deve riguardare le sole informazioni strettamente pertinenti a tale finalità, sia in caso di risposta a questionari inviati anche per via telematica, sia nel caso in cui i candidati forniscano dati di propria iniziativa, in particolare attraverso l'invio di *curricula*.

Non è consentito il trattamento dei dati:

a) idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni a carattere religioso, filosofico, politico o sindacale, l'origine razziale ed etnica, e la vita sessuale;

b) inerenti a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

c) in violazione delle norme in materia di pari opportunità o volte a prevenire discriminazioni.

3) Comunicazione e diffusione dei dati

I dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui ai punti 1) e 2), a soggetti pubblici o privati che siano specificamente menzionati nella dichiarazione di consenso dell'interessato.

I dati sensibili non possono essere diffusi.

4) Norme finali

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti.

CAPO V - MEDIAZIONE A FINI MATRIMONIALI

1) Soggetti ai quali è rilasciata l'autorizzazione

La presente autorizzazione è rilasciata alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati che esercitano, anche attraverso agenzie autorizzate, un'attività di mediazione a fini matrimoniali o di instaurazione di un rapporto di convivenza.

2) Finalità del trattamento

L'autorizzazione è rilasciata ai soli fini dell'esecuzione dei singoli incarichi conferiti in conformità alle leggi e ai regolamenti.

3) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare i soli dati sensibili attinenti alle persone direttamente interessate al matrimonio o alla convivenza.

Non è consentito il trattamento di dati relativo a persone minori di età in base all'ordinamento del Paese di appartenenza o, comunque, in base alla legge italiana.

4) Categorie di dati oggetto di trattamento

Il trattamento può riguardare i soli dati e le sole operazioni che risultino indispensabili in relazione allo specifico profilo o alla personalità descritto o richiesto dalle persone interessate al matrimonio o alla convivenza.

I dati devono essere forniti personalmente dai medesimi interessati.

L'informativa preliminare al consenso scritto deve porre in particolare evidenza le categorie di dati trattati e le modalità della loro comunicazione a terzi.

5) Comunicazione dei dati

I dati possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lettera *c*), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

L'eventuale diffusione anche per via telematica di taluni dati sensibili deve essere oggetto di apposita autorizzazione di questa Autorità.

6) Norme finali

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti, in particolare nell'ambito della legge penale e della disciplina di pubblica sicurezza, nonché in materia di tutela dei minori.

CAPO VI - PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati idonei a rivelare lo stato di salute

Il trattamento dei dati idonei a rivelare lo stato di salute deve essere effettuato anche nel rispetto dell'autorizzazione n. 2/2005, rilasciata il 21 dicembre 2005.

Il trattamento dei dati genetici non è consentito nei casi previsti dalla presente autorizzazione.

2) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, dagli articoli 31 e seguenti del Codice e dall'Allegato B) al Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità indicate nei capi che precedono.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Resta inoltre fermo l'obbligo di informare l'interessato, ai sensi dell'art. 13, commi 1, 4 e 5 del Codice, anche quando i dati sono raccolti presso terzi.

3) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità, ovvero per adempiere agli obblighi o agli incarichi menzionati nei precedenti capi. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

Restano fermi i diversi termini di conservazione previsti dalle leggi o dai regolamenti.

Resta altresì fermo quanto previsto nel capo II in materia di sondaggi e di ricerche.

4) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

5) Norme finali

Restano fermi gli obblighi previsti da norme di legge o di regolamento e dalla normativa

comunitaria, che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dalla legge 20 maggio 1970, n. 300;
b) dalla legge 5 giugno 1990, n. 135;
c) dal decreto legislativo 10 settembre 2003, n. 276.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici, previsti anche dai codici deontologici e di buona condotta adottati in attuazione dell'art. 12 del Codice.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati.

6) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

31 Autorizzazione n. 6/2005 al trattamento dei dati sensibili da parte degli investigatori privati 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. *c*), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo è necessario per svolgere una investigazione difensiva ai sensi della legge 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, e che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato il diritto sia di rango pari a quello dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale inviolabile;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di diciotto mesi;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che il Garante ha rilasciato un'autorizzazione di ordine generale relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale (n. 2/2005, rilasciata il 21 dicembre 2005), anche in riferimento alle predette finalità di ordine giudiziario;

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1 [doc. *web* n. 1203950 vers. EN n. 1208785]

Considerato che numerosi trattamenti aventi tali finalità sono effettuati con l'ausilio di investigatori privati, e che è pertanto opportuno integrare anche le prescrizioni dell'autorizzazione n. 2/2005 mediante un ulteriore provvedimento di ordine generale che tenga conto dello specifico contesto dell'investigazione privata, anche al fine di armonizzare le prescrizioni da impartire alla categoria;

Considerato che ulteriori misure ed accorgimenti saranno prescritti dal Garante all'atto della sottoscrizione del citato codice di deontologia e di buona condotta in via di emanazione (art. 12 del Codice);

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visti gli articoli 42 e seguenti del Codice in materia di trasferimento di dati personali all'estero;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il dott. Giuseppe Fortunato;

Autorizza

gli investigatori privati a trattare i dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

1) Ambito di applicazione

La presente autorizzazione è rilasciata, anche senza richiesta, alle persone fisiche e giuridiche, agli istituti, agli enti, alle associazioni e agli organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

2) Finalità del trattamento

Il trattamento può essere effettuato unicamente per l'espletamento dell'incarico ricevuto dai soggetti di cui al punto 1) e in particolare:

a) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto, che, quando i dati siano idonei a rivelare lo stato di salute e la vita sessuale dell'interessato, deve essere di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;

b) su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (art. 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397)

Restano ferme le altre autorizzazioni generali rilasciate ai fini dello svolgimento delle investigazioni in relazione ad un procedimento penale o per l'esercizio di un diritto in sede giudiziaria, in particolare:

a) nell'ambito dei rapporti di lavoro (autorizzazione n. 1/2005, rilasciata il 21 dicembre 2005);
b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2005, rilasciata il 21 dicembre 2005);
c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione n. 3/2005, rilasciata il 21 dicembre 2005);
d) da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione n. 4/2005, rilasciata il 21 dicembre 2005);
e) relativamente ai dati di carattere giudiziario (autorizzazione n. 7/2005, rilasciata il 21 dicembre 2005).

3) Categorie di dati e interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità di cui al punto 1), che non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

I dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti.

4) Modalità di trattamento

Gli investigatori privati non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di dati. Tali attività possono essere eseguite esclusivamente sulla base di un apposito incarico conferito per iscritto, anche da un difensore, per le esclusive finalità di cui al punto 2).

L'atto di incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa.

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità di cui al punto 2).

L'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'art. 13 del Codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati.

Nel caso in cui i dati sono raccolti presso terzi, è necessario informare l'interessato e acquisire il suo consenso scritto (art. 13, commi 1, 4 e 5 e art. 26, comma 4, del Codice), solo se i dati sono trattati per un periodo superiore a quello strettamente necessario per esercitare il diritto in sede giudiziaria o per svolgere le investigazioni difensive, oppure se i dati sono utilizzati per ulteriori finalità non incompatibili con quelle precedentemente perseguite.

Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

L'investigatore privato deve eseguire personalmente l'incarico ricevuto e non può avvalersi di altri investigatori non indicati nominativamente all'atto del conferimento dell'incarico.

Nel caso in cui si avvalga di collaboratori interni designati quali responsabili o incaricati del trattamento in conformità a quanto previsto dagli articoli 29 e 30 del Codice, l'investi-

gatore privato deve vigilare con cadenza almeno settimanale sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione ad essi richiesta.

Per quanto non previsto nella presente autorizzazione, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato nel rispetto delle ulteriori prescrizioni contenute nell'autorizzazione generale n. 2/2005 e, allorché rilasciata, in quella prevista dall'art. 90 del Codice, in particolare per ciò che riguarda le informazioni relative ai nascituri e ai dati genetici.

Il trattamento dei dati deve inoltre rispettare le prescrizioni del codice di deontologia e di buona condotta di cui all'articolo 135 del Codice in via di definizione.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice i dati sensibili possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto.

A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico.

La mera pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

6) Comunicazione e diffusione dei dati

I dati possono essere comunicati unicamente al soggetto che ha conferito l'incarico.

I dati non possono essere comunicati ad un altro investigatore privato, salvo che questi sia stato indicato nominativamente nell'atto di incarico e la comunicazione sia necessaria per lo svolgimento dei compiti affidati.

I dati idonei a rivelare lo stato di salute possono essere comunicati alle autorità competenti solo se è necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

7) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

8) Norme finali

Restano fermi gli obblighi previsti dalla normativa comunitaria, ovvero da norme di

legge o di regolamento, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare:

a) dagli articoli 4 (impianti e apparecchiature per finalità di controllo a distanza dei lavoratori) e 8 (indagini sulle opinioni del lavoratore o su altri fatti non rilevanti ai fini della valutazione dell'attitudine professionale) della legge 20 maggio 1970, n. 300 e dall'art. 10 (indagini sulle opinioni del lavoratore e trattamenti discriminatori) del decreto legislativo 10 settembre 2003, n. 276;

b) dalla legge 5 giugno 1990, n. 135, in materia di sieropositività e di infezione da HIV;

c) dalle norme volte a prevenire discriminazioni;

d) dall'art. 734-*bis* del Codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano fermi, in particolare, gli obblighi previsti in tema di liceità e di correttezza nell'uso di strumenti o apparecchiature che permettono la raccolta di informazioni anche sonore o visive, ovvero in tema di accesso a banche dati o di cognizione del contenuto della corrispondenza e di comunicazioni o conversazioni telefoniche, telematiche o tra soggetti presenti.

Resta ferma la facoltà per le persone fisiche di trattare direttamente dati per l'esclusivo fine della tutela di un proprio diritto in sede giudiziaria, anche nell'ambito delle investigazioni relative ad un procedimento penale. In tali casi, il Codice non si applica anche se i dati sono comunicati occasionalmente ad una autorità giudiziaria o a terzi, sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione (art. 5, comma 3, del Codice).

9) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

32 Autorizzazione n. 7/2005 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici 21 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto l'art. 4, comma 1, lett. *e*), del Codice, il quale individua i dati giudiziari;

Visti, in particolare, gli articoli 21, comma 1, e 27 del Codice, che consentono il trattamento di dati giudiziari, rispettivamente, da parte di soggetti pubblici e di privati o di enti pubblici economici, soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni eseguibili;

Visti gli articoli 20, commi 2 e 4, e le disposizioni relative a specifici settori di cui alla Parte II, del Codice e, in particolare, i Capi III e IV del Titolo IV, nel quale sono indicate finalità di rilevante interesse pubblico che rendono ammissibile il trattamento di dati giudiziari da parte di soggetti pubblici;

Visto l'art. 22 del Codice, il quale prevede i principi applicabili al trattamento di dati sensibili e giudiziari da parte di soggetti pubblici;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 31 dicembre 2005, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dall'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di diciotto mesi;

Visti gli articoli 51 e 52 del Codice in materia di informatica giuridica e ritenuta la necessità di favorire la prosecuzione dell'attività di documentazione, studio e ricerca in campo giuridico, in particolare per quanto riguarda la diffusione di dati relativi a precedenti giurisprudenziali, in ragione anche dell'affinità che tali attività presentano con quelle di manifestazione del pensiero già disciplinate dall'art. 137 del Codice;

(*) *G.U.* 3 gennaio 2006, n. 2, *S. O.* n. 1 [doc. *web* n. 1203942 vers. EN n. 1208801]

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

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

Relatore il dott. Giuseppe Chiaravalloti;

Autorizza

i trattamenti di dati giudiziari per le finalità di rilevante interesse pubblico di seguito specificate ai sensi degli articoli 21 e 27 del Codice, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

CAPO I - RAPPORTI DI LAVORO

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta, a persone fisiche e giuridiche, enti, associazioni ed organismi che:

a) sono parte di un rapporto di lavoro;
b) utilizzano prestazioni lavorative anche atipiche, parziali o temporanee;
c) conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

Il trattamento deve essere indispensabile per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario.

L'autorizzazione è altresì rilasciata a soggetti che in relazione ad un'attività di composizione di controversie esercitata in conformità alla legge svolgono un trattamento indispensabile al medesimo fine.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti a soggetti che hanno assunto o intendono assumere la qualità di:

a) lavoratori subordinati, anche se parti di un contratto di apprendistato, o di formazione e lavoro, o di inserimento, o di lavoro ripartito, o di lavoro intermittente o a chiamata, ovvero prestatori di lavoro nell'ambito di un contratto di somm-

nistrazione, o in rapporto di tirocinio, ovvero di associati anche in compartecipazione o di titolari di borse di lavoro e di rapporti analoghi;
b) amministratori o membri di organi esecutivi o di controllo;
c) consulenti e liberi professionisti, agenti, rappresentanti e mandatari.

CAPO II - ORGANISMI DI TIPO ASSOCIATIVO E FONDAZIONI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata anche senza richiesta:
a) ad associazioni anche non riconosciute, ivi compresi partiti e movimenti politici, associazioni ed organizzazioni sindacali, patronati, associazioni a scopo assistenziale o di volontariato, a fondazioni, comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché a cooperative sociali e società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818;
b) ad enti ed associazioni anche non riconosciute che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi.

Il trattamento deve essere indispensabile per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti:
a) ad associati, soci e aderenti, nonché, nei casi in cui l'utilizzazione dei dati sia prevista dall'atto costitutivo o dallo statuto, a soggetti che presentano richiesta di ammissione o di adesione;
b) a beneficiari, assistiti e fruitori delle attività o dei servizi prestati dall'associazione, dall'ente o dal diverso organismo.

CAPO III - LIBERI PROFESSIONISTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata anche senza richiesta ai:
a) liberi professionisti, anche associati, tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata, anche in conformità al decreto legislativo 2 febbraio 2001, n. 96 o alle norme di attuazione dell'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza;
b) soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato;
c) sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

2) Interessati ai quali i dati si riferiscono

Il trattamento può riguardare dati attinenti ai clienti.

I dati relativi ai terzi possono essere trattati solo ove ciò sia strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

CAPO IV - IMPRESE BANCARIE ED ASSICURATIVE ED ALTRI TRATTAMENTI

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta:

a) ad imprese autorizzate o che intendono essere autorizzate all'esercizio dell'attività bancaria e creditizia, assicurativa o dei fondi pensione, anche se in stato di liquidazione coatta amministrativa, ai fini:
   1. dell'accertamento, nei casi previsti dalle leggi e dai regolamenti, del requisito di onorabilità nei confronti di soci e titolari di cariche direttive o elettive;
   2. dell'accertamento, nei soli casi espressamente previsti dalla legge, di requisiti soggettivi e di presupposti interdittivi;
   3. dell'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana;
   4. dell'accertamento di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, in relazione ad illeciti direttamente connessi con la medesima attività. Per questi ultimi casi, limitatamente ai trattamenti di dati registrati in una specifica banca di dati ai sensi dell'art. 4, comma 1, lett. *p*), del Codice, il titolare deve inviare al Garante una dettagliata relazione sulle modalità del trattamento;

b) a soggetti titolari di un trattamento di dati svolto nell'ambito di un'attività di richiesta, acquisizione e consegna di atti e documenti presso i competenti uffici pubblici, effettuata su incarico degli interessati;

c) alle società di intermediazione mobiliare, alle società di investimento a capitale variabile, e alle società di gestione del risparmio e dei fondi pensione, ai fini dell'accertamento dei requisiti di onorabilità in applicazione della normativa in materia di intermediazione finanziaria e di previdenza o di forme pensionistiche complementari, e di eventuali altre norme di legge o di regolamento.

2) Ulteriori trattamenti

L'autorizzazione è rilasciata altresì:

a) a chiunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato e i dati siano trattati esclusivamente per tale finalità e per il periodo strettamente necessario per il suo perseguimento;

b) a chiunque, per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

c) a persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

Il trattamento deve essere necessario:

1) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero di un diritto della personalità o di un altro diritto fondamentale ed inviolabile;

2) su incarico di un difensore in riferimento ad un procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (articolo 190 del codice di procedura penale e legge 7 dicembre 2000, n. 397);

d) a chiunque, per adempiere ad obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale, contenute anche nella legge 19 marzo 1990, n. 55, e successive modificazioni ed integrazioni, o per poter produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto;

e) a chiunque, ai fini dell'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalla normativa in materia di appalti.

CAPO V - DOCUMENTAZIONE GIURIDICA

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati per finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali, nel rispetto di quanto previsto dagli articoli 51 e 52 del Codice.

CAPO VI - PRESCRIZIONI COMUNI A TUTTI I TRATTAMENTI

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati trattati

Possono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2) Modalità di trattamento

Il trattamento dei dati deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto agli obblighi, ai compiti o alle finalità precedentemente indicati. Fuori dei casi previsti dai Capi IV, punto 2 e V, o nei quali la notizia è acquisita da fonti accessibili a chiunque, i dati devono essere forniti dagli interessati nel rispetto della disciplina prevista dal d.P.R. 14 novembre 2002, n. 313.

3) Conservazione dei dati

Con riferimento all'obbligo previsto dall'art. 11, comma 1, lett. *e*), del Codice, i dati possono essere conservati per il periodo di tempo previsto da leggi o regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per le finalità perseguite.

Ai sensi dell'art. 11, comma 1, lett. *c*), *d*) ed *e*), del Codice, i soggetti autorizzati verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi. Al fine di assicurare che i dati siano strettamente pertinenti, non eccedenti e indispensabili rispetto alle finalità medesime, i soggetti autorizzati valutano specificamente il rapporto tra i dati e i singoli obblighi, compiti e prestazioni. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente gli obblighi, i compiti e le prestazioni.

4) Comunicazione e diffusione

I dati possono essere comunicati e, ove previsto dalla legge, diffusi, a soggetti pubblici o privati nei limiti strettamente indispensabili per le finalità perseguite e nel rispetto, in ogni caso, del segreto professionale e delle altre prescrizioni sopraindicate.

5) Richieste di autorizzazione

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione al Garante, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante si riserva l'adozione di ogni altro provvedimento per i trattamenti non considerati nella presente autorizzazione.

Per quanto riguarda invece i trattamenti disciplinati nel presente provvedimento, il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle relative prescrizioni, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute nell'art. 8 della legge 20 maggio 1970, n. 300, fatto salvo dall'art. 113 del Codice, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore e dall'art. 10 del d.lg. 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare determinate indagini o comunque trattamenti di dati ovvero di preselezione di lavoratori.

6) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 1° gennaio 2006 fino al 30 giugno 2007, salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 21 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

33 Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento dei dati personali verso l'Argentina 9 giugno 2005 (*)

Registro delle Deliberazioni
n. 10 del 9 giugno 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi 1 e 2, della direttiva 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 30 giugno 2003 n. 2003/490/Ce (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 168/19 del 5 luglio 2003) con la quale si è ritenuto che l'Argentina garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del citato art. 25, paragrafo 6 della direttiva;

Visti gli artt. 43, 44 e 45 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003), secondo i quali il trasferimento dei dati personali diretto verso Paesi non appartenenti all'Unione europea può avvenire qualora ricorra uno dei casi previsti dall'art. 43 oppure, ai sensi degli artt. 44, comma 1 e 45, quando sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: a) individuate dalla medesima Autorità anche in relazione a garanzie prestate con un contratto; b) individuate con le decisioni della Commissione previste dagli artt. 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/Ce; c) altrimenti, fuori dai casi di cui agli artt. 43 e 44, qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato nei termini di cui all'art. 45;

Considerata l'esigenza di adottare un provvedimento necessario per l'applicazione della decisione della Commissione in conformità al citato art. 44, comma 1, lett. *b*);

Ritenuto che le disposizioni di rango costituzionale e le altre norme vigenti in Argentina relative alla protezione dei dati personali, in base alla valutazione svolta dalla Commissione europea, prevedono garanzie per i diritti dell'interessato che, in conformità al diritto comunitario, vanno ritenute adeguate in base al citato art. 44, comma 1, lett. *b*);

Visti gli artt. 2 e 3 della decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di

(*) *G.U.* 25 luglio 2005, n. 171
[doc. *web* n. 1151846 vers. EN n. 1214136]

dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva 95/46/Ce sul diritto nazionale applicabile;

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta decisione disponendo la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

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

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE:

1. fatta salva l'applicazione delle ulteriori disposizioni previste dal Codice in materia di protezione dei dati personali, autorizza i trasferimenti di dati personali dal territorio dello Stato verso l'Argentina, con effetto dal termine previsto dall'art. 5 della decisione della Commissione europea del 30 giugno 2003 n. 2003/490/Ce e in conformità alla decisione medesima;
2. si riserva, in conformità alla normativa comunitaria, al Codice in materia di protezione dei dati personali e all'art. 3 della decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;
3. dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 9 giugno 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

34 Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento di dati personali dal territorio dello Stato all'Ufficio statunitense "Cbp" del Ministero della sicurezza interna (Department of Homeland Security) 14 luglio 2005 (*)

Registro delle Deliberazioni
n. 18 del 14 luglio 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi 1 e 2, della direttiva 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 14 maggio 2004 n. 2004/535/Ce (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 235/11 del 6 luglio 2004) con la quale si è ritenuto che l'Ufficio statunitense delle dogane e della protezione delle frontiere (United States Bureau of Customs and Border Protection, "Cbp") del Ministero della sicurezza interna (Department of Homeland Security) è in grado di offrire un livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei (Passenger Name Record, "Pnr") trasmessi dalla Comunità per quanto riguarda i voli con destinazione o partenza dagli Stati Uniti, in conformità alla "Dichiarazione d'impegno del Ministero per la sicurezza interna (Department for Homeland Security) - Ufficio delle dogane e della protezione delle frontiere (Cbp) dell'11 maggio 2004" ("Dichiarazione d'impegno") che figura in allegato alla medesima decisione;

Vista la decisione del Consiglio delle Comunità europee del 17 maggio 2004 n. 2004/496/Ce (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 183/83 del 20 maggio 2004) relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, "Pnr") da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del Ministero per la sicurezza interna degli Stati Uniti;

Visto il conseguente accordo firmato a Washington il 28 maggio 2004, che prevede che: a) il Cbp può accedere elettronicamente ai dati Pnr provenienti dai sistemi di prenotazione/controllo ("sistemi di prenotazione") dei vettori aerei situati nel territorio degli Stati membri della Comunità europea, in conformità alla decisione, per il periodo in cui la decisione è applicabile e finché non sia in vigore un sistema soddisfacente che permetta

(*) *G.U.* 25 luglio 2005, n. 171
[doc. *web* n. 1149808 vers. EN n. 1214157]

la trasmissione di tali dati da parte dei vettori aerei; b) ciascun vettore aereo che assicura il trasporto di passeggeri da o per gli Stati Uniti nello spazio aereo estero tratta i dati Pnr contenuti nei suoi sistemi automatizzati di prenotazione come richiesto dal Cbp ai sensi della normativa statunitense, in conformità alla decisione, per il periodo in cui la decisione è applicabile;

Considerato che gli Stati membri devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del citato art. 25, paragrafo 6, della direttiva;

Visti gli artt. 43, 44 e 45 del Codice in materia di protezione dei dati personali, secondo i quali il trasferimento dei dati personali diretto verso Paesi non appartenenti all'Unione europea può avvenire qualora ricorra uno dei casi previsti dall'art. 43 oppure, ai sensi degli artt. 44, comma 1 e 45, quando sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: a) individuate dalla medesima Autorità anche in relazione a garanzie prestate con un contratto; b) individuate con le decisioni della Commissione previste dagli artt. 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/Ce; c) altrimenti, fuori dai casi di cui agli artt. 43 e 44, qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato nei termini di cui all'art. 45;

Considerato che, secondo la valutazione svolta dalla Commissione europea, i criteri utilizzati dal Cbp per trattare i dati Pnr dei passeggeri, in base alla legislazione statunitense e alla Dichiarazione d'impegno del Cbp, includono i principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche;

Considerata l'esigenza di adottare un provvedimento necessario per l'applicazione della decisione della Commissione in conformità al citato art. 44, comma 1, lett. *b)*;

Visti gli artt. 2 e 3 della decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva 95/46/Ce sul diritto nazionale applicabile;

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta decisione disponendo la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

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

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE:

1. fatta salva l'applicazione delle ulteriori disposizioni previste dal Codice in materia di protezione dei dati personali, autorizza il trasferimento fuori dal territorio dello Stato all'Ufficio statunitense delle dogane e della protezione delle frontiere (United States Bureau of Customs and Border Protection, "Cbp") del Ministero della sicurezza interna (Department of Homeland Security), da parte dei vettori aerei che assicurano il trasporto di passeggeri con destinazione o in partenza dagli Stati Uniti, dei dati personali contenuti nelle schede nominative dei passeggeri ("Pnr") nella misura in cui tali dati siano stati raccolti e memorizzati nei relativi sistemi informatici di prenotazione, sulla base dei presupposti e in conformità a quanto previsto dalla decisione della Commissione europea del 14 maggio 2004 n. 2004/535/Ce ed alla Dichiarazione di impegno ivi allegata e con effetto dal termine previsto dall'art. 6 della decisione medesima;
2. si riserva, in conformità alla normativa comunitaria, al Codice in materia di protezione dei dati personali e all'art. 3 della decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trat-

tamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;
3. dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 14 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

35 Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso Paesi terzi 9 giugno 2005 (*)

Registro delle deliberazioni
n. 12 del 9 giugno 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice-presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi 1 e 2, della direttiva 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto l'art. 26 della predetta direttiva il quale individua alcune deroghe al menzionato principio, prevedendo anche che uno Stato membro possa autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un Paese terzo che non garantisce un livello di protezione adeguato, qualora il titolare del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, risultanti anche da clausole contrattuali appropriate;

Visto il paragrafo 4 del medesimo art. 26 relativo alle decisioni della Commissione europea in materia di clausole contrattuali tipo;

Rilevato che la Commissione europea, con la decisione del 15 giugno 2001, n. 2001/497/Ce, ha individuato un primo insieme di clausole contrattuali tipo, allegate alla medesima decisione, che costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi in caso di trasferimento di dati personali verso paesi terzi a norma della direttiva 95/46/Ce;

Vista la decisione della Commissione europea del 27 dicembre 2004, n. 2004/915/Ce (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 385/74 del 29 dicembre 2004) che modifica la citata decisione della Commissione n. 2001/497/Ce introducendo un insieme alternativo di clausole contrattuali tipo, allegate alla medesima decisione, che secondo la Commissione costituiscono anch'esse garanzie sufficienti ai fini della tutela della riservatezza, dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi in caso di trasferimento di dati personali verso paesi terzi a norma della direttiva 95/46/Ce;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 4, del citato art. 26 della direttiva;

Visti gli artt. 43, 44 e 45 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003), secondo i quali il trasferimento dei dati personali diretto verso paesi non appartenenti all'Unione europea può avvenire qualora ricorra uno dei casi previsti dal-

(*) G.U. 25 luglio 2005, n. 171
[doc. web n. 1151949 vers. EN n. 1214121]

l'art. 43 oppure, ai sensi degli artt. 44, comma 1 e 45, quando sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: a) individuate dalla medesima Autorità anche in relazione a garanzie prestate con un contratto; b) individuate con le decisioni della Commissione previste dagli artt. 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/Ce; c) altrimenti, fuori dai casi di cui agli artt. 43 e 44, qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato nei termini di cui all'art. 45;

Vista la deliberazione n. 35 del 10 ottobre 2001 con la quale questa Autorità ha autorizzato il trasferimento di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione n. 2001/497/Ce, ora denominato "Insieme I" ai sensi dell'art. 1, paragrafo 4, della decisione della Commissione n. 2004/915/Ce;

Ritenuto che le clausole contrattuali tipo, contenute nell'"Insieme II" dell'allegato alla decisione n. 2004/915/Ce, su cui si è espressa la Commissione, prevedono alcune garanzie per i diritti dell'interessato da ritenere adeguate ai sensi del citato art. 44, comma 1, lett. *b*);

Rilevato che la decisione della Commissione riguarda unicamente l'adeguatezza della tutela dei dati garantita dall'uso delle clausole contrattuali tipo in caso di trasferimenti di dati effettuati a partire dal territorio dello Stato da un titolare del trattamento avente sede nella Comunità (soggetto esportatore) ad un diverso titolare del trattamento (soggetto importatore) residente in un Paese terzo che non assicura un livello di protezione adeguato;

Rilevato che i soggetti che intendono utilizzare le clausole contrattuali tipo possono optare per uno degli insiemi di clausole - I o II- contenuti nell'allegato alla decisione della Commissione n. 2001/497/Ce, così come modificato dall'art. 1 della decisione n. 2004/915/Ce;

Considerato che i soggetti che utilizzano le citate clausole non possono modificarle, né combinare singole clausole, né gli insiemi citati;

Ritenuta la necessità di assicurare ulteriore pubblicità alle clausole contrattuali tipo di cui all'"Insieme II", disponendo la loro pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Ritenuta la necessità di formulare alcune prescrizioni inerenti alle informazioni da fornire a questa Autorità in relazione ai compiti ad essa affidati e richiamati dalla citata decisione della Commissione, nei limiti necessari per la prima fase di applicazione del presente provvedimento e nei termini di cui al seguente dispositivo;

Ritenuto di dover riservare la scelta del Garante di svolgere o meno, caso per caso, il ruolo di mediazione previsto dalla clausola V, lett. b), della decisione n. 2004/915/Ce;

Riservata la specificazione di ulteriori criteri e modalità in base all'esperienza maturata nell'utilizzazione delle clausole, anche in sede comunitaria;

Vista la documentazione d'ufficio;

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

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE:

1) fatta salva l'applicazione delle ulteriori disposizioni previste dal Codice in materia di protezione dei dati personali, autorizza, con effetto dal 1° aprile 2005, i trasferimenti di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione

della Commissione europea del 27 dicembre 2004, n. 2004/915/Ce e sulla base dei presupposti indicati nella medesima decisione;

2) dispone che:

a) la copia del contratto relativo al trasferimento e le altre informazioni necessarie devono essere fornite al Garante solo su sua richiesta (clausola I, lett. e), e art. 157 del Codice);

b) deve essere comunicata al Garante la scelta che è stata effettuata in caso di controversia non risolta in via amichevole e sottoposta all'esame di un soggetto diverso dal Garante o dall'autorità giudiziaria (clausola V, e art. 157 del Codice);

3) si riserva di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento in conformità al Codice in materia di protezione dei dati personali ed alla normativa comunitaria (art. 4 della decisione della Commissione n. 2001/497/Ce, come modificato dall'art. 1, paragrafo 2, della decisione n. 2004/915/Ce);

4) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 9 giugno 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

36 Trasferimento dei dati personali all'estero - Autorizzazione al trasferimento dei dati personali verso l'Isola di Man 9 giugno 2005 (*)

Registro delle deliberazioni
n. 11 del 9 giugno 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi 1 e 2, della direttiva 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 28 aprile 2004 n. 2004/411/Ce (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 151/50 del 30 aprile 2004), come rettificata nel testo pubblicato sulla *Gazzetta Ufficiale delle Comunità europee* L 208/47 del 10 giugno 2004, con la quale si è ritenuto che l'Isola di Man garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del citato art. 25, paragrafo 6 della direttiva;

Visti gli artt. 43, 44 e 45 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003), secondo i quali il trasferimento dei dati personali diretto verso Paesi non appartenenti all'Unione europea può avvenire qualora ricorra uno dei casi previsti dall'art. 43 oppure, ai sensi degli artt. 44, comma 1 e 45, quando sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: a) individuate dalla medesima Autorità anche in relazione a garanzie prestate con un contratto; b) individuate con le decisioni della Commissione previste dagli artt. 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/Ce; c) altrimenti, fuori dai casi di cui agli artt. 43 e 44, qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato nei termini di cui all'art. 45;

Considerata l'esigenza di adottare un provvedimento necessario per l'applicazione della decisione della Commissione in conformità al citato art. 44, comma 1, lett. *b*);

Ritenuto che le norme vigenti nell'Isola di Man relative alla protezione dei dati personali, in base alla valutazione svolta dalla Commissione europea, prevedono garanzie per i diritti dell'interessato che, in conformità al diritto comunitario, vanno ritenute adeguate in base al citato art. 44, comma 1, lett. *b*);

Visti gli artt. 2 e 3 della decisione in tema di controlli e provvedimenti delle autorità di

(*) *G.U.* 25 luglio 2005, n. 171
[doc. *web* n. 1151889 vers. EN n. 1214144]

garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva 95/46/Ce sul diritto nazionale applicabile;

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta decisione disponendo la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

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

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE:

1. fatta salva l'applicazione delle ulteriori disposizioni previste dal Codice in materia di protezione dei dati personali, autorizza i trasferimenti di dati personali dal territorio dello Stato verso l'Isola di Man, con effetto dal termine previsto dall'art. 6 della decisione della Commissione europea del 28 aprile 2004 n. 2004/411/Ce e in conformità alla decisione medesima;
2. si riserva, in conformità alla normativa comunitaria, al Codice in materia di protezione dei dati personali e all'art. 3 della decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;
3. dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 9 giugno 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

37 Investigazioni difensive: riapertura dei lavori sul codice deontologico 16 febbraio 2006 (*)

Registro delle deliberazioni
n. 3 del 16 febbraio 2006

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la deliberazione del 10 febbraio 2000(1), pubblicata sulla *Gazzetta Ufficiale* della Repubblica italiana del 25 febbraio 2000, n. 46, con la quale il Garante ha promosso la sottoscrizione di alcuni codici di deontologia e di buona condotta in conformità alla legge n. 675/1996 (artt. 22, comma 4 e 31, comma 1, lettera *h*));

Rilevato che tra tali codici figurava anche quello relativo ai dati personali trattati per svolgere le 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'attività di investigazione privata autorizzata in conformità alla legge;

Rilevato che alcuni soggetti pubblici e privati hanno aderito all'invito formulato pubblicamente dal Garante comunicando a questa Autorità la volontà di partecipare all'adozione di tale codice di deontologia e di buona condotta;

Rilevato che su questa base sono stati avviati, tra le categorie interessate, i lavori preparatori del medesimo codice di deontologia e di buona condotta;

Rilevato che è successivamente entrato in vigore il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) che ha riproposto le previsioni normative relative sia al predetto codice di deontologia e di buona condotta (art. 135), sia ai compiti del Garante di:

a) promuovere nell'ambito delle categorie interessate la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali;
b) verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati;
c) contribuire a garantirne la diffusione e il rispetto;

Visto l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva, adottate dagli Stati membri;

Rilevata la necessità di promuovere la ripresa dei lavori preparatori relativi al codice deontologia e di buona condotta di cui al citato art. 135, dopo la pausa dei medesimi lavori che si è registrata nel periodo antecedente e successivo all'entrata in vigore del Codice del 2003;

Considetato che pur non essendo intervenute sostanziali modifiche normative di rilievo per il medesimo codice di deontologia e di buona condotta, sussiste la necessità di verificare

(*) *G.U.* 1 marzo 2006, n. 50
[doc. *web* n. 1237162]

(1) [doc. *web* n. 1086086]

eventuali novità intervenute nelle categorie interessate, rilevanti ai fini dell'applicazione del principio di rappresentatività (art. 12 del Codice);

Rilevata l'esigenza, nel quadro della ripresa dei predetti lavori preparatori, di invitare i soggetti pubblici e privati interessati al medesimo codice di deontologia e di buona condotta a comunicare all'Autorità, entro il 31 marzo 2006, eventuali mutamenti intervenuti nel loro ambito -o altre circostanze utili- rilevanti ai fini della rappresentatività (in particolare, per effetto della formazione di nuovi soggetti rappresentativi, del mutamento di denominazione o configurazione di alcuni di essi, o dell'eventuale mancata comunicazione all'Autorità in adesione all'invito formulato con la predetta deliberazione del 10 febbraio 2000);

Ritenuta l'opportunità di dare ampia pubblicità a tale nuovo invito, anche attraverso la pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana;

Riservata ogni valutazione in ordine al rispetto del principio di rappresentatività, ai sensi del predetto art. 12 del Codice;

Vosti gli atti d'ufficio;

Viste le proposte e le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15, comma 1 del regolamento n. 1/2000;

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE:

nel quadro della ripresa dei lavori preparatori relativi al codice di deontologia e di buona condotta previsto dall'art. 135 del Codice, invita tutti i rappresentanti delle categorie interessate, aventi titolo a partecipare, in base al principio di rappresentatività (art. 12 del Codice), all'adozione del medesimo codice, a dare comunicazione a questa Autorità di eventuali mutamenti intervenuti nel loro ambito -o altre circostanze utili- rilevanti ai fini della rappresentatività.

La comunicazione dovrà essere inoltrata al Garante per la protezione dei dati personali, Piazza di Monte Citorio n. 121, 00186 Roma, entro il 31 marzo 2006 (n. fax 06.69677785; *e-mail*: codiceforense@garanteprivacy.it).

Roma, 16 febbraio 2006

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

38 Avviso relativo ai termini di conservazione dei dati personali presso i sistemi di informazioni creditizie 6 marzo 2006 (*)

In relazione al codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (Del. Garante 16 novembre 2004[1], n. 8, nella *Gazzetta Ufficiale* 23 dicembre 2004, n. 300; art. 6, comma 6, del predetto codice ivi allegato), esaminate anche le valutazioni espresse dall'organismo di verifica previsto dal medesimo codice (art. 13, commi 4 e 7), ha disposto la pubblicazione del presente avviso per indicare che i dati personali relativi ad informazioni creditizie di tipo positivo restino conservati nei sistemi di informazione creditizie per un termine non superiore a trentasei mesi.

(*) *G.U.* 6 marzo 2006, n. 54
[doc. *web* n. 1245761]

(1) [doc. *web* n. 1070713]

39 *"Fidelity card"* e garanzie per i consumatori 24 febbraio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Esaminati i reclami e le segnalazioni pervenuti in ordine al trattamento di dati personali raccolti attraverso carte o tessere di "fidelizzazione";

Ritenuta la necessità di prescrivere alcune misure necessarie ed opportune al fine di rendere il trattamento conforme alle disposizioni vigenti (art. 154, comma 1, lett. *c*), del Codice in materia di protezione dei dati personali);

Vista la documentazione acquisita a seguito degli accertamenti avviati e della consultazione pubblica effettuata;

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

Relatore il prof. Gaetano Rasi;

PREMESSO

1. La "fidelizzazione" nell'ambito della grande distribuzione

Il Garante ha ricevuto reclami e segnalazioni su trattamenti di dati effettuati nell'ambito della crescente utilizzazione di carte o tessere di "fidelizzazione" volte a creare un rapporto duraturo con la clientela per acquisti e servizi.

Gli intestatari delle "carte" usufruiscono di alcuni vantaggi per effetto della titolarità della carta, oppure del genere o volume di spesa o delle prestazioni richieste (*ad es.*, sconti per l'acquisto di prodotti; premi o *bonus* correlati; priorità; servizi accessori; facilitazioni di pagamento).

Le prescrizioni contenute nel presente provvedimento riguardano in termini generali tutti i tipi di "carte" nel settore della *cd.* grande distribuzione, siano esse rilasciate o meno gratuitamente, su supporto cartaceo o elettronico, presso punti-vendita oppure *on line*, nominativamente ovvero assegnando un codice identificativo, accumulando o meno punti rapportati a spese e servizi.

Il fenomeno ha assunto ampia portata interessando, oltre alla commercializzazione di beni di consumo, la prestazione di servizi nei trasporti, nel credito, nella telefonia, nell'editoria, nel noleggio, ecc.. I principi normativi richiamati in questa sede per la grande distribuzione hanno carattere generale e sono già applicabili in diversi ambiti.

Il Garante esamina in questa sede i profili di competenza rilevanti per il trattamento dei dati personali, senza valutare specificamente requisiti prescritti da leggi o regolamenti in altri ambiti (*ad es.*, dal d.P.R. 26 ottobre 2001, n. 430, in materia di concorsi, operazioni a premio e manifestazioni di sorte).

(*) [doc. web n. 1103045 vers. EN n. 1109624]

Il rilascio delle carte (spesso preceduto dalla compilazione di un modulo di adesione e di

un questionario), e la loro utilizzazione (che determina la registrazione di acquisti di beni e servizi), comportano un trattamento dei dati personali dei clienti e, a volte, dei loro familiari.

Accanto a dati anagrafici e recapiti anche di posta elettronica, sono spesso raccolte altre informazioni relative al cliente o a suoi familiari, non necessarie per attribuire i vantaggi collegati alla carta (titolo di studio, professione, interessi, abitudini, preferenze, modalità di acquisti, ecc.).

Tali informazioni vengono di frequente trattate unitariamente, per finalità diverse che richiedono quindi modalità differenziate; non di rado, è fornita solo un'informativa generica che descrive i trattamenti in modo non adeguatamente distinto.

Le analisi svolte sulle abitudini e scelte di consumo presentano rischi per gli interessati, anche quando i dati non sono comunicati a terzi.

Consumatori, relativi nuclei familiari ed altre persone da essi indicati, ricevendo i vantaggi legati alla fidelizzazione, sono monitorati in dettaglio nei loro comportamenti, vengono profilati anche all'interno di specifiche banche dati centrali o locali e fatti oggetto di raffronto con altri clienti, senza esserne peraltro consapevoli non avendo ricevuto un'adeguata informativa.

Si definiscono anche profili individuali o di gruppo (segmenti di clientela con caratteristiche omogenee, *cd. cluster*), ovvero propensioni al consumo, senza che gli interessati vi abbiano potuto acconsentire sulla base di informazioni chiare e specifiche. L'acquisto di beni e di servizi può persino determinare, in talune circostanze particolari, la raccolta di dati di natura sensibile, il cui trattamento non è di regola consentito per le finalità in esame.

A ciò si aggiungono eventuali contatti diretti con la clientela per operazioni di *marketing,* comunicazioni commerciali o pubblicitarie, vendite dirette o per ricerche di mercato, effettuati da chi rilascia la carta o da terzi.

Attesa la crescente diffusione del fenomeno, e a garanzia degli interessati, il Garante prescrive ai titolari del trattamento di adottare alcune misure necessarie od opportune al fine di conformare i trattamenti alle vigenti disposizioni in materia di protezione dei dati personali (art. 154, comma 1, lett. *c*), del Codice).

2. Necessità e proporzionalità

Le seguenti prescrizioni sono impartite tenendo conto delle distinzioni relative alle tre principali finalità indicate (fidelizzazione in senso stretto, realizzata attribuendo i vantaggi cui si è fatto cenno; profilazione mediante analisi di abitudini e scelte di consumo; *marketing* diretto), che rendono necessario diversificare le modalità del trattamento, in particolare per quanto riguarda le tipologie di dati e la loro conservazione.

I trattamenti devono svolgersi rispettando i principi di necessità, liceità, correttezza, qualità dei dati e di proporzionalità (artt. 3 e 11 del Codice).

In particolare:

- in applicazione del principio di necessità (art. 3 del Codice), i sistemi informativi e i programmi informatici devono essere configurati, già in origine, in modo da ridurre al minimo l'utilizzo di informazioni relative a clienti identificabili. Il trattamento di dati personali relativi a clienti non è lecito se le finalità del trattamento, in particolare di profilazione, possono essere perseguite con dati anonimi o solo indirettamente identificativi;
- nel rispetto del principio di proporzionalità nel trattamento (art. 11, comma 1, lett. *d*), del Codice), tutti i dati personali e le varie modalità del loro trattamento devono essere pertinenti e non eccedenti rispetto alle finalità perseguite.

Come premesso, l'utilizzazione di dati sensibili (art. 4, comma 1, lett. *d*), del Codice) non è di regola ammessa per alcuna delle finalità indicate, fatta salva l'ipotesi eccezionale nella quale il trattamento di dati sia realmente indispensabile in rapporto allo specifico bene

o servizio richiesto e sia stato autorizzato dal Garante, oltre che acconsentito per iscritto dall'interessato. Ciò, vale anche per eventuali ricerche di mercato, sondaggi ed altre ricerche campionarie (*cfr.* Aut. Gen. del Garante n. 5/2004, in *G.U.* 14 agosto 2004, n. 190).

Vanno a questo punto indicate le modalità di attuazione di questi principi in rapporto alle diverse finalità.

3. Finalità di "fidelizzazione" in senso stretto

Possono essere trattati esclusivamente i dati necessari per attribuire i vantaggi connessi all'utilizzo della carta.

Si tratta:

-dei dati direttamente correlati all'identificazione dell'intestatario della carta, quali le informazioni anagrafiche;

-dei dati eventualmente relativi al volume di spesa globale progressivamente realizzato (senza, cioè, riferimenti di dettaglio ai singoli prodotti), nella misura in cui sia realmente necessario trattarli –e in particolare conservarli– per attribuire i vantaggi medesimi, e per il tempo a ciò strettamente necessario. L'eventuale conservazione di dati di dettaglio relativi alle particolari tipologie di beni e servizi acquistati, o ai vantaggi conseguiti (punti, premi, *bonus*, ecc.), non è di regola necessaria specie se si persegue la sola finalità di "fidelizzazione"; nei casi particolari in cui essa è lecita, deve essere rispettato il principio di proporzionalità.

4. Finalità di "profilazione" della clientela

L'attività di profilazione riguardante singoli individui o gruppi può essere svolta, in diversi casi, disponendo solo di dati anonimi o non identificativi (ad esempio, un codice numerico), senza una relazione tra i dati che permettono di individuare gli interessati e le indicazioni analitiche relative alla loro sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo). Se la finalità può essere perseguita con tali modalità (specie per quanto riguarda la profilazione della clientela per categorie omogenee), non è lecito utilizzare –e tanto meno conservare– dati personali o identificativi.

Negli altri casi, le informazioni che si intende acquisire (sia all'atto dell'adesione del cliente all'iniziativa, sia per effetto dell'eventuale registrazione di singoli beni e servizi accessori), e le modalità del loro trattamento, devono essere pertinenti e non eccedenti rispetto alla tipologia dei beni commercializzati o dei servizi resi.

Il principio di proporzionalità va osservato anche per quanto riguarda l'eventuale intenzione di registrare le informazioni in banche di dati, tanto più se centrali. Inoltre, queste ultime non devono essere interconnesse -o fonte di intrecci e raffronti di dati- con quelle utilizzate per la fidelizzazione in senso stretto.

Per quanto concerne i dati sensibili va rilevato, oltre a quanto già richiamato, che non è lecito utilizzare a fine di profilazione dati idonei a rivelare la stato di salute e la vita sessuale (*cfr. Autorizzazioni generali* del Garante nn. 2 e 5/2004, in *G.U.* 14 agosto 2004, n. 190).

5. Finalità di *"marketing"* diretto

Possono essere raccolti ed utilizzati i dati pertinenti e non eccedenti per l'invio di materiale pubblicitario -anche attraverso riviste di settore- o di comunicazioni commerciali o per la vendita diretta. Si tratta, di regola, dei soli dati direttamente correlati all'identificazione dell'intestatario della carta o di suoi familiari, ovvero di persone da esso indicate. L'eventuale utilizzazione di dati personali derivanti dalla profilazione deve essere oggetto di un consenso differenziato dei diretti interessati.

6. Informativa agli interessati

Prima del conferimento dei dati e del rilascio della carta deve essere fornita al cliente un'informativa chiara e completa, al fine di consentire un'adesione pienamente consapevole alle iniziative proposte.

Nel rispetto del principio di correttezza (art. 11, comma 1, lett. *a*), del Codice), non sono consentiti comportamenti suscettibili di incidere sulle scelte libere e consapevoli del cliente nell'adesione ai "programmi di fidelizzazione".

Nello svolgimento delle operazioni preordinate al rilascio della "carta", non è corretto indurre il cliente ad aderire al programma senza aver avuto le spiegazioni e il tempo necessari per essere previamente informati e maturare un consenso consapevole riguardo ai dati da fornire, specie in ordine alla profilazione o al *marketing* (come potrebbe ad esempio accadere sollecitando una rapida sottoscrizione mentre il cliente è in fila alla cassa senza un esame preventivo di un'informativa).

L'informativa può utilizzare formule sintetiche e colloquiali, purché chiare e inequivoche; deve contenere comunque tutti gli elementi richiesti dal Codice (art. 13, comma 1).

Non sono consentiti generici rinvii a regolamenti di servizio non acclusi per le parti di riferimento. L'informativa inserita all'interno di moduli deve essere adeguatamente evidenziata e collocata in modo autonomo e unitario in un apposito riquadro, ed essere così agevolmente individuabile rispetto ad altre clausole del regolamento di servizio eventualmente riportato in calce o a margine.

In particolare, devono essere poste in distinta e specifica evidenza le caratteristiche dell'eventuale attività di profilazione e/o di *marketing*, come pure l'intenzione di cedere a terzi specificamente individuati i dati per finalità da indicare puntualmente.

Deve risultare parimenti chiara la circostanza che, per questi scopi, il conferimento dei dati e il consenso sono liberi e facoltativi rispetto alle ordinarie attività legate alla fidelizzazione in senso stretto.

7. Adesione al "programma di fidelizzazione" e consenso al trattamento.

Per ottenere la carta di fidelizzazione e fruire dei relativi vantaggi occorre di regola accettare condizioni generali di contratto predisposte dal titolare del trattamento (di regola, lo stesso emittente della "carta").

Poiché il trattamento di dati preordinato alla fidelizzazione in senso stretto è "*necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato*" non è corretto, in questo caso, sollecitare il consenso al trattamento dei dati (art. 24, comma 1, lett. *b*), del Codice).

Ogni altra finalità di trattamento (profilazione e ricerche di mercato da un lato; *marketing* dall'altro) che comporti l'identificabilità degli interessati necessita, invece, del loro consenso specifico, informato e distinto per ciascuna di esse (art. 23 del Codice). Il consenso deve essere quantomeno documentato per iscritto a cura del titolare del trattamento, ovvero reso necessariamente per iscritto dall'interessato nel caso di dati sensibili.

L'eventuale accettazione per iscritto delle clausole del regolamento di servizio deve essere distinta dalle formule utilizzate per ciascuna di queste due manifestazioni di libero consenso. L'adesione all'iniziativa di fidelizzazione non può essere condizionata alla manifestazione di tale consenso.

Non è quindi lecito raccogliere un consenso generale ricorrendo ad una generica dichiarazione, comprendendo anche i casi in cui il consenso non è necessario o a prescindere dalle finalità perseguite.

Per alcune forme di comunicazione mediante posta elettronica, fax, sistemi automatizzati di chiamata e messaggi del tipo *Mms* o *Sms* o di altro tipo, la necessità del consenso deriva anche da apposite disposizioni in tema di comunicazioni indesiderate o di vendite a distanza, le quali prevedono, altresì, regole particolari per l'offerta di servizi analoghi tramite posta elettronica (art. 130 del Codice; art. 10 d.lg. n. 185/1999). E' opportuno che copia della documentazione attestante l'informativa fornita e il consenso eventualmente prestato sia rilasciata all'interessato, per consentirgli di verificare in ogni momento le proprie scelte e di modificarle.

8. Tempi di conservazione

In applicazione del menzionato principio di proporzionalità, va prescritta ai titolari del trattamento l'identificazione di termini massimi di conservazione dei dati da osservare presso banche dati sia centrali, sia locali.

Tale identificazione va effettuata dopo aver esaminato la possibilità di raccogliere e conservare dati nei termini consentiti per ciascuna delle finalità sopradescritte, tenendo conto di eventuali scelte degli interessati sopravvenute.

Il principio da osservare è quello secondo cui i dati personali dei quali non è necessaria la conservazione in relazione agli scopi per i quali sono stati trattati devono essere cancellati o trasformati in forma anonima (art. 11, comma 1, lett. *e*), del Codice).

In ogni caso, i dati relativi al dettaglio degli acquisti con riferimento a clienti individuabili possono essere conservati per finalità di profilazione o di *marketing* per un periodo non superiore, rispettivamente, a dodici e a ventiquattro mesi dalla loro registrazione, salva la reale trasformazione in forma anonima che non permetta, anche indirettamente o collegando altre banche di dati, di identificare gli interessati. Eventuali intenzioni di trattare i dati oltre tali termini potranno essere attuate solo previa valutazione di questa Autorità ai sensi dell'art. 17 del Codice.

Nel caso di eventuale ritiro, disabilitazione per mancato utilizzo entro un determinato arco temporale, scadenza o restituzione della carta, deve essere individuato un termine di conservazione dei dati personali per esclusive finalità amministrative (e non anche di profilazione o di *marketing*), non superiore ad un trimestre (fatti salvi eventuali specifici obblighi di legge sulla conservazione di documentazione contabile). Occorre specificare questi aspetti nell'informativa e predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi cui gli stessi siano stati eventualmente comunicati (specie per la profilazione o di *marketing*).

9. Notificazione del trattamento e misure di sicurezza

Restano fermi, in aggiunta alle prescrizioni del presente provvedimento, gli obblighi che il Codice detta ai titolari del trattamento.

Ci si riferisce, in particolare:

- all'obbligo di notificazione al Garante dei trattamenti effettuati mediante l'ausilio di strumenti elettronici volti a definire profili di consumatori o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati (artt. 37, comma 1, lett. *d*), e 163 del Codice);
- agli obblighi relativi all'adozione delle misure anche minime di sicurezza (artt. 31-35 e Allegato B) del Codice;
- alla selezione dei soggetti che, in qualità di incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite (artt. 29 e 30 del Codice);
- all'obbligo dei titolari del trattamento di adottare le misure necessarie per agevolare l'esercizio dei diritti degli interessati e il relativo riscontro tempestivo (art. 10, comma 1, del Codice), con particolare riferimento alle concrete notizie da fornire in caso di richiesta di spiegazioni sulle finalità e modalità del trattamento (art. 7, comma 2, lett. *b*)) o di opposizione al trattamento.

In questo quadro, è necessario che:

- i dati eventualmente trattati a fini di profilazione o di ricerche di mercato siano conservati con adeguate modalità che portino a limitare l'ambito di circolazione dei dati allo stretto indispensabile, circoscrivendo qualitativamente e quantitativamente il numero di addetti aventi eventuale accesso alle informazioni;
- sia escluso l'uso di sistemi e programmi che permettano, fuori dei casi consentiti, una ricostruzione organica di scelte, comportamenti e profili di interessati identificabili non soggetta alle previe valutazioni di questa Autorità ai sensi dell'art. 17 del Codice;
- non si eludano, attraverso la preposizione di soggetti esterni quali responsabili del

trattamento, le richiamate garanzie in tema di comunicazione e conservazione dei dati e di trasparenza nell'informativa riguardo alle finalità e ai soggetti che le perseguono;

- si pongano a disposizione degli interessati, anche nell'informativa, specifici recapiti, anche di posta elettronica, per un agevole esercizio dei diritti.

10. Informazioni al Garante

Ai sensi e per gli effetti di cui agli artt. 157, 164 e 168 del Codice, i titolari del trattamento indicati negli atti di procedimenti pendenti presso l'Ufficio sono invitati a confermare al Garante, entro e non oltre il 15 maggio 2005, che i trattamenti di dati da essi effettuati sono conformi alle prescrizioni del presente provvedimento, indicando ogni informazione utile al riguardo ed allegando la pertinente documentazione.

TUTTO CIÒ PREMESSO, IL GARANTE

prescrive ai titolari di trattamenti di dati personali oggetto del presente provvedimento, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, di adottare le misure necessarie ed opportune ivi indicate al fine di rendere i trattamenti medesimi conformi alle disposizioni vigenti.

Roma, 24 febbraio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

40 TV interattiva e trattamento dei dati 3 febbraio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Esaminati i reclami e le segnalazioni pervenuti in ordine al trattamento di dati personali in relazione alla prestazione di servizi televisivi interattivi o ad accesso condizionato;

Ritenuta la necessità di prescrivere alcune misure necessarie ed opportune al fine di rendere il trattamento di tali dati conforme alle disposizioni vigenti (art. 154, comma 1, lett. *c*), del Codice in materia di tutela dei dati personali);

Vista la documentazione acquisita a seguito degli accertamenti avviati e della consultazione pubblica effettuata;

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

RELATORE il dott. Mauro Paissan;

PREMESSO

1. Nuovi servizi televisivi

La crescente integrazione tra le più recenti tecnologie utilizzate nella televisione, nelle comunicazioni elettroniche e nell'informatica rende disponibili prodotti e servizi innovativi basati anche sullo sviluppo di tecnologie digitali. Utenti e abbonati possono usufruire di svariati prodotti anche interattivi, accessibili via etere (terrestre o satellitare) o via cavo, utilizzando soluzioni a pagamento (abbonamento, *pay per view* e *video on demand*, ecc.) o altre forme di accesso condizionato.

Per usufruire di servizi e prodotti ci si deve dotare di un *decoder* o *set-top-box* che rende visibili segnali anche criptati ed è collegabile a una linea telefonica comunicazione dati (*cd.* "canale di ritorno"). Si può in tal modo comunicare con il fornitore del servizio attraverso un telecomando o un'apposita tastiera, inviando richieste o informazioni secondo diversi livelli di interazione. In tal modo è così possibile visionare film ed eventi sportivi, partecipare a sondaggi, giochi o *test*, formare palinsesti personalizzati, accedere a servizi di *telebanking*, televendita, ecc. Abbonati e utenti assumono così un ruolo attivo nei rapporti con i fornitori, interagiscono con essi in un'ottica di crescente personalizzazione e sono talvolta identificati nominativamente.

Le prescrizioni del presente provvedimento riguardano in termini generali tutti i predetti ambiti, diversi dai tradizionali servizi di radiodiffusione che vengono offerti ad un pubblico indifferenziato senza identificare gli utenti. Si prescinde, quindi, dalla tecnologia impiegata per prestare il servizio, dalla tecnica di trasmissione (analogica o digitale), dalla modalità di pagamento prescelta (*es.*, carte prepagate) o dai dispositivi utilizzati (digitazione di una tastiera o telecomando, ecc.). In presenza di un canale di ritorno sempre attivo, i servizi televisivi interattivi offerti via cavo permettono maggiori opportunità di costante monitoraggio e profilazione (non richiedendo l'attivazione reiterata del canale di ritorno) e presuppongono, pertanto, maggiori cautele nell'attuazione delle prescrizioni di seguito indicate.

(*) [doc. web n. 1109503 vers. EN n. 1116787]

Richiedono, poi, ulteriore considerazione in altra sede le specifiche problematiche poste

dal possibile coinvolgimento delle reti di telefonia mobile (anche per quanto riguarda l'identificazione della linea chiamante) o dall'offerta di altri tipi di servizi (come quelli sanitari, che comportano il trattamento di dati sensibili, o come quelli che permettono di accedere ad alcuni servizi di pubblica utilità attualmente in fase di sperimentazione, specie in sede locale: richiesta di certificati o documenti amministrativi o di svolgimento di pratiche, accesso a canali civici, ricerche in banche dati, ecc.). In questi casi, si pongono infatti problemi particolari specie per quanto riguarda i flussi di dati, l'informativa e l'eventuale richiesta di consenso.

Il Garante esamina qui i profili di competenza rilevanti per il trattamento dei dati personali, considerando che la necessità di assicurare agli utenti un livello elevato di tutela dei loro diritti e libertà fondamentali (nonché della dignità), affermata dal Codice in materia (d.lg. n. 196/2003), è stata ribadita da recenti norme sull'assetto del sistema radiotelevisivo (art. 4, comma 3, l. 3 maggio 2004, n. 112).

La possibilità che l'abbonato o l'utente trasmettano inconsapevolmente, mediante il canale di ritorno (ovvero via cavo), svariate informazioni che li riguardano -e che possono essere inviate da differenti utenti anche in ambito familiare- rende necessario individuare specifiche garanzie volte a prevenire illecite operazioni di profilazione e forme invasive di controllo su gusti e abitudini di persone, le quali vanno poste in grado di effettuare le proprie scelte liberamente e in modo informato.

A garanzia degli interessati, il Garante prescrive quindi ai titolari del trattamento di adottare alcune misure necessarie od opportune al fine di conformare i trattamenti alle vigenti disposizioni in materia di protezione dei dati personali (art. 154, comma 1, lett. *c*), del Codice), che sono applicabili anche nella parte riguardante le comunicazioni elettroniche (Titolo X, artt. 121 ss.), quando vengono in considerazione abbonati o utenti riceventi identificati o identificabili (*cfr.* art. 4, comma 2, lett. *a*)).

2. Necessità e proporzionalità

Il trattamento dei dati deve rispettare i principi di necessità, liceità, correttezza, qualità dei dati e di proporzionalità (artt. 3 e 11 del Codice).

In particolare:

- applicando il principio di necessità (art. 3 del Codice), i sistemi informativi e i programmi informatici devono essere configurati, già dall'origine, in modo da ridurre al minimo l'utilizzo delle informazioni relative ad abbonati ed utenti identificabili. Il trattamento di tali informazioni non è lecito se le finalità possono essere perseguite utilizzando solo dati realmente anonimi o indirettamente identificativi;
- nel rispetto del principio di proporzionalità nel trattamento (art. 11, comma 1, lett. *d*), del Codice), tutti i dati personali e le varie modalità del loro trattamento nelle singole fasi ed occasioni di utilizzazione devono essere pertinenti e non eccedenti rispetto alle finalità perseguite.

All'atto dell'eventuale acquisto di un *decoder* o di un *set top box* va distinto il caso in cui si debba contestualmente instaurare necessariamente un rapporto contrattuale con un abbonato identificato, dalle ipotesi nelle quali tale identificazione (e la possibile associazione tra nominativo e numero seriale dell'apparecchio *decoder*) non è lecita, essendo ad esempio il *decoder* utilizzato solo con schede prepagate non identificative.

Anche nel caso in cui eventuali e specifici obblighi di legge prescrivano puntualmente di identificare l'acquirente, occorre valutare le finalità di tale identificazione, che potrebbe essere eventualmente prescritta solo a fini fiscali di documentazione giustificativa per eventuali contributi statali. Dal punto di vista della protezione dei dati personali devono ritenersi parimenti illecite eventuali banche dati di titolari possessori di antenne televisive o satellitari, a prescindere dall'eventuale, e più problematica, associazione di tali dati ad altre informazioni personali.

Rispetto alle garanzie previste dal Codice è più indicata l'utilizzazione di carte prepagate impersonali, in luogo di abbonamenti nominativi.

Se ricorrono necessità di fatturazione non è poi lecito trattare eventuali dati personali relativi a tempi di connessione, visioni di programmi ed eventi, fasce orarie di utilizzazione del mezzo televisivo, interruzioni di ascolto, cambi di canale ed analisi del comportamento in presenza di spazi pubblicitari, se non nella misura, modalità e tempi effettivamente necessari.

L'eventuale richiesta –rivolta dal fornitore ai singoli utenti– di identificarsi nominativamente al momento in cui essi inviano informazioni attraverso il canale di ritorno è lecita solo se sottoposta all'esame preliminare di questa Autorità (art. 17 del Codice).

In occasione di altri eventi di *cd.* televoto deve essere evitata, fin dal momento della ricezione delle informazioni trasmesse dall'utente, la raccolta e/o la registrazione di dati associabili a persone identificabili, anche quando le domande riguardino solo gradimenti, gusti o preferenze e non siano richieste anche opinioni di natura sensibile su persone, fenomeni sociali o profili politico-religiosi o sindacali. Ricerche di mercato, altre ricerche campionarie e sondaggi devono essere effettuati in forma anonima, evitando l'afflusso di risposte relative a soggetti identificabili, oppure (se ciò è tecnicamente inevitabile) rendendo tali risposte realmente anonime subito dopo la loro raccolta, escludendo a maggior ragione ogni eventuale comunicazione a terzi o diffusione dei dati personali.

Infine, non ogni richiesta degli utenti o acquisto di determinati prodotti o partecipazione a sondaggi determinano, di per sé stessi, il trattamento di dati sensibili. Nel caso in cui, per le specifiche informazioni trasmesse dagli utenti o per le modalità della loro utilizzazione si intenda raccogliere dati sensibili (art. 4, comma 1, lett. *d*), del Codice), deve tenersi presente che il loro trattamento non è di regola ammesso né per l'ordinaria prestazione di servizi televisivi, né per eventuali finalità di profilazione o fidelizzazione della clientela, fatta salva l'ipotesi eccezionale nella quale il medesimo trattamento sia realmente indispensabile in rapporto ad uno specifico bene o servizio richiesto e sia altresì autorizzato dal Garante, oltre che acconsentito dall'interessato in forma scritta o telematica equiparabile allo scritto. Ciò, vale anche per eventuali ricerche di mercato, sondaggi ed altre ricerche campionarie *(cfr. Autorizzazione generale* del Garante n. 5/2004, in *G.U.* 14 agosto 2004, n. 190).

3. Informativa

L'informativa ora fornita all'atto della richiesta della *smart card* non è idonea in rapporto alla delicatezza e complessità dei flussi di informazioni, i quali possono peraltro riguardare più utenti facenti capo ad un medesimo abbonato e permettere a posteriori una ricostruzione dei loro comportamenti anche in ambito domestico, non solo, quindi, dal fornitore in occasione della fatturazione. Finalità e modalità del trattamento dei dati potrebbero inoltre differire da caso a caso, oltre che nel tempo.

Prima della costituzione del rapporto contrattuale, l'abbonato deve ricevere un'informativa chiara e completa, al fine di aderire in modo pienamente consapevole alle iniziative proposte.

Nel rispetto del principio di correttezza (art. 11, comma 1, lett. *a*), del Codice), al pari di quanto già prescritto da questa Autorità a proposito delle iniziative di fidelizzazione *(Provv.* 24 febbraio 2005, in *www.garanteprivacy.it* [doc. *web* n. 1103045]), deve ritenersi non consentito al fornitore di adottare comportamenti suscettibili di incidere sulle scelte libere e consapevoli degli abbonati rispetto ad eventuali iniziative di profilazione che portino, anche attraverso codici numerici, a monitorare le scelte degli interessati e la loro sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo).

L'informativa fornita sia al momento della costituzione del rapporto contrattuale, sia successivamente, riveste particolare importanza, considerati i rischi di sottovalutazione o di errore da parte dell'interessato.

Non è corretto indurre l'abbonato o l'utente a fornire informazioni personali senza aver avuto le spiegazioni e il tempo necessari per essere adeguatamente informati e maturare - allorché ciò è necessario- un consenso consapevole.

Si possono utilizzare formule sintetiche e colloquiali, purché chiare e inequivoche. L'informativa deve contenere tutti gli elementi richiesti dal Codice (art. 13, comma 1), evitando rinvii generici a regolamenti di servizio non acclusi per le parti di riferimento; deve specificare, altresì, la natura dei dati di traffico trattati e la durata del loro trattamento (art. 123, comma 4, del Codice).

L'informativa inserita all'interno di moduli deve essere adeguatamente evidenziata e collocata in modo autonomo e unitario in un apposito riquadro, e risultare altresì agevolmente individuabile rispetto ad altre clausole del regolamento di servizio eventualmente riportato in calce o a margine.

La persona fisica che accede ai servizi interattivi, o che viene abilitata caso per caso all'accesso condizionato (sia essa l'abbonato o meno), deve essere informata nuovamente in modo rapido e con brevi frasi efficaci circa l'eventuale utilizzo di dati personali, con una schermata di primo avviso (del tipo: "*Ecco come sono utilizzati i tuoi dati personali*") che permetta, premendo un tasto, di accedere ad un'idonea informativa leggibile anche a distanza.

4. Consenso

Il trattamento di eventuali dati personali preordinato strettamente alla prestazione di servizi richiesti è "*necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato*". In questi casi, non è corretto che il fornitore del servizio solleciti il consenso al trattamento, tantomeno in termini generali (art. 24, comma 1, lett. *b*), del Codice).

Se si pone in essere un'eventuale monitoraggio o profilazione, o si intende cedere dati personali a terzi specificamente individuati, queste circostanze e le relative finalità devono essere indicate puntualmente e con evidenza sia all'atto della costituzione del rapporto, sia prima di evadere le singole richieste di servizio o sollecitare le risposte degli utenti. Deve risultare chiara la circostanza che per questi scopi (come pure per la partecipazione a sondaggi che devono avere scopi fini chiaramente determinati e legittimi), il conferimento dei dati e il consenso sono liberi e facoltativi rispetto all'ordinaria prestazione dei servizi, e non possono ottenersi sulla base di pressioni o condizionamenti.

Nell'interfaccia grafica contenente il menzionato supplemento di informativa all'utente deve apparire l'indicazione su come acconsentire allo specifico trattamento, premendo ad esempio un tasto.

L'indicazione La comunicazione in modalità interattiva di dati sensibili da parte dell'utente al fornitore deve essere possibile solo mediante credenziali di autenticazione associate ad una parola chiave riservata.

5. Pagamenti e fatturazione

L'accesso ai servizi televisivi interattivi e ad accesso condizionato può essere gratuito o comportare specifici pagamenti aggiuntivi, attraverso carte pre-pagate o addebiti periodici (abbonamento o *pay per view*).

Mentre utilizzando carte prepagate il credito viene scalato in automatico, in caso di abbonamento la fattura può indicare gli eventuali "eventi" *pay per view* da pagare.

Essendo possibile che soggetti diversi accedano al medesimo apparecchio televisivo e, dunque, ai servizi televisivi, il fornitore deve porre in essere adeguate misure ed operare un corretto bilanciamento fra la tutela della riservatezza degli effettivi fruitori dei servizi e l'esigenza dell'abbonato di verificare la correttezza degli addebiti.

In applicazione dei menzionati principi di proporzionalità e necessità, i dati che compaiono nelle fatture non devono risultare eccedenti rispetto alla finalità perseguita. Deve essere offerta all'abbonato la possibilità di non ricevere una fatturazione dettagliata. I servizi *pay-per-view* devono essere menzionati per importo totale, data e costo di fruizione, indicando solo su successiva richiesta i "titoli" specifici dei singoli "eventi" acquistati.

6. Conservazione dei dati

Nella prestazione di servizi televisivi interattivi o ad accesso condizionato sono trattate tipologie diverse di dati, per differenti finalità.

Accanto a dati "amministrativi" di carattere generale, sono a volte trattati dati inerenti alla fatturazione di singoli consumi televisivi, i quali rilevano in determinati casi come "*dati di traffico*" *(cfr.* art. 4, comma 2, lett. *h)* del Codice), anche quando siano trattati dal fornitore del servizio, oltre che dal gestore telefonico (ad esempio, il numero telefonico o il numero della *smart card*; ora di inizio e durata della comunicazione elettronica relativa al servizio richiesto). Talvolta, come si è visto, possono venire in rilievo anche dati sensibili.

In applicazione del menzionato principio di proporzionalità, va prescritta ai titolari del trattamento l'identificazione di termini massimi di conservazione dei dati, anche nel corso del rapporto.

Tale identificazione va effettuata dopo aver esaminato la possibilità di raccogliere lecitamente e conservare dati nei termini consentiti per ciascuna delle finalità del trattamento che si intende effettuare, tenendo conto di eventuali scelte degli interessati sopravvenute.

Il principio da osservare è quello secondo cui i dati personali dei quali non è necessaria la conservazione in relazione agli scopi per i quali essi sono stati raccolti o successivamente trattati devono essere cancellati o trasformati in forma anonima (art. 11, comma 1, lett. *e*), del Codice).

Se non ricorrono esigenze di specifica fatturazione dei singoli prodotti, e non vi è un distinto e specifico consenso alla profilazione, i dati personali desumibili dal voto televisivo, da sondaggi, acquisti, ecc. non possono essere registrati ed utilizzati per l'una o l'altra di queste finalità.

Decorso il termine per le singole fatturazioni e le relative contestazioni, i dati personali relativi ai singoli servizi o programmi acquistati devono essere cancellati. La cancellazione deve riguardare anche la memorizzazione del consenso -acquisito nei soli casi in cui esso è, come si è detto, necessario- manifestato in forma scritta o telematica equiparabile allo scritto.

Anche laddove sia stato acquisito uno specifico consenso, di dati di dettaglio su acquisti e servizi possono essere eventualmente conservati per un periodo comunque non superiore a dodici mesi dalla loro registrazione, in riferimento a finalità commerciali, pubblicitarie o di profilazione, perseguite anche da parte di terzi, salva la loro trasformazione in forma anonima che non permetta di identificare gli interessati, anche indirettamente o collegando banche di dati. Eventuali intenzioni di trattare i dati oltre tali termini potranno essere attuate solo previa valutazione di questa Autorità ai sensi dell'art. 17 del Codice. In caso di cessazione del rapporto deve cessare ogni loro utilizzazione per le predette finalità.

Deve essere individuato un termine di conservazione dei dati personali una volta cessato il rapporto anche in relazione ad eventuali finalità amministrative, non superiore ad un trimestre (fatti salvi eventuali specifici obblighi di legge sulla conservazione di documentazione contabile, evitando una loro applicazione impropria). Occorre specificare questi aspetti nell'informativa e predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi ai quali gli stessi siano stati eventualmente comunicati (specie a fini di profilazione o di *marketing*).

I dati personali che rientrano nella nozione di "dati di traffico" possono essere trattati nei soli limiti di legge (artt. 123 e 132 del Codice). Non è consentito accedere ad informazioni archiviate nell'apparecchio terminale dell'abbonato o utente al fine di archiviare informazioni o monitorare le operazioni effettuate (art. 122, comma 1, del Codice).

Infine, laddove uno stesso soggetto (ad esempio, un centro servizi) svolga la propria attività per conto di più fornitori deve essere garantita una separazione nella gestione dei dati personali. In particolare, le eventuali banche di dati costituite non possono essere interconnesse.

7. Ulteriori prescrizioni

Restano fermi, in aggiunta alle prescrizioni del presente provvedimento, gli obblighi che il Codice detta ai titolari del trattamento, obblighi che potranno essere sviluppati attraverso il previsto codice di deontologia e di buona condotta per i servizi di comunicazione elettronica (artt. 122 e 133 del Codice), e la cui inosservanza espone all'inutilizzabilità dei dati trattati (art. 11 del Codice) oltre che alle pertinenti sanzioni amministrative e penali (artt. 161 ss. del Codice).

Ci si riferisce, in particolare:

a) all'obbligo di notificazione al Garante dei trattamenti effettuati
   - con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica, con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti (art. 37, comma 1, lett. *d*), del Codice);
   - con dati sensibili per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie (art. 37, comma 1, lett. *e*), del Codice);
   - con dati idonei a rivelare lo stato di salute e la vita sessuale ai fini di "...*prestazione di servizi sanitari per via telematica* ..." (art. 37, comma 1, lett. *b*), del Codice);

b) agli obblighi relativi all'adozione delle misure di sicurezza rapportate alle conoscenze acquisite in base al progresso tecnico (artt. 31-35 e Allegato B) del Codice), anche di tipo "minimo", in particolare per ciò che riguarda la verifica dei profili di autenticazione e autorizzazione, anche al fine di prevenire la fatturazione di servizi non richiesti;

c) alla selezione dei soggetti che, in qualità di incaricati e responsabili del trattamento, sono autorizzati a compiere le operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite, sotto la diretta autorità del fornitore (artt. 29 e 30 del Codice). L'eventuale preposizione di eventuali responsabili ed incaricati "esterni" incontra, nel settore in esame, precisi limiti di legge (art. 123, comma 5, del Codice) e non può portare ad eludere le garanzie di abbonati ed utenti in tema di comunicazione dei dati a terzi, di trasparenza nell'informativa e di rispetto delle finalità dichiarate;

d) all'obbligo di adottare le misure necessarie per agevolare l'esercizio dei diritti degli interessati e il relativo riscontro tempestivo, anche per il tramite degli stessi strumenti interattivi utilizzati per la prestazione dei servizi richiesti (artt. 9, comma 1 e 10, comma 1, del Codice).

8. Informazioni al Garante

Ai sensi e per gli effetti di cui agli artt. 157, 164 e 168 del Codice, i titolari del trattamento indicati negli atti di procedimenti pendenti presso l'Ufficio sono invitati a confermare al Garante, entro e non oltre il 15 maggio 2005, che i trattamenti di dati da essi effettuati sono conformi alle prescrizioni del presente provvedimento, indicando ogni informazione utile al riguardo ed allegando la pertinente documentazione.

TUTTO CIÒ PREMESSO IL GARANTE:

prescrive, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, ai titolari del trattamento dei dati relativi ai servizi televisivi interattivi, le misure necessarie ed opportune indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti.

Roma, 3 febbraio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

41 Disposizioni in materia di comunicazione e di propaganda politica 3 marzo 2005(*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Considerato che il 3 e il 4 aprile e nel mese di maggio 2005 si terranno alcune elezioni amministrative e che nella primavera del 2005 è prevista altresì una consultazione referendaria;

Considerato che candidati e forze politiche intraprendono numerose iniziative di comunicazione e di propaganda e che ciò comporta l'impiego di dati personali per l'inoltro di messaggi elettorali e politici al fine di rappresentare le proprie posizioni in relazione alle elezioni e ai referendum;

Considerato che il diritto riconosciuto a tutti i cittadini di concorrere con metodo democratico a determinare la politica nazionale (art. 49 Cost.) deve essere esercitato nel rispetto dei diritti e delle libertà fondamentali delle persone cui si riferiscono le informazioni utilizzate e, in particolare, del diritto fondamentale alla protezione dei dati personali (art. 1 del Codice);

Visto l'art. 13, comma 4, del Codice ai sensi del quale, se i dati non sono raccolti presso la persona cui si riferiscono, l'informativa di cui al comma 1 del medesimo articolo è fornita all'interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione;

Considerato che, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, il Garante ha il compito di dichiarare se l'adempimento da parte di un determinato titolare del trattamento all'obbligo di informativa comporta o meno un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato, e di prescrivere in tal caso eventuali misure appropriate;

Visto il provvedimento generale di questa Autorità del 12 febbraio 2004(1) (pubblicato sulla *Gazzetta Ufficiale* 24 febbraio 2004, n. 45, allegato al presente provvedimento e le cui prescrizioni si intendono qui integralmente richiamate), con il quale sono stati indicati i presupposti e le garanzie in base alle quali partiti e movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare lecitamente, a fini di propaganda elettorale, dati personali estratti in particolare da fonti pubbliche;

Considerato che il quadro di garanzie e di adempimenti richiamati con il predetto provvedimento del 12 febbraio 2004 opera anche in relazione alle prossime consultazioni elettorali sopraindicate;

Considerato che, per il solo perseguimento delle iniziative referendarie e per i trattamenti a ciò finalizzati, non è necessaria alcuna manifestazione di consenso ulteriore rispetto alla sottoscrizione delle richieste referendarie, per la cui validità i promotori sono tenuti a raccogliere, per legge, alcuni dati personali dei sottoscrittori (artt. 7 e 8 l. 25 maggio 1970, n. 352; art. 24, comma 1, lett. *a*), d.lg. n. 196/2003), e a darne comunicazione

(*) *G.U.* 18 marzo 2005, n. 64
[doc. *web* n. 1107658]

(1) [doc. *web* n. 634369]

agli organi preposti alla verifica della regolarità delle richieste (artt. 9 ss. l. 25 maggio 1970, n. 352; art. 24, comma 1, lett. *a*), citato);

Considerato che, invece, coloro che intendono eventualmente trattare i predetti dati per finalità diverse da quelle collegate alla richiesta referendaria devono previamente richiedere un consenso informato, libero, scritto e distinto dalla predetta sottoscrizione delle richieste referendarie;

Considerato che, con il predetto provvedimento, i soggetti che effettuano propaganda elettorale sono stati altresì esonerati temporaneamente, a determinate condizioni, dall'obbligo di fornire previamente l'informativa ai soggetti interessati al trattamento (art. 13 del Codice);

Ritenuto necessario richiamare nel presente provvedimento le garanzie già segnalate dal Garante nel citato provvedimento del 12 febbraio 2004;

Considerata la necessità di esonerare in via temporanea dall'obbligo dell'informativa di cui all'art. 13 del Codice partiti e movimenti politici, comitati promotori, sostenitori e candidati che trattano dati personali per esclusiva finalità di comunicazione politica o di propaganda, nel circoscritto ambito temporale concernente le menzionate tornate di consultazioni elettorali amministrative e referendarie;

Ritenuto che, applicando i principi affermati nel citato provvedimento del 12 febbraio 2004 a proposito dell'obbligo di informativa, deve ritenersi proporzionato rispetto ai diritti degli interessati esonerare il soggetto che utilizza i dati per esclusivi fini di propaganda elettorale dall'obbligo di fornire l'informativa, sino alla data del 30 giugno 2005; ciò, con riferimento all'informativa dovuta a persone cui si riferiscono dati personali estratti da fonti pubbliche accessibili a chiunque, che non siano contattate da chi utilizza i dati o che ricevano materiale di propaganda diverso da lettere articolate o messaggi di posta elettronica, che non permetta l'inserimento dell'informativa;

Ritenuto che, decorsa la data del 30 giugno 2005, partiti e movimenti politici, comitati promotori, sostenitori e candidati possano continuare a trattare (anche mediante mera conservazione) dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per esclusive finalità di propaganda elettorale e di connessa comunicazione politica, solo se informeranno gli interessati entro il 30 settembre 2005 nei modi previsti dall'art. 13 del Codice;

Ritenuto che, nel caso in cui partiti e movimenti politici, comitati promotori, sostenitori e candidati non informino gli interessati entro il predetto termine del 30 settembre 2005 nei modi previsti dall'art. 13 del Codice, i dati dovranno essere cancellati o distrutti;

Rilevato che l'interessato può esercitare i diritti di cui all'art. 7 del Codice, con riferimento ai quali il titolare del trattamento è tenuto a fornire un idoneo riscontro;

Vista la documentazione in atti;

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

Relatore il prof. Giuseppe Santaniello;

TUTTO CIÒ PREMESSO, IL GARANTE:

a) prescrive ai titolari di trattamento interessati, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare le misure necessarie ed opportune richiamate nel presente provvedimento, al fine di rendere il trattamento conforme alle disposizioni vigenti;
b) ai sensi dell'art. 13, comma 5, del Codice dispone che partiti e movimenti politici, comitati promotori, sostenitori e candidati, i quali trattino dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per esclusive finalità

di propaganda elettorale e di connessa comunicazione politica in occasione delle consultazioni elettorali, amministrative e referendarie del primo semestre del 2005, possano astenersi dall'informare gli interessati alle condizioni e nei limiti indicati in motivazione; c) dispone che il presente provvedimento sia pubblicato sulla *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 3 marzo 2005

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

42 Trattamento dei dati sensibili nella pubblica amministrazione 30 giugno 2005(*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria e il Codice in materia di protezione dei dati personali (direttiva n. 95/46/Ce; d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO:

1. Considerazioni introduttive

Il Codice entrato in vigore il 1° gennaio 2004 ha riunito in modo organico la normativa di tutela relativa al trattamento dei dati personali; ha offerto all'intera amministrazione pubblica un'occasione significativa per portare a compimento il processo di modernizzazione, in modo da adeguare il proprio assetto organizzativo e funzionale dando idonee risposte alle istanze dei cittadini rivolte al massimo rispetto dei diritti e delle libertà fondamentali.

In questo quadro, il Garante rileva, però, con rammarico che numerose amministrazioni pubbliche non hanno dato piena attuazione al Codice.

In particolare, questa Autorità segnala che non sono state ancora introdotte le garanzie previste in ordine al trattamento di alcune informazioni che riguardano profili particolarmente delicati della sfera privata delle persone, ovvero dei *cd.* dati "sensibili".

La vicenda incide in termini rilevanti sulla sfera dei diritti dei cittadini.

L'utilizzo di queste informazioni (concernenti la salute, la vita sessuale, la sfera religiosa, politico-sindacale o filosofica, nonché l'origine razziale ed etnica) è inoltre soggetto a rigorose cautele anche in base alla disciplina comunitaria, la quale vieta il loro trattamento a meno che ricorrano specifici motivi di interesse pubblico rilevante e siano altresì assicurate opportune garanzie (art. 8 direttiva cit.). Analoghe cautele sono previste per i dati di carattere giudiziario. L'inerzia delle pubbliche amministrazioni lede, quindi, non solo il diritto dei cittadini alla protezione dei dati personali, ma comporta anche una violazione del diritto comunitario.

Il ritardo accumulato su questo piano è eccessivo. Sin dal 1997, vigente la legge n. 675/1996, ed anche dopo l'approvazione del Codice nel 2003, i soggetti pubblici hanno infatti potuto avvalersi di un lungo periodo transitorio e di diverse proroghe. L'eventuale protrarsi dell'inerzia delle amministrazioni anche dopo il 31 dicembre 2005 (data di scadenza dell'ultima proroga) risulterebbe del tutto ingiustificata.

L'Autorità esprime viva preoccupazione in relazione al rispetto del termine di legge del 31 dicembre prossimo.

(*) *G.U.* 23 luglio 2005, n. 170
[doc. *web* n. 1144445]

Se non interverranno per tale data i necessari atti di natura regolamentare il trattamento dei dati sensibili e giudiziari dovrà essere infatti interrotto a decorrere dal 1° gennaio prossimo. La prosecuzione del trattamento di dati sensibili e giudiziari dopo tale data concretizzerebbe un illecito, con conseguenti responsabilità di diverso ordine, anche contabile e per danno erariale; potrebbe inoltre comportare l'inutilizzabilità dei dati trattati indebitamente, nonché il possibile intervento di provvedimenti anche giudiziari di blocco o di divieto del trattamento (art. 154 del Codice; art. 3 d.l. 24 giugno 2004, n. 158, come modificato dalla l. 27 luglio 2004, n. 188; art. 11, commi 1, lett. *a*) e 2, del Codice).

Nel quadro della tematica in esame, le amministrazioni pubbliche hanno l'obbligo - accanto ad altri doveri in materia- di rendere trasparenti ai cittadini quali informazioni vengono raccolte tra quelle particolarmente delicate cui si è fatto riferimento; devono altresì chiarire come utilizzano queste informazioni per le finalità di rilevante interesse pubblico individuate con legge. Tali indicazioni vanno trasfuse in un atto regolamentare cui va data ampia pubblicità (artt. 4, comma 1, lett. *d*) ed *e*), 20, comma 2 e 21, comma 2, del Codice).

Non si tratta di un mero adempimento formale, oppure di una semplice ricognizione di prassi esistenti, poiché da tali regolamenti discenderanno effetti sostanziali per i cittadini interessati.

Gli schemi dei regolamenti devono essere sottoposti al Garante per l'espressione del parere, cui i soggetti pubblici devono poi conformarsi.

Considerata l'ampiezza del settore, il Codice prevede anche la possibilità che siano redatti schemi tipo per insiemi omogenei di amministrazioni, sui quali può essere pertanto espresso un unico parere.

Per contribuire alla corretta applicazione del Codice, il Garante ha intensificato la collaborazione finalizzata alla predisposizione di tali schemi tipo con organismi rappresentativi di regioni, autonomie locali ed università, nonché, in riferimento alle rispettive funzioni istituzionali, con la Presidenza del Consiglio dei ministri e il Dipartimento della funzione pubblica.

Il Garante resta però in attesa di ricevere per il parere sia gli schemi tipo eventualmente proposti, sia gli schemi di regolamento predisposti da singole amministrazioni.

2. Aspetti procedurali

Diversi documenti del Garante e più di una circolare evidenziano da tempo la problematica e la circostanza, ribadita dal Codice, che le amministrazioni non possono avvalersi, nel caso di specie, di meri atti che, anche se denominati regolamenti, non hanno, anche per la loro eventuale rilevanza solo interna, la necessaria natura di fonte normativa suscettibile di incidere su diritti e libertà fondamentali di terzi (*Provv.* del 17 gennaio 2002[1], in *Boll.* n. 24, p. 40 e 16 giugno 1999[2], in *Boll.* n. 9, p. 19; *note* del Garante rivolte alla Presidenza del Consiglio dei ministri il 10 settembre 1999[3], il 10 novembre 2000[4] e il 3 maggio 2001[5], in *Boll.* n. 9, p. 31, n. 14-15, p. 26 e n. 20, p. 36).

Spetta ai soggetti pubblici che trattano i dati adottare l'atto di natura regolamentare, o avvalendosi dei poteri ad essi riconosciuti dall'ordinamento di riferimento, oppure promuovendo l'adozione di un regolamento da parte della competente amministrazione di riferimento la quale eserciti, ad esempio, poteri di indirizzo e controllo (*es.*: artt. 4 e 14 d.lg 30 marzo 2001 n. 165 e, a titolo esemplificativo, artt. 8 e ss. d.lg. 30 luglio 1999, n. 300 e 9 d.lg. 29 ottobre 1999, n. 419).

(1) [doc. *web* n. 1064681]

(2) [doc. *web* n. 42312]

(3) [doc. *web* n. 1091923]

(4) [doc. *web* n. 1087943]

(5) [doc. *web* n. 1076053]

Gli atti di natura regolamentare da adottare devono essere predisposti previa ricognizione attenta dei trattamenti di dati sensibili e giudiziari in fase di attuale trattamento o che si intende trattare in futuro.

Occorre poi tenere presente che potranno essere prese in considerazione nei regolamenti le sole finalità di rilevante interesse pubblico già individuate specificamente dal Codice o,

come quest'ultimo prevede, da un'espressa previsione di legge che, anche se collocata fuori del Codice, le evidenzi comunque puntualmente nei termini richiesti (art. 20 e Parte II del Codice).

La ricognizione, che presuppone il necessario coinvolgimento delle articolazioni interne del soggetto pubblico interessato, permette a quest'ultimo di effettuare anche un'ulteriore verifica circa la rispondenza dei trattamenti in corso con i principi del Codice oggi già direttamente applicabili (e ovviamente da rispettare anche in sede regolamentare), nonché di adeguare prontamente procedure in atto eventualmente non conformi a legge (principio di indispensabilità in rapporto alle finalità perseguite; verifiche periodiche dei vari requisiti dei dati –esattezza, aggiornamento, pertinenza, completezza, ecc.– e del loro rapporto con gli adempimenti da svolgere; scelta di modalità volte a prevenire violazioni di diritti e libertà fondamentali; raccolta dei dati sensibili e giudiziari di regola presso gli interessati; particolari cautele rispetto a dati riferiti a terzi non direttamente interessati ai compiti o adempimenti da svolgere; divieto di diffusione di dati sulla salute ecc.: *cfr.* art. 22 del Codice).

3. Il parere del Garante

Gli atti di natura regolamentare devono essere adottati, in ogni caso, in conformità al parere del Garante. Come accennato, il parere può essere espresso anche su schemi tipo, il che contribuisce a rendere più organiche le garanzie in riferimento ad altre amministrazioni e semplifica, inoltre, l'iter di approvazione degli atti.

Infatti, una volta espresso dal Garante il parere su uno schema tipo riguardante l'attività di soggetti pubblici che svolgono attività omogenee, lo schema di ciascun regolamento non deve essere sottoposto singolarmente a questa Autorità, sempreché il trattamento ipotizzato sia attinente e conforme allo schema tipo esaminato.

É invece necessario sottoporre al Garante uno schema di regolamento per uno specifico parere solo se:

a) manca uno schema tipo già esaminato dall'Autorità;
b) vi è uno schema tipo al quale l'amministrazione deve apportare modifiche sostanziali o integrazioni non formali che riguardano (a causa di ulteriori categorie di dati o di altre rilevanti operazioni di trattamento) casi in esso non considerati nello schema tipo.

Anche in questi due casi, il Garante è impegnato ad esprimere il parere nel termine di 45 gg. dal ricevimento della richiesta (o nei 20 gg. dal ricevimento degli elementi istruttori ricevuti dalle amministrazioni interessate), decorsi i quali, se non interviene un parere formale, il soggetto può adottare comunque il regolamento e proseguire poi il trattamento (art. 154, comma 5, del Codice).

4. Contenuto dell'atto regolamentare e pubblicità

In questa sede, Il Garante intende fornire alle amministrazioni che non potranno avvalersi di schemi tipo alcune prescrizioni di carattere generale per contribuire all'adozione di adeguate bozze di regolamento più attente ai profili sostanziali di tutela, più comprensibili da parte dei cittadini e non basate su approcci meramente formali alla tematica.

Questa particolare attenzione è ancor più necessaria se si tiene conto che, dal 1° gennaio 2006 non sarà lecito alcun trattamento dei dati sensibili e giudiziari che non sia disciplinato espressamente nei regolamenti.

Lo schema di regolamento deve contenere sinteticamente, ma in termini adeguati ed agevolmente comprensibili, le seguenti indicazioni specificate per categorie.

Dati indispensabili

Occorre individuare le tipologie di informazioni sensibili e giudiziarie che si devono necessariamente utilizzare in rapporto alle attività istituzionali svolte, avendo cura che a ciascun adempimento corrisponda il trattamento delle sole informazioni per ciò strettamente

indispensabili (art. 22, comma 3, del Codice). I dati vanno indicati solo per tipologie, evitando elencazioni eccessivamente sommarie.

Operazioni di trattamento indispensabili

Vanno parimenti individuate le operazioni che si devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico puntualmente individuate per legge, mettendo in particolare evidenza le operazioni che possono spiegare effetti maggiormente significativi per l'interessato e per le quali sono pertanto necessarie più garanzie. Anche in questo caso la descrizione è per tipologie, evitando indicazioni del tutto generiche circa l'impiego delle informazioni.

Tra tali operazioni rientrano, in particolare, quelle svolte pressoché interamente mediante siti web, o volte a definire in forma completamente automatizzata profili o personalità di interessati, le interconnessioni e i raffronti tra banche di dati gestite da diversi titolari, oppure con altre informazioni sensibili e giudiziarie detenute dal medesimo titolare del trattamento (art. 22, c. 9, 10 e 11, del Codice), nonché la comunicazione dei dati a terzi.

Si possono invece indicare più sinteticamente le operazioni "ordinarie" e più ricorrenti di trattamento (raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione ecc.).

Ulteriore contenuto dello schema di regolamento

É opportuno che il soggetto pubblico descriva sinteticamente, in termini comunicativi, anche la complessiva attività svolta, con particolare riguardo agli aspetti più incisivi per i diritti dei cittadini.

Non è quindi necessario scendere in eccessivi livelli di dettaglio non richiesti dal Codice; né è richiesta la riproduzione analitica delle disposizioni del Codice (in particolare, degli artt. 3, 11, 18-22, 85 s. e 95 s.).

Andrebbe altresì evitato di disciplinare situazioni già adeguatamente regolate sul piano legislativo e regolamentare quanto ai tipi di dati e di operazioni, come avviene nel caso dei dati personali trattati per effetto di un accesso a documenti amministrativi (artt. 59 e 60 del Codice; l. n. 241/1990 e successive modificazioni ed integrazioni).

Va inoltre rilevato in questa sede che la normativa sugli obblighi e compiti che rendono indispensabile utilizzare dati sensibili e giudiziari deve essere oggetto di un espresso riferimento nell'informativa da rendere agli interessati (art. 22, comma 2, del Codice). L'indicazione di tale normativa può essere quindi utile anche nell'ambito dello schema tipo, contribuendo ad evitare che il regolamento prenda erroneamente in considerazione attività che, pur essendo demandate al soggetto pubblico, non rientrano tra quelle che una fonte primaria non ha ritenuto di importanza tale da legittimare il trattamento di dati sensibili e giudiziari, in quanto non considerate "rilevanti finalità di interesse pubblico".

Da ultimo, tra le garanzie individuate dal Codice figura il diritto dei cittadini di conoscere con quali modalità sono utilizzate le predette informazioni che lo riguardano (art. 20, comma 2, del Codice).

Va pertanto prescritto ai soggetti pubblici interessati di intraprendere, in aggiunta alla pubblicità legale da assicurare agli atti regolamentari secondo i singoli ordinamenti, adeguate iniziative per assicurare idonea conoscibilità alle scelte adottate a proposito dei dati sensibili e giudiziari, utilizzando non solo i siti web istituzionali, ma anche le iniziative di comunicazione istituzionale cui essi sono tenuti.

Riservandosi di concludere rapidamente in separata sede i processi di collaborazione già avviati con alcuni organismi rappresentativi di soggetti pubblici, il Garante ritiene infine doveroso prescrivere in questa sede a tutti i soggetti pubblici interessati di adottare le predette misure, necessarie o, a seconda dei casi, opportune.

A tal fine, il Garante pone anche a disposizione dei soggetti pubblici, in allegato al pre-

sente provvedimento, un modello di riferimento per redigere gli schemi. Questo modello aggiorna quello già predisposto dal Garante il 17 gennaio 2002.

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive ai titolari di trattamenti di dati personali oggetto del presente provvedimento di adottare le misure necessarie ed opportune ivi indicate al fine di rendere i trattamenti medesimi conformi alle disposizioni vigenti;
b) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale*, ai sensi dell'art. 143, comma 2, del Codice.

Roma, 30 giugno 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

Art. ...
1. Il presente regolamento, in attuazione del Codice in materia di protezione dei dati personali (artt. 20, comma 2, e 21, comma 2, del decreto legislativo 30 giugno 2003, n. 196), identifica le tipologie di dati sensibili e di operazioni indispensabili a ... per perseguire le finalità di rilevante interesse pubblico espressamente individuate da apposita previsione di legge.

Art. ...
1. Ai sensi dell'art. 1, ... , per le finalità di ... tratta le seguenti tipologie di dati sensibili e giudiziari mediante i tipi di operazioni di seguito indicati.

INDICAZIONE DEL TRATTAMENTO E DESCRIZIONE RIASSUNTIVA DEL CONTESTO

Indicare sinteticamente il contesto in cui il trattamento è effettuato (*es.*: gestione del rapporto di lavoro del personale), descrivendo anche, con linguaggio chiaro e comunicativo, le caratteristiche principali del trattamento e del flusso informativo

FINALITÀ DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE

Indicare le finalità di rilevante interesse pubblico specificamente indicate dal Codice o da una norma di legge e il relativo riferimento normativo (*es.*, instaurare e gestire il rapporto di lavoro di qualunque tipo con il personale dipendente, anche a tempo parziale o temporaneo, nonché altre forme di lavoro non subordinato).

FONTE NORMATIVA

Indicare, se possibile, le fonti normative sull'attività istituzionale cui il trattamento è collegato (*es.*: artt. 2094-2134 del codice civile); legge n. 300/1970; d.lg. n. 165/2001; d.lg. n. 151/2001).

TIPI DI DATI TRATTATI *(barrare le caselle corrispondenti)*

❑ origine	O razziale	O etnica	
❑ convinzioni	O religiose	O filosofiche	O d'altro genere
❑ convinzioni	O politiche	O sindacali	
❑ stato di salute	O patologie attuali	O patologie pregresse	
	O terapie in corso	O anamnesi familiare	

❑ vita sessuale

❑ dati di carattere giudiziario (art. 4, comma1, lett. *e*), del Codice)?

OPERAZIONE ESEGUITE *(barrare le caselle corrispondenti)*

Particolari forme di trattamento

❑ Interconnessioni e raffronti di dati:

O con altre informazioni o banche dati dello stesso soggetto pubblico (*specificare quali ed indicarne i motivi*): ...

O con altri soggetti pubblici o privati (*specificare quali ed indicare la base normativa*): ...

❑ Trattamento automatizzato volto a definire il profilo o la personalità dell'interessato ai fini dell'adozione di un provvedimento amministrativo o giudiziario (*specificare quali ed indicarne i motivi o la base normativa*): ...

❑ Comunicazione ai seguenti soggetti per le seguenti finalità (i*ndicare l'eventuale base normativa*): ...

❑ Diffusione (*specificare l'ambito ed indicare l'eventuale base normativa*): ...

❑ Altre operazioni (*indicare eventuali altre operazioni effettuate sui dati, diverse da quelle sopra indicate*): ...

Altre tipologie più ricorrenti di trattamento

❑ Raccolta:	O presso gli interessati	O presso terzi
❑ Elaborazione:	O in forma cartacea	O con modalità informatizzate

Altre operazioni indispensabili rispetto alla finalità del trattamento e diverse da quelle "ordinarie" quali la registrazione, la conservazione, la cancellazione o il blocco nei casi previsti dalla legge (*specificare*): ...

43 Sicurezza presso il C.e.d. del Dipartimento della pubblica sicurezza 7 luglio 2005 (*)

Registro delle deliberazioni
n. 16 del 7 luglio 2005

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria e il Codice in materia di protezione dei dati personali (direttiva n. 95/46/Ce; d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

Premesso che ai trattamenti di dati personali effettuati in riferimento al Centro elaborazione dati (C.e.d.) del Dipartimento della pubblica sicurezza del Ministero dell'interno, di cui all'articolo 8 della legge 1° aprile 1981, n. 121, e successive modificazioni, si applicano le disposizioni del Codice in materia di protezione dei dati personali, anche in relazione alle misure di sicurezza da adottare (artt. 3, 11, 31, 33, 53 ss. del Codice);

Considerato che le disposizioni del Codice attuano anche la Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali, applicabile anche ai trattamenti sopra descritti, e della Raccomandazione R(87)15 del Consiglio d'Europa volta a disciplinare l'utilizzo dei dati a carattere personale nel settore della polizia, adottata il 17 settembre 1987, e che in base alla Dichiarazione relativa alla protezione dei dati firmata a margine dell'Accordo di Schengen il Governo italiano ha assunto il formale impegno ad introdurre le disposizioni nazionali necessarie ad assicurare, nel predetto settore, un livello di protezione dei dati almeno uguale a quello indicato nei predetti atti internazionali, per poter applicare il predetto Accordo e la relativa Convenzione di applicazione;

Considerato che le vigenti disposizioni concernenti le procedure di raccolta, di accesso, di comunicazione e di correzione dei dati registrati nel predetto C.e.d., nonché le relative misure di sicurezza contenute nel regolamento approvato con d.P.R. 3 maggio 1982, n. 378, devono essere rese pienamente conformi ai principi e alle regole del Codice, in particolare per quanto riguarda l'aggiornamento dei dati, la loro conservazione e gli standard di sicurezza;

Considerato che l'articolo 57 del Codice prevede che, con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, devono essere individuate le modalità di attuazione dei principi del Codice in relazione al trattamento dei dati effettuato dal predetto C.e.d., anche al fine di integrare e modificare il predetto d.P.R. 3 maggio 1982 n. 378, in attuazione della citata Raccomandazione R(87)15 del Consiglio d'Europa, anche sotto il profilo dell'aggiornamento e dell'efficacia delle misure di sicurezza;

(*) [doc. *web* n. 1170253]

Ritenuto di dover, allo stato, prescrivere al Ministero dell'interno, ai sensi dell'articolo 154, comma 1, lett. *c*), del Codice, di adottare ogni opportuna misura volta ad incrementare i livelli di sicurezza nel trattamento dei dati, anche mediante accelerazione dell'iter per l'adozione, su proposta del medesimo Ministero, del predetto regolamento previsto dall'articolo 57 del Codice;

TUTTO CIÒ PREMESSO E CONSIDERATO IL GARANTE:

ai sensi dell'articolo 154, comma 1, lett. *c*), del Codice prescrive al Ministero dell'interno di adottare ogni opportuna misura volta ad incrementare i livelli di sicurezza nel trattamento dei dati, anche mediante accelerazione dell'iter per l'adozione del regolamento previsto dall'articolo 57 del Codice.

Roma, 7 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

44 Elenchi telefonici: semplificate le procedure per i "categorici" 14 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan, del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 129, comma 2, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) che, in attuazione della disciplina comunitaria e in particolare della direttiva comunitaria n. 2002/58/Ce, ha individuato nella "mera ricerca dell'abbonato per comunicazioni interpersonali" la finalità primaria degli elenchi telefonici;

Visto il provvedimento del 23 maggio 2002[1] e del 15 luglio 2004[2] con il quale questa Autorità ha segnalato e prescritto a tutti gli operatori le garanzie necessarie per trattare dati personali al fine di formare i nuovi elenchi telefonici e prestare i servizi di informazione all'utenza;

Viste le note pervenute da vari soggetti che intendono pubblicare elenchi telefonici organizzati per categorie merceologiche/professionali (*cd.* elenchi "categorici"), con le quali è stato chiesto al Garante di fornire un chiarimento in ordine all'applicabilità o meno a tali elenchi categorici della disciplina contenuta nell'art. 129 del Codice, nonché delle prescrizioni riportate nei predetti provvedimenti dell'Autorità del 23 maggio 2002 e del 15 luglio 2004;

Considerata la particolare complessità ed onerosità delle procedure necessarie per adempiere all'obbligo di informativa (art. 13 del Codice) in relazione ai dati raccolti presso terzi concernenti tutti gli interessati che verranno inseriti negli elenchi *cd.* categorici, e rilevato che l'informativa resa in questo caso secondo le ordinarie modalità comporterebbe un impiego di mezzi manifestamente sproporzionati rispetto al diritto tutelato (art. 13, comma 5, lett. *c*), del Codice), visto anche il numero particolarmente elevato di interessati, in particolare di soggetti imprenditoriali e di liberi rofessionisti, che dovrebbero essere altrimenti informati singolarmente;

Ritenuta la necessità di prescrivere ai titolari del trattamento interessati in quanto editori di elenchi categorici, ai sensi degli artt. 154, comma 1, lett. *c*) e 13, commi 4 e 5, lett. *c*) del Codice, le misure che devono essere da essi adottate con particolare riferimento, rispettivamente, alle modalità di acquisizione ed inserimento dei dati personali e all'informativa;

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

Relatore il dott. Giuseppe Fortunato;

PREMESSO CHE:

- gli elenchi "categorici" hanno carattere commerciale e promozionale, contenendo varie informazioni relative allo svolgimento delle attività economiche ed equiparate dei soggetti interessati, in particolare aziende, professionisti, esercizi commerciali ed enti;
- le specifiche finalità di tali elenchi non sono interamente riconducibili a quelle degli elenchi "alfabetici" del servizio universale contenenti i dati degli abbonati ai servizi di telefonia fissa e mobile, il cui scopo, secondo quanto previsto dalla nuova disciplina in fase di attuazione, è invece quello di consentire la "mera ricerca del-

(*) [doc. *web* n. 1151640]

(1) [doc. *web* n. 1032397]

(2) [doc. *web* n. 1032381]

l'abbonato per comunicazioni interpersonali" (art. 129, comma 2, del Codice);

- agli elenchi "categorici" non si applicano, quindi, le prescrizioni contenute nel provvedimento adottato dal Garante il 15 luglio 2004 ai sensi dell'art. 129 del Codice, e che per la loro formazione i soggetti che trattano i dati destinati a figurare nei medesimi elenchi possono utilmente applicare, in conformità alle prescrizioni di legge, la previsione di carattere generale che permette di prescindere dal consenso dei soggetti interessati in quanto il trattamento "riguarda dati relativi allo svolgimento di attività economiche" (art. 24, comma 1, lett. *d*), del Codice);
- la pubblicazione degli elenchi "categorici" deve comunque rispettare gli altri obblighi e diritti in materia di protezione dei dati personali;
- tale rispetto deve riguardare anche: a) la necessaria completezza dei dati relativi ad interessati compresi nelle categorie che verranno riportate, a seconda dei casi, nelle distinte tipologie di elenchi pubblicati; b) la necessità che gli elenchi "categorici", ove formati attingendo alla base di dati unica di cui all'allegato II del predetto provvedimento del 15 luglio 2004, non comprendano gli estremi identificativi di soggetti che abbiano eventualmente chiesto di non figurare nei predetti elenchi "alfabetici" (essendosi anche avvalsi del modello di informativa di cui all'allegato IV del medesimo provvedimento o, comunque, in altra forma), fermo restando che tale esclusione non fa venir meno il predetto requisito della completezza;
- l'art. 13, comma 5, del Codice prevede che il Garante, con esclusivo riferimento al caso in cui i dati siano raccolti presso terzi, anziché presso i diretti interessati, può disporre l'"esonero" in tutto o in parte dall'obbligo dell'informativa o altra soluzione equipollente, qualora l'informativa con modalità ordinarie comporterebbe un impiego di mezzi che il Garante dichiari manifestamente sproporzionato rispetto al diritto tutelato; rilevato che tale manifesta sproporzione può essere ravvisata dal Garante sia caso per caso, sia, come rilevato con deliberazione del 26 novembre 1998[1] (pubblicata nel *Bollettino* ufficiale del Garante "Cittadini e Società dell'Informazione", 1998, anno II, n. 6, p. 81), "in riferimento a settori o tipi di trattamento";
- ritenuto che, in base agli atti acquisiti, la singola informativa da parte di ciascun titolare comporterebbe un impiego di mezzi sproporzionato rispetto al diritto tutelato (art. 13, comma 5, del Codice), stanti, nel caso di specie, le varie operazioni di distinti soggetti che dovrebbero effettuare, con riferimento a più interessati, informative aventi caratteristiche omogenee;
- è tuttavia necessario assicurare un'informativa generale comunque adeguata, prescrivendo in questa sede ai soggetti interessati una misura appropriata ai sensi del medesimo art. 13, comma 5, consistente nelle informative di cui al seguente dispositivo;

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive ai titolari del trattamento di dati personali connessi all'edizione e pubblicazione di elenchi categorici di conformare il medesimo trattamento agli obblighi e ai diritti richiamati in motivazione, in particolare per quanto riguarda: 1) la necessaria completezza dei dati relativi ad interessati compresi nelle categorie che verranno riportate, a seconda dei casi, nelle distinte tipologie di elenchi pubblicati; 2) la necessità che gli elenchi "categorici", ove formati attingendo alla base di dati unica di cui all'allegato II del predetto provvedimento del 15 luglio 2004, non comprendano gli estremi identificativi di soggetti che abbiano eventualmente chiesto di non figurare nei predetti elenchi "alfabetici", essendosi anche avvalsi del modello di informativa di cui all'allegato IV del medesimo provvedimento o, comunque, in altra forma;

b) ai sensi dell'art. 13, commi 4 e 5, lett. *c*), del Codice autorizza ciascun titolare del trattamento di dati personali connessi all'edizione e pubblicazione di elenchi categorici, in relazione al caso in cui i dati personali siano raccolti non dall'interessato, ma presso terzi, anche in caso di estrazione dei dati dalla base di dati unica di cui all'allegato II al provvedimento del Garante del 15 luglio 2004, ad effettuare l'informativa prevista dal medesimo art. 13, comma 1, mediante pubblicazione di almeno un avviso da pubblicarsi, a

(1) [doc. *web* n. 39624]

cura di ciascun titolare, nei mesi di settembre e ottobre 2005, su almeno tre quotidiani ad ampia diffusione nazionale e con dimensioni non inferiori a 1/4 di pagina, con tenore e modalità che la rendano facilmente leggibile. L'informativa -da trasmettere a questa Autorità allegando copia dell'inserzione- dovrà altresì figurare in una chiara avvertenza inserita, con evidenza, nella parte iniziale dell'elenco categorico cartaceo, oppure pubblicato con modalità elettroniche. In entrambi i casi, l'informativa dovrà comprendere, oltre che agli elementi indicati all'art. 13 del Codice, un riferimento alla disciplina applicabile agli elenchi categorici, nonché alle peculiari garanzie operanti, anche per gli elenchi categorici, in caso di comunicazioni di carattere commerciale nei modi di cui all'art. 130 del Codice (uso di sistemi automatizzati di chiamata; posta elettronica; *telefax*, messaggi del tipo *Mms* o *Sms* o di altro tipo).

Roma, 14 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

45 Ricette mediche, tessera sanitaria e monitoraggio della spesa 21 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la richiesta di parere del Ministro dell'economia e delle finanze;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali e, in particolare, la direttiva n. 95/46/Ce del 24 ottobre 1995;

Visto l'articolo 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visto l'articolo 50, comma 10, del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, in materia di monitoraggio della spesa nel settore sanitario;

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO:

Nel quadro della problematica riguardante il monitoraggio della spesa sanitaria lo schema di decreto in esame, trasmesso dal Ministro dell'economia e delle finanze per il prescritto parere, concerne il particolare profilo dell'approvazione del protocollo riguardante i dati rilevati dalle ricette mediche (e comunicati, per il tramite del medesimo Ministero, al Ministero della salute e alle regioni), nonché le modalità della loro trasmissione.

OSSERVA:

Lo schema precisa, nel preambolo, che i dati in questione, utilizzati dal Ministero dell'economia e delle finanze ai soli fini di liquidazione provvisoria dei rimborsi dovuti alle strutture di erogazione dei servizi sanitari, possono essere trattati dal medesimo Ministero "per scopi statistici ed altri compiti istituzionali solo in forma anonima, eliminato ogni riferimento ad informazioni che rendono identificabili gli interessati, come il codice fiscale, il codice a barre della tessera sanitaria e il numero progressivo regionale delle ricette".

In coerenza con tale precisazione, lo schema aggiornato di decreto prevede che i dati trasmessi dal Ministero dell'economia e delle finanze al Ministero della salute, all'Agenzia italiana del farmaco (Aifa) e alle regioni abbiano le stesse caratteristiche di anonimato di quelli detenuti e comunicati dal medesimo Ministero (dati anonimi, privi di ogni riferimento ad informazioni che rendono identificabili gli interessati, quali il codice fiscale e il codice a barre della tessera sanitaria).

Conseguenti precisazioni sono state opportunamente apportate nel disciplinare tecnico allegato allo schema di decreto.

(*) [doc. *web* n. 1152167]

Le previsioni dello schema di decreto risultano in linea con le finalità statistiche dell'utilizzo di tali dati da parte delle amministrazioni destinatarie della comunicazione del Ministero dell'economia e delle finanze, fermo restando che le aziende sanitarie locali e le altre strutture sanitarie autorizzate potranno utilizzare le informazioni per lo svolgimento, in conformità alla legge, delle proprie attività istituzionali, ivi compresa la verifica di appropriatezza delle prescrizioni sanitarie.

Ciò premesso, il Garante esprime parere favorevole sullo schema di decreto.

TUTTO CIÒ PREMESSO IL GARANTE:

esprime parere favorevole sullo schema di decreto.

Roma, 21 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

46 Uso delle impronte digitali per i sistemi di rilevamento delle presenze nei luoghi di lavoro 21 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata da Landini S.p.A. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa al trattamento di dati personali biometrici al fine di verificare le presenze sul luogo di lavoro dei dipendenti;

Visti gli elementi acquisiti a seguito degli accertamenti avviati ai sensi dell'art. 154, comma 1, lettere a), del Codice;

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

Relatore il dott. Mauro Paissan;

PREMESSO:

1. Trattamento di dati personali biometrici nel rapporto di lavoro con finalità di verifica della presenza dei dipendenti

Landini S.p.A., industria di coperture in fibrocemento e metalliche che occupa circa trecento dipendenti, ha presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici dei propri dipendenti finalizzato ad accertarne la presenza sul luogo di lavoro e commisurare, così, la retribuzione ordinaria e straordinaria da corrispondere.

Il funzionamento di questo sistema presuppone una fase di raccolta di dati biometrici (*cd. enrollment*) nella quale la società, avvalendosi di apparecchiature elettroniche dotate di lettore di impronte digitali e di apposito *software*, trasformerebbe l'immagine di una porzione dell'impronta digitale dei lavoratori in un codice numerico, associandolo a ciascun lavoratore con la sua memorizzazione nel sistema informativo aziendale (senza sottoporlo a cifratura o ad altre tecniche equivalenti). Tale codice verrebbe utilizzato quale termine di paragone dei codici numerici ricavati dalla lettura delle (parti di) impronte digitali dei lavoratori, rilevate, in occasione di ciascun ingresso e uscita dal luogo di lavoro, attraverso lettori dislocati in diverse aree dell'azienda e connessi al relativo sistema informativo.

Il trattamento dei dati biometrici non perseguirebbe altra finalità che quella ora descritta. Stando alle dichiarazioni rese dalla società titolare del trattamento (e dal produttore del sistema), una volta terminata la fase di enrollment, non vi sarebbe ulteriore memorizzazione dell'impronta digitale. Ad avviso della società, non sarebbe possibile, inoltre, risalire all'impronta stessa a partire dal codice numerico generato.

Il trattamento di dati biometrici viene giustificato dall'esigenza di prevenire alcune condotte, anche abusive, da parte di alcuni dipendenti (consistenti nello scambio dei *badge*) e lo smarrimento delle tessere magnetiche attualmente in uso; viene quindi ritenuto che il trattamento dei dati biometrici consentirebbe di ovviare a tali inconvenienti, assicurando un grado elevato di certezza nell'identificazione dei lavoratori.

(*) [doc. *web* nn. 1150679, vers. EN 1166892]

Stando alle dichiarazioni rese, verrebbe comunque assicurato ai lavoratori che siano impossibilitati a partecipare all'enrollment (in ragione delle proprie caratteristiche fisiche) o che non intendano acconsentire al trattamento, di attestare la propria presenza sul luogo di lavoro mediante l'apposizione della propria sottoscrizione in un registro delle presenze ubicato presso l'ufficio del personale con riconoscimento "a vista" o, ancora, ricorrendo ad altri "sistemi convenzionali".

2. Trattamento di dati biometrici e applicabilità della disciplina di protezione dei dati personali

Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali.

I dati biometrici che verrebbero rilevati nel caso di specie (porzione dell'impronta digitale) sono informazioni ricavate dalle caratteristiche fisiche di interessati che si vorrebbero identificare in modo univoco, mediante un modello di riferimento (*template*). Quest'ultimo consiste nell'insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.

Sia le impronte dattiloscopiche (*cfr. Provv.* Garante 19 novembre 1999[1], in *Boll.* n. 10, p. 68), ancorché raccolte in modo parziale e solo ai fini del completamento della fase dell'enrollment, sia i codici numerici successivamente utilizzati per le descritte operazioni di confronto, in quanto informazioni riferibili ai singoli lavoratori, sono dati personali (art. 4, comma 1, lett. *b*), del Codice). Ne discende, pertanto, l'applicazione della disciplina contenuta nel Codice, così nella fase dell'enrollment, come pure in relazione alle successive operazioni di confronto (con il correlato tracciamento degli orari di ingresso/uscita dal luogo di lavoro).

3. Qualità dei dati, misure di sicurezza e informativa rispetto al trattamento dei dati biometrici

Con riguardo al principio di qualità dei dati, dall'istruttoria svolta emergono perplessità in ordine al corretto funzionamento del sistema che si intende installare.

Allo stato, non risultano documentati i presupposti per un elevato grado di affidabilità del sistema medesimo, tanto che è stata programmata una fase di prova per testarne l'affidabilità. La società non è inoltre in grado, al momento, di indicare il livello della sua accuratezza ricorrendo ai parametri tecnici idonei ad individuare i "falsi negativi" (Frr-*False Rejection Rate*) e i "falsi positivi" (Far-*False Acception Rate*). I sistemi di rilevazione di dati come quelli in esame devono invece offrire una rigorosa garanzia di affidabilità ed integrità dei dati, anche sulla base di certificazioni od omologazioni dei dispositivi che tengano eventualmente conto delle valutazioni di comitati tecnici indipendenti.

Inoltre, dagli elementi forniti non è possibile ricavare con certezza se siano adeguate le misure di sicurezza predisposte a protezione della rete di comunicazione elettronica sulla quale i dati biometrici sono trasmessi dai singoli lettori al sistema centralizzato di acquisizione dati. A tale proposito, una misura opportuna da parte del titolare del trattamento consisterebbe ad esempio nell'utilizzo di chiavi di cifratura dei dati biometrici, indicato anche a livello europeo (*v., ad es.*, il *Documento di lavoro sulla biometria* del Gruppo per la tutela dei dati personali di cui all'art. 29 della direttiva n. 95/46/Ce del 1° Agosto 2003 (punto 3.6), in *http://europa.eu.int/...pdf*).

Anche l'informativa predisposta non risulta adeguata rispetto al trattamento che si intende porre in essere: come detto, dalle dichiarazioni acquisite emerge che, i lavoratori sarebbero liberi di aderire o meno al sistema di rilevazione delle presenze basato sull'utilizzo di dati biometrici; strumenti alternativi sarebbero previsti anche per i lavoratori impossibilitati, per ragioni fisiche, a registrare le presenze mediante l'impiego del sistema bometrico.

(1) [doc. *web* n. 42058]

Tali dichiarazioni, però, non trovano conferma nell'informativa predisposta per gli interessati, secondo la quale il conferimento dei dati, ivi compresi i dati biometrici (espressamente richiamati sotto la voce *"ulteriori specificazioni particolari"*), avrebbe natura obbligatoria. Ciò, ha rilievo anche per la circostanza che il sistema potrebbe operare (con riguardo all'enrollment e ai successivi accessi nei luoghi di lavoro) solo con l'attiva collaborazione personale dei lavoratori interessati, i quali dovrebbero rendersi così disponibili –in assenza di una disposizione di legge che lo imponga ed impregiudicati i profili eventualmente connessi al coinvolgimento delle rappresentanze sindacali– a sottoporre una parte del proprio corpo alle operazioni necessarie per la rilevazione biometrica.

Manca, inoltre, nell'informativa ogni riferimento a tecniche alternative per la rilevazione delle presenze, contravvenendosi, così, all'art. 13 del Codice secondo il quale è necessario che le informazioni da rendere agli interessati enuncino chiaramente tutte le modalità impiegate nel trattamento e la tipologia di dati personali utilizzati per ciascuna di esse.

4. Dati biometrici e principi di protezione dei dati personali: finalità, necessità e pertinenza

Se le ragioni illustrate denotano più di un rilievo in ordine al sistema di rilevazione in esame, la sua liceità deve essere verificata altresì, sotto altri profili concernenti i principi di necessità, proporzionalità, finalità e correttezza, nonché di qualità dei dati (artt. 3 e 11 del Codice; art. 6, direttiva n. 95/46/Ce).

A questo proposito, se pure rientra tra le legittime facoltà del datore di lavoro sovrintendere all'esecuzione della prestazione lavorativa (art. 2094 c.c.) verificando le presenze dei dipendenti e il rispetto dell'orario di lavoro anche ai fini del calcolo della retribuzione, ad esempio attraverso badge, non risulta documentato che il trattamento di dati biometrici in esame (con particolare riguardo all'impronta digitale) sia conforme ai principi di necessità e proporzionalità.

L'utilizzo di tali dati in luoghi di lavoro può essere giustificato in casi particolari, in relazione alle finalità e al contesto in cui essi sono trattati (ad esempio, accessi a particolari aree dell'azienda per le quali debbano essere adottati livelli di sicurezza particolarmente elevati in ragione di specifiche circostanze o attività ivi svolte), oppure per finalità di sicurezza del trattamento di dati personali (*v.* Allegato B) al Codice).

Non può invece ritenersi lecito un uso generalizzato e incontrollato dei medesimi dati, specie se si tratta di impronte digitali per le quali occorre anche prevenire eventuali utilizzi impropri e possibili abusi.

Considerata l'utilizzabilità di idonee modalità alternative per un accertamento parimenti rigoroso dell'identità personale, ma meno problematiche per la dignità stessa dei lavoratori interessati (art. 2 del Codice, modalità di cui non è stata rappresentata l'inefficacia nel caso di specie), l'illustrata finalità di computo dell'orario di lavoro in un'azienda come quella istante non risulta, dagli atti, legittimare la rilevazione di impronte digitali le quali sono comunque associate, contrariamente a quanto rilevato dall'istante, ai relativi interessati.

Al di là dei controlli ordinari e a campione circa la presenza dei lavoratori alle uscite e nei luoghi di lavoro, peraltro di agevole accertamento, non è stata dimostrata l'inefficacia, nel caso di specie, di misure che (senza ricorrere al trattamento di dati biometrici, nel rispetto dell'art. 3 del Codice) possono comunque contenere significativamente il rischio di pratiche abusive.

Il titolare del trattamento, per verificare la puntuale osservanza dell'orario di lavoro da parte dei lavoratori, impedendo in pari tempo condotte abusive dei medesimi, può disporre di altri sistemi meno invasivi della sfera personale, della libertà individuale e che non coinvolgano il corpo del lavoratore –aspetti entrambi costitutivi della dignità personale, a presidio della quale sono dettate le discipline di protezione dei dati personali (art. 2 del Codice)–.

Il trattamento in esame deve ritenersi sproporzionato anche in considerazione delle

modalità tecniche prefigurate (centralizzazione dei codici identificativi derivati dall'esame del dato biometrico), ben potendosi adottare, anche da questo punto di vista, misure tecnologiche meno invasive. Infatti, anche a mente della disposizione contenuta nell'art. 3 del Codice, è da ritenere comunque preferibile, laddove sia ammesso il ricorso a dati biometrici, la memorizzazione del codice identificativo su un supporto che resti nell'esclusiva disponibilità dell'interessato (una volta completato il *cd. enrollment*), piuttosto che la registrazione dello stesso a livello centralizzato nel sistema informativo aziendale (con conseguenti più gravi ripercussioni per i diritti individuali in caso di violazione delle misure di sicurezza, di accessi di persone non autorizzate o, comunque, di abuso delle informazioni memorizzate, anche ad opera di terzi).

In conformità con il quadro comunitario (il quale prescrive, non a caso, che i trattamenti di dati che comportano rischi specifici per i diritti e le libertà fondamentali degli interessati, come quello in esame, siano consentiti solo in presenza di una verifica preliminare volta ad appurare la liceità e correttezza del trattamento e ad impartire misure ed accorgimenti a garanzia degli interessati: art. 20 direttiva n. 95/46/Ce; art. 17 del Codice), deve pertanto riscontrarsi l'assenza nel caso di specie nei presupposti di legge per un trattamento di dati corrispondenti ad impronte digitali.

In conclusione, il trattamento oggetto di richiesta non può ritenersi lecito, nei termini di cui in motivazione.

TUTTO CIÒ PREMESSO, IL GARANTE:

ai sensi e per gli effetti di cui agli artt. 3, 11, 17 e 154, comma 1, lett. *d*) del Codice dichiara che il trattamento che Landini S.p.A. intenderebbe effettuare non risulta lecito, nei termini di cui in motivazione, e ne vieta pertanto lo svolgimento se effettuato per le finalità e con le modalità ivi descritte.

Roma, 21 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

47 Portfolio: garanzie nei processi formativi degli alunni 26 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali (direttiva n. 95/46/Ce), anche in relazione agli articoli 2, 10, 11 e 33 della Costituzione;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visto il d.lg. 19 aprile 2004, n. 59 (Definizione delle norme generali relative alla scuola dell'infanzia e al primo ciclo dell'istruzione, a norma dell'art. 1 della l. 28 marzo 2003, n. 53);

Vista la documentazione in atti;

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

Relatore il dott. Mauro Paissan;

CONSIDERATO:

1. Premessa

La riforma della scuola dell'infanzia e del primo ciclo di istruzione -scuola primaria e scuola secondaria di primo grado- ha introdotto la redazione di un documento di valutazione ed orientamento, denominato "Portfolio (o cartella) delle competenze individuali", da redigere singolarmente per ciascun alunno.

Il Portfolio documenta nei predetti cicli di istruzione i processi formativi degli alunni e ne accompagna in tali ambiti il percorso scolastico illustrando in un unico contesto, come strumento didattico, la formazione, l'orientamento e i progressi educativi.

La normativa di riferimento (d.lg. 19 aprile 2004, n. 59) prevede a tal fine una documentazione sistematica anche degli elaborati degli alunni, volta a comprendere ed interpretare i loro interessi, le attitudini, i comportamenti e le aspirazioni personali.

Il Portfolio è compilato e aggiornato (nella scuola d'infanzia) dai docenti di sezione, ovvero (nella scuola primaria e secondaria di primo grado) dal docente coordinatore-tutor dell'alunno in collaborazione con altri docenti, alunni e loro genitori, i quali possono apportarvi alcune annotazioni (allegati A, B) e C) del citato decreto).

Il Garante ha ricevuto reclami e segnalazioni di genitori di alunni che lamentano possibili violazioni della riservatezza derivanti dalle modalità con cui istituti scolastici pubblici e privati trattano dati di carattere personale in relazione al Portfolio.

Rispondendo alla richiesta dell'Autorità (nota del 31 maggio 2005), il Ministero dell'istruzione, dell'università e della ricerca-Dipartimento per l'istruzione (lettera del 20 giugno 2005) ha fornito alcune informazioni.

Il Ministero ha anche convenuto sulla necessità di raccogliere nel Portfolio "dati perso-

(*) *G.U.* 8 agosto 2005, n. 183
[doc. *web* n. 1155253]

nali esclusivamente se pertinenti e non eccedenti e, nel caso dei dati sensibili, solamente se indispensabili per la valutazione e l'orientamento dell'alunno"; si è poi dichiarato disponibile ad inviare una nota esplicativa da far pervenire, tramite gli uffici scolastici regionali, a tutte le istituzioni scolastiche, affinché queste si conformino al Codice in materia di protezione dei dati personali nella compilazione e gestione del Portfolio.

A conclusione dell'esame preliminare dei reclami e delle segnalazioni, il Garante ritiene necessario prescrivere a tutti gli istituti scolastici di adottare alcune misure volte a favorire il rispetto dei diritti e delle libertà fondamentali dei cittadini, nonché della loro dignità, con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali (art. 2, comma 1, del Codice), considerata la quantità, la varietà e la delicatezza delle informazioni che possono essere inserite nel Portfolio e l'ingente numero dei minori e familiari interessati.

2. Le principali questioni

Le problematiche rappresentate al Garante riguardano la liceità e la correttezza del trattamento dei dati personali confluenti nel Portfolio, relativi al percorso scolastico e alla vita privata e sociale degli alunni.

Non è previsto, a livello nazionale, un modello tipo di Portfolio sul piano della forma e dei contenuti in dettaglio del documento.

Ciò determina la proliferazione di documenti molto diversi da scuola a scuola, come dimostrano alcuni modelli già esaminati dal Garante, nei quali è richiesto l'inserimento di tipologie di dati personali assai differenti (o è possibile inserirli o chiedere il loro inserimento) e nei quali l'alunno può illustrare rapporti interpersonali di natura privata e vicende familiari.

Dalle risposte fornite ad alcune delle domande proposte nei modelli esaminati (quali, ad esempio, l'indicazione dell'utilizzo della lingua madre solo nel paese di origine, la motivazione alla base di un trasferimento, anche di nazione, del bambino, la descrizione di particolari vicende che hanno caratterizzato il periodo post-natale), possono evincersi informazioni particolarmente delicate come lo stato di adozione di un minore, nei confronti delle quali l'ordinamento impone precise cautele (l. 4 maggio 1983, n. 184, in particolare art. 28).

In alcuni casi, sono richieste informazioni relative al profilo psicologico dell'alunno (descrizione di paure o disagi del minore), al suo stato di salute (notizie su particolari patologie sofferte, eventuali ricoveri ospedalieri), al suo credo religioso, all'ambiente sociale di estrazione (acquisizione di informazioni sui suoi familiari) e ad altri delicati aspetti della sfera privata e a quella di natura strettamente familiare.

La diversità dei modelli di Portfolio agevola, quindi, una più ampia annotazione di informazioni sensibili (che il Codice individua nei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale: art. 4, comma 1, lett. *d*), del Codice).

3. Come trattare i dati personali

La compilazione e la tenuta del Portfolio determina un trattamento di dati personali. L'istituto scolastico frequentato dall'alunno ne è il titolare, stante l'autonomia funzionale, didattica, organizzativa e di ricerca, sperimentazione e sviluppo ad esso riconosciuta (artt. 4, comma 1, lett. *f*) e 28 del Codice; d.P.R. 8 marzo 1999, n. 275).

Tale trattamento deve rispettare le disposizioni del Codice e, in particolare, i principi di seguito richiamati. In caso di loro violazione, i dati personali trattati non possono essere utilizzati (art. 11, comma 2, del Codice).

Principio di finalità (art. 11, comma 1, lett. *b*), del Codice)

Il trattamento di dati personali effettuato mediante il Portfolio è consentito solo per raggiungere le finalità individuate direttamente dalla predetta legislazione di riforma (d.lg. n. 59/2004 cit.), ovvero per valutare l'apprendimento e il comportamento degli studenti e per certificare le competenze da essi acquisite.

Non sono perseguibili ulteriori finalità attinenti, ad esempio, all'individuazione del profilo psicologico degli alunni o alla raccolta di informazioni sul loro ambiente sociale e culturale di provenienza.

Principio di necessità (art. 3 del Codice)

Laddove le finalità del Portfolio possono essere perseguite anche senza trattare dati personali, oppure dati identificativi, il trattamento deve riguardare solo dati anonimi (che non riguardano, cioè, interessati identificati o identificabili), oppure, rispettivamente, dati non identificativi (che permettono, cioè, di identificare direttamente un interessato).

Principio di proporzionalità (art. 11, comma 1, lett. *d*), del Codice)

Quando, osservando il principio di necessità, si devono trattare dati personali, deve verificarsi in ogni singola fase del loro trattamento se, e come, determinate operazioni (di raccolta, esame, annotazione, eventuale registrazione, ecc.) siano effettivamente pertinenti e non eccedenti rispetto alla finalità di valutazione dell'alunno.

Principio di indispensabilità (art. 22, comma 3; aut. gen. nn. 2/2004 e 3/ 2004)

Particolare rigore deve essere osservato per quanto riguarda l'eventuale raccolta e registrazione di dati sensibili, i quali sono acquisibili, attraverso una valutazione obiettiva e selettiva, solo se realmente indispensabili per valutare il processo formativo.

4. Prescrizioni da osservare

Con il presente provvedimento, a garanzia degli interessati, il Garante prescrive ai titolari del trattamento di osservare, in attuazione dei predetti principi, anche le seguenti misure volte a conformare pienamente i trattamenti alle vigenti disposizioni in materia di protezione dei dati personali (art. 154, comma 1, lett. *c*), del Codice), invitando il Ministero dell'istruzione, dell'università e della ricerca a recepire le prescrizioni medesime nella nota esplicativa che lo stesso si è riservato di far pervenire, tramite gli uffici scolastici regionali, a tutti gli istituti scolastici.

Ciascun istituto scolastico, in qualità di titolare del trattamento, deve attuare le seguenti misure:

Predisposizione del modello di Portfolio

Nel predisporre il modello di Portfolio, occorre adottare ogni opportuna soluzione per prevenire che vengano raccolti dati sensibili o che sono oggetto, nell'ordinamento, di particolari cautele (*es.*, dati relativi allo stato di affidamento o di adozione), quando gli stessi non siano strettamente indispensabili per raggiungere le finalità di documentazione perseguite. Ciò, con particolare riferimento ai campi nei quali l'alunno potrebbe descrivere alcuni suoi rapporti interpersonali di natura privata o vicende familiari. I riferimenti a tali vicende sono del tutto eventuali nel Portfolio, che deve rimanere uno strumento didattico per favorire solo la personalizzazione dei processi formativi scolastici.

Informare gli interessati

Prima di consentire la compilazione del Portfolio, chi esercita la potestà sull'alunno deve essere informato specificamente in merito al trattamento dei dati personali.

Nell'informativa occorre indicare gli elementi previsti dall'art. 13 del Codice e, in particolare, quali sono le finalità perseguite, se è necessario o facoltativo conferire i dati di natura personale, quali sono le conseguenze di un eventuale rifiuto a fornirli, quali soggetti possono consultare il Portfolio e per quali scopi.

Istruzioni per la compilazione

L'istituto deve impartire idonee istruzioni ai docenti che sovraintendono alla compilazione del Portfolio, affinché adottino particolari cautele nel momento in cui inseriscono o

consentono di inserire dati personali, in particolare quelli particolarmente delicati o sensibili sopra evidenziati.

Presupposti per inserire dati sensibili

Per quanto riguarda i dati sensibili, alcuni presupposti giuridici per trattare i dati sono diversi a seconda che l'istituto scolastico sia di natura privata o pubblica.

Le istituzioni scolastiche private devono acquisire il consenso specifico, preventivo e scritto da parte degli esercenti la potestà; devono poi rispettare le prescrizioni contenute nelle autorizzazioni generali del Garante al trattamento dei dati sensibili (art. 26 del Codice e autorizzazioni nn. 2[1] e 3[2] del 2004, rinvenibili anche sul sito *www.garanteprivacy.it*, efficaci sino al 31 dicembre 2005).

Le istituzioni scolastiche pubbliche non devono richiedere il consenso; devono invece indicare nell'atto di natura regolamentare che deve essere adottato entro il 31 dicembre 2005, in conformità al parere del Garante, i tipi di dati trattabili e le operazioni eseguibili in relazione alla tematica in esame (artt. 20 e 154 del Codice, *cfr. Provv.* Garante del 30 giugno 2005[3]). Mancando un potere regolamentare in capo ai singoli istituti scolastici, e in relazione ai compiti attribuiti al Ministero (art. 75 l. 30 luglio 1999, n. 300), l'Autorità ha rivolto a quest'ultimo l'invito ad adottare uno schema di regolamento per il trattamento dei dati sensibili effettuato da parte di tutti gli istituti scolastici pubblici, da sottoporre al parere del Garante.

Designare gli incaricati

L'istituto deve designare i soggetti che possono accedere ai dati contenuti nel Portfolio quali incaricati o, eventualmente, responsabili del trattamento (artt. 30 e 29 del Codice).

Sicurezza dei dati

Occorre garantire che il trattamento dei dati in questione avvenga nel pieno rispetto delle misure di sicurezza prescritte direttamente dal Codice (artt. 31-36 e Allegato B)).

Garantire l'esercizio dei diritti

Va garantito l'esercizio da parte di tutti gli interessati (e in particolare degli esercenti la potestà), dei diritti individuati dal Codice (art. 7) e, in particolare, del diritto di chiedere l'aggiornamento, la rettificazione, l'integrazione dei dati (quando vi sia interesse), la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione alle finalità di valutazione della formazione scolastica.

Breve conservazione dei dati

Occorre individuare brevi periodi di eventuale conservazione dei dati personali raccolti nel Portfolio, in modo tale che gli stessi siano conservati solo in una forma che consenta di identificare gli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati (art. 11, comma 1, lett. *e*), del Codice).

Rilascio all'interessato

Il Portfolio (alla stregua di quanto indicato negli allegati B) e C) al citato d.lg. n. 59/2004, secondo cui, nel passaggio al ciclo scolastico successivo, il Portfolio "si innesta su quello portato" dall'alunno) deve essere rilasciato allo studente alla fine del corso degli studi, affinché lo stesso lo consegni, solo ove ciò sia previsto, al nuovo istituto scolastico.

TUTTO CIÓ PREMESSO, IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive agli istituti scolastici di adottare le misure necessarie ed opportune indicate in motivazione, al fine di conformare i trattamenti di dati alle vigenti disposizioni;
b) dispone che copia del presente provvedimento sia inviata al Ministero dell'istruzione dell'università e della ricerca-Dipartimento per l'istruzione, anche per il seguito indicato in motivazione;

(1) [doc. *web* n. 1037043] vers. EN n. 1115285]

(2) [doc. *web* n. 1037047] vers. EN n. 1113111]

(3) [doc. *web* n. 1144445]

c) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* ai sensi dell'art. 143, comma 2, del Codice.

Roma, 26 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

48 Procreazione assistita - Registro nazionale delle strutture sanitarie 26 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la richiesta di parere del Ministro della salute;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali e, in particolare, la direttiva n. 95/46/Ce del 24 ottobre 1995;

Visto l'articolo 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Vista la legge 19 febbraio 2004, n. 40, recante "Norme in materia di procreazione medicalmente assistita";

Vista la documentazione in atti;

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

Relatore il dott. Mauro Paissan;

PREMESSO:

Il Ministro della salute ha chiesto il parere del Garante in ordine ad uno schema di decreto recante l'istituzione del registro nazionale delle strutture autorizzate ad applicare le tecniche di procreazione medicalmente assistita, degli embrioni formati e dei nati a seguito delle tecniche medesime, da adottare in attuazione dell'articolo 11 della legge 19 febbraio 2004, n. 40.

Il parere tiene conto degli elementi di valutazione forniti dal Ministero della salute a seguito dei quali, il 20 luglio u.s., è stato sottoposto per l'esame un nuovo schema di decreto.

OSSERVA:

Lo schema attua la legge n. 40/2004 nella parte in cui istituisce il registro nazionale delle strutture autorizzate all'applicazione delle tecniche di procreazione medicalmente assistita, degli embrioni formati e dei nati (art. 11, comma 1, l. n. 40/2004).

Responsabile dell'attuazione e del funzionamento del registro sarà l'Istituto superiore di sanità, indicato espressamente nello schema quale titolare del trattamento dei dati personali che vi saranno registrati (artt. 1, comma 2, e 3, comma 1, dello schema).

Per quanto riguarda dati personali relativi a soggetti identificati o identificabili, lo schema prevede che nel registro siano registrati solo dati personali relativi alle strutture autorizzate all'applicazione delle predette tecniche, necessari al loro censimento, e quelli concernenti le relative autorizzazioni di legge, il cui conferimento è obbligatorio.

(*) [doc. *web* n. 1151435]

Al riguardo, non vi sono rilievi di fondo da formulare (artt. 18 e 19 del Codice; art. 11, comma 1, l. n. 40/2004; art. 1, commi 3 e 5, lett. a) e b), dello schema). È, peraltro, necessario specificare nell'allegato tecnico che il riferimento al personale operante presso le strutture ("personale medico", "personale laboratorio di biologia", "medico anestesista", "infermieristico", "amministrativo") attiene solo al dato numerico, non dovendo essere indicati in questa sede anche i dati identificativi dei singoli dipendenti interessati (all. 1, "set anagrafico della struttura"). Ciò, in linea con quanto previsto nell'allegato 2, che contiene anch'esso solo dati anonimi numerici.

Lo schema prevede, inoltre, che possano essere raccolti, comunicati o diffusi anche altri dati, relativi alle coppie che accedono alle predette tecniche, agli embrioni ed ai nati. Si tratta, però, solo di dati in forma anonima anche aggregata, e di eventuali altri dati raccolti in via sperimentale, ma anch'essi solo anonimi (art. 11, comma 3, l. n. 40/2004; artt. 3, 11 e 22, comma 3, del Codice; settimo periodo del preambolo, art. 1, commi 3 e 5, lett. c), e all. 2 dello schema).

Anche a tale riguardo non vi sono rilievi generali da formulare. Risulta, peraltro, necessario coordinare sul piano formale il settimo e l'ottavo periodo del preambolo del decreto, inserendo anche in quest'ultimo periodo, dopo la parola "dati", le parole "anonimi anche aggregati,".

Riservandosi di valutare le modalità di raccolta e di conservazione dei dati nel registro, l'individuazione dei soggetti autorizzati alla consultazione dei dati registrati e le relative modalità di accesso, in occasione dell'ulteriore parere da formulare su un altro provvedimento di cui è prevista l'adozione (art. 4 dello schema), il Garante esprime parere favorevole sull'odierno schema di decreto, a condizione che vengano apportate le modifiche sopra indicate.

TUTTO CIÒ PREMESSO IL GARANTE:

esprime parere favorevole nei termini di cui in motivazione.

Roma, 26 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

49 Passaporto elettronico 26 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la richiesta di parere del Ministro degli affari esteri;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali e, in particolare, la direttiva n. 95/46/Ce del 24 ottobre 1995;

Visto l'articolo 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visto il regolamento del Consiglio dell'Unione europea n. 2252/2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio;

Vista la legge 21 novembre 1967, n. 1185 e successive modificazioni ed integrazioni, recante norme in materia di passaporti;

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO:

Lo schema di decreto in esame, trasmesso dal Ministro degli affari esteri per il prescritto parere, concerne l'adozione di un nuovo passaporto ordinario elettronico, contenente dati biometrici del titolare, in ottemperanza agli obblighi fissati in sede comunitaria con l'approvazione del regolamento del Consiglio dell'Unione europea n. 2252/2004 del 13 dicembre 2004, nonché della decisione della Commissione C(2005)409 del 28 febbraio 2005 volta a stabilire le specifiche tecniche relative alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri.

OSSERVA:

Lo schema individua, nel preambolo, la necessità di aggiornare il modello del passaporto ordinario italiano con riferimento, da un lato, all'introduzione della normativa comunitaria richiamata (la quale ha definito un modello uniforme di passaporto per gli Stati membri dell'Unione europea, individuandone le caratteristiche) e, dall'altro, alla legge 31 marzo 2005, n. 43 (la quale, all'articolo 7-*vicies*, stabilisce che a decorrere dal 1° gennaio 2006 il passaporto su supporto cartaceo sia sostituito dal passaporto elettronico, secondo il modello uniforme definito in sede comunitaria).

Lo schema di decreto prevede che le nuove prescrizioni di carattere generale relative ai passaporti debbano essere riferite anche ai passaporti "speciali", quali quelli diplomatici e di servizio. Conseguentemente, le prescrizioni relative all'utilizzo di dati biometrici individuate

(*) [doc. *web* n. 1153396]

nel medesimo schema si applicheranno anche ai passaporti di cui al decreto del Ministero degli affari esteri del 5 aprile 2005, che integra il decreto 23 dicembre 2004, n. 1679-bis, relativo all'istituzione di un nuovo modello di passaporto diplomatico.

Le previsioni dello schema di decreto che riguardano le caratteristiche di sicurezza del passaporto, nonché le modalità di raccolta e conservazione dei dati biometrici, rispettano il principio di finalità nell'utilizzo di tali dati. É infatti espressamente previsto che i dati biometrici raccolti (l'immagine del volto e le impronte degli indici delle due mani) siano inseriti in un chip integrato nel passaporto e che, per la verifica dell'autenticità del documento e dell'identità del titolare, quando la legge prevede che siano necessari il passaporto o altro documento di viaggio, l'utilizzo dei dati biometrici contenuti nel chip al fine indicato avverrà "attraverso elementi comparativi direttamente disponibili" (art. 2 dello schema di decreto).

Tale espressione –che pure corrisponde ad un'analoga disposizione del regolamento n. 2252/2004 (art. 4, paragrafo 3, lettera *b*))– non chiarisce inequivocabilmente che non si procederà alla raccolta e alla conservazione dei dati biometrici in una banca di dati centralizzata.

A tale riguardo un chiarimento appare quindi necessario, integrando tale previsione con la specificazione che i dati biometrici raccolti ai fini del rilascio del passaporto non saranno, appunto, conservati in banche di dati.

Riservandosi di formulare in separata sede, e comunque prima che inizi l'effettiva emissione del nuovo modello di passaporto, prescrizioni in ordine alle modalità di raccolta ed utilizzo dei dati biometrici in esame, nonché alle collegate misure di sicurezza da garantire anche in relazione al supporto utilizzato, il Garante esprime parere favorevole sullo schema di decreto a condizione che lo schema sia integrato nei termini descritti.

TUTTO CIÓ PREMESSO IL GARANTE:

esprime parere favorevole sullo schema di decreto, nei termini di cui in motivazione.

Roma, 26 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

50 Servizi di radiotaxi 26 luglio 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminate le segnalazioni presentate da interessati e da associazioni di consumatori, relative al trattamento di dati personali nell'ambito della fornitura di autoservizi pubblici non di linea con riguardo alle operazioni svolte da soggetti che raccolgono richieste di corse taxi;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali e, in particolare, la direttiva n. 95/46/Ce del 24 ottobre 1995;

Visto l'articolo 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visti gli artt. 85 e 86 del d.lg. 30 aprile 1992, n. 285 (Nuovo codice della strada) e la legge 15 gennaio 1992, n. 21 (Legge quadro per il trasporto mediante autoservizi pubblici non di linea);

Visti gli elementi acquisiti e ritenuta la necessità di prescrivere, ai sensi dell'art. 154, comma 1, lett. *c*) e *d*), del Codice, misure ed accorgimenti a garanzia degli interessati al fine di conformare il trattamento dei dati personali alle disposizioni vigenti, e di vietare i trattamenti illeciti oggetto di segnalazioni;

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

Relatore il dott. Giuseppe Chiaravalloti;

PREMESSO:

1. Trattamento di dati da parte dei soggetti che gestiscono servizi radiotaxi

Sono pervenute a questa Autorità segnalazioni da parte di singoli e di associazioni per la tutela dei diritti dei consumatori, concernenti il trattamento di dati personali della clientela effettuato da soggetti che forniscono servizi radiotaxi. Questi ultimi raccolgono (generalmente per via telefonica) richieste di corse taxi nell'interesse dei titolari di licenza (art. 7 l. n. 21/1992) e, a tal fine, registrano alcuni dati, di regola limitati al solo indirizzo di prelievo.

Non di rado, però, vengono richiesti all'interessato anche un numero di telefono (fisso o mobile) e, talvolta, anche il suo nominativo, in particolare ove venga prenotata una corsa per un tempo differito (anche al fine di effettuare al cliente una chiamata di conferma, o avvertire circa ritardi o arrivi sul luogo indicato).

In talune circostanze, il *cd.* indirizzo di prelievo ed eventualmente il nominativo del cliente vengono ricavati, senza rivolgere al medesimo un'espressa richiesta, associando anche in modo automatizzato il numero telefonico ad informazioni ricavate da elenchi pubblici.

In altri casi, i dati raccolti al momento del primo contatto, concernenti il numero telefonico e l'indirizzo del cliente (e, seppur di rado, anche il suo nominativo), vengono registrati

(*) [doc. *web* n. 1151997]

per prestare il servizio in modo più sollecito (essendo l'indirizzo di prelievo preregistrato).

In ulteriori altri casi, vengono raccolte informazioni aggiuntive relative a comportamenti tenuti dal cliente, con particolare riguardo alla sua assenza presso l'indirizzo di prelievo e/o al mancato pagamento della corsa. Questa specifica raccolta di dati è preordinata ad individuare e/o contattare in seguito il cliente per ottenere il pagamento della corsa o per perseguire ulteriori finalità non riferibili alla sola esecuzione del contratto (finalità consistenti, in particolare, nel negare una successiva prestazione richiesta al medesimo servizio radiotaxi).

Dagli elementi acquisiti in atti, emerge che non è sempre prevista una cancellazione automatica dei dati, e che gli stessi sono talvolta conservati a lungo, anche per un biennio. La raccolta e la prolungata conservazione dei dati da parte del gestore del servizio radiotaxi avvengono comunque, di regola, all'insaputa degli interessati, in particolare per quanto riguarda le finalità diverse da quelle direttamente collegate all'esecuzione della prestazione.

Sotto altro profilo, è emersa anche l'eccedenza e non pertinenza dei dati raccolti rispetto a quelli reputati necessari per prestare il servizio richiesto dal cliente (ossia, di regola, il solo indirizzo di prelievo e non anche l'indirizzo di destinazione).

Al fine di conformare i trattamenti effettuati nell'ambito dei servizi radiotaxi alla disciplina vigente in materia di protezione dei dati personali, tenendo conto delle finalità perseguite e delle circostanze rappresentate in concreto, il Garante, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive ai titolari del trattamento l'adozione delle misure e degli accorgimenti a garanzia degli interessati di seguito specificamente indicati, e vieta il trattamento illecito dei dati.

2. Finalità del trattamento; pertinenza e non eccedenza dei dati

L'attività di radiotaxi, nelle sue diverse forme, può comportare un trattamento di dati personali.

Fuori dei casi in cui venga fornito il solo indirizzo di prelievo, viene posto in essere un trattamento di dati personali relativo a soggetti identificati o identificabili, quando l'indirizzo stesso è ad esempio associato al dato nominativo di un cliente o ad un numero di utenza telefonica.

Ciò comporta l'applicazione della disciplina contenuta nel Codice (art. 4, comma 1, lett. *b*)). Tale trattamento deve quindi svolgersi nel rispetto dei principi di finalità, necessità, liceità e correttezza, proporzionalità e qualità dei dati (artt. 3 e 11). In caso di inosservanza di tali principi, i dati personali trattati non possono essere utilizzati (art. 11, comma 2).

Il gestore del servizio radiotaxi, titolare del trattamento, può raccogliere solo i dati personali pertinenti e non eccedenti rispetto alla finalità principale legittimamente perseguita, che consiste nel mettere in contatto il cliente con il taxi indicato per effettuare la corsa (art. 11, comma 1, lett. *b*)).

In particolare, oltre all'indirizzo di prelievo, possono essere trattati, quando ciò sia necessario per dare attuazione al rapporto contrattuale agevolando l'esatta esecuzione della prestazione, i dati relativi al nominativo del cliente ed al suo recapito telefonico (fisso o mobile). In alcune situazioni, tali informazioni possono, infatti, rendersi necessarie, ad esempio, per segnalare una sopravvenienza (quale la sostituzione del taxi o il suo arrivo anticipato o ritardato) o, con specifico riferimento alla raccolta del nominativo, per assicurarsi che il servizio venga reso solo a chi lo abbia effettivamente richiesto (anziché a persona diversa).

Presso il servizio radiotaxi, non possono in ogni caso formare oggetto di registrazione, trattandosi di informazioni non pertinenti, i tragitti effettuati dalla clientela. Fatta salva l'esigenza di far valere o difendere un diritto in sede giudiziaria (trattando i dati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento), nello svolgimento del servizio radiotaxi non possono inoltre essere trattati i dati personali della clientela inerenti ad eventuali inadempimenti loro attribuiti; non possono essere altresì regi-

strati, oltre il tempo strettamente necessario a rispondere ad eventuali contestazioni, informazioni relative all'assenza del cliente presso l'indirizzo di prelievo indicato.

I trattamenti da ultimo indicati sono infatti collegati ad una finalità diversa ed ulteriore rispetto a quella volta a rendere possibile il trasporto della clientela, la sola per la quale il gestore del servizio radiotaxi può raccogliere lecitamente i dati. Infatti, i dati personali "devono essere raccolti e registrati per scopi determinati espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi" (art. 11, comma 1, lett. *b*)): tale compatibilità non sussiste nel caso di specie –come peraltro confermato dagli elementi in atti– posto che i dati così raccolti vengono utilizzati al fine di valutare se rendere o meno in futuro il medesimo servizio al cliente in relazione al quale vengono ascritti gli inadempimenti appena menzionati. Condotta, questa, illegittima alla luce dei principi di protezione dei dati personali ed altresì contraria all'espresso precetto contenuto nell'art. 2, comma 2, della legge n. 21/1992 secondo il quale "all'interno delle aree comunali o comprensoriali [...] la prestazione del servizio è obbligatoria".

I dati personali –dei quali non sia più necessaria la conservazione in relazione all'esecuzione del servizio offerto al cliente (sia esso quello principale e/o quello aggiuntivo)– devono essere cancellati o trasformati in forma anonima (ad esempio, per utilizzarli in valutazioni da effettuarsi in forma aggregata volte a migliorare la gestione del servizio), una volta esauriti gli specifici scopi per i quali sono stati richiesti (art. 11, comma 1, lett. *e*), del Codice), salva l'osservanza di eventuali puntuali obblighi di legge che eventualmente ne legittimino un'ulteriore conservazione.

Resta fermo che, quando per far eseguire la singola corsa è necessario raccogliere dati personali, questi ultimi possono essere conservati dal titolare del trattamento solo per il periodo di tempo necessario a perseguire scopi non incompatibili con detta finalità (quali, ad esempio, la restituzione di oggetti smarriti dal cliente o la gestione di eventuali contestazioni connesse all'esecuzione della prestazione).

La conservazione per tali finalità non può eccedere il termine di trenta giorni.

Dalle considerazioni svolte, ed in applicazione dei principi contenuti negli artt. 3 e 11 del Codice, deriva infine che, con riguardo alle sopra evidenziate finalità legittimamente perseguibili, i sistemi informativi impiegati dal titolare del trattamento devono essere configurati, già in origine, in modo da minimizzare l'utilizzo di dati identificativi dei clienti; del pari, devono essere predisposti meccanismi di cancellazione automatica delle informazioni allo scadere del termine definito secondo i criteri sopra indicati, a prescindere da eventuali richieste degli interessati.

3. Informativa agli interessati e modalità semplificate

La disciplina di protezione dei dati attribuisce particolare rilevanza alla circostanza che i trattamenti di informazioni personali non si svolgano all'insaputa dell'interessato.

Questo principio generale, riaffermato dal Codice (art. 11, comma 1, lett. *b*)) secondo il quale i dati personali devono essere raccolti e registrati per scopi determinati ed espliciti, trova puntuale concretizzazione nell'ulteriore precetto nel quale vengono indicate le informazioni che devono essere fornite all'interessato in relazione ai trattamenti di dati personali a lui riferiti (art. 13 del Codice).

Le informazioni rese con l'informativa devono enunciare chiaramente, accanto alle modalità impiegate nel trattamento, le finalità perseguite e la tipologia di dati personali utilizzati per ciascuna di esse, nonché la facoltà riconosciuta agli interessati di avvalersi dei diritti di cui all'art. 7 del Codice. È altresì necessario indicare, anche per categorie, i soggetti cui siano eventualmente comunicati i dati e coloro i quali possano venirne a conoscenza in qualità di responsabili o incaricati del trattamento (art. 13, comma 1, lett. *d*)).

Tenuto conto della peculiarità del mezzo trasmissivo utilizzato (ossia, di regola, il telefono) e della natura del servizio reso, che più di altri richiede di essere svolto con la massima celerità (anzitutto nell'interesse della clientela), i singoli gestori dei servizi radiotaxi

potranno rivolgere a questa Autorità una motivata richiesta volta a rendere lecitamente utilizzabile un'informativa semplificata, resa al telefono in sede di prenotazione del servizio e mediante un sintetico avviso consultabile sul taxi (art. 13, comma 3, del Codice).

Il gestore, anche avvalendosi dei tempi di attesa in linea del cliente, potrebbe infatti ricorrere a testi preregistrati sintetici, purché chiari, utilizzando formule del tipo: "...taxi utilizzerà i suoi dati solo per svolgere il servizio richiesto. Nel taxi troverà ulteriori precisazioni.".

In tal caso l'informativa semplificata resa telefonicamente deve essere integrata con un testo contenente tutti gli elementi menzionati nell'art. 7 del Codice, resa all'interno del taxi, in particolare mediante affissione (e redatta eventualmente avvalendosi del modello allegato alla presente decisione).

Il Garante autorizza tutti i titolari del trattamento che gestiscono servizi radiotaxi (anche quelli non interessati dal presente procedimento) ad avvalersi delle sopra indicate modalità semplificate per rendere l'informativa agli interessati nei termini di cui al seguente dispositivo, utilizzando il modulo disponibile sul sito *web* dell'Autorità all'indirizzo *www.garanteprivacy.it.*

4. Consenso al trattamento

Poiché la raccolta e il successivo trattamento dei dati della clientela, preordinati alla esecuzione della singola prestazione di trasporto richiesta, sono indispensabili per eseguire gli "obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato", il consenso al trattamento dei dati dell'interessato non è necessario per l'ordinaria prestazione di tale servizio (art. 24, comma 1, lett. *b*), del Codice).

Ogni altra finalità del trattamento che comporti un'ulteriore conservazione dei dati personali raccolti (ad esempio, fornire, anche su registrazione o abbonamento, servizi o comodità aggiuntive rispetto alla singola corsa di volta in volta richiesta; compiere ricerche di mercato, operazioni di marketing o profilazioni, ecc.) necessita, invece, del consenso specifico, informato e distinto da parte del cliente (art. 23 del Codice). Tale consenso, reso anche oralmente, deve essere documentato per iscritto a cura del titolare del trattamento.

5. Ulteriori adempimenti

Al di là delle misure necessarie per conformare i trattamenti di dati personali effettuati, restano fermi gli adempimenti che, in generale, la legge prescrive ai titolari del trattamento. Ci si riferisce, in particolare:

a) agli obblighi relativi all'adozione delle misure anche minime di sicurezza (artt. 31-35 e Allegato B) del Codice;

b) alla selezione dei soggetti che, in qualità di incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite (artt. 29 e 30 del Codice);

c) all'obbligo dei titolari del trattamento di adottare le misure necessarie per agevolare l'esercizio dei diritti degli interessati e il relativo tempestivo riscontro (art. 10, comma 1, del Codice).

TUTTO CIÒ PREMESSO, IL GARANTE:

a) accertata, nei termini di cui in motivazione, l'illiceità del trattamento effettuato, vieta ai titolari del trattamento di cui in atti, ai sensi dell'art. 154, comma 1, lett. *d*), del Codice, la prosecuzione delle operazioni di trattamento di dati personali effettuate in violazione dei principi contenuti nel Codice;

b) prescrive, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, ai medesimi titolari del trattamento di cui al punto a), nei termini di cui in motivazione, le misure necessarie indicate nel presente provvedimento al fine di conformare il trattamento alle disposizioni vigenti;

c) invita, ai sensi e per gli effetti di cui agli artt. 157, 164 e 168 del Codice, i titolari del trattamento indicati negli atti a comunicare al Garante, entro e non oltre il 30 ottobre 2005, che i trattamenti di dati da essi effettuati sono conformi alle prescrizioni del pre-

sente provvedimento, indicando ogni informazione utile al riguardo ed allegando la pertinente documentazione;
d) autorizza, ai sensi dell'art. 13, comma 3, del Codice, previa specifica e motivata richiesta in tal senso indirizzata al Garante, tutti i soggetti che gestiscono il servizio radiotaxi ad effettuare l'informativa in conformità alle modalità semplificate descritte in motivazione. Il testo dell'informativa resa al momento della chiamata e quello destinato ad essere esposto nel taxi, dovrà essere trasmesso a questa Autorità unitamente alla richiesta sopra indicata. Resta salvo il potere del Garante di esigere chiarimenti o integrazioni nel termine di sessanta giorni dal ricevimento della richiesta, decorso il quale la richiesta stessa si intende accolta.

Roma, 26 luglio 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO

SERVIZIO RADIOTAXI: COME SONO UTILIZZATI I DATI PERSONALI
(art. 13 del Codice in materia di protezione dei dati personali)

Se il servizio è stato prenotato, [*indicare gli estremi identificativi del servizio radiotaxi titolare del trattamento]* può utilizzare alcuni dati connessi alla prenotazione, raccolti da chi ha chiesto il servizio o da [*indicare altra origine*].

I dati sono trattati temporaneamente, anche elettronicamente, nella misura strettamente necessaria per il servizio di trasporto [*indicare eventuali ulteriori finalità*].

Altre finalità [*descriverle sinteticamente: es. a) prestazione di servizi aggiuntivi; b) marketing; etc.*] sono perseguibili solo con l'espresso e libero consenso dell'interessato.

Non è prevista la comunicazione a terzi (oppure: alcune informazioni saranno comunicate a ... *indicare per tipologia i soggetti*).

Responsabile del trattamento è ... [*da menzionare se designato*].

L'interessato ha diritto di accedere in ogni momento ai dati che lo riguardano; può anche chiedere la correzione, l'aggiornamento o l'integrazione dei dati inesatti o incompleti, la cancellazione o il blocco per quelli trattati in violazione di legge, opporsi al loro utilizzo.

L'istanza ai sensi dell'art. 7 del Codice va inoltrata a:

Titolare/responsabile del trattamento:

Recapiti utili (indirizzo, telefono, fax, e-mail):

51 Propaganda elettorale: il "decalogo" del Garante 7 settembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria e il Codice in materia di protezione dei dati personali (direttive nn. 95/46/Ce e 2002/58/Ce; d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

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

Relatore il dott. Giuseppe Chiaravalloti;

PREMESSO:

1. Finalità del provvedimento

Le iniziative di propaganda elettorale, o collegate a referendum o alla selezione di candidati alle elezioni, costituiscono un momento particolarmente significativo della partecipazione alla vita democratica (art. 49 Cost.).

In vista delle prossime consultazioni il Garante richiama l'attenzione sui principali casi nei quali partiti, organismi politici, comitati di promotori e sostenitori e singoli candidati possono utilizzare dati personali per iniziative di propaganda rispettando i diritti e le libertà fondamentali degli interessati (art. 2 del Codice).

2. Dati utilizzabili senza consenso

A) Liste elettorali

Possono essere anzitutto utilizzati, senza il preventivo consenso degli interessati, i dati contenuti nelle liste elettorali che ciascun comune tiene, aggiorna costantemente e rilascia in copia anche su supporto elettronico. L'intera platea degli elettori può essere così contattata agevolmente.

Possono essere altresì utilizzati i seguenti altri elenchi e registri in materia di elettorato attivo e passivo:

- elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo;
- elenco aggiornato dei cittadini italiani residenti all'estero finalizzato a predisporre le liste elettorali, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (Aire) e degli schedari consolari;
- elenco dei cittadini italiani residenti all'estero aventi diritto al voto per l'elezione del Comitato degli italiani all'estero (Comites);
- *cd.* liste aggiunte degli elettori di uno Stato membro dell'Unione europea residenti in Italia e che intendano esercitare il diritto di voto alle elezioni del Parlamento europeo.

B) Altri elenchi e registri pubblici

Oltre alle liste elettorali, possono essere utilizzate per la propaganda, anche in questo caso senza il consenso degli interessati, altre fonti documentali detenute da soggetti pubblici, qualora esse siano liberamente accessibili a chiunque senza limitazioni di sorta in base

(*) *G.U.* 12 settembre 2005, n. 212
[doc. *web* n. 1165613]

ad una specifica disposizione normativa. Occorre tuttavia rispettare le modalità eventualmente stabilite per accedere a tali fonti (*es.*, identificazione di chi ne chiede copia; accessi consentiti solo in determinati periodi) o per utilizzarle (*es.*, obbligo di indicare la fonte dei dati nel materiale di propaganda; rispetto delle finalità per le quali determinati elenchi sono resi pubblici).

C) Dati raccolti da titolari di cariche elettive e di altre funzioni pubbliche

I titolari di cariche elettive possono utilizzare le informazioni raccolte nel quadro delle relazioni interpersonali con cittadini ed elettori.

Alcune specifiche disposizioni di legge prevedono altresì che il titolare della carica elettiva possa richiedere agli uffici di fornire notizie utili all'esercizio del mandato, che possono essere utilizzate solo per finalità pertinenti a tale esercizio. L'eventuale impiego di tali informazioni per iniziative di propaganda rivolte agli interessati è pertanto consentita solo in casi particolari nei quali le iniziative stesse possano risultare in concreto obiettivamente riconducibili ad attività e compiti espletati nel corso del mandato.

È illegittima l'eventuale richiesta di ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per la propaganda fuori dai predetti casi riconducibili ad attività e compiti espletati nel corso del mandato.

Non può ritenersi parimenti consentito, da parte di soggetti titolari di altre cariche pubbliche non elettive, l'utilizzo per finalità di propaganda di dati acquisiti per svolgere i relativi compiti istituzionali.

D) Dati raccolti nell'esercizio di attività professionali e di impresa

I dati personali raccolti in quanto necessari nell'esercizio di attività professionali e di impresa per prestazioni d'opera o per fornire beni e servizi non sono utilizzabili. La finalità di propaganda non è infatti riconducibile agli scopi per i quali i dati sono raccolti.

E) Iscritti a partiti, organismi politici e comitati

Nell'ambito di partiti, organismi politici, comitati di promotori e sostenitori, si possono utilizzare lecitamente, senza un apposito consenso, dati personali relativi ad iscritti ed aderenti, nonché ad altri soggetti con cui intrattengono regolari contatti (*cfr.* art. 26, comma 4, lett. *a*), del Codice).

F) Iscritti ad altri organismi associativi a carattere non politico

Altri enti, associazioni ed organismi senza scopo di lucro (associazioni sindacali, professionali, sportive, di categoria, ecc.), possono prevedere che tra i propri scopi vi siano anche le finalità di propaganda di cui al presente provvedimento che, se perseguite direttamente dai medesimi enti, organismi o associazioni, non richiedono il consenso (*cfr.* artt. 24, comma, 1, lett. *h*) e 26, comma 4, lett. *a*), del Codice).

3. Fonti documentali non utilizzabili per propaganda

Alcune fonti documentali detenute da soggetti pubblici non sono utilizzabili, neanche da parte di titolari di cariche elettive, in ragione della specifica normativa che ne precluda l'acquisizione a fini di propaganda, oppure del segreto d'ufficio o della circostanza che esse sono state acquisite in base ad una normativa che ne vincola l'utilizzo. Ciò avviene ad esempio nei seguenti casi:

- archivi dello stato civile;
- anagrafe della popolazione residente, utilizzabile però per la comunicazione istituzionale di amministrazioni pubbliche;
- liste elettorali di sezione già utilizzate nei seggi, sulle quali sono annotati dati relativi ai non votanti e che sono utilizzabili solo per controllare la regolarità delle operazioni elettorali;
- dati annotati privatamente nei seggi da scrutatori e rappresentanti di lista, durante operazioni elettorali;
- particolari indirizzari e dati raccolti solo per svolgere le attività istituzionali del soggetto pubblico o, in generale, per la prestazione di servizi, anche di cura.

4. Dati utilizzabili previo consenso

Con il consenso preventivo degli interessati possono essere utilizzate per iniziative di propaganda altre fonti documentali.

A) Simpatizzanti e persone contattate

Partiti, organismi politici, comitati di promotori e sostenitori e singoli candidati possono utilizzare lecitamente dati relativi a simpatizzanti o ad altre persone già contattate per singole iniziative o che vi hanno partecipato occasionalmente (petizioni, proposte di legge, richieste di referendum, raccolte di firme, ecc).

In questi casi, occorre però aver acquisito preventivamente il consenso scritto, trattandosi di dati sensibili. Tale consenso può essere anche manifestato una tantum.

B) Elenchi telefonici

Nei nuovi elenchi telefonici, cartacei ed elettronici, derivanti dalla disciplina di origine comunitaria vincolante per il legislatore nazionale, accanto ai nominativi di alcuni abbonati figurano due simboli che attestano il consenso prestato, rispettivamente, alla ricezione di posta a domicilio o di chiamate telefoniche per finalità diverse dalla comunicazione interpersonale.

In tali casi, i nominativi sono pertanto utilizzabili anche per inviare a domicilio materiale di propaganda, oppure per effettuare chiamate aventi finalità di propaganda, a seconda dei simboli apposti sull'elenco.

C) Particolari modalità di comunicazione

In base alla disciplina di origine comunitaria vincolante per il legislatore nazionale, alcune particolari modalità di comunicazione richiedono il consenso specifico di abbonati a servizi di comunicazione elettronica, compresi gli abbonati a servizi di telefonia mobile e gli utilizzatori di schede di traffico prepagato (invio di fax, di messaggi tipo *Sms* o *Mms*; chiamate telefoniche preregistrate; messaggi di posta elettronica).

Il consenso, che anche in questo caso può essere acquisito una tantum, deve comunque precedere la chiamata o il messaggio e deve essere raccolto sulla base di formule chiare che specifichino espressamente la finalità di propaganda politica o elettorale. Non è possibile ricorrere a modalità di silenzio-assenso.

Senza un preventivo consenso informato non è lecito l'invio di messaggi, newsletter e di altro materiale di propaganda quando si utilizzano:

- dati raccolti automaticamente in Internet tramite appositi *software*;
- liste di abbonati ad un *provider*;
- dati pubblicati su siti *web* per specifiche finalità di informazione aziendale, comunicazione commerciale o attività istituzionale od associativa;
- dati ricavati da *forum* o *newsgroup*;
- dati consultabili in Internet solo per le finalità di applicazione della disciplina sulla registrazione dei nomi a dominio.

D) Dati raccolti e messi a disposizione da terzi

L'eventuale acquisizione dei dati personali da un soggetto terzo (il quale potrebbe averli raccolti in base ad un consenso riferito ai più diversi scopi, compresi quelli di tipo promozionale o commerciale) non esime il partito, l'organismo politico, il comitato o il candidato dall'onere di verificare, anche con modalità a campione e avvalendosi del mandatario elettorale, che il terzo:

- abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda e abbia ottenuto il loro consenso idoneo ed esplicito. Il consenso deve risultare manifestato liberamente, in termini differenziati rispetto all'eventuale prestazione di beni e servizi e documentato per iscritto;
- non abbia violato il principio di finalità nel trattamento dei dati associando informazioni provenienti da più archivi, anche pubblici, aventi finalità incompatibili (artt. 11 e 61 del Codice).

Queste cautele vanno adottate anche quando il terzo, oltre a fornire i dati, svolge le funzioni di responsabile del trattamento designato da chi effettua la propaganda.

5. Obbligo di informativa

Se i dati sono raccolti presso l'interessato, quest'ultimo deve essere comunque informato a norma di legge delle caratteristiche del trattamento, salvo che per gli elementi che gli siano già noti (art. 13, commi 1 e 2). Quando i dati sono raccolti altrove, e il caso non rientra tra quelli di cui al successivo punto 6, l'informativa va fornita all'atto della registrazione o della prima, eventuale comunicazione a terzi (art. 13, commi 4 e 5).

L'informativa sintetica, ma efficace, può essere basata sulla seguente formula semplificata che può essere inserita anche nei messaggi di posta elettronica o nelle lettere di propaganda (art. 13, comma 3, del Codice):

INFORMATIVA

(Art. 13 del Codice in materia di protezione dei dati personali)

"I dati che ha fornito liberamente (oppure: che sono stati estratti da ...) sono utilizzati da ... (*indicare il titolare del trattamento*) solo a fini di propaganda (o per la selezione dei candidati ...; *indicare anche se i dati verranno utilizzati per analoghe iniziative o anche da singoli candidati, oltre che da parte degli organi della forza politica*), anche con strumenti informatici, e non saranno comunicati a terzi (*indicare, se utilizzata, l'eventuale organizzazione esterna che cura l'inoltro*). Lei può in ogni momento accedere ai dati, ottenere di non ricevere più materiale di propaganda, opporsi al trattamento dei dati o chiedere di integrarli, rettificarli, ecc., rivolgendosi a ..." (*indicare le coordinate del predetto titolare del trattamento o di un suo referente, ad esempio del responsabile del trattamento facoltativamente designato*).

6. Casi in cui l'informativa non è dovuta

Il Garante ritiene che nei due seguenti casi il partito, l'organismo politico, il comitato di promotori e sostenitori o il singolo candidato non debbano fornire l'informativa agli interessati secondo le ordinarie modalità di legge relativamente alle iniziative e consultazioni in programma sino al 30 giugno 2006.

Questa Autorità, analogamente a quanto già provveduto in passato, ritiene infatti che l'impiego dei mezzi necessario per le finalità in esame sia sproporzionato rispetto ai diritti tutelati (art. 13, comma 5, lett. *c*), del Codice), qualora il partito, l'organismo politico, il comitato di promotori e sostenitori o il singolo candidato utilizzi i dati solo per le finalità di cui al presente provvedimento e:

a) li raccolga direttamente da pubblici registri, elenchi, atti o altri documenti conoscibili da chiunque senza contattare gli interessati, oppure
b) invii materiale propagandistico di dimensioni ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non renda possibile inserire un'idonea informativa anche sintetica.

L'Autorità intende anche evitare che, in un breve arco di tempo, un alto numero di interessati riceva un elevato numero di informative analoghe da parte di più soggetti impegnati in iniziative politiche e campagne elettorali.

Qualora gli interessati siano invece contattati mediante lettere cartacee, messaggi per posta elettronica o missive e plichi contenenti più documenti anche di dimensioni ridotte, l'informativa –secondo la predetta formula semplificata– potrà essere inserita nella lettera, nel messaggio, nella missiva o plico, anziché essere inviata all'atto della registrazione dei dati (art. 13, comma 5, lett. *c*), del Codice).

Dopo il 31 ottobre 2006, partiti, movimenti politici, comitati di promotori e sostenitori e singoli candidati che intendano conservare i dati per i quali non si sia già provveduto all'informativa dovranno informare gli interessati nei modi previsti dal predetto art. 13 qualora intendano inviare loro una comunicazione.

7. Garanzie e adempimenti

Nelle iniziative di propaganda e di selezione di candidati che comportano l'utilizzo di dati personali va posta attenzione alle garanzie che il Codice prevede a tutela delle persone a cui essi si riferiscono, i quali sono a volte di natura sensibile.

Il trattamento non deve essere comunque notificato al Garante (art. 37 del Codice), quale che sia il soggetto titolare (partito, organismo politico, comitato di promotori e sostenitori o singolo candidato).

È altresì facoltativo designare uno o più responsabili del trattamento (art. 29 del Codice).

Occorre però designare le persone fisiche incaricate del trattamento (art. 30 del Codice) e adottare, in conformità al Codice, idonee misure di sicurezza conformi a quelle previste, a seconda dei casi, dagli artt. 31-36 e dall'Allegato B) del medesimo Codice.

Deve essere infine dato tempestivo riscontro ad eventuali richieste con le quali gli interessati esercitino i propri diritti, ad esempio per accedere ai dati che li riguardano, conoscerne l'origine e alcune modalità del trattamento od opporsi al loro utilizzo, ad esempio all'ulteriore ricezione di materiale o chiamate (art. 7 del Codice). Qualora il titolare di trattamento non fornisca un riscontro idoneo l'interessato può rivolgersi all'autorità giudiziaria, oppure presentare un ricorso al Garante; può altresì presentare a questa Autorità una segnalazione o un reclamo.

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 154, comma 1, lett. *c*), del Codice prescrive ai titolari interessati di conformare il trattamento dei dati personali ai principi richiamati nel presente provvedimento;
b) ai sensi dell'art. 13, comma 5, del Codice, dispone che partiti e movimenti politici, comitati di promotori e sostenitori e singoli candidati possano prescindere dall'informativa agli interessati nei casi indicati nel punto del presente provvedimento;
c) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 7 settembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

52 Il caso Laziomatica. Prescrizioni a tutti i comuni sulla gestione delle anagrafi 6 ottobre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del prof. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Viste le segnalazioni pervenute in ordine all'utilizzazione illecita di dati personali estratti da banche dati anagrafiche del Comune di Roma;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO:

Il Garante ha eseguito alcuni accertamenti ispettivi a seguito di segnalazioni concernenti accessi illeciti a dati anagrafici detenuti presso il Comune di Roma, nonché il rispetto delle misure di sicurezza nel trattamento dei dati, in correlazione ad un caso di falsa sottoscrizione di candidature alle elezioni regionali del 3 e 4 aprile 2005.

Gli accertamenti effettuati anche nell'esercizio di funzioni di polizia giudiziaria hanno fatto emergere notizie di reato che sono state comunicate alla competente autorità giudiziaria.

La violazione degli obblighi e delle garanzie richiamate dal Codice in materia di protezione dei dati personali risulta già accertata in base agli atti acquisiti dal Garante, a prescindere da ogni eventuale responsabilità penale per gli illeciti configurabili.

Tra il 9 e il 14 marzo di quest'anno, presso Laziomatica S.p.A. (società per azioni a prevalente capitale regionale istituita dalla Regione Lazio, che le ha affidato la gestione del Sistema informativo regionale-S.I.R.: *v.* l. r. 3 agosto 2001, n. 20), risultano infatti effettuati alcuni accessi illeciti –per finalità e con modalità non consentite– ad un *data-base* anagrafico del Comune di Roma che la Regione era stata autorizzata a consultare solo per alcune finalità sanitarie, sulla base di un protocollo di intesa.

Le persone che hanno agito presso tale società hanno provveduto, senza averne titolo, ad accogliere la richiesta di un avvocato (che avrebbe potuto essere presentata solo al Comune), con la quale si chiedeva di applicare la disciplina sulle *cd.* indagini difensive (art. 391-*quater* c.p.p.).

Gli accessi in grande quantità, effettuati in singolari circostanze (utilizzo di *password* altrui; consultazioni in orari non di servizio, notturni e festivi; asseriti interventi di manutenzione straordinaria che hanno determinato la cancellazione di dati di tracciamento di accessi), hanno permesso di consultare ed utilizzare illecitamente vari dati personali inerenti anche a documenti di identità, per finalità diverse da quelle per le quali i dati anagrafici erano stati resi accessibili alla Regione.

Gli accertamenti effettuati dal Garante sulla base di una segnalazione sono stati estesi anche alla sicurezza dei dati presso i *data-base* anagrafici del Comune di Roma, ove è emerso il mancato aggiornamento del documento programmatico di sicurezza (di cui è stata data notizia, anche in questo caso, all'autorità giudiziaria con denuncia di reato nei riguardi dei

(*) *G.U.* 24 ottobre 2005, n. 248
[doc. *web* n. 1179484]

competenti dirigenti), unitamente ad alcune inosservanze della disciplina applicabile alla gestione dell'anagrafe della popolazione residente.

A conclusione del complesso procedimento, il Garante dichiara accertate con il presente provvedimento le violazioni intercorse relativamente ai profili di propria competenza, e prescrive alla predetta società e agli enti direttamente interessati le misure necessarie per conformare i trattamenti di dati personali alle disposizioni vigenti. Analoghe prescrizioni vengono impartite in termini generali a tutti i comuni per quanto riguarda la consultazione diretta degli atti anagrafici.

1. Regione Lazio e Laziomatica S.p.A.

A prescindere dai fatti sopra riassunti, è risultato accertato che Laziomatica S.p.A. abbia comunque trattato illecitamente, nell'ambito dell'attività svolta per conto della Regione, i dati personali provenienti dai *data-base* anagrafici del Comune di Roma.

Come premesso, il rapporto Regione-Comune si è basato su un "Protocollo di intesa per la cooperazione nello sviluppo dei servizi al cittadino" stipulato il 12 maggio 2004, che prevede uno scambio di dati tra i due enti per verifiche attinenti solo a prestazioni sanitarie (ticket, scelta del medico), inclusivo di un accesso diretto anche a dati anagrafici detenuti dal Comune.

Tali verifiche sono state affidate dalla Regione a Laziomatica S.p.A. sulla base di una convenzione stipulata nel 2003, con la quale si è conferito alla società il compito di consultare *on-line* i predetti dati anagrafici.

I profili di illiceità emersi sono i seguenti:

a) sono risultate comprovate, anzitutto, alcune inosservanze della convenzione stessa: la società ha infatti violato la clausola che la impegna a non rivelare od utilizzare notizie, informazioni e dati messi a disposizione dalla Regione per finalità diverse da quelle stabilite nella convenzione medesima, e non ha altresì rispettato il distinto impegno contrattuale ad osservare le disposizioni in materia di trattamento dei dati personali;

b) in secondo luogo, sono state violate le disposizioni normative sul responsabile del trattamento. All'apparente designazione in tal senso della società –pur menzionata nella convenzione– non ha fatto seguito, come necessario, né l'elencazione scritta dei compiti affidati rispetto al trattamento dei dati, né l'indicazione delle istruzioni operative (art. 29 del Codice). La società ha anche legittimato all'accesso diretto ulteriori utenti esterni presso altri organismi come le aziende sanitarie locali.

Pertanto, la Regione Lazio (che aveva adottato solo un documento di carattere generale sulle misure di sicurezza presso le strutture della giunta regionale, applicabile ai responsabili del trattamento) potrà continuare ad avvalersi lecitamente della collaborazione della società a condizione che alla designazione di quest'ultima quale responsabile (designazione che in passato è stata al più puramente nominale), conseguano prontamente sia la specificazione analitica dei predetti compiti e istruzioni, sia una vigilanza sulla loro osservanza anche in ordine alla sicurezza dei dati.

Nessuna persona fisica, operante presso la società o la Regione, potrà trattare i dati personali comunicati dal Comune di Roma senza essere stata previamente designata quale incaricato, in conformità al Codice, anche per quanto riguarda l'individuazione del trattamento consentito e le istruzioni da impartire (art. 30 del Codice);

c) la Regione ha avuto accesso ai dati anagrafici provenienti dal Comune di Roma con modalità non consentite. Unitamente all'interrogazione *on-line* di alcuni servizi (documenti; carte di identità, leva militare, vaccinazioni), il predetto Protocollo di intesa ha infatti previsto che la Regione, direttamente o per il tramite della società, possa accedere *on-line* ai dati di origine comunale che la disciplina anagrafica consente invece di ottenere solo con le modalità e con le cautele illustrate più avanti.

Il Protocollo di intesa deve essere quindi rivisto, prevedendo nel congruo termine di cui al seguente dispositivo una diversa modalità di comunicazione dei dati di provenienza comunale, analogamente a quanto dovrà essere disposto, a cura del Comune di Roma, nei riguardi di altri enti ed amministrazioni. Tale revisione, unitamente a quella concernente il rapporto con Laziomatica S.p.a., dovrà essere eseguita nel termine di cui al dispositivo dandone esaustiva comunicazione a questa Autorità.

2. La gestione del sistema informativo anagrafico del Comune di Roma

In base alle disposizioni dell'ordinamento anagrafico, l'ufficiale d'anagrafe può rilasciare attestazioni o certificazioni relativamente al contenuto delle schede che compongono l'anagrafe della popolazione residente, ed entro certi limiti può anche rilasciare elenchi. Ad eccezione del personale autorizzato delle forze di polizia, le medesime schede non possono essere invece consultate direttamente da parte di chiunque, anche facente parte del personale comunale, sia estraneo all'ufficio di anagrafe (artt. 1, 33, 34 e 37 d.P.R. 30 maggio 1989, n. 223).

Più specificamente, gli ufficiali d'anagrafe rilasciano a chiunque ne faccia richiesta "certificati concernenti la residenza e lo stato di famiglia", mentre le altre notizie desumibili dagli atti anagrafici (ad eccezione di quelle riportate nelle schede anagrafiche concernenti, ad esempio, la professione, arte o mestiere, la condizione non professionale, il titolo di studio), possono essere oggetto di attestazione o certificazione, d'ordine del sindaco, "qualora non vi ostino gravi o particolari esigenze di pubblico interesse" (art. 33, commi 1 e 2, del d.P.R. n. 223/1989). L'ufficiale di anagrafe rilascia elenchi degli iscritti nell'anagrafe della popolazione residente, ma solo ad "amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità". Tale utilizzo è consentito anche da parte del comune che detiene i dati, per fini di comunicazione istituzionale, ma sempre su motivata richiesta questa volta "interna" all'ente (art. 177, comma 1, del Codice). Altri soggetti anche privati possono ottenere solo dati anagrafici resi anonimi ed aggregati, su richiesta per fini statistici e di ricerca (art. 34, commi 1 e 2, d.P.R. n. 223/1989).

Queste disposizioni riguardano il particolare contesto degli atti anagrafici, i quali giustificano soluzioni specifiche per quanto riguarda le modalità della loro consultazione. Tale specificità mantiene attualità in un quadro di sistema che prevede opportunamente misure generali di semplificazione dell'azione amministrativa mediante flussi di dati, trasmissioni o consultazioni telematiche di dati ed archivi (artt. 2, comma 5, l. 15 maggio 1997, n. 127; art. 43 d.P.R. 28 dicembre 2000, n. 445).

In termini generali, il Codice non ha inciso sulla portata delle predette disposizioni sull'anagrafe della popolazione. Il Codice ha però ribadito la necessità del perdurante rispetto delle vigenti norme che regolano la conoscibilità e la pubblicità di taluni atti (*cfr., ad es.*, gli artt. 19, comma 3, 24, comma 1, lett. *c*), 59 e 61 del Codice), che subordinano la consultazione di materiale documentale al rispetto di determinati limiti temporali (*ad es.*, con esclusione dei periodi in cui un elenco è in fase di aggiornamento), soggettivi, oppure di talune modalità (*ad es.*, documentazione dell'identità del soggetto che intende consultare un registro) o finalità (*es.*: fini statistici e di ricerca).

Gli accertamenti effettuati hanno evidenziato che nella prassi amministrativa osservata presso il Comune di Roma nei rapporti con numerosi enti, inclusa la Regione, tale quadro normativo non è stato invece preso nella dovuta considerazione, essendosi consentita la consultazione diretta per via telematica di dati anagrafici mediante lo stesso meccanismo di "anagrafe aperta" impropriamente utilizzato per la Regione Lazio.

Riportando i dati anagrafici in una "*data-base* popolazione" contenente anche numerose altre informazioni (relative anche a "vaccinazioni, elettorale, leva militare", dati relativi alla carta d'identità ed al codice fiscale), si è realizzato un sistema telematico che prevede, anzitutto, un'impropria consultazione diretta di dati anagrafici da parte di altro personale comunale non facente parte dei servizi di anagrafe e di stato civile (centrali e dei municipi).

La consultazione diretta dei dati anagrafici per via telematica viene inoltre consentita a numerosi soggetti esterni al Comune di Roma (amministrazioni centrali, militari e sanitarie; uffici giudiziari ed enti locali; ecc.), senza peraltro verificare sempre e compiutamente

né la concreta motivazione di pubblica utilità in base alla quale viene richiesto di conoscere i dati, né le singole utilizzazioni dei dati consentite a regime presso enti a struttura complessa che perseguono differenti finalità. Le procedure di abilitazione all'accesso non soddisfano compiutamente l'esigenza di ottenere la comunicazione dei dati in rapporto solo ad una specifica attività funzionale svolta dal soggetto richiedente. Un ampio numero di utenti è stato infine abilitato in base ad un'istruttoria non approfondita o per utenze per diverso tempo inattive oppure disponibili a soggetti non agevolmente contattabili. Tali criticità sussistono anche nei riguardi di utenti abilitati soltanto alla consultazione dei dati e non anche a modificarli, e sono più marcate nei confronti di soggetti posti in condizione di operare diversi tipi di interrogazione del sistema, oppure di abilitare a loro volta -senza titolo- all'accesso ulteriori utenti.

In sostituzione di tali procedure, il Comune di Roma dovrà pertanto individuare entro il congruo termine di cui al seguente dispositivo un diverso meccanismo che, pur permettendo di comunicare i dati richiesti anche con strumenti automatizzati e per via telematica (e, quindi, di perseguire le finalità di snellimento ed efficienza dell'azione amministrativa a supporto del cittadino). Le richieste di certificazione o attestazione, oppure di rilascio di elenchi ad amministrazioni pubbliche motivato da ragioni accertate di pubblica utilità, potranno essere inoltrate e riscontrate anche automaticamente, per via telematica, escludendo però la consultazione diretta, anche *on-line*, degli atti di provenienza anagrafica da parte di soggetti interni ed esterni diversi da quelli preposti all'ufficio anagrafe. Dovrà altresì aversi cura di:

a) verificare più attentamente la qualifica soggettiva dei richiedenti e la motivazione di pubblica utilità da essi perseguita;

b) porre maggiore attenzione a presupposti, limiti e modalità previste dalla disciplina che riguarda singoli atti e documenti (*cfr.*, per i dati sulle vaccinazioni, art. 4 della legge 4 febbraio 1966, n. 51; art. 3 della legge 5 marzo 1963, n. 292; per il servizio elettorale, art. 51 del d.P.R. 20 marzo 1967, n. 223; per la carta d'identità, art. 289 del r.d. 6 maggio 1940, n. 635; per le liste di leva, artt. 37 e 48 del d.P.R. 14 febbraio 1964, n. 237);

c) individuare soluzioni più idonee per consentire il tracciamento di operazioni di richiesta e di comunicazione di dati presso postazioni di lavoro individuate e da parte di utenti parimenti identificati, monitorando utilizzi impropri e prevenendo accessi multipli realizzati utilizzando una stessa chiave di accesso presso più postazioni di lavoro.

Nel conformare a norma i trattamenti di dati anagrafici, il Comune dovrà altresì:

d) escludere soggetti privati esterni dalla facoltà di consultare direttamente i dati, di acquisirne elenchi su richiesta e di abilitare all'accesso altri soggetti. Nel caso in cui tali soggetti privati comprovino la qualità di effettivi responsabili del trattamento per conto di soggetti pubblici, il rilascio anche informatico di elenchi dovrà essere regolato in primo luogo con il soggetto pubblico, verificando anche l'effettivo rispetto delle modalità richiamate a proposito del rapporto tra titolare e responsabile del trattamento;

e) rivedere l'attuale configurazione della gestione in *outsourcing* del servizio anagrafico, attualmente affidata ad associazioni temporanee di imprese di ampie dimensioni. Dovranno essere adeguate al Codice le prassi seguite per la specificazione dei compiti, per impartire istruzioni riguardo al trattamento dei dati e per la vigilanza anche tramite verifiche periodiche, coordinata con mezzi e soluzioni adeguate alla delicatezza e alla complessità delle questioni trattate e dei flussi di dati.

Le misure da adottare per ottemperare alle predette prescrizioni dovranno essere eseguite nel termine di cui al dispositivo dandone esaustiva comunicazione a questa Autorità.

3. Il trattamento di dati anagrafici da parte delle amministrazioni comunali

Il Garante ritiene necessario prescrivere a tutte le amministrazioni comunali di conformare il trattamento dei dati anagrafici ai principi ed ai limiti richiamati in questa sede. Si sottolinea, in particolare, la necessità di escludere che, nel fornire ad amministrazioni pubbliche elenchi di dati anagrafici per motivi di pubblica utilità, anche telematicamente o

attuando mediante convenzioni flussi di dati verso altri soggetti pubblici (art. 2, comma 5, legge n. 127/1997), si permetta di consultare direttamente i dati dell'anagrafe della popolazione, riportati sia nelle schede anagrafiche informatiche, sia in eventuali elenchi duplicati in *data-base* di "lavoro".

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive:

a) alla Regione Lazio, a Laziomatica S.p.A. e al Comune di Roma di conformare, ove non vi abbiano già provveduto in termini conformi a quanto indicato, i trattamenti di dati personali alle disposizioni e ai princìpi sopra richiamati, procedendo all'attuazione delle misure indicate in motivazione entro centottanta giorni dalla data di ricezione del presente provvedimento;

b) a tutti i comuni di adottare tali misure parimenti necessarie per conformare i trattamenti di dati anagrafici ai principi richiamati nel presente provvedimento;

c) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 6 ottobre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

53 Strutture sanitarie: rispetto della dignità 9 novembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali (direttiva n. 95/46/Ce), anche in relazione agli articoli 2, 10, 11 e 32 della Costituzione;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

CONSIDERATO:

1. Premessa

Sono pervenuti a questa Autorità reclami e segnalazioni con i quali si rappresenta che alcune strutture sanitarie, nell'erogare prestazioni e servizi per finalità di prevenzione, diagnosi, cura e riabilitazione, non rispetterebbero le garanzie previste dalla legge a tutela, in particolare, della dignità e della riservatezza delle persone interessate.

In materia di trattamento dei dati personali in ambito sanitario, il Codice prevede che gli organismi sanitari pubblici e privati adottino misure ed accorgimenti di carattere supplementare rispetto a quelle già previste per il trattamento dei dati sensibili e per il rispetto delle misure di sicurezza. In particolare, l'art. 83 individua alcune specifiche prescrizioni che devono tradursi anche in adeguate misure organizzative, ferma restando la necessità di adottare comunque tutti gli ulteriori accorgimenti che si rendessero opportuni per garantire il più ampio rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

Con il presente provvedimento, il Garante intende richiamare l'attenzione dei soggetti che operano in ambito sanitario in ordine alla necessità di adeguare il funzionamento e l'organizzazione delle strutture sanitarie alle previsioni stabilite dal Codice in materia di protezione di dati personali (art. 83). I medesimi soggetti sono altresì invitati ad adottare tutte le misure ritenute necessarie ed opportune, conformemente ai principi generali, per garantire il rispetto della dignità della persona e il massimo livello di tutela degli interessati in ambito sanitario.

2. Ambito di applicazione delle misure per il rispetto dei diritti degli interessati

Le misure organizzative in esame devono essere adottate per espresso obbligo di legge da tutti gli organismi sanitari, sia pubblici (*es.* aziende sanitarie territoriali, aziende ospedaliere), sia privati (*es.* case di cura).

Sono tenuti alla loro adozione anche i servizi e le strutture di soggetti pubblici operanti in ambito sanitario o aventi competenza in materia di prevenzione e sicurezza del lavoro (*es.* osservatori epidemiologici regionali, servizi di prevenzione e sicurezza sul lavoro).

(*) [doc. *web* n. 1191411]

I medici di medicina generale e i pediatri di libera scelta, nonché, deve ritenersi, anche i medici specialisti operanti in studi medici privati, non sono invece destinatari dell'obbligo di adottare dette misure, che riguardano l'organizzazione di strutture. I medesimi soggetti devono comunque ottemperare ai principi cui si ispirano le disposizioni in esame, predisponendo in ogni caso misure idonee a garantire il rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, secondo modalità adeguate a garantire un rapporto personale e fiduciario con gli assistiti (art. 83, comma 2-*bis*, del Codice).

3. Garanzie per l'interessato

Gli organismi sanitari pubblici e privati, in qualità di titolari del trattamento dei dati personali, devono garantire, in particolare, il rispetto dei seguenti princìpi:

a) dignità dell'interessato (art. 83, comma 2, lett. *e*) del Codice)

La prestazione medica e ogni operazione di trattamento dei dati personali deve avvenire nel pieno rispetto della dignità dell'interessato (artt. 2 e 83 del Codice).

La tutela della dignità personale deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria, con particolare riguardo a fasce deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno.

Particolare riguardo deve essere prestato nel rispettare la dignità di pazienti sottoposti a trattamenti medici invasivi o nei cui confronti è comunque doverosa una particolare attenzione anche per effetto di specifici obblighi di legge o di regolamento o della normativa comunitaria (*ad es.*, in riferimento a sieropositivi o affetti da infezione da Hiv –l. 5 giugno 1990, n. 135–, all'interruzione di gravidanza –l. 22 maggio 1978, n. 194– o a persone offese da atti di violenza sessuale –art. 734-*bis* del codice penale–).

Nei reparti di rianimazione dove si possono visitare i degenti solo attraverso vetrate o videoterminali devono essere adottati accorgimenti, anche provvisori (*ad es.*, mediante paraventi), che delimitino la visibilità dell'interessato durante l'orario di visita ai soli familiari e conoscenti.

La necessità di rispettare la dignità è stata rappresentata a questa Autorità anche in relazione alle modalità di visita e di intervento sanitario effettuati nelle aziende ospedaliero-universitarie alla presenza di studenti autorizzati. Le strutture che intendono avvalersi di questa modalità devono indicare nell'informativa da fornire al paziente che (art. 13 del Codice), in occasione di alcune prestazioni sanitarie, si perseguono anche finalità didattiche, oltre che di cura e prevenzione (*cfr.* d.lg. n. 517/1999). Durante tali prestazioni devono essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.

b) riservatezza nei colloqui e nelle prestazioni sanitarie (art. 83, comma 2, lett. *c*) e *d*))

É doveroso adottare idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario (*ad es.*, in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

Il rispetto di questa garanzia non ostacola la possibilità di utilizzare determinate aree per più prestazioni contemporanee, quando tale modalità risponde all'esigenza terapeutica di diminuire l'impatto psicologico dell'intervento medico (*ad es.*, alcuni trattamenti sanitari effettuati nei confronti di minori).

c) notizie su prestazioni di pronto soccorso (art. 83, comma 2, lett. *f*))

L'organismo sanitario può dare notizia, anche per via telefonica, circa una prestazione di pronto soccorso, ovvero darne conferma a seguito di richiesta anche per via telefonica.

La notizia o la conferma devono essere però fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso.

Questo genere di informazioni riguarda solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso, e non attiene ad informazioni più dettagliate sullo stato di salute.

L'interessato –se cosciente e capace– deve essere preventivamente informato dall'organismo sanitario (*ad es.*, in fase di accettazione), e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

Il personale incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'interessato.

d) dislocazione dei pazienti nei reparti (art. 83, comma 2, lett. *g*))
Il Codice incentiva le strutture sanitarie a prevedere, in conformità agli ordinamenti interni, le modalità per fornire informazioni ai terzi legittimati circa la dislocazione dei degenti nei reparti, allorché si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato.

L'interessato cosciente e capace deve essere, anche in questo caso, informato e posto in condizione (*ad es.*, all'atto del ricovero) di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Occorre altresì rispettare l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota neanche ai terzi legittimati (*cfr.* Carta dei servizi pubblici sanitari, d.P.C.M. 19 maggio 1995).

Come per le prestazioni di pronto soccorso, questo genere di informazioni riguarda la sola presenza nel reparto e non anche informazioni sullo stato di salute.

Possono essere fornite informazioni sullo stato di salute a soggetti diversi dall'interessato quando sia stato manifestato un consenso specifico e distinto al riguardo, consenso che può essere anche manifestato da parte di un altro soggetto legittimato, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato (art. 82).

e) distanza di cortesia (art. 83, comma 2, lett. *b*))
Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari (*es.* operazioni di sportello, acquisizione di informazioni sullo stato di salute), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.

Vanno in questa prospettiva prefigurate appropriate soluzioni, sensibilizzando gli utenti con idonei inviti, segnali o cartelli.

f) ordine di precedenza e di chiamata (art. 83, comma 2, lett. *a*))
All'interno dei locali di strutture sanitarie, nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (*ad es.*, in caso di analisi cliniche), devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa (*ad es.*, attribuendo loro un codice numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione). Ovviamente, tale misura non deve essere applicata durante i colloqui tra l'interessato e il personale medico o amministrativo.

Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (*ad es.*, in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), possono essere utilizzati altri accorgimenti adeguati ed equivalenti (*ad es.*, con un contatto diretto con il paziente).

Non risulta giustificata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di

intervento effettuato o ancora da erogare (*es.* liste di degenti che devono subire un intervento operatorio). Non devono essere, parimenti, resi facilmente visibili da terzi non legittimati i documenti riepilogativi di condizioni cliniche dell'interessato (*es.* cartelle infermieristiche poste in prossimità del letto di degenza) (artt. 22, comma 8, e 26, comma 5, del Codice).

g) correlazione fra paziente e reparto o struttura (art. 83, comma 2, lett. *h*))

Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato.

Tali cautele devono essere orientate anche alle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura (*ad es.*, per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale).

Analoghe garanzie devono essere adottate da tutti i titolari del trattamento, ivi comprese le farmacie, affinché nella spedizione di prodotti non siano indicati, sulla parte esterna del plico postale, informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato (*ad es.*, indicazione della tipologia del contenuto del plico o del reparto dell'organismo sanitario mittente).

h) regole di condotta per gli incaricati (art. 83, comma 2, lett. *i*))

Il titolare del trattamento deve designare quali incaricati o, eventualmente, responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate (artt. 30 e 29 del Codice).

Fermi restando, in quanto applicabili, gli obblighi in materia di segreto d'ufficio, deve essere previsto che, al pari del personale medico ed infermieristico, già tenuto al segreto professionale (art. 9 del codice di deontologia medica del 3 ottobre 1998; art. 4 del codice deontologico per gli infermieri del maggio del 1999), gli altri soggetti che non sono tenuti per legge al segreto professionale (*ad es.*, personale tecnico e ausiliario) siano sottoposti a regole di condotta analoghe (*cfr.* anche art. 10 del codice di deontologia medica).

A tal fine, anche avvalendosi di iniziative di formazione del personale designato, occorre mettere in luce gli obblighi previsti dalla disciplina in materia di protezione dei dati personali con particolare riferimento all'adozione delle predette misure organizzative (artt. 30 e 35 del Codice e punto 19.6 del disciplinare tecnico allegato B) al Codice), evidenziando i rischi, soprattutto di accesso non autorizzato, che incombono sui dati idonei a rivelare lo stato di salute e le misure disponibili per prevenire effetti dannosi.

4. Comunicazione di dati all'interessato

Gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico (individuato dallo stesso interessato, oppure dal titolare del trattamento) o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (*ad es.*, un infermiere designato quale incaricato del trattamento ed autorizzato per iscritto dal titolare).

La necessità di rispettare queste modalità andrebbe menzionata nelle istruzioni impartite agli incaricati del trattamento (art. 84, comma 2, del Codice). Nel caso in cui l'interessato riceva una comunicazione dalla struttura sanitaria che documenti gli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.

Il personale designato deve essere istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato (*es.* referti diagnostici). In riferimento alle numerose segnalazioni pervenute, va rilevato che le certificazioni rilasciate dai laboratori di analisi o dagli altri organismi sanitari pos-

sono essere ritirate anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa.

5. Altri adempimenti da rispettare

I titolari del trattamento in ambito sanitario devono infine rispettare gli obblighi che attengono:

a) alla notificazione al Garante, dovuta nei soli casi di cui all'art. 37 del Codice (*cfr.* anche provvedimento del Garante n. 1/2004 del 31 marzo 2004 recante i casi da sottrarre all'obbligo di notificazione, pubblicato sulla *G.U.* 6 aprile 2004, n. 81 e disponibile sul sito dell'Autorità *www.garanteprivacy.it* [doc. *web* n. 852561]);

b) alla predisposizione dell'informativa da fornire agli interessati (art. 13 del Codice);

c) all'acquisizione del consenso per i trattamenti di dati personali connessi all'erogazione delle prestazioni e dei servizi per svolgere attività di prevenzione, diagnosi, cura e riabilitazione (artt. 22, 26 e 76 del Codice);

d) per gli organismi sanitari pubblici, al rispetto delle disposizioni contenute nel regolamento per il trattamento dei dati sensibili per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione adottato ai sensi dell'art. 20 del Codice (*cfr. Provv.* del 30 giugno 2005[1]);

e) al rispetto delle autorizzazioni generali rilasciate dal Garante ed, in particolare, dell'autorizzazione generale al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (artt. 26 e 76 del Codice);

f) alle misure di sicurezza (artt. 31-36 del Codice e Allegato B) al Codice).

TUTTO CIÒ PREMESSO, IL GARANTE:

a) prescrive a tutti i titolari del trattamento di dati personali interessati in ambito sanitario, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice di adottare, ove già non attuate, le misure necessarie od opportune al fine di rendere il trattamento dei medesimi dati conforme alle disposizioni vigenti, sulla base dei principi richiamati nel presente provvedimento e dei primi chiarimenti con esso forniti;

b) prescrive ai medesimi titolari, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice di adottare comunque tutte le ulteriori misure per garantire, in materia di trattamento dei dati personali nell'ambito sanitario, il massimo rispetto del principio di dignità;

c) avvia una consultazione allo scopo di acquisire elementi di informazione e documentazione da parte di organismi sanitari, nonché di soggetti, portatori di interessi pubblici e privati e portatori di interessi diffusi, costituiti in associazioni e comitati, in ordine alle modalità di attuazione adottate ed alle problematiche riscontrate.

Roma, 9 novembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

(1) [doc. *web* n. 1144445]

54 Liceità, correttezza e pertinenza nell'attività di recupero crediti 30 novembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Esaminate le segnalazioni presentate da singoli ed associazioni di tutela dei consumatori concernenti il trattamento di dati personali nell'ambito dell'attività di recupero crediti;

Visti gli elementi acquisiti a seguito degli accertamenti avviati ai sensi dell'art. 154, comma 1, lettere *a*) e *b*), del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Ritenuta la necessità di prescrivere ai titolari del trattamento alcune misure necessarie al fine di rendere detti trattamenti conformi alle disposizioni vigenti (art. 154, comma 1, lett. *c*), del Codice);

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

Relatore il dott. Giuseppe Fortunato;

PREMESSO:

1. Il trattamento di dati personali nelle attività di recupero crediti

Sono pervenute a questa Autorità numerose segnalazioni concernenti trattamenti di dati personali (e comportamenti) posti in essere a danno di debitori (e, più in generale, di soggetti comunque tenuti all'adempimento) in occasione dello svolgimento di attività di recupero crediti. Tale attività può essere realizzata direttamente dal creditore come pure, nel suo interesse, da terzi, di regola operanti in virtù di contratti di collaborazione (in particolare, attraverso la figura del mandato o dell'appalto di servizi). In quest'ultima ipotesi, l'attività di recupero crediti è preceduta dalla messa a disposizione di dati personali relativi al debitore. Si tratta, per lo più, di dati anagrafici, di informazioni utili per contattarlo (quali, ad esempio, i recapiti telefonici), oltre ai dati relativi alla somma dovuta (entità della medesima causale eventualmente indicata, termini apposti all'obbligazione pecuniaria, oltre che titolo della stessa).

Le risultanze hanno evidenziato l'esistenza di alcune prassi finalizzate al recupero stragiudiziale dei crediti, caratterizzate da modalità di ricerca e di presa di contatto invasive e, talora, lesive della riservatezza e della dignità personale.

In particolare, le modalità di ricerca, presa di contatto, sollecitazione, o altrimenti connesse all'esazione della somma dovuta, si manifestano nelle forme più varie: visite al domicilio o sul luogo di lavoro; sollecitazioni su utenze di telefonia fissa o mobile, comprensive dell'invio di messaggi sms di sollecito; comunicazioni telefoniche il cui contenuto a carattere sollecitatorio è preregistrato, poste in essere senza intervento di un operatore (con il rischio che soggetti diversi dal destinatario vengano a conoscenza del contenuto della chiamata); invii di avvisi relativi all'apertura della procedura di recupero crediti tramite comunicazioni individualizzate, con l'inoltro di corrispondenza recante informazioni idonee a lasciar trasparire la situazione debitoria (ad esempio, plichi recanti all'esterno la scritta "recupero crediti" o locuzioni simili) relativa agli interessati o contenenti riferimenti suscettibili di indurre il destinatario in errore circa il valore e la provenienza dell'intimazione a pagare

(*) [doc. *web* n. 1213644]

(usuale è il ricorso a formule quali "preavviso esecuzione notifica" o il richiamo di norme di rito con il riferimento alla futura attivazione di "ufficiali giudiziari"); affissioni di avvisi di mora sulla porta del debitore.

Non di rado, inoltre, l'attività preordinata al recupero crediti, coinvolge non soltanto il debitore, ma anche terzi, con modalità tali da metterli a conoscenza di vicende personali riferite a quest'ultimo (ad esempio, familiari, conoscenti o vicini di casa, anche utilizzando recapiti non forniti al momento della stipula del contratto e non reperibili in pubblici elenchi).

Al fine di rendere conformi alle disposizioni vigenti in materia di protezione dei dati personali i trattamenti effettuati nell'ambito dell'attività di recupero crediti il Garante, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive ai titolari del trattamento l'adozione delle misure necessarie di seguito specificamente indicate, evidenziando che il creditore deve comunque adoperarsi affinché i principi richiamati con il presente provvedimento siano rispettati nell'attività materiale di recupero crediti, anche se affidata a terzi, e che gli interessati, ove i comportamenti tenuti in sede di recupero crediti integrino un illecito civile (per quanto attiene al profilo del risarcimento del danno eventualmente subito) o penale (in quanto suscettibili di integrare fattispecie di reato quali le molestie o le minacce), possono ricorrere all'autorità giudiziaria ordinaria per i profili di rispettiva competenza.

2. Principio di liceità nel trattamento

Chiunque effettui un trattamento di dati personali nell'ambito dell'attività di recupero crediti deve osservare il principio di liceità nel trattamento: tale precetto è violato dal comportamento (attuato da taluni operatori economici) consistente nel comunicare ingiustificatamente a soggetti terzi rispetto al debitore (quali, ad esempio, familiari, coabitanti, colleghi di lavoro o vicini di casa), informazioni relative alla condizione di inadempimento nella quale versa l'interessato (comportamento talora tenuto per esercitare indebite pressioni sul debitore al fine di conseguire il pagamento della somma dovuta).

Integra, altresì, un trattamento illecito il ricorso alle descritte comunicazioni telefoniche preregistrate volte a sollecitare il pagamento, realizzate senza l'intervento di operatore, essendo tale modalità di contatto suscettibile di rendere edotti soggetti diversi dal debitore della sua asserita condizione di inadempimento.

Del pari, diffusione illecita di dati personali si ha con l'affissione ad opera di incaricati del recupero crediti di avvisi di mora (o, comunque, di sollecitazioni di pagamento) sulla porta del debitore, potendo tali dati personali venire a conoscenza di una serie indeterminata di soggetti nell'intervallo di tempo (talora prolungato) in cui l'avviso risulta visibile.

3. Principio di correttezza nel trattamento

In occasione dello svolgimento delle attività di recupero crediti deve altresì essere osservata la clausola generale di correttezza (art. 11, comma 1, lett. *a*), del Codice): in base ad essa sono preclusi, sia in fase di raccolta delle informazioni sul debitore, sia nel tentativo di prendere contatto con il medesimo (anche attraverso terzi), comportamenti suscettibili di incidere sulla sua dignità, qui riguardata sul solo piano della disciplina di protezione dei dati personali.

Sono pertanto illecite le operazioni di trattamento consistenti nel sollecitare il pagamento con modalità che palesino ad osservatori esterni il contenuto della comunicazione: ciò può accadere nel caso di utilizzo di cartoline postali o tramite l'invio di plichi recanti all'esterno la scritta "recupero crediti" (o locuzioni simili dalle quali possa comunque desumersi l'informazione relativa all'asserito stato di inadempimento del destinatario della comunicazione).

Attesa la natura delle informazioni trattate e l'elevato rischio di diffusione a terzi di informazioni personali relative al debitore, è pertanto necessario che le sollecitazioni di pagamento siano portate a conoscenza del solo debitore, ricorrendo a plichi chiusi, che riportino all'esterno le sole indicazioni necessarie ad identificare il mittente, prive di dati eccedenti rispetto a quelli necessari al recapito della comunicazione (in questo senso, al fine di evitare un'inutile divulgazione di dati personali, *v.* già in materia di notificazione degli atti giudiziari, *Provv.* 22 ottobre 1998[1], in *Boll.* n. 6/1998, p. 13; *v.* altresì, con riferimento ad una fattispecie particolare, *Provv.* 12 giugno 2000[2], in *Boll.* n. 13/2000, p. 38, 41).

(1) [doc. *web* n. 1104097]

(2) [doc. *web* n. 30923]

In tal senso, inoltre, depongono alcune innovazioni apportate al codice di procedura civile (*cfr.*, in particolare, gli artt. 137, comma 3, 140, 250, comma 2, c.p.c., come modificati dall'art. 174 del Codice), introdotte per rendere tale disciplina compatibile con le finalità di protezione dei valori personali menzionati all'art. 2, comma 1, del Codice, come pure alcune norme (settoriali) che, disciplinando la modalità trasmissiva di intimazioni di pagamento, ne prevedono la comunicazione in plico chiuso (*cfr.*, ad esempio, art. 26 d.P.R. 29 settembre 1973 n. 602, Disposizioni sulla riscossione delle imposte sul reddito, relativo alla notificazione della cartella di pagamento; art. 11, comma 1, d.m. 14 giugno 2004, Approvazione delle modalità di gestione del fondo di garanzia per il credito al consumo, di cui al d.m. 22 dicembre 2003; art. 4, comma 1, d.m. 9 marzo 2001 n. 124, Regolamento concernente le modalità di istituzione del Fondo di garanzia sulle operazioni di credito relative al programma "P.C. per gli studenti").

4. Principi di pertinenza e finalità

Il trattamento delle informazioni personali effettuato nell'ambito delle attività di recupero crediti deve svolgersi, altresì, nel rispetto dei principi di pertinenza, finalità e qualità dei dati (artt. 11 del Codice).

A tal fine possono formare oggetto di trattamento i soli dati necessari all'esecuzione dell'incarico, con particolare riferimento ai dati anagrafici riferiti al debitore, codice fiscale (o partita Iva del medesimo), ammontare del credito vantato (unitamente alle condizioni del pagamento) e recapiti (anche telefonici), di norma forniti dall'interessato in sede di conclusione del contratto o comunque desumibili da elenchi o registri pubblici.

Salvo l'assolvimento di specifici obblighi di legge (ad esempio, per rendere conto delle attività svolte), che può richiedere una conservazione prolungata dei dati raccolti, una volta portato a termine l'incarico, i medesimi non devono formare oggetto di ulteriore trattamento.

La loro eventuale conservazione ulteriore deve essere realizzata con modalità comunque tali da precluderne agli incaricati del trattamento la normale consultabilità (con l'adozione di opportune misure logiche o provvedendo alla trasposizione dei dati in archivi separati).

5. Informativa agli interessati

In attuazione dei principi di protezione dei dati personali, il titolare del trattamento deve rendere edotti gli interessati (di norma in sede di conclusione del contratto) delle informazioni previste all'art. 13 del Codice, con particolare riferimento all'indicazione degli eventuali responsabili del trattamento ai quali è rimesso l'incarico di procedere al recupero crediti (se del caso, ai sensi dell'art. 13, comma 1, lett. *f*), del Codice, indicandoli nel proprio sito Internet e facendo ad esso espresso riferimento nell'informativa resa).

Ove i dati vengano raccolti presso terzi trova applicazione l'art. 13, comma 4, del Codice.

TUTTO CIÒ PREMESSO, IL GARANTE

prescrive, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, ai titolari di trattamenti di dati personali nell'ambito dell'attività di recupero crediti le misure necessarie ed opportune di cui ai punti da 1 a 5 del presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti.

Roma, 30 novembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

55 Luoghi di lavoro: accertamenti della tossicodipendenza per particolari addetti 15 dicembre 2005 (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la richiesta di parere del Ministero del lavoro e delle politiche sociali;

Visto l'articolo 125 del d.P.R. 9 ottobre 1990, n. 309, e successive modificazioni, recante il testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza;

Visto l'articolo 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

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

Relatore il dott. Mauro Paissan;

PREMESSO:

Il Ministero del lavoro e delle politiche sociali ha chiesto il parere del Garante su uno schema di regolamento che individua le categorie di lavoratori destinati a mansioni che comportano rischi per la sicurezza, l'incolumità e la salute dei terzi, da sottoporre ad accertamento dell'assenza di tossicodipendenza, nonché la periodicità e le modalità di tali accertamenti.

OSSERVA:

1. Considerazioni generali

La disposizione del decreto del 1990 (art. 125 d.P.R. 9 ottobre 1990, n. 309) che trova ora attuazione riguarda una tematica di particolare delicatezza che ha implicazioni rilevanti sia per la sicurezza, l'incolumità e la salute di terzi e della collettività, sia per i diritti fondamentali dei lavoratori interessati.

Gli accertamenti in esame, comprensivi di prelievi ed analisi, rappresentano un "trattamento sanitario" alla luce anche di quanto rilevato dalla giurisprudenza costituzionale (art. 32 Cost.; *cfr.* sentenza Corte cost. n. 218 del 1994). La legge può imporli in ragione di rilevanti necessità di terzi o della collettività, ma sul presupposto del rispetto delle persone che vi vengono sottoposte e, pertanto, di un'efficace protezione, in particolare, della loro dignità e riservatezza, anche per prevenire ingiustificate discriminazioni o emarginazioni nella vita lavorativa e di relazione. Assume, quindi, particolare rilievo la circostanza che gli accertamenti sull'assenza di tossicodipendenza siano improntati a garantire in modo efficace anche i diritti dei lavoratori interessati, considerata la particolare natura dei dati trattati che possono essere idonei a rivelare lo stato di salute.

Il trattamento di dati personali relativo agli accertamenti in esame deve essere effettuato da datori di lavoro e strutture sanitarie per tutelare la sicurezza, l'incolumità e la salute di

(*) [doc. *web* n. 1209068]

terzi e della collettività, ed è previsto da una disposizione di legge (art. 125 d.P.R. n. 309/1990; artt. 11, comma 1, lett. *a*), 18, 19 e 20 del Codice).

Secondo i ministeri interessati, le attività lavorative che comportano un elevato rischio per la sicurezza, l'incolumità e la salute dei terzi sono individuate in quelle elencate nell'allegato I allo schema di decreto.

Gli accertamenti sanitari verrebbero disposti, stante la formulazione della disposizione di legge che si intende attuare, solo nei confronti di "lavoratori" destinati alle predette attività; non sarebbero interessati, invece, né coloro che svolgono le medesime attività in proprio, né il datore di lavoro che le esegua personalmente.

2. Ambito e modalità degli accertamenti

Il presente parere è reso solo per i profili di competenza del Garante.

Va a tal fine rilevato che alcune disposizioni dello schema riguardanti l'individuazione dei lavoratori interessati o i casi in cui gli accertamenti sanitari dovrebbero essere effettuati, devono essere riformulate in ossequio al principio di proporzionalità nel trattamento dei dati personali (art. 11, comma 1, lett. *d*), del Codice, in riferimento agli artt. 3 e 5, comma 3 dello schema).

Le specificazioni di seguito indicate sono necessarie anche nella prospettiva dell'impostazione armonica di altri tipi di accertamenti sanitari obbligatori di cui dovrebbero essere disciplinati analogamente alcuni profili (in particolare, in materia di controlli alcolimetrici nei luoghi di lavoro –art. 15 l. 30 marzo 2001, n. 125– e di trasmissione dell'infezione da Hiv –*cfr.* art. 5 l. 5 giugno 1990, n. 135–).

In questa prospettiva, deve essere meglio tipizzata la previsione (art. 5, comma 3, lett. a)) che impone esami complementari tossicologici a carico del lavoratore il quale presenti "sintomi di tossicodipendenza", previsione che risulterebbe di problematica applicazione e non conforme alla norma primaria da attuare. Deve risultare più evidente che gli esami complementari vanno eseguiti solo se ricorrono fattori sintomatici di una "dipendenza" da sostanze stupefacenti o psicotrope, anziché solo di un uso -anche occasionale- delle sostanze medesime. Tale specificazione va apportata nello schema, non apparendo sufficiente né un rinvio al decreto sulle procedure analitiche (art. 8, comma 4), né l'applicazione dell'altro d.m. del Ministro della salute che verrebbe applicato provvisoriamente (*v.* art. 12, comma 2).

Va altresì individuata con precisione la casistica degli incidenti sul lavoro che possono imporre un esame complementare tossicologico (art. 5, comma 3, lett. b), dello schema). Attualmente, si prevede che debbano essere sottoposti a tale esame tutti i lavoratori comunque coinvolti a qualsiasi titolo in un incidente sul lavoro, anche senza colpa e senza una qualche attinenza ad un fattore sintomatico di una tossicodipendenza. L'obbligo di sottoporsi ad esame tossicologico dovrebbe essere invece previsto proporzionatamente solo in presenza di incidenti che, per le loro caratteristiche e valutando il profilo comportamentale degli interessati coinvolti, si rivelino appunto sintomatici di una tossicodipendenza.

3. Trattamento dei dati personali

3.1. Applicabilità del Codice

Il trattamento dei dati personali cui si procederà in applicazione del decreto è già disciplinato dal Codice in materia di protezione dei dati personali, il quale individua specifiche regole per i datori di lavoro pubblici e privati e per le strutture sanitarie riguardo, in particolare, all'adeguata informativa da fornire ai lavoratori interessati, alle specifiche modalità di trattamento, alla conservazione dei dati nel tempo, alla necessaria designazione degli incaricati del trattamento e alle misure di sicurezza (*v.* anche artt. 20 e 112, comma 2, lett. *c*), *e*) ed *i*), del Codice, in relazione all'individuazione dei tipi di dati sensibili e di operazioni di trattamento in ambito pubblico).

Si richiama altresì l'attenzione sul requisito della qualità dei dati personali (art. 11 del Codice) che va rispettato con particolare cura nel trattamento di quelli in esame, specie per quanto riguarda l'esattezza, l'aggiornamento, la pertinenza e non eccedenza dei dati. Ciò,

anche alla luce delle conseguenze che si possono trarre dagli accertamenti e dalla circostanza che il decreto prevede anche che si prendano in considerazione dati relativi a fenomeni meramente sintomatici (art. 5, comma 3, lett. *a*), dello schema).

3.2 Finalità del trattamento dei dati

Appare necessario inserire nel testo una precisa, ed importante, "clausola di finalità" per affermare che nelle procedure di accertamento dell'assenza di tossicodipendenza possono essere trattati solo dati personali indispensabili per perseguire le finalità di cui al decreto e che i medesimi dati possono essere utilizzati esclusivamente per le medesime finalità di tutela della sicurezza, incolumità e salute di terzi.

Risulta, altresì, necessario specificare la finalità per la quale i dati del personale marittimo devono essere comunicati anche al Ministero delle infrastrutture e dei trasporti e da questo ulteriormente utilizzati (art. 8, comma 9, dello schema).

3.3. Riservatezza del flusso di dati personali

La specifica previsione di riservatezza sull'esito degli accertamenti (art. 8, comma 9, dello schema) deve essere formulata anche in riferimento all'attività della struttura sanitaria e alle comunicazioni al datore di lavoro da essa effettuate, oltre che al successivo trattamento dei dati da parte del datore di lavoro (si veda la simmetrica previsione di riservatezza relativa alla richiesta di accertamenti: art. 5, comma 4, dello schema). Tale riformulazione va apportata con specifica attenzione anche ai casi in cui la struttura sanitaria si avvalga a sua volta di altre strutture convenzionate (art. 8, comma 2).

3.4. Accertamenti presso forze armate e di polizia

Occorre prevedere nell'art. 6, comma 1, secondo periodo, dello schema (tenuto conto dell'art. 1, comma 2), che gli ulteriori accertamenti specifici presso forze di polizia, forze armate e il Corpo nazionale dei vigili del fuoco sono effettuabili solo nei casi previsti dalla normativa di settore.

In conclusione, nel ricordare che l'ulteriore decreto previsto per disciplinare le "procedure analitiche" degli accertamenti dovrà essere sottoposto al preventivo parere di questa Autorità, stanti i profili di interesse per il trattamento dei dati personali (art. 8, comma 4, dello schema), si formula il parere richiesto con le osservazioni che precedono.

TUTTO CIÒ PREMESSO IL GARANTE:

esprime il parere sullo schema di decreto con le osservazioni di cui ai punti 2 e 3 relative all'individuazione dei lavoratori da sottoporre ad esami complementari tossicologici, alle finalità del trattamento dei dati, alla qualità dei medesimi dati, alla riservatezza del loro flusso e ad accertamenti specifici presso forze armate e di polizia.

Roma, 15 dicembre 2005

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

Unione europea

56 Conservazione dei dati trattati nell'ambito della fornitura di servizi di comunicazione elettronica (*)

L 105/54 IT Gazzetta ufficiale dell'Unione europea 13.4.2006

DIRETTIVA 2006/24/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 15 marzo 2006

riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 95,

vista la proposta della Commissione,

visto il parere del Comitato economico e sociale europeo (1),

deliberando secondo la procedura di cui all'articolo 251 del trattato (2),

considerando quanto segue:

(1) Conformemente alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (3), gli Stati membri sono tenuti a tutelare i diritti e le libertà delle persone fisiche relativamente al trattamento dei dati personali, e in particolare il diritto alla vita privata, per assicurare la libera circolazione dei dati personali nella Comunità.

(2) La direttiva 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (4), traduce i principi enunciati nella direttiva 95/46/CE in norme specifiche per il settore delle comunicazioni elettroniche.

(3) Gli articoli 5, 6 e 9 della direttiva 2002/58/CE definiscono le norme applicabili al trattamento, da parte dei fornitori di reti e servizi, dei dati relativi al traffico e dei dati relativi all'ubicazione generati dall'uso di servizi di comunicazione elettronica. Questi dati devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, tranne per quanto riguarda i dati necessari per la fatturazione o per il pagamento dell'interconnessione. Previo consenso, alcuni dati possono anche essere trattati a fini di commercializzazione o per la fornitura di servizi a valore aggiunto.

(4) L'articolo 15, paragrafo 1, della direttiva 2002/58/CE enumera le condizioni a cui gli Stati membri possono limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi 1, 2, 3 e 4, e all'articolo 9 di tale direttiva. Ogni restrizione di questo tipo deve essere necessaria, opportuna e proporzionata, all'interno di una società democratica, per specifici fini di ordine pubblico, vale a dire per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, o per la prevenzione, indagine, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato dei sistemi di comunicazione elettronica.

(5) Diversi Stati membri hanno adottato normative sulla conservazione di dati da parte dei fornitori dei servizi a fini di prevenzione, indagine, accertamento e perseguimento dei reati. Le disposizioni delle varie legislazioni nazionali differiscono considerevolmente.

(6) Le differenze giuridiche e tecniche fra le disposizioni nazionali relative alla conservazione dei dati ai fini di prevenzione, indagine, accertamento e perseguimento dei reati costituiscono un ostacolo al mercato interno delle comunicazioni elettroniche, giacché i fornitori dei servizi devono rispettare esigenze diverse per quanto riguarda i tipi di dati relativi al traffico e i tipi di dati relativi all'ubicazione da conservare e le condizioni e la durata di tale conservazione.

(7) Le conclusioni del Consiglio «Giustizia e affari interni» del 19 dicembre 2002 sottolineano che, a motivo dell'importante aumento delle possibilità offerte dalle comunicazioni elettroniche, i dati relativi all'uso di queste ultime costituiscono uno strumento particolarmente importante e valido nella prevenzione, indagine, accertamento e perseguimento dei reati, in particolare della criminalità organizzata.

(8) Con la dichiarazione sulla lotta al terrorismo, adottata il 25 marzo 2004, il Consiglio europeo ha incaricato il Consiglio di esaminare misure relative all'istituzione di norme sulla conservazione dei dati relativi al traffico delle comunicazioni da parte dei fornitori di servizi.

(1) Parere espresso il 19 gennaio 2006 (non ancora pubblicato nella Gazzetta ufficiale).

(2) Parere del Parlamento europeo del 14 dicembre 2005 (non ancora pubblicato nella Gazzetta ufficiale) e decisione del Consiglio del 21 febbraio 2006.

(3) GU L 281 del 23.11.1995, pag. 31. Direttiva modificata dal regolamento (CE) n. 1882/2003 (GU L 284 del 31.10.2003, pag. 1).

(4) GU L 201 del 31.7.2002, pag. 37.

(*) *G.U.U.E.* 13 aprile 2006, L 105/54 [doc. *web* n. 1295222]

57 Miglioramento della cooperazione di polizia, con particolare riferimento ai confini interni (*) (modifica della Convenzione di applicazione Schengen)

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 18.7.2005
COM(2005)317 final

2005/0131(CNS)

Proposal for a

COUNCIL DECISION

on the improvement of police cooperation between the Member States of the European Union, especially at the internal borders and amending the Convention implementing the Schengen Agreement

(presented by the Commission)

EN EN

(*) [doc. *web* n. 1296371]

58 Decisione sull'istituzione del Sistema informativo Schengen di seconda generazione (Sis II) (*)

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.5.2005
COM(2005) 230 final

2005/0103 (CNS)

Proposal for a

COUNCIL DECISION

on the establishment, operation and use of the second generation Schengen information system (SIS II)

(presented by the Commission)

(*) [doc. *web* n. 1296377]

59 Regolamento sull'istituzione del Sistema informativo Schengen di seconda generazione (Sis II) (*)

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.5.2005
COM(2005) 236 final

2005/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment, operation and use of the second generation Schengen information system (SIS II)

(presented by the Commission)

(*) [doc. *web* n. 1296381]

60 Accesso al Sistema informativo Schengen di seconda generazione (Sis II) per l'emissione delle carte di circolazione dei veicoli (*)

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 31.05.2005
COM(2005)237 final

2005/0104(COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates

(presented by the Commission)

EN EN

(*) [doc. *web* n. 1296386]

61 Protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (*)

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 4.10.2005
COM(2005) 475 definitivo

2005/0202 (CNS)

Proposta di

DECISIONE QUADRO DEL CONSIGLIO

sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale

{SEC(2005) 1241}

(presentata dalla Commissione)

(*) [doc. *web* n. 1296390]

62 Scambio di informazioni in virtù del principio di disponibilità (*)

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 12.10.2005
COM(2005) 490 definitivo

2005/0207 (CNS)

Proposta di

DECISIONE QUADRO DEL CONSIGLIO

sullo scambio di informazioni in virtù del principio di disponibilità

(presentata dalla Commissione)

{SEC(2005) 1270}

(*) [doc. *web* n. 1296154]

63 Formato uniforme per i permessi di soggiorno dei cittadini di Paesi terzi (*)

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 10.3.2006
COM(2006) 110 final

2003/0218 (CNS)

Modified proposal for a

COUNCIL REGULATION

amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals

(presented by the Commission pursuant to Article 250 (2) of the EC Treaty)

EN **EN**

(*) [doc. *web* n. 1296394]

Consiglio dell'Unione europea

64 Requisiti minimi comuni di sicurezza per le carte di identità nazionali (*)

DRAFT

CONCLUSIONS OF THE REPRESENTATIVES OF THE GOVERNMENTS OF THE MEMBER STATES ON COMMON MINIMUM SECURITY STANDARDS FOR MEMBER STATES' NATIONAL IDENTITY CARDS

Recognising the mandate given to Member States by the Hague Programme and the 13 July 2005 Justice and Home Affairs Council;

Recognising the importance of ensuring the security of travel and other identity documents;

Recognising that the mandate relates only to security standards, not to any domestic uses of national identity cards and that no legally binding standards or timetables are being imposed;

Without prejudging the issue of the possible legal basis for a measure harmonising minimum security standards for national identity cards and without affecting the right of each Member State to decide whether or not to issue national identity cards and whether to use biometric identifiers;

Recognising the priority to be attached to compliance with the standards established by the European Union in Council Regulation (EC) 2252/2004 on passports, and the draft regulations amending legislation on visas and residence permits;

Building upon the work already done on security features for passports, and bearing in mind the need for interoperability based on ICAO standards;

The Member States of the European Union, working together on an intergovernmental basis:

1. Have decided to accept the following interim conclusions of the experts working in the Committee created by Article 6 of Council Regulation (EC) 1683/95, which will be followed by more detailed technical standards in due course:

(*) [doc. *web* n. 1296403]

65 Convenzione di Prüm sulla lotta al terrorismo, al crimine transfrontaliero e all'immigrazione clandestina 27 maggio 2005 (*)

Convention

between

the Kingdom of Belgium,
the Federal Republic of Germany,
the Kingdom of Spain,
the French Republic,
the Grand Duchy of Luxembourg,
the Kingdom of the Netherlands and
the Republic of Austria

on the

stepping up of cross-border cooperation,
particularly in combating terrorism, cross-border crime and illegal migration

(*) [doc. *web* n. 1296398]

Gruppo art. 29

66 Livello di protezione garantito in Canada ai fini della trasmissione, da parte delle compagnie aeree, dei dati sui viaggiatori (*)

Gruppo di lavoro per la tutela dei dati – Articolo 29

1112/05/IT
WP 103

Parere 1/2005 sul livello di protezione garantito in Canada per la trasmissione, da parte delle compagnie aeree, dei dati di identificazione delle pratiche e di informazioni anticipate sui viaggiatori

Adottato il 19 gennaio 2005

Il Gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE.

Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, proprietà intellettuale e industriale, media e protezione dei dati) della Direzione generale "Mercato interno" della Commissione europea, B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136.

Sito Internet: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1296159]

67 Questioni di protezione dati relative ai diritti di proprietà intellettuale (*)

ARTICLE 29 Data Protection Working Party

xxxx/05/EN
WP 104

Working document on data protection issues related to intellectual property rights

January 18, 2005

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1295268]

68 Protezione dati e tecnologie *Rfid* (*)

ARTICLE 29 Data Protection Working Party

10107/05/EN
WP 105

Working document on data protection issues related to RFID technology

January 19, 2005

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1296164]

69 Notificazione dei trattamenti di dati e ruolo dei *privacy officer* (*)

ARTICLE 29 Data Protection Working Party

10211/05/EN
WP 106

Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union

Adopted on 18 January 2005

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate D (Knowledge-based economy) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1295406]

70 Trasferimento all'estero di dati e "regole vincolanti nell'impresa" (*)

ARTICLE 29 Data Protection Working Party

05/EN
WP107

Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"

Adopted on April 14th, 2005

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Justice, Freedom and Security Directorate-General.

Website: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1296182]

71 Modello di richiesta ai fini dell'approvazione di "regole vincolanti nell'impresa" (*)

ARTICLE 29 Data Protection Working Party

05/EN
WP108

Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules

Adopted on April 14th, 2005

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article30 of Directive95/46/EC and Article 15 of Directive2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Justice, Freedom and Security Directorate-General.
Website: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1296173]

72 Sistema di informazione visti (Vis) e scambio di dati sui visti per soggiorni di breve durata (*)

ARTICOLO 29 Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

1022/05/IT
WP 110

Parere
sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata
(COM(2004) 835 def.)

Adottato il 23 giugno 2005

Il presente gruppo è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo consultivo europeo indipendente preposto alla tutela delle persone con riguardo al trattamento dei dati personali e alla protezione della vita privata. Le sue mansioni sono descritte all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segretariato sono garantite dalla direzione C (Giustizia civile, diritti e cittadinanza) della Commissione europea, direzione generale Giustizia, libertà e sicurezza, B-1049 Bruxelles, Belgio, ufficio LX-46 01/43.

Sito Internet: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

(*) [doc. *web* n. 1296179]

73 Caratteristiche di sicurezza ed elementi biometrici nei passaporti e nei documenti di viaggio (*)

Gruppo di lavoro ARTICOLO 29, protezione dati

1710/05/IT riv.
WP 112
04/09/12

Progetto di parere
riguardante l'attuazione del regolamento (CE n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri
(*Gazzetta ufficiale L 385 del 29.12.2004, pp. 1-6*)

Adottato il 30 settembre 2005

Questo gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta di un organo consultivo europeo indipendente, che si occupa della salvaguardia e della riservatezza dei dati. I suoi compiti sono descritti all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Alla segreteria provvede la Direzione C (Giustizia civile, diritti e cittadinanza) della Direzione generale Giustizia, libertà e sicurezza della Commissione europea, Ufficio LX-46 01/43, B-1049 Bruxelles, Belgio.

Sito web: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

(*) [doc. *web* n. 1296183]

74 Conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica (*)

ARTICOLO 29 - Gruppo per la tutela dei dati personali

1868/05/IT
WP 113

Parere /2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE (COM(2005)438 definitivo del 21.9.2005)

Adottato il 21 ottobre 2005

Il gruppo, istituito in virtù dell'articolo 29 della direttiva 95/46/CE, è l'organo consultivo indipendente dell'UE per la tutela dei dati personali e del diritto alla riservatezza. I suoi compiti sono fissati all'articolo 30 della richiamata direttiva e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Giustizia civile, diritti fondamentali e cittadinanza) della Commissione europea, direzione generale Giustizia, libertà e sicurezza, B 1049 Bruxelles, Belgio, ufficio LX-46 01/43

Sito Web: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

(*) [doc. *web* n. 1296193]

75 Trasferimento all'estero dei dati e adeguatezza: linee di interpretazione armonizzata (*)

Gruppo di lavoro ARTICOLO 29

2093-01/05/IT
WP 114

Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1 della direttiva 95/46/CE del 24 ottobre 1995

Adottato il 25 novembre 2005

Il Gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta di un organo consultivo europeo indipendente, che si occupa della protezione dei dati e della vita privata. I suoi compiti sono stabiliti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 15 della direttiva 2002/58/CE.

Il servizio di segretariato è fornito dalla Direzione C (Giustizia civile, diritti e cittadinanza – Protezione dei dati) della Commissione europea, Direzione generale Giustizia, Libertà e Sicurezza, B-1049, Bruxelles, Belgio, Ufficio No LX46 1/143.

Indirizzo Internet:

(*) [doc. *web* n. 1296197]

76 Uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (*)

ARTICOLO 29 - Gruppo per la tutela dei dati personali

2130/05/IT
WP 115

Gruppo di lavoro per la tutela dei dati "Articolo 29" sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto

Adottato il 25 novembre 2005

Il gruppo di lavoro è stato istituito dall'articolo 29 della direttiva 95/46/CE. Si tratta dell'organo indipendente di consulenza dell'UE per la protezione dei dati e della vita privata. I suoi compiti sono stabiliti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 15 della direttiva 2002/58/CE.

Il servizio di segretariato è fornito dalla Direzione C (Giustizia civile, diritti e cittadinanza) della Commissione europea, Direzione generale Giustizia, Libertà e Sicurezza, B-1000 Bruxelles, Belgio

Sito Internet: www.europa.eu.int/comm/privacy

(*) [doc. *web* n. 1296202]

77 Istituzione del Sis II e accesso per il rilascio delle carte di circolazione (*)

ARTICOLO 29 - Gruppo per la tutela dei dati personali

2067/05/IT
WP 116

Parere 116/2005 sulle proposte di regolamento del Parlamento europeo e del Consiglio (COM(2005) 236 definitivo) e di decisione del Consiglio (COM(2005) 230 definitivo) sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II), e sulla proposta di regolamento del Parlamento europeo e del Consiglio sull'accesso al sistema d'informazione Schengen di seconda generazione (SIS II) da parte dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (COM(2005) 237 definitivo)

Adottato il 25 novembre 2005

Il gruppo, istituito in virtù dell'articolo 29 della direttiva 95/46/CE, è l'organo consultivo indipendente dell'UE per la tutela dei dati personali e del diritto alla riservatezza. I suoi compiti sono fissati all'articolo 30 della richiamata direttiva e all'articolo 15 della direttiva 2002/58/CE.[1]

Le funzioni di segreteria sono espletate dalla direzione C (Giustizia civile, diritti fondamentali e cittadinanza) della Commissione europea, direzione generale Giustizia, libertà e sicurezza, B 1049 Bruxelles, Belgio, ufficio LX-46 01/43.

Sito Web: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

(*) [doc. *web* n. 1296208]

78 Linee guida per i *terminated merchant database* (*)

ARTICLE 29 - DATA PROTECTION WORKING PARTY

Brussels, 11 January 2005

Subject: Guidelines for Terminated Merchant Databases

Dear Colleagues,

Please find attached the final "Guidelines for Terminated Merchant Databases" that have been negotiated between the payment industry and the Working Party over the last two years, and that were discussed at our last meeting in late November.

At our November meeting the latest version of the Guidelines was presented, and you were all invited to provide further comments with a view to finalizing the Guidelines by the end of this year. A number of comments have been received and the payment industry has produced a new version of the Guidelines that takes such comments into account. All changes from the version discussed in November are indicated in the text.

After consulting with the Commission, I have examined these changes and I am of the opinion that they adequately address the questions and comments received. While the Guidelines remain in the nature of best practices and apply without prejudice to the provisions of the applicable national legislation, I believe that these Guidelines provide a satisfactory protection for data subjects and that their use will increase the level of personal data protection for terminated merchant databases. I further believe that the Working Party's endorsement of documents such as this can provide an important mechanism for addressing data protection issues in particular sectors in a timely and yet effective fashion.

Based on the above, I hereby endorse the final version of the Guidelines as attached. I have therefore asked that these Guidelines be officially published on the website of the Working Party together with this letter. The Working Party shall then monitor their implementation by the payment industry, the review of the Guidelines being scheduled in early 2006.

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC. The Secretariat is provided by:

Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.
Website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

(*) [doc. *web* n. 1296410]

79 Rapporto annuale per il 2004 (*)

Eighth Annual Report

on the situation regarding the protection of individuals
with regard to the processing of personal data
in the European Union and in third countries

Covering the year 2004

Adopted in November 2005

(*) [doc. *web* n. 1296417]

Garante europeo per la protezione dei dati

80 Sistema di informazione visti (Vis) e scambio di dati tra Stati membri sui visti per brevi soggiorni (*)

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (COM(2004) 835 definitivo)

(2005/C 181/06)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in particolare l'articolo 41,

vista la richiesta di parere, ricevuta il 25 gennaio 2005 dalla Commissione, a norma dell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001,

HA ADOTTATO IL SEGUENTE PARERE:

1. INTRODUZIONE

1.1 Premessa

L'istituzione del sistema d'informazione visti (VIS) costituisce una parte importante della politica comune dell'UE in materia di visti e ha formato oggetto di vari strumenti fra loro connessi.

— Nell'aprile 2003 è stato presentato uno studio di fattibilità (1) sul VIS, commissionato dalla Commissione.

— Nel settembre 2003 la Commissione ha proposto la modifica (2) di un precedente regolamento che istituisce un modello uniforme per i visti. L'obiettivo principale consiste nell'introdurre nel nuovo modello di visto i dati biometrici (immagine del volto e due impronte digitali) da memorizzare su chip.

(1) *Visa Information System*, relazione finale, commissionata dalla Commissione e realizzata dalla Trasys, aprile 2003.
(2) COM(2003) 558 defin. (2003/0217 (CNS) e 2003/0218 (CNS))

(*) ***G.U.U.E.*** **23 luglio 2005, C 181/13 [doc. *web* n. 1296422]**

81 Accordo tra la Comunità europea e il Governo del Canada sul trattamento delle informazioni sui passeggeri (*)

C 218/6 IT Gazzetta ufficiale dell'Unione europea 6.9.2005

Garante europeo della protezione dei dati

Parere del Garante europeo della protezione dei dati (GEPD) sulla proposta di decisione del Consiglio relativa alla conclusione di un accordo tra la Comunità europea e il governo del Canada sul trattamento delle informazioni anticipate sui passeggeri (Advance Passenger Information, API) e dei dati delle pratiche passeggeri (Passenger Name Record, PNR) (COM(2005) 200 def.)

(2005/C 218/06)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in particolare l'articolo 41,

vista la richiesta di parere a norma dell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001 ricevuta il 26 maggio 2005 dalla Commissione,

HA ADOTTATO IL SEGUENTE PARERE:

1. Introduzione

1. Il GEPD si compiace di essere stato consultato in base all'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001. Questo conferma il punto di vista, espresso dal GEPD nel suo documento orientativo del 18 marzo 2005 («Il GEPD in quanto consulente delle istituzioni comunitarie sulle proposte legislative e sui documenti connessi»), secondo cui la funzione consultiva si estende alla conclusione di accordi tra la CE e paesi terzi e/o organizzazioni internazionali riguardo al trattamento dei dati personali.

2. Considerato il carattere vincolante dell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001, il presente parere dovrebbe essere citato nel preambolo della decisione del Consiglio.

3. Secondo i considerando, l'accordo in questione, tra la Comunità europea e il Canada, riguarda una decisione della Commissione, ai sensi dell'articolo 25, paragrafo 6 della direttiva 95/46/CE, con la quale si considera che la competente autorità canadese assicura un livello di protezione adeguato dei dati API/PNR («*decisione della Commissione*»). Il GEPD ritiene che anche la decisione della Commissione avrebbe dovuto essere trasmessa per consultazione, in quanto parte del pacchetto giuridico complessivo.

(*) *G.U.U.E.* 6 settembre 2005, C 218/6
[doc. *web* n. 1296426]

82 Istituzione del Sis II e accesso per il rilascio delle carte di circolazione (*)

C 91/38 IT Gazzetta ufficiale dell'Unione europea 19.4.2006

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati (GEPD) sulla

— proposta di decisione del Consiglio sull'istituzione, l'esercizio e l'uso del sistema di informazione Schengen di seconda generazione (SIS II) (COM(2005)230 defin.);

— proposta di regolamento del Parlamento europeo e del Consiglio sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (COM(2005)236 defin.) e

— proposta di regolamento del Parlamento europeo e del Consiglio sull'accesso al sistema d'informazione Schengen di seconda generazione (SIS II) dei servizi competenti negli Stati membri per il rilascio delle carte di circolazione (COM(2005)237 defin.)

(2006/C 91/11)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in particolare l'articolo 41,

vista la richiesta, ricevuta il 17 giugno 2005 dalla Commissione, a norma dell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001,

HA ADOTTATO IL SEGUENTE PARERE:

1. INTRODUZIONE

1.1. Cronistoria

Il sistema d'informazione Schengen (SIS) è un sistema informatico europeo su vasta scala creato come misura volta a compensare la soppressione dei controlli alle frontiere interne dello spazio Schengen. Il SIS consente alle autorità competenti degli Stati membri di scambiare informazioni che sono utilizzate per il controllo delle persone e degli oggetti alle frontiere esterne o all'interno del territorio, nonché per il rilascio di visti e di permessi di soggiorno.

La convenzione Schengen, entrata in vigore nel 1995, è un accordo intergovernativo. Il SIS, come parte della convenzione Schengen, è stato successivamente integrato nel quadro dell'UE dal trattato di Amsterdam.

Un nuovo sistema d'informazione Schengen di seconda generazione (SIS II) sostituirà il sistema attuale, in modo da consentire di estendere lo spazio Schengen ai nuovi Stati membri dell'UE. Esso introdurrà anche nuove funzionalità nel sistema. Le disposizioni Schengen, elaborate in forma di quadro intergovernativo, saranno interamente trasformate in strumenti giuridici europei classici.

Il 1° giugno 2005 la Commissione europea ha presentato tre proposte per l'istituzione del SIS II. Si tratta delle proposte seguenti:

— la proposta di regolamento fondata sul titolo IV del trattato CE (visti, asilo, immigrazione e altre politiche connesse con la libera circolazione delle persone), che disciplinerà gli aspetti del SIS II del primo pilastro (immigrazione), (di seguito «la proposta di regolamento»);

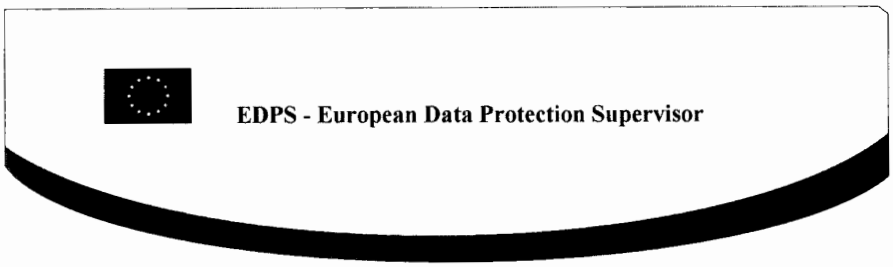
— la proposta di decisione fondata sul titolo VI del trattato UE (cooperazione di polizia e giudiziaria in materia penale), che disciplinerà il ricorso al SIS ai fini del terzo pilastro, (di seguito «la proposta di decisione»);

— la proposta di regolamento fondata sul titolo V (trasporti) concernente in modo specifico l'accesso delle autorità incaricate del rilascio delle carte di circolazione ai dati del SIS; la proposta sarà esaminata separatamente (cfr. infra punto 4.6.).

Va osservato in questo contesto che la Commissione presenterà nei prossimi mesi una comunicazione relativa all'interoperabilità e alle sinergie potenziate tra i sistemi d'informazione dell'UE (SIS, VIS, Eurodac).

(*) *G.U.U.E.* 19 aprile 2006, C 91/38
[doc. *web* n. 1296433]

83 Accesso alla documentazione amministrativa e protezione dati (*)



Public access to documents and data protection

Background Paper Series

July 2005

(*) [doc. *web* n. 1296438]

84 Relazione annuale per il 2005 (*)

Annual Report

2005

EUROPEAN DATA
PROTECTION SUPERVISOR

(*) [doc. *web* n. 1295359]

Autorità di controllo Schengen

85 Base giuridica proposta per il Sis II (*)

OPINION ON THE PROPOSED LEGAL BASIS FOR SIS II

Chapter I

1. Introduction

The need to develop a new, second-generation Schengen Information System (SIS), as well as the wish to introduce new functions for the SIS have been the subject of discussion for several years.

On 31 May 2005 the Commission presented its proposals for a legal basis for the new Schengen Information System, the SIS II:

- a proposal for a Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II) COM (2005) 230, 2005/0103 (CNS), hereinafter referred to as 'the Decision';
- a proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) COM (2005) 236, 2005/0106 (COD), hereinafter referred to as 'the Regulation';
- a proposal for a Regulation of the European parliament and of the Council regarding the access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM (2005) 237, 2005/-104 (COD), hereinafter referred to as 'the vehicle registration Regulation'.

The proposed legal basis for SIS II will be a crucial milestone in the further establishment of an area of freedom, security and justice, including the creation of an area without frontiers. The experience of the past decade, which has seen cooperation between states in the present Schengen Information System, has demonstrated that the legal basis for such a system is not only crucial for facilitating cooperation between states, it also provides the best means of guaranteeing adequate protection of fundamental rights and ensuring effective supervision.

The Schengen Joint Supervisory Authority (the JSA) has followed the development of the SIS II with interest, and has taken a number of initiatives to encourage discussion of the subject – one notable example being a seminar on SIS II, organised by the JSA and held in the European Parliament in October 2003.

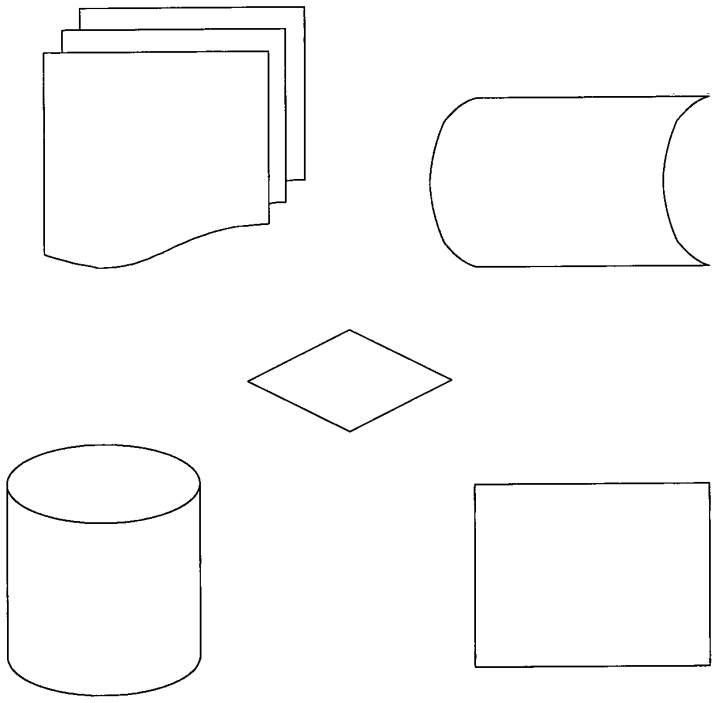
(*) [doc. *web* n. 1295363]

86 Accertamenti svolti sull'inserimento delle segnalazioni nel Sis ai sensi dell'art. 96 della Convenzione (*)

JOINT SUPERVISORY AUTHORITY — JSA ACC SCHENGEN — AUTORITÉ COMMUNE DE CONTRÔLE

ARTICLE 96 INSPECTION

Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System



Brussels, 20 June 2005

SCHENGEN

Joint Supervisory Authority of Schengen • Autorité Commune de Contrôle de Schengen
Data Protection Secretariat - 175, Rue de la Loi - B-1048 Bruxelles

(*) [doc. *web* n. 1296443]

Consiglio d'Europa

87 Applicazione della Convenzione ETS 108 al trattamento di dati biometrici (*)

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, February 2005 T-PD (2005) BIOM E

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

PROGRESS REPORT ON THE APPLICATION OF THE PRINCIPLES OF CONVENTION 108 TO THE COLLECTION AND PROCESSING OF BIOMETRIC DATA

As finalised by the T-PD at its 21st meeting (2-4 February 2005)

Secretariat document
prepared by the
Directorate General of Legal Affairs

(*) [doc. web n. 1296447]

Corte europea dei diritti dell'uomo

88 Diffusione di foto segnaletiche nell'attività di polizia (*)

CONSEIL DE L'EUROPE — COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

QUATRIÈME SECTION

AFFAIRE SCIACCA c. ITALIE

(Requête n° 50774/99)

ARRÊT

STRASBOURG

11 janvier 2005

Cet arrêt deviendra définitif dans les conditions définies à l'article 44 § 2 de la Convention. Il peut subir des retouches de forme.

(*) Ricorso n. 50774/99
[doc. *web* n. 1296452]

Rete Ue di esperti indipendenti

89 Diritti fondamentali e misure di prevenzione del reclutamento di potenziali terroristi (*)

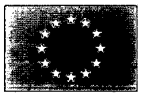
E.U. NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS
RÉSEAU U.E. D'EXPERTS INDÉPENDANTS EN MATIÈRE DE DROITS FONDAMENTAUX
(*CFR-CDF*)

The requirements of fundamental rights in the framework of the measures of prevention of violent radicalisation and recruitment of potential terrorists – Opinion n° 3-2005

Les exigences des droits fondamentaux dans le cadre des mesures de prévention de la radicalisation de la violence et du recrutement de terroristes potentiels – Avis n° 3-2005

23 août 2005

Ref. CFR-CDF.Avis3-2005.doc



The E.U. Network of Independent Experts on Fundamental Rights has been set up by the European Commission upon request of the European Parliament. It monitors the situation of fundamental rights in the Member States and in the Union, on the basis of the Charter of Fundamental Rights. It issues reports on the situation of fundamental rights in the Member States and in the Union, as well as opinions on specific issues related to the protection of fundamental rights in the Union. The content of this opinion does not bind the European Commission. The Commission accepts no liability whatsoever with regard to the information contained in this document .

(*) [doc. web n. 1295382]

90 Relazione annuale per il 2005 (*)

EU NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS
RÉSEAU U.E. D'EXPERTS INDÉPENDANTS EN MATIÈRE DE DROITS FONDAMENTAUX
CFR-CDF

REPORT ON THE SITUATION OF FUNDAMENTAL RIGHTS IN THE EUROPEAN UNION AND ITS MEMBER STATES IN 2005:

CONCLUSIONS AND RECOMMENDATIONS

Ref.: CFR-CDF/Conclusions 2005

The E.U. Network of Independent Experts on Fundamental Rights has been set up by the European Commission upon request of the European Parliament. It monitors the situation of fundamental rights in the Member States and in the Union, on the basis of the Charter of Fundamental Rights. It issues reports on the situation of fundamental rights in the Member States and in the Union, as well as opinions on specific issues related to the protection of fundamental rights in the Union

(*) [doc. *web* n. 1296456]

Autorità di controllo Europol

91 Accesso di Europol al Sis II (*)

AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL

Parere dell'ACC in merito alla proposta tecnica per l'accesso dell'Europol al SIS.

Alla cortese attenzione del:
Presidente del Comitato dell'articolo 36
Sig. Peter Storr
Rue de la Loi 175
B-1048 Bruxelles

DOCUMENTO 05/33

AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL

I. Introduzione

Il 3 agosto 2005 il presidente del Comitato dell'articolo 36 ha chiesto all'Autorità di controllo comune dell'Europol (ACC) di formulare un parere sulla proposta tecnica per l'accesso dell'Europol al sistema d'informazione Schengen (SIS).

La proposta tecnica esposta nel documento SISTECH 62 SIRIS 73 COMIX 470 11168/05 contiene un'ulteriore elaborazione delle condizioni per l'accesso dell'Europol definite nella decisione 2005/211/JHA del Consiglio del 24 febbraio 2005[1].

[1] GU n. L 68, del 15.3.2005, pagg. 44-48

Autorità di controllo comune dell'Europol
Segretariato, Rue de la Loi 175, B-1048 Bruxelles
Tel: +32(0)2 2858602(5)(26)
Fax: +32(0)2 2855126

(*) [doc. *web* n. 1296460]

92 Livello di tutela dei dati in Australia (*)

AUTORITÀ DI CONTROLLO COMUNE
DELL'EUROPOL

Parere dell'ACC in merito al
livello di protezione dei dati in Australia

All'attenzione de:
il presidente del
Consiglio di amministrazione dell'Europol
Sig. Rob Wainwright
L'Aia DOCUMENTO 05/35
Paesi Bassi

AUTORITÀ DI CONTROLLO COMUNE DELL'EUROPOL

A. Osservazioni introduttive

1. L'ACC è stata incaricata di elaborare un parere in merito alle leggi e alla prassi amministrativa dell'Australia nel settore della protezione dei dati, sulla base della relazione fascic. n. 2644-01 datata del 12 settembre 2005.

2. Detta relazione è stata sottoposta all'esame dell'ACC dal consiglio di amministrazione dell'Europol, in conformità dell'articolo 1, paragrafo 5, della decisione del Consiglio che autorizza il direttore dell'Europol ad avviare negoziati per la conclusione di accordi con Stati terzi ed organismi non connessi all'Unione europea.

3. Ai sensi dell'articolo 3, paragrafo 3, seconda parte, delle norme per la trasmissione di dati di carattere personale a Stati ed organismi terzi, l'ACC è altresì chiamata a formulare un parere durante la procedura in cui il Consiglio dell'Unione europea deve decidere se approvare o meno un accordo tra l'Europol e l'Australia. L'ACC fa notare che il presente parere riguarda unicamente l'eventuale esistenza di ostacoli all'avvio dei negoziati tra l'Europol e l'Australia suscettibili di condurre al raggiungimento di un accordo sulla trasmissione di dati di carattere personale all'Australia da parte dell'Europol.

(*) [doc. *web* n. 1296464]

27ma Conferenza dei Garanti privacy

93 Dichiarazione di Montreux (*)

DICHIARAZIONE DI MONTREUX

"La protezione dei dati personali e della privacy in un mondo globalizzato: un diritto universale che rispetta le diversità"

L'Autorità federale svizzera per la protezione dei dati, con il sostegno dell'Incaricato federale tedesco per la protezione dei dati, dell'Agenzia spagnola per la protezione dei dati, dell'Ispettore generale per la protezione dei dati personali della Polonia, del Commissario per la privacy della Nuova Zelanda, del Commissario per la privacy del Canada, del Garante europeo per la protezione dei dati, del Commissario per la privacy di Hong Kong, dell'Ispettorato statale per la protezione dei dati della Lituania, dell'Autorità olandese per la protezione dei dati, dell'Ufficio per la protezione dei dati della Repubblica Ceca, dell'Autorità italiana per la protezione dei dati personali, del Commissario per la privacy di Guernsey, del Commissario per la privacy di Victoria (Australia), dell'Incaricato per la protezione dei dati e la libertà di informazione della città di Berlino, del Commissario per la protezione dei dati del Cantone di Zug (Svizzera), propone l'adozione della seguente Dichiarazione:

Le Autorità per la protezione dei dati e della privacy riunite a Montreux in occasione della 27ma Conferenza internazionale (14-16 settembre 2005) hanno stabilito di comune accordo di promuovere il riconoscimento della natura universale dei principi di protezione dei dati, ed hanno adottato la seguente Dichiarazione finale:

1. Facendo seguito alla dichiarazione adottata in occasione della 22ma Conferenza internazionale delle Autorità per la protezione dei dati e della privacy, tenutasi a Venezia;
2. Richiamandosi alla Risoluzione sulla protezione dei dati e gli organismi internazionali adottata in occasione della 25ma Conferenza internazionale delle Autorità per la protezione dei dati e della privacy, tenutasi a Sydney;
3. Riconoscendo che lo sviluppo della società dell'informazione è dominato dalla globalizzazione degli scambi di informazioni, dall'impiego di tecnologie per l'elaborazione dei dati di crescente invasività, e da un incremento delle misure di sicurezza;
4. Preoccupate per i rischi crescenti di sorveglianza pervasiva delle persone a livello mondiale;
5. Rilevando i benefici ed i rischi potenziali inerenti alle nuove tecnologie dell'informazione;
6. Preoccupate per le attuali disuguaglianze fra i sistemi giuridici nelle diverse parti del mondo, in particolare per l'assenza di misure a salvaguardia della protezione dei dati in alcune zone che compromette l'efficacia della protezione dei dati a livello globale;
7. Consapevoli che la rapida espansione delle conoscenze nel settore della genetica può fare del DNA umano il dato personale più sensibile in assoluto; consapevoli, inoltre, che questa accelerazione della conoscenza accresce l'importanza di un'adeguata tutela giuridica dei dati in oggetto;

(*) Montreux, 14-16 settembre 2005 [doc. *web* n. 1170512 vers. EN n. 1171231]

8. Ricordando che la raccolta ed il successivo trattamento di dati personali devono avvenire tenendo presenti i requisiti della protezione dei dati e della privacy;
9. Riconoscendo l'esigenza, in una società democratica, di combattere efficacemente il terrorismo e la criminalità organizzata, ma ricordando che questi obiettivi possono essere raggiunti nel migliore dei modi quando si rispettano i diritti umani, ed in particolare la dignità umana;
10. Convinte che il diritto alla protezione dei dati e della privacy rappresenti una condizione essenziale, in una società democratica, per garantire il rispetto dei diritti delle persone, la libera circolazione delle informazioni, ed un'economia di mercato aperta;
11. Convinte che il diritto alla protezione dei dati e della privacy rappresenti un diritto umano fondamentale;
12. Convinte dell'esigenza di rafforzare la natura universale di tale diritto al fine di ottenere il riconoscimento universale dei principi che disciplinano il trattamento di dati personali rispettando, al contempo, le diversità giuridiche, politiche, economiche e culturali;
13. Convinte dell'esigenza di garantire i diritti della persona a tutti i cittadini del mondo senza discriminazioni di sorta, indipendentemente dal luogo e dal momento in cui i dati personali che li riguardano sono sottoposti a trattamento;
14. Ricordando che il Vertice Mondiale sulla Società dell'Informazione tenutosi a Ginevra nel 2003 ha sottolineato, nella Dichiarazione sui principi ed il programma d'intervento, l'importanza della protezione dei dati e della privacy ai fini dello sviluppo della società dell'informazione;
15. Ricordando la Raccomandazione formulata dall'International Working Group on Data Protection in Telecommunications di tenere presente il Decalogo elaborato nel 2000, al fine di tutelare la privacy nell'ambito di accordi multilaterali in materia di privacy;
16. Riconoscendo che i principi di protezione dei dati discendono da strumenti giuridici internazionali a carattere sia vincolante sia non vincolante, quali le Linee-Guida dell'OCSE in materia di protezione della privacy e dei flussi transfrontalieri di dati personali, la Convenzione del Consiglio d'Europa per la protezione delle persone fisiche rispetto al trattamento automatizzato di dati personali, le Linee-Guida ONU relative agli archivi di dati personali informatizzati, la Direttiva dell'Unione Europea 95/46 sulla protezione delle persone fisiche con riguardo al trattamento di dati personali ed alla libera circolazione di tali dati, e l'Accordo-quadro in materia di privacy nell'ambito della cooperazione economica Asia-Pacifico;
17. Ricordando che i principi in questione sono, in particolare, quelli di seguito indicati:
    - principio di liceità e correttezza nella raccolta e nel trattamento dei dati;
    - principio di accuratezza;
    - principio di finalità;
    - principio di proporzionalità;
    - principio di trasparenza;
    - principio di partecipazione individuale, in particolare la garanzia del diritto di accesso da parte della persona interessata;
    - principio di non discriminazione;
    - principio di sicurezza dei dati;
    - principio di responsabilità;
    - principio del controllo indipendente e dell'esistenza di sanzioni previste per legge;
    - principio del livello adeguato di protezione in caso di flussi transfrontalieri di dati personali.

Alla luce di quanto precede,

Le Autorità per la protezione dei dati e della privacy esprimono l'intenzione di potenziare il riconoscimento internazionale della natura universale di tali principi. Stabiliscono di comune accordo di collaborare, in particolare, con i governi e gli organismi internazionali e sovranazionali al fine di mettere a punto una convenzione universale per la protezione delle persone fisiche rispetto al trattamento di dati personali.

A tal fine, le Autorità fanno appello:

a. alle Nazioni Unite affinché preparino uno strumento giuridico vincolante che stabilisca in modo chiaro e specifico i diritti alla protezione dei dati e della privacy come diritti umani sanzionabili;
b. a tutti i governi del mondo affinché promuovano l'adozione di strumenti giuridici in materia di protezione dei dati e della privacy conformi ai principi fondamentali della protezione dei dati, ed inoltre estendano tali principi ai rapporti reciproci;
c. al Consiglio d'Europa perché, a norma dell'Articolo 23 della Convenzione per la protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali, inviti gli Stati che non sono membri del Consiglio d'Europa e già dispongono di normativa in materia di protezione dei dati ad aderire alla Convenzione ed al suo protocollo addizionale.

Inoltre, le Autorità invitano:

I Capi di Stato e di governo che converranno a Tunisi in occasione del Vertice mondiale sulla società dell'informazione (16-18 novembre 2005) ad inserire nella dichiarazione finale l'impegno a sviluppare o potenziare un quadro giuridico di riferimento che garantisca il diritto alla privacy ed alla protezione dei dati a tutti i cittadini nella società dell'informazione, coerentemente con l'impegno assunto dai Capi iberoamericani di Stato e di governo in occasione del Vertice di Santa Cruz (Bolivia) (novembre 2003) nonché dai Capi di Stato e di governo dei Paesi francofoni in occasione del Vertice di Ougadougou (novembre 2004).

Le Autorità fanno appello altresì:
a. agli organismi internazionali e sovranazionali affinché si impegnino a rispettare principi che siano compatibili con i maggiori strumenti internazionali in materia di protezione dei dati e della privacy, ed in particolare ad istituire autorità di vigilanza indipendenti dotate di poteri di controllo;
b. alle organizzazioni non governative internazionali, quali le associazioni di imprese e di consumatori, affinché mettano a punto standard basati sui principi fondamentali della protezione dei dati ovvero compatibili con tali principi;
c. ai produttori di hardware e software affinché sviluppino prodotti e sistemi che incorporino tecnologie per il potenziamento della privacy.

Inoltre, le Autorità stabiliscono di comune accordo:
a. di intensificare, in particolare, gli scambi di informazioni, il coordinamento delle rispettive attività di vigilanza, la definizione di standard comuni, la promozione delle informazioni relative alle attività ed alle risoluzioni di questa Conferenza;
b. di promuovere la cooperazione con i Paesi che ancora non dispongono di autorità di vigilanza indipendenti in materia di protezione dei dati personali;
c. di promuovere lo scambio di informazioni con organizzazioni non governative internazionali che si occupano di protezione dei dati e privacy;
d. di collaborare con gli incaricati per la protezione dei dati nei vari enti;
e. di creare un sito web permanente che funga, in particolare, da base comune per la gestione delle informazioni e delle risorse.

Le Autorità per la protezione dei dati e della privacy stabiliscono di valutare periodicamente la realizzazione degli obiettivi della presente Dichiarazione, ad iniziare dalla 28ma Conferenza Internazionale nel 2006.

94 Risoluzione sull'utilizzo della biometria per passaporti, carte di identità e titoli di viaggio (*)

RISOLUZIONE SULL'UTILIZZO DELLA BIOMETRIA IN PASSAPORTI, CARTE DI IDENTITÀ E TITOLI DI VIAGGIO

L'Incaricato federale tedesco per la protezione dei dati e l'Incaricato per la protezione dei dati e la libertà di informazione della città di Berlino, con il sostegno della Direzione nazionale per la protezione dei dati dell'Argentina, dell'Autorità austriaca per la protezione dei dati, e dell'Autorità italiana per la protezione dei dati, propongono l'adozione della seguente Risoluzione:

La 27ma Conferenza internazionale delle Autorità di protezione dei dati e della privacy adotta la presente Risoluzione:

Rilevando che governi e organismi internazionali, ed in particolare l'Organizzazione internazionale dell'aviazione civile (ICAO), stanno attualmente completando la definizione di norme e standard tecnici volti ad integrare dati biometrici (impronte digitali, riconoscimento del volto) in passaporti e titoli di viaggio ai fini della lotta al terrorismo e della velocizzazione dei controlli alle frontiere e delle procedure di imbarco;

Consapevole che anche il settore privato ricorre in misura crescente al trattamento di dati biometrici, prevalentemente su base volontaria;

Considerando che i dati biometrici possono essere raccolti all'insaputa dell'interessato, poiché quest'ultimo può lasciare tracce biometriche in modo inconsapevole;

Ricordando che la biometria consentirà la "lettura automatica" del corpo umano, e che i dati biometrici potrebbero essere utilizzati come identificatori univoci a livello globale;

Sottolineando che l'utilizzo diffuso della biometria avrà un effetto di lunga portata sulla società a livello globale e, pertanto, dovrebbe essere oggetto di un dibattito aperto a tutte le istanze globali;

La Conferenza chiede:

1. che si dia attuazione in fase precoce ad efficaci garanzie onde limitare i rischi inerenti alla natura della biometria;
2. che si tengano rigidamente distinti i dati biometrici raccolti e memorizzati per finalità di natura pubblica (ad esempio, i controlli alle frontiere) in base ad obblighi di legge, e quelli raccolti e memorizzati per finalità contrattuali sulla base del consenso;
3. che si limiti tecnicamente l'impiego della biometria in passaporti e carte di identità alle finalità di verifica, tramite il confronto fra i dati contenuti nel documento e i dati forniti dal titolare all'atto della presentazione del documento stesso.

(*) Montreux, 14-16 settembre 2005 [doc. *web* n. 1170552 vers. EN n. 1170622]

95 Risoluzione sull'utilizzo di dati personali per la comunicazione politica (*)

RISOLUZIONE SULL'UTILIZZO DI DATI PERSONALI PER LA COMUNICAZIONE POLITICA

Presentata dall'Autorità italiana per la protezione dei dati con il sostegno dell'Autorità federale svizzera per la protezione dei dati, l'Autorità federale tedesca per la protezione dei dati, l'Ispettore Generale per la protezione dei dati della Polonia, il Commissario per la protezione dei dati della città di Berlino

La Conferenza

Considerando che la comunicazione politica costituisce uno strumento fondamentale per la partecipazione di cittadini, forze politiche e candidati alla vita democratica, e riconoscendo l'importanza di una libera comunicazione politica quale diritto fondamentale;

Considerando che la condizione di cittadino presuppone il diritto di ottenere informazioni e di essere informati adeguatamente durante campagne elettorali politiche e amministrative; che tale diritto trova applicazione anche in riferimento ad altre materie, altri eventi e posizioni politiche utili al fine di compiere scelte informate su altri temi della vita politica: referendum, elezione di candidati, accesso alle informazioni detenute da organismi politici o provenienti da rappresentanti eletti;

Considerando che le forze politiche e, in generale, gli organismi politici ed i rappresentanti eletti ricorrono a vari strumenti di comunicazione e di finanziamento, a molteplici fonti di informazione, ed alle nuove tecnologie, per stabilire contatti diretti e personalizzati con le più diverse categorie di interessati;

Considerando che in un numero crescente di Paesi vi è la tendenza ad un'espansione della comunicazione istituzionale operata da candidati e soggetti eletti, anche a livello locale o attraverso forme di e-government; che queste attività, che talora necessitano il trattamento di dati personali, riflettono il diritto dei cittadini di essere informati sull'attività degli eletti di cui sopra;

Considerando che, in tale contesto, una mole considerevole di dati personali viene continuamente raccolta da organismi politici, ed è talora sottoposta a trattamento con modalità aggressive attraverso le più diverse tecniche quali sondaggi, raccolta di indirizzi di posta elettronica attraverso programmi o motori di ricerca, sollecitazioni di voto a livello di intere città, ovvero forme di decisione politica raggiunte attraverso la TV interattiva, o forme di profilazione degli elettori; che i dati in oggetto talora comprendono illecitamente (oltre a indirizzi postali, numeri di telefono, indirizzi di posta elettronica, informazioni sulle attività professionali ed il contesto familiare) dati sensibili relativi alle opinioni o attività morali e politiche, reali o ipotizzate, ovvero alle attività di voto;

Considerando l'esistenza di forme invasive di profilazione rispetto a persone che vengono classificate –talora in modo impreciso, o sulla base di contatti superficiali– come simpatizzanti, sostenitori, aderenti o iscritti al fine di potenziare la comunicazione personalizzata rivolta a singoli gruppi di cittadini;

Considerando che tali attività devono aver luogo secondo modalità lecite e corrette;

Considerando che è necessario tutelare i diritti e le libertà fondamentali degli interessati

(*) Montreux, 14-16 settembre 2005 [doc. *web* n. 1170546 vers. EN n. 1170616]

evitando, attraverso opportuni provvedimenti, indebite intrusioni, danni e costi a carico degli interessati stessi, in particolare effetti negativi e discriminazioni a livello della loro sfera personale ovvero la rinuncia ad alcune forme di partecipazione alla vita politica;

Considerando che tale tutela potrebbe essere conseguita tenendo conto del pertinente interesse pubblico connesso ad alcune attività di comunicazione politica, nonché di adeguate modalità e garanzie in rapporto alle comunicazioni interne rivolte a iscritti a partiti ovvero a semplici cittadini;

Considerando che, in tale contesto, è possibile promuovere attività responsabili di marketing senza limitare la circolazione di idee e proposte politiche, e che nonostante la comunicazione politica condivida talora molte delle caratteristiche delle attività promozionali, essa presenta alcuni tratti che la distinguono dal marketing per finalità commerciali;

Considerando l'esigenza di garantire il rispetto dei principi di protezione dei dati mettendo a punto uno standard minimo a livello globale che possa contribuire ad armonizzare i livelli di tutela degli interessati, anche sulla base di codici deontologici nazionali ed internazionali e tenendo conto delle soluzioni e delle norme specificamente individuate in vari Paesi;

Considerando che le autorità per la protezione dei dati possono svolgere un ruolo crescente nel pianificare interventi coordinati, anche in collaborazione con altre autorità di controllo competenti per i settori delle telecomunicazioni, dell'informatica, dei sondaggi elettorali, e delle attività elettorali;

adotta
la seguente Risoluzione:

Ogni attività di comunicazione politica che comporti il trattamento di dati personali, sia essa legata o meno a campagne elettorali, dovrebbe rispettare i diritti e le libertà fondamentali degli interessati, fra cui il diritto alla protezione dei dati personali, nell'osservanza di principi consolidati in materia, ed in particolare:

Principio di necessità
I dati personali dovrebbero essere oggetto di trattamento esclusivamente se ciò risulta necessario per il raggiungimento delle finalità per cui sono specificamente raccolti.

Liceità e correttezza della raccolta

La raccolta di dati personali dovrebbe avvenire attraverso fonti accessibili lecitamente, ed il trattamento dei dati dovrebbe essere effettuato in modo corretto. Si dovrebbe verificare che, ai sensi di legge, le fonti siano pubbliche ovvero siano utilizzabili esclusivamente per scopi specifici o secondo determinate modalità o per periodi limitati o in particolari occasioni.

È necessaria particolare attenzione qualora gli interessati siano contattati attraverso modalità aggressive.

Qualità dei dati
Nel corso del trattamento è necessario rispettare gli altri principi concernenti la qualità dei dati. In particolare, i dati dovrebbero essere accurati, pertinenti, non eccedenti e aggiornati in rapporto alle specifiche finalità per cui sono raccolti, soprattutto qualora le informazioni siano relative alle opinioni sociali o politiche, o alle convinzioni etiche, dell'interessato.

Principio di finalità
I dati personali ricavati da fonti, istituzioni o associazioni pubbliche o private possono essere utilizzati per scopi di comunicazione politica se il loro trattamento ulteriore è compatibile con le finalità per cui sono stati raccolti e di cui gli interessati sono già stati informati, in particolare qualora si tratti di dati sensibili. I rappresentanti eletti devono rispettare tali principi qualora utilizzino per scopi di comunicazione politica dati personali raccolti nell'esercizio delle rispettive funzioni istituzionali.

I dati personali raccolti originariamente per attività di marketing sulla base di un consenso informato possono essere utilizzati se le finalità di comunicazione politica sono menzionate specificamente nella dichiarazione di prestazione del consenso.

Proporzionalità

Il trattamento di dati personali dovrebbe avvenire esclusivamente attraverso modalità ed operazioni pertinenti agli scopi, particolarmente nel caso di dati relativi ad elettori potenziali o del confronto fra dati ricavati da archivi o banche dati di tipo diverso.

Il trattamento ulteriore di dati personali, soprattutto quelli conservati successivamente alla circostanza in rapporto alla quale sono stati raccolti, è ammissibile se le finalità perseguite dalla comunicazione politica sono in via di raggiungimento.

Informativa agli interessati

Prima di raccogliere il dato presso l'interessato, i destinatari devono ricevere un'informativa adeguata ai mezzi di comunicazione prescelti, in cui siano specificate l'identità del titolare (singoli candidati, responsabile esterno della campagna elettorale, associazione locale di sostenitori, o associazioni locali o di altro tipo; il partito politico nel suo insieme, ecc.) e le tipologie di flussi attese fra tali soggetti.

L'informativa dovrebbe essere fornita anche quando i dati non sono raccolti presso l'interessato, almeno nel caso in cui i dati non siano destinati ad essere conservati solo in via temporanea.

Consenso

Occorre verificare che il trattamento di dati personali si fondi sul consenso dell'interessato o su un altro presupposto legittimo previsto dalla legge. Il trattamento dovrebbe rispettare le norme specifiche in vigore nei singoli Paesi in rapporto alle fonti o ai mezzi di comunicazione utilizzati, in particolare per quanto riguarda gli indirizzi di posta elettronica, i numeri di fax, i messaggi SMS e/o altri messaggi di natura testuale o visiva ed i messaggi telefonici preregistrati.

Conservazione dei dati e misure di sicurezza

Ogni titolare, sia esso una forza politica o un singolo candidato, deve adottare tutte le misure di sicurezza di natura tecnica ed organizzativa necessarie a tutelare l'integrità delle informazioni raccolte ed a prevenire la perdita e/o l'utilizzo abusivo dei dati.

Diritti degli interessati

Agli interessati dovrebbero essere riconosciuti i diritti di accesso, rettifica, blocco e/o cancellazione nonché il diritto di opporsi alle comunicazioni indesiderate, e il diritto di chiedere, gratuitamente e con modalità semplici, di non ricevere ulteriori messaggi. L'esistenza di tali diritti dovrebbe essere menzionata nelle informative fornite agli interessati.

Dovrebbero essere previsti adeguati rimedi giuridici e sanzioni in caso di violazione dei diritti di cui sopra.

Conferenza di primavera 2005

96 Dichiarazione sulla lotta al terrorismo internazionale (*)

Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005

DECLARATION

Various initiatives at EU level aim to establish the European Union's objective of an area of freedom, security and justice. In its new multi annual programme - The Hague Programme - the Union reiterates the need to fight organised cross-border crime and to repress the threat of terrorism.

The 2005 Spring Conference of European Data Protection Authorities is well aware of the need for closer co-operation between law enforcement authorities, within the EU and with third States. At the same time it is evident that the 1981 Council of Europe Convention on data protection (Convention 108) applicable in the Union and in Member States is too general to effectively safeguard data protection in the area of law enforcement. Given the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection.

The Conference noted with satisfaction that The Hague Programme subjects the availability principle to strict conditions of respect for data protection principles.

The Conference also welcomes the approach of the Commission in advocating a core set of guiding principles for the treatment of personal data under the Third Pillar, to be developed in close co-operation with data protection authorities. Furthermore, the Conference is encouraged by the steps taken by the Commission towards developing a new legal framework for data protection in the Third Pillar which, it is hoped, will provide an appropriate set of rules applicable to law enforcement activities consistent with the current level of data protection in the First Pillar. When developing these detailed data protection rules, the standard of data protection found in Directive 95/46/EC should serve as a basis.

(*) Cracovia 25-26 aprile 2005 [doc. *web* n. 1296471]