ATTI PARLAMENTARI

XIV LEGISLATURA

CAMERA DEI DEPUTATI

Doc. CXXXVI
n. 5

RELAZIONE

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

(Anno 2004)

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

Presentata dal Garante per la protezione dei dati personali

(RODOTÀ)

Trasmessa alla Presidenza il 9 febbraio 2005

TIPOGRAFIA DEL SENATO (200)

PAGINA BIANCA

Relazione 2004

Discorso del Presidente

Stefano Rodotà

PAGINA BIANCA

Signor Presidente della Repubblica,

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

Una rivoluzione pacifica

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

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

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

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

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

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

rando allo sviluppo della legislazione e degli strumenti di garanzia.

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

Senza una forte tutela delle loro informazioni, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la *privacy* si presenta così come un elemento fondamentale della **società dell'eguaglianza**. Senza una forte tutela dei dati riguardanti i loro rapporti con le istituzioni o l'appartenenza a partiti, sindacati, associazioni, movimenti, i cittadini rischiano d'essere esclusi dai processi democratici: così la *privacy* diventa una condizione essenziale per essere inclusi nella **società della partecipazione**. Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale: diventa così evidente che la *privacy* è uno strumento necessario per salvaguardare la **società della libertà**. Senza una resistenza continua alle microviolazioni, ai controlli continui, capillari, oppressivi o invisibili che invadono la stessa vita quotidiana, ci ritroviamo nudi e deboli di fronte a poteri pubblici e privati: la *privacy* si specifica così come una componente ineliminabile della **società della dignità**.

La *privacy* è di tutti

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

Siamo, dunque, ben lontani da un'immagine della *privacy* come strumento a disposizione solo di gruppi ristretti. Mai come in questo momento gli interventi del

Garante rendono evidente che la protezione dei dati personali è davvero affare di tutti. Il codice deontologico sull'attività dei sistemi privati di informazione creditizia, appena entrato in vigore, interessa milioni di persone, così messe al riparo da forme improprie di classificazione, come "cattivo pagatore". In un incontro da noi promosso nei giorni scorsi, vari operatori sanitari, pubblici e privati, hanno potuto mettere in evidenza soluzioni innovative e a basso costo per la tutela della dignità e della riservatezza dei pazienti e, insieme, della loro salute, bene primario d'ogni persona. È ormai avviata la definizione del codice deontologico per *Internet*. Decine di milioni di persone, cioè tutti i titolari di utenze telefoniche fisse e mobili, stanno ricevendo dalle società che gestiscono i servizi un modulo che le metterà nella condizione di stabilire se figurare o no nei nuovi elenchi, se ricevere o no pubblicità per posta o per telefono, se comparire con il nome per esteso o soltanto puntato, e via dicendo. Mai s'era svolta nel nostro Paese una consultazione di massa di queste dimensioni, dalla quale sarà possibile trarre indicazioni importanti sul modo in cui ciascuno tende a percepire se stesso nella società della comunicazione totale.

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

Persona e informazione totale

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

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

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

trando nel sistema dell'informazione. Uno sguardo ai titoli di otto anni fa, sulla diffusione senza remore di nomi e di immagini di protagonisti veri o supposti di vicende di cronaca, ci consente di misurare una distanza, poiché oggi molte immagini sono oscurate, molti nomi sono di fantasia, molte informazioni sono fornite in modo più sobrio.

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

Un diritto di "uscita"

Ma non è solo nella società della spettacolarizzazione continua che emerge con forza il bisogno di ritirarsi dietro le quinte per riflettere, per rifiatare. Più cresce la nostra immersione nella società dell'informazione totale, più si diffondono le tec-

nologie dell'informazione e della comunicazione, più si amplia l'area in cui si forniscono beni e servizi in cambio di dati personali, maggiore diventa l'esigenza di precisare la posizione in cui si trova ciascuno di noi. Questo esige uno sguardo nuovo sugli strumenti giuridici disponibili, sull'utilizzazione delle stesse tecnologie come fattori di tutela della *privacy* e, in conclusione, sulla nuova dimensione costituzionale che sta emergendo.

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

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

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

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

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

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

ai produttori la necessità di progettare i videotelefoni e le "etichette intelligenti" in modo tale da escludere fin dall'origine alcuni rischi per la *privacy*.

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

Opponendosi ad ingiustificate derive tecnologiche, all'idea semplicistica e rischiosa che qualsiasi strumento nuovo possa e debba essere adottato per il solo fatto che esiste, il Garante vuol dare un contributo proprio all'uso razionale della tecnologia. Le regole sulla videosorveglianza, ad esempio, non servono soltanto ad evitarne usi che interferiscono indebitamente sulle libertà delle persone. Sono anche un contributo per evitare sprechi. Agganciando la legittimità dei sistemi di videosorveglianza a serie esigenze, infatti, si può evitare quel che le cronache ci dicono, parlando di comuni che giustificano il ricorso a sistemi costosi con l'unico argomento dell'"entrata nella modernità", e che poi si trovano nella condizione di non disporre dei fondi necessari per la manutenzione e il funzionamento adeguato dei sistemi acquistati.

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

La costruzione elettronica della persona

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

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

Vi sono usi delle *Rfid* per sole finalità di gestione aziendale che, non implicando trattamenti di dati personali, sono esclusi dall'applicazione delle relative norme. Vi sono etichettature di prodotti che, potendo determinare un controllo sui movimenti e le utilizzazioni degli acquirenti, esigono valutazioni di proporzionalità, informative adeguate, consenso, esercizio di un "diritto di uscita" grazie alla disattivazione dell'etichetta. Vi sono impianti di *microchip* sottopelle che, potendo

portare ad una modifica del corpo contrastante con la dignità della persona, devono essere in via di principio esclusi, salvo casi eccezionali di uso proporzionato a tutela della salute.

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

L'"etichettatura" delle persone viene giustificata anche con l'argomento che, grazie ai controlli a distanza, alcune categorie di persone, come gli anziani, avranno migliori opportunità di essere aiutate in situazioni di emergenza. Ma possiamo affidare un numero crescente di persone solo ad un "Angelo Custode Digitale"? Il rispetto della dignità delle persone esige che siano interrotte derive che propongono cura elettronica e determinano abbandono sociale.

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

La capacità di intercettare il futuro, inoltre, è stata mostrata dal Garante anche intervenendo sulla conservazione dei dati di traffico telefonico e sulle proposte di

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

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

Un nuovo quadro costituzionale

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

Il costante riferimento alla necessità di "rispetto dei diritti e delle libertà fondamentali" (art. 2.1 del Codice) non implica soltanto un confronto continuo tra le specifiche forme di trattamento dei dati personali ed i singoli diritti e libertà. Impone ormai una ricostruzione di libertà e diritti aderente all'ambiente tecnolo-

gico nel quale vengono esercitati. Non si può sfuggire ad alcune domande: le "formazioni sociali" (art. 2 Cost.) possono essere anche le comunità virtuali create nel ciberspazio? Le garanzie della libertà personale (art. 13) devono essere estese anche al corpo "elettronico", seguendo la traiettoria della rilettura dell'*habeas corpus* come *habeas data*? Qual è la portata della libertà di circolazione (art. 16) in presenza della videosorveglianza e del diffondersi delle tecniche di localizzazione? Regge la distinzione tra dati "esterni" e "interni" delle comunicazioni quando queste si svolgono su *Internet*, modificando i termini in cui deve parlarsi della loro libertà e segretezza (art. 15)? Come si atteggiano in rete la libertà di associazione (art. 18), la stessa libertà religiosa (art. 19)? Il diritto di manifestare liberamente il proprio pensiero (art. 21) deve essere messo in rapporto con il diritto all'anonimato nelle comunicazioni elettroniche, con il diritto a respingere i controlli sulle proprie relazioni elettroniche (lo abbiamo segnalato in una lettera al Presidente del Senato)? L'accessibilità alla proprietà (art. 42.2), quando si traduce nella libera appropriabilità di determinati beni per via elettronica, secondo una logica dei *commons*, dei beni comuni, deve anche escludere l'identificazione personale dei soggetti che accedono?

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

Il Garante e l'interesse generale

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

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

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

L'omessa consultazione non può essere in nessun caso giustificata con l'argomento che la richiesta di parere avrebbe ritardato l'emanazione dell'atto ministeriale. Quando è stata prospettata l'urgenza dell'intervento, il Garante è intervenuto con assoluta tempestività, addirittura esprimendo il suo parere nel giro di un paio d'ore,

com'è avvenuto in occasione della ricerca telefonica dei dispersi nel Sud-est asiatico.

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

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

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

Indipendenza ed efficienza

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

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

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

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

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

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

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

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

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

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

Questo, per noi, è tanto più vero perché l'esperienza di questi anni ci ha resi consapevoli dei limiti dell'azione passata e dei problemi per quella futura. Sappiamo che dev'essere accentuata la capacità di regolazione attraverso un dialogo sociale che coinvolga tutti gli interessati: ma questa è attività costosa e intellettualmente impegnativa. È necessario allargare l'attività di ispezione, non per una volontà repressiva, ma perché sono i cittadini ad esigere un rigoroso rispetto delle norme da parte dei soggetti che utilizzano i loro dati. Dobbiamo mantenere una forte e qualificata presenza internazionale, non solo per rimanere in una posizione di avanguardia fatico-

samente costruita, ma per non escluderci da un circuito di conoscenze e di riflessioni essenziali anche per la qualità del lavoro interno.

Un valore fondamentale

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

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

Né letture anguste della disciplina della protezione dei dati, dunque, né sue

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

È soltanto un uomo trasparente, flessibile, controllato, mitridatizzato, quello che incontriamo alla fine, provvisoria, di questo cammino? O pure una persona munita di nuovi poteri, sempre più consapevole, un soggetto sociale rafforzato anche dalla presenza di una autorità che lo affianca?

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

PAGINA BIANCA

IL CODICE

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

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. Trattamento dei dati personali nell'esercizio dell'attività giornalistica
A.2. Trattamento di dati personali per scopi storici
A.3. Trattamenti di dati personali a scopi statistici in ambito Sistan
A.4. Trattamenti di dati personali per scopi statistici e scientifici
A.5. Sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti

Allegato B

Misure di sicurezza

Disciplinare tecnico in materia di misure minime di sicurezza

Allegato C

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

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:

(*) Testo aggiornato al 31 gennaio 2005, in base ai seguenti provvedimenti legislativi:

decreto-legge 9 novembre 2004, n. 266, convertito in l. 27 dicembre 2004, n. 306.

decreto-legge 24 giugno 2004, n. 158, convertito in l. 27 luglio 2004, n. 188.

decreto-legge 29 marzo 2004, n. 81, convertito, con modificazioni, in l. 26 maggio 2004, n. 138.

decreto-legge 24 dicembre 2003, n. 354, convertito, con modificazioni, in l. 26 febbraio 2004, n. 45.

decreto legislativo 22 gennaio 2004, n. 42.

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 del-

l'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 rac-

colti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

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

Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne 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, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente personali e non destinati 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 applicabili al trattamento di dati giudiziari

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

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

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

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

2. Nel fornire l'informativa di cui all'articolo 13 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 risperto 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.[1] *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.

(1) Comma aggiunto dall'art. 2-*quinquies*, decreto-legge 29 marzo 2004, n. 81, nel testo modificato dalla legge di conversione 26 maggio 2004, n. 138.

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

non si applicano le seguenti disposizioni del codice:

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

b) articoli da 145 a 151.

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

Art. 54. Modalità di trattamento e flussi di dati

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

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

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

Art. 57. Disposizioni di attuazione

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

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

a) al principio secondo cui la raccolta dei dati è correlata alla specifica finalità perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati, in particolare per quanto riguarda i trattamenti effettuati per finalità di analisi;
b) all'aggiornamento periodico dei dati, anche relativi a valutazioni effettuate in base alla legge, alle diverse modalità relative ai dati trattati senza l'ausilio di strumenti elettronici e alle modalità per rendere conoscibili gli aggiornamenti da parte di altri organi e uffici cui i dati sono stati in precedenza comunicati;
c) ai presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari, anche ai fini della verifica dei requisiti dei dati ai sensi dell'articolo 11, dell'individuazione delle categorie di interessati e della conservazione separata da altri dati che non richiedono il loro utilizzo;
d) all'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, 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 suc-

cessive 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 n. 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, incomparibilità 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'articolo 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 veicoli e 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 sanitarie e 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 semplificare rela-

tive 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 e dai 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 servizi 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.[2] *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,

(2) Comma aggiunto dall'art. 2-*quinquies*, decreto-legge 29 marzo 2004, n. 81, nel testo modificato dalla legge di conversione 26 maggio 2004, n. 138.

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 parti-

colari 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.[3] *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.

(3) Comma aggiunto dall'art. *2-quinques*, decreto-legge 29 marzo 2004, n. 81, nel testo modificato dalla legge di conversione 26 maggio 2004, n. 138.

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 spropor-

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

Art. 112. Finalità di rilevante interesse pubblico

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

2. Tra i trattamenti effettuati per le finalità di cui al 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 2, comma 5-*quater*, del decreto legge 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge 26 maggio 2000, n. 137, e successive modificazioni.

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 acces-

sibili 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, 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 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. È 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[4]

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico tele-

(4) Articolo così sostituito dall'art. 3 del decreto-legge 24 dicembre 2003, n. 354, nel testo modificato dalla legge di conversione 26 febbraio 2004, n. 45.

fonico sono conservati dal fornitore per ventiquattro mesi, per finalità di accertamento e repressione di reati.

2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico sono conservati dal fornitore per ulteriori ventiquattro 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 giudice su istanza del pubblico ministero o 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.*

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 rapportate 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 DINANZI 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'interessato 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 vice presidente, 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 inte-

ressati 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 lire quattromila euro a lire ventiquattromila 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 sé 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 sé 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 - DISPOSIZIONI 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 con-

segna 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 febbraio 1993, 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'arti-*

colo 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, in fine, 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 in fine le seguenti parole: *", ovvero, limitatamente alla violazione di cui all'articolo 10, al Garante per la protezione dei dati personali".*

[*4. Dopo l'articolo 107 del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, è inserito il seguente:*

"Articolo 107-bis. Trattamento di dati personali per scopi storici

1. I documenti per i quali è autorizzata la consultazione ai sensi dell'articolo 107, comma 2, conservano il loro carattere riservato e non possono essere diffusi.

2. I documenti detenuti presso l'Archivio centrale dello Stato e gli Archivi di Stato sono conservati e consultabili anche in caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 13 della legge 31 dicembre 1996, n. 675, qualora ciò risulti necessario per scopi storici. Ai documenti è allegata la documentazione relativa all'esercizio dei diritti. Su richiesta di chiunque vi abbia interesse ai sensi del medesimo articolo 13, può essere comunque disposto il blocco dei dati personali, qualora il loro trattamento comporti un concreto pericolo di lesione della dignità, della riservatezza o dell'identità personale degli interessati e i dati non siano di rilevante interesse pubblico.".][5]

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 *30 giugno 2005*.[6]

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 *30 settembre 2005*.[7]

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 dicembre 2005*;[8]

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) le modalità semplificate per l'informativa e la manifestazione del consenso, ove necessario, possono essere utilizzate dal medico di medicina generale, dal pediatra di libera scelta e dagli organismi sanitari anche in occasione del primo ulteriore contatto con l'interessato, al più tardi entro il 30 settembre 2004;*][9]

f) l'utilizzazione dei modelli di cui all'articolo 87, comma 2, è obbligatoria a decorrere dal 1° gennaio 2005.

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.

(5) Comma abrogato dall'art. 184 del decreto legislativo 22 gennaio 2004, n. 42, a decorrere dal 1° maggio 2004, ai sensi dell'art. 183 del medesimo decreto legislativo (in argomento v., ora, artt. 123 e 126 d.lg. 22 gennaio, n. 42).

(6) (7) Come modificato dall'art. 3 del decreto-legge 24 giugno 2004, n. 158, convertito dalla legge 27 luglio 2004, n. 188, nonché dall'art. 6 del decreto-legge 9 novembre 2004, n. 266, nel testo modificato dalla legge di conversione 27 dicembre 2004, n. 306.

(8) Come modificato dall'art. 3 del decreto-legge 24 giugno 2004, n. 158, nel testo modificato dalla legge di conversione 27 luglio 2004, n. 188.

(9) Lettera abrogata dall'art. 2-*quinquies*, del decreto-legge 29 marzo 2004, n. 81, nel testo modificato dalla legge di conversione 26 maggio 2004, n. 138.

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.[10] *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;

(10) Comma aggiunto dall'articolo 4 del decreto-legge 24 dicembre 2003, n. 354, nel testo modificato dalla legge di conversione 26 febbraio 2004, n. 45.

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 95/46/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. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 30 giugno 2003

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 n. 95/46/CE
	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. n. 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 del Parlamento europeo e del Consiglio n. 2002/58/CE
lett. b)	cfr. art. 2, lett. e), dir. n. 2002/58/CE
lett. c)	cfr. art. 2, par. 1, lett. a), direttiva del Parlamento europeo e del Consiglio n. 2002/21/CE
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), d.lg. n. 281/1999
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. n. 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. n. 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. n. 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, 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. n. 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. n. 95/46/CE
	art. 31, comma 1, lett. h), l. n. 675/1996
comma 2	art. 20, comma 4, d.lg. 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. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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, d.lg. 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. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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, d.lg. 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. n. 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. n. 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. n. 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. n. 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. n. 95/46/CE

Art. 46. Titolari dei trattamenti — —

Art. 47. Trattamenti per ragioni di giustizia — art. 3, par. 2, (primo periodo) dir. n. 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. n. 95/46/CE
CAPO I - PROFILI GENERALI	
Art. 53. Ambito applicativo e titolari dei trattamenti	art. 3, par. 2, (primo periodo) dir. n. 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. n. 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. n. 95/46/CE

Art. 75. Ambito applicativo art. 1, d.lg. n. 282/1999

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), d.lg. 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. n. 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. 675/1996
comma 2 art. 9, comma 1-*bis*, l. 675/1996
comma 3 art. 16, comma 2, lett. c-*bis*), l. 675/1996

Art. 100. Dati relativi ad attività di studio e di ricerca art. 6, comma 4, d.lg. n. 204/1998

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, d.l. 28 marzo 2000, n. 70, conv. da l. 26 maggio 2000, n. 137

TITOLO X - COMUNICAZIONI ELETTRONICHE
CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121. Servizi interessati cfr. art. 3, dir. n. 2002/58/CE

Art. 122. Informazioni raccolte nei riguardi dell'abbonato e dell'utente cfr. art. 5, par. 3, dir. n. 2002/58/CE

Art. 123. Dati relativi al traffico	
comma 1	cfr. art. 6, dir. n. 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. n. 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. n. 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. n. 2002/58/CE
Art. 127. Chiamate di disturbo e di emergenza	
comma 1	cfr. art. 10, dir. n. 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. n. 2002/58/CE
	art. 8, comma 1, d.lg. n. 171/1998
Art. 129. Elenchi di abbonati	cfr. art. 12, dir. n. 2002/58/CE
	art. 9, d.lg. n. 171/1998
Art. 130. Comunicazioni indesiderate	cfr. art. 13, dir. n. 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. n. 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. n. 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. n. 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. n. 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. n. 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	—

PAGINA BIANCA

Allegati

PAGINA BIANCA

Codici di deontologia

A1 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, in *Gazzetta Ufficiale* 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

ORDINE DEI GIORNALISTI - 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, nonchè 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.

A2 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 del 14 marzo 2001, in *Gazzetta Ufficiale* 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 N. 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.

A3 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 pro-

(*) Provvedimento del Garante n. 13 del 31 luglio 2002, in *Gazzetta Ufficiale* 16 agosto 1999, n. 191.

fessionale 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 art. 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 n. 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.

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.

A4 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, in *Gazzetta Ufficiale* del 14 agosto 2004, n. 190. Decreto del Ministro della giustizia del 14 gennaio 2005, di allegazione al Codice.

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 n. R (83)10 adottata il 23 settembre del 1983 e n. 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 n. 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.

A5 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 legge 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, in *Gazzetta Ufficiale* 23 dicembre 2004, n. 300.
Decreto del Ministro della giustizia del 14 gennaio 2005, di allegazione al Codice.

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-legge 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-legge 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-legge 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-legge 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. 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:

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, nonchè 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. 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.

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.

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

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.....)*

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 formazione 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.

PAGINA BIANCA

Relazione 2004

L'attuazione del Codice nel quadro della Costituzione per l'Europa

I. STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Il quadro normativo

1.1. L'entrata in vigore del Codice

1.2. Le modifiche (già) apportate

1.3. Legge finanziaria 2005 e altre novità normative con riflessi in materia di protezione dei dati personali

1.4. Il monitoraggio delle leggi regionali

1.5. Lavori parlamentari

II. L'ATTIVITÀ SVOLTA DAL GARANTE

Prologo

2. Trattamenti effettuati in ambito pubblico

2.1. Notazioni introduttive

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 cd. 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 svolti da regioni ed enti locali

2.11. Attività giudiziaria e informatica giuridica

3. Sanità

3.1. Trattamento di dati idonei a rivelare lo stato di salute

3.2. Trattamento di dati personali in occasione dell'accertamento dell'infezione da Hiv

3.3. Notificazioni in ambito sanitario

3.4. Protezione dei dati e procreazione medicalmente assistita

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 p.s.

6.2. Controllo sui trattamenti effettuati dai servizi di informazione e di sicurezza

6.3. Il controllo sul Sistema di informazione Schengen

6.4. Altri casi di intervento del Garante in relazione a diverse attività svolte dalle forze di polizia

7. Attività giornalistica e mezzi di informazione

7.1. Profili generali

7.2. Tutela dei minori

7.3. Cronache giudiziarie

7.4. Dati idonei a rivelare lo stato di salute

7.5. Libertà di informazione e personaggi pubblici

7.6. Esercizio dei diritti e diritto all'oblio

8. Associazioni, movimenti politici e partiti

8.1. Associazioni

8.2. Movimenti politici e propaganda elettorale

9. Attività economiche

9.1. Trattamenti in ambito bancario e finanziario

9.2. Trattamenti effettuati nell'ambito dei sistemi di informazione creditizia

9.3. Archivio degli assegni bancari e postali e delle carte di pagamento irregolari

9.4. Trattamenti in ambito assicurativo

9.5. *Marketing*

9.6. Carte di fidelizzazione

9.7. Flussi transfrontalieri

10. Libere professioni

10.1. Ordini e collegi professionali

10.2. Liberi professionisti

11. Rapporto di lavoro e previdenza

11.1. Dati trattati nel corso del rapporto di lavoro

11.2. Rapporto di lavoro in ambito pubblico

11.3. Previdenza

12. Videosorveglianza

12.1. Protezione dei dati e videosorveglianza

12.2. Videosorveglianza in ambito pubblico

13. Condomìni e multiproprietà

13.1. Protezione dei dati e condomìni

14. Dati biometrici

14.1. Protezione dei dati e biometria

15. Reti di comunicazione elettronica

15.1. Notazioni introduttive

15.2. Dati di traffico

15.3. I nuovi elenchi telefonici

15.4. *Spam*

15.5. *Sms* istituzionali

15.6. Videochiamate

15.7. Servizi di comunicazione elettronica offerti a titolo gratuito

15.8. Il codice deontologico

15.9. La televisione digitale: i servizi interattivi

15.10. Dati relativi all'ubicazione

15.11. *Radio Frequency Identification*

16. Sicurezza dei dati e dei sistemi

16.1. Le misure minime di sicurezza

17. Registro dei trattamenti

17.1. La notificazione

17.2. Il registro dei trattamenti e futuri sviluppi

17.3. Alcuni dati statistici

18. Esercizio dei diritti e 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. Profili generali

20.2. Procedure

20.3. I casi più rilevanti

20.4. Alcuni riferimenti statistici

20.5. L'attività sanzionatoria del Garante

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

21.4. Attività di cooperazione con altre istituzioni

21.5. Collaborazione con la Guardia di finanza

22. Relazioni internazionali

22.1. Lo stato di recepimento delle direttive comunitarie negli Stati membri dell'Unione europea

22.2. Le iniziative a livello europeo per una migliore applicazione delle direttive comunitarie

22.3. Le conferenze tra autorità di protezione dei dati a livello europeo

22.4. Conferenze delle autorità su scala internazionale

22.5. La cooperazione tra autorità garanti nell'Unione europea: il Gruppo *ex* art. 29

22.6. Il trasferimento dei dati *Pnr* dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea

22.7. Cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni

22.8. L'attività del Garante nell'Autorità di controllo comune Schengen

22.9. Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso

22.10. Il Sistema informativo doganale: l'attività dell'Autorità di controllo comune

22.11. La partecipazione ad altri comitati e gruppi di lavoro

22.12. Consiglio d'Europa

22.13. Ocse

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. Il rapporto con il pubblico

23.5. Le attività di formazione

23.6. Manifestazioni e conferenze

23.7. L'attività di 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. Lo sviluppo del sistema informativo e l'attività in ambito tecnologico

25. Dati statistici

25.1. Grafici e tabelle

DOCUMENTAZIONE

Provvedimenti normativi

26. Decreto legislativo 22 gennaio 2004, n. 42
Codice dei beni culturali e del paesaggio
ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137

27. Legge 26 febbraio 2004, n. 45
Conversione in legge, con modificazioni,
del decreto-legge 24 dicembre 2003, n. 354, recante disposizioni
urgenti per il funzionamento dei tribunali delle acque,
nonché interventi per l'amministrazione della giustizia

28. Legge 26 maggio 2004, n. 138
Conversione in legge, con modificazioni,
del decreto-legge 29 marzo 2004, n. 81, recante interventi urgenti
per fronteggiare situazioni di pericolo per la salute pubblica

29. Legge 27 luglio 2004, n. 188
Conversione in legge, con modificazioni, del decreto-legge
24 giugno 2004, n. 158, concernente permanenza in carica
degli attuali consigli degli ordini professionali e proroga di termini
in materia di difesa d'ufficio e procedimenti civili davanti al tribunale
per i minorenni, nonché di protezione dei dati personali

30. Legge 27 dicembre 2004, n. 306
Conversione in legge, con modificazioni, del decreto-legge 9 novembre
2004, n. 266, recante proroga o differimento di termini
previsti da disposizioni legislative. Disposizioni di proroga
di termini per l'esercizio di deleghe legislative

Provvedimenti del Garante

31. Autorizzazione n. 1/2004
al trattamento dei dati sensibili nei rapporti di lavoro

32. Autorizzazione n. 2/2004
al trattamento dei dati idonei a rivelare lo stato di salute
e la vita sessuale

33. Autorizzazione n. 3/2004
al trattamento dei dati sensibili da parte degli organismi
di tipo associativo e delle fondazioni

34. Autorizzazione n. 4/2004
al trattamento dei dati sensibili da parte dei liberi professionisti

35. Autorizzazione n. 5/2004
al trattamento dei dati sensibili da parte
di diverse categorie di titolari

36. Autorizzazione n. 6/2004
al trattamento dei dati sensibili da parte degli investigatori privati

37. Autorizzazione n. 7/2004
al trattamento dei dati a carattere giudiziario da parte di privati,
di enti pubblici economici e di soggetti pubblici

38. Disposizioni in materia di comunicazione e di propaganda politica

39. Casi da sottrarre all'obbligo di notificazione al Garante

40. Sistemi di informazioni creditizie e bilanciamento di interessi

41. Contributo spese in caso di esercizio dei diritti dell'interessato

Unione europea

42. Decisione della Commissione del 28 aprile 2004
sulla adeguata protezione dei dati personali nell'Isola di Man

43. Decisione della Commissione del 14 maggio 2004,
relativa al livello di protezione adeguato dei dati personali
contenuti nelle schede nominative dei passeggeri aerei
trasferiti all'Ufficio delle dogane e della protezione delle frontiere
degli Stati Uniti - *United States Bureau*
of Customs and Border Protection

44. Decisione del Consiglio del 17 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 Dipartimento per la sicurezza interna degli Stati Uniti

45. Accordo fra la Comunità europea e gli Stati Uniti d'America
sul trattamento ed il trasferimento di dati PNR
da parte di vettori aerei al *Department of Homeland Security*,
Bureau of Customs and Border Protection degli Stati Uniti

46. Decisione della Commissione del 27 dicembre 2004
che modifica la decisione 2001/497/CE per quanto riguarda
l'introduzione di un insieme alternativo di clausole contrattuali
tipo per il trasferimento di dati personali a Paesi Terzi

47. Documento di lavoro della Commissione
L'attuazione della Decisione della Commissione 520/2000/CE
sulla protezione adeguata dei dati personali
offerta dai principi di "*Safe Harbour*" in materia di *privacy*
e dalle relative Domande più frequenti,
pubblicati dal *Department of Commerce* degli USA

48. Studio sull'attuazione della decisione relativa al *Safe Harbour*,
redatto su richiesta della Commissione Europea,
DG Mercato Interno

49. Regolamento (CE) n. 871/2004 del Consiglio
del 29 aprile 2004 relativo all'introduzione
di alcune nuove funzioni del sistema d'informazione Schengen,
compresa la lotta contro il terrorismo

50. Decisione del Consiglio n. 2004/512/CE dell'8 giugno 2004
che istituisce il sistema di informazione visti (VIS)

51. Lettera inviata il 30 novembre 2004 dal Gruppo *ex* art. 29
al Presidente del Consiglio dell'UE, Jan Peter Balkenende,
al Presidente del Parlamento europeo, Josep Borrell Fontelles,
ed al Presidente della Commissione per le libertà civili, la giustizia
e gli affari interni del Parlamento europeo, Jean-Louis Bourlanges,
in merito alla Proposta di Regolamento del Consiglio
sullo standard applicabile agli elementi di sicurezza e biometrici
nei passaporti dei cittadini dell'Unione europea

52. 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

53. Rete Ue di esperti indipendenti in materia di diritti fondamentali
(CFR-CDF) – Rapporto sulla situazione dei diritti fondamentali
nell'Unione europea nel 2003

Autorità di controllo comune dell'Europol

54. La seconda relazione di attività
dell'Autorità di controllo comune dell'Europol

Autorità di controllo comune Schengen

55. Il parere 2004 SIS II

56. Attività dell'Autorità di controllo comune,
Sesto Rapporto (gennaio 2002 - dicembre 2003)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

(art. 29 direttiva 95/46/CE)

57. Parere 1/2004
sul livello di protezione garantito in Australia
per la trasmissione dei dati delle registrazioni
dei nomi dei passeggeri da parte delle compagnie aeree

58. Documento di lavoro sulle piattaforme informatiche fidate,
in particolare per quanto riguarda il lavoro
effettuato da *Trusted Computing Group* (Gruppo TCG)

59. Parere 2/2004
sul livello di protezione adeguato dei dati a carattere personale
contenuti nelle pratiche Passeggeri (PNR - *Passenger Name Records*)
trasferite all'Ufficio delle dogane e della protezione di frontiera
degli Stati Uniti
(*Bureau of Customs and Border Protection* - US CBP)

60. Parere 3/2004
sul livello di protezione assicurato in Canada
ai fini della trasmissione da parte di vettori aerei
dei *Passenger Name Records*
e di informazioni avanzate sui passeggeri

61. Parere 4/2004
relativo al trattamento dei dati personali
mediante videosorveglianza

62. Parere 5/2004
relativo alle comunicazioni indesiderate
a fini di commercializzazione diretta
ai sensi dell'articolo 13 della direttiva 2002/58/CE

63. Documento di lavoro sui dati genetici

64. Dichiarazione comune
in risposta agli attentati terroristici di Madrid

65. Parere 6/2004
sull'attuazione della Decisione della Commissione
del 14 maggio 2004 relativa al livello di protezione adeguato
dei dati personali contenuti nelle schede nominative
dei passeggeri aerei trasferiti all'Ufficio delle dogane
e della protezione delle frontiere degli Stati Uniti
(*United States Bureau of Customs and Border Protection*),
e dell'Accordo fra la Comunità europea e gli Stati Uniti d'America
sul trattamento ed il trasferimento di dati PNR
da parte di vettori aerei al *Department of Homeland Security*,
Bureau of Customs and Border Protection degli Stati Uniti

66. Parere 7/2004
relativo all'inserimento di elementi biometrici
nei permessi di soggiorno e nei visti, alla luce dell'istituzione
del Sistema informativo europeo sui visti (VIS)

67. Parere 8/2004
sull'informazione dei passeggeri
in merito al trasferimento di schede nominative dei passeggeri aerei
(PNR) sui voli tra l'Unione europea e gli Stati Uniti d'America

68. Documento strategico

69. Parere 9/2004
relativo ad una proposta di Decisione Quadro
sulla memorizzazione di dati trattati e conservati allo scopo
di fornire servizi pubblici di comunicazioni elettroniche
o di dati disponibili su reti pubbliche di comunicazioni,
ai fini della prevenzione, delle indagini, dell'accertamento
e del perseguimento di atti criminali, compreso il terrorismo
[Proposta presentata da Francia, Irlanda, Svezia e Gran Bretagna
(Documento del Consiglio 8958/04del 28 aprile 2004)]

70. Parere relativo ad una maggiore armonizzazione delle informative
(Allegato n. 1)

71. Dichiarazione del Gruppo di lavoro *ex* art. 29 sulle attività di *enforcement*

72. Lista di controllo
Istanza di approvazione di norme aziendali vincolanti (*Binding Corporate Rules*)

Consiglio d'Europa

73. Principi guida per la protezione dei dati personali in relazione alle "carte intelligenti" (*smart card*)

26ª Conferenza internazionale sulla protezione dei dati Wroclaw (Polonia) 13-16 settembre 2004

74. Risoluzione della Conferenza europea per la protezione dei dati relativa all'istituzione di un *forum* comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia (protezione dei dati nel Terzo Pilastro)

75. Risoluzione relativa alla proposta di uno standard-quadro ISO in materia di *privacy*

76. Versione emendata della Risoluzione della Conferenza internazionale del 2003 relativa agli aggiornamenti automatici di *software*

Elenco delle abbreviazioni

La presente Relazione è riferita al 2004 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 25 gennaio 2005, relative a sviluppi che si è ritenuto opportuno menzionare.

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.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
Pa	Pubblica amministrazione
par.	paragrafo
Provv.	provvedimento
Relazione	Relazione del Garante per la protezione dei dati personali
r.d.	regio decreto
reg.	regolamento
S.p.A.	società per azioni
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Il quadro normativo

1.1. *L'entrata in vigore del Codice*

L'entrata in vigore del "Codice in materia di protezione dei dati personali" (decreto legislativo 30 giugno 2003, n. 196, di seguito, semplicemente, "Codice"), avvenuta il 1° gennaio 2004, ha rappresentato una tappa fondamentale per la tutela dei diritti della persona e ha concluso il processo di recepimento delle direttive europee in materia (95/46/CE e 2002/58/CE). È stato così completato il complesso percorso di razionalizzazione della disciplina inizialmente introdotta con la legge 31 dicembre 1996, n. 675, riunendo in un unico testo una regolamentazione che si era, nel tempo, stratificata a seguito di numerosi interventi modificativi e integrativi.

In un quadro complessivo di rafforzate garanzie –con il riconoscimento del diritto alla protezione dei dati personali (art. 1 del Codice), in armonia con quanto ora previsto nel Trattato che ha adottato la Costituzione europea– la nuova disciplina ha provveduto a semplificare alcuni adempimenti e ad attribuire un ruolo significativo, anche in una prospettiva di deflazione legislativa, ai codici di deontologia e di buona condotta, soggetti alla preventiva verifica da parte del Garante.

1.2. *Le modifiche (già) apportate*

Devono comunque rilevarsi alcuni segnali che sembrano muoversi in controtendenza rispetto al progetto di "stabilizzare" le regole di protezione dei dati personali.

Già nel primo anno di vigenza del Codice, infatti, sono stati introdotti alcuni, seppur circoscritti, interventi modificativi in settori di rilievo, e segnatamente in relazione al regime dei dati relativi al traffico telefonico, nel contesto sanitario e con riferimento alle ripetute proroghe dei termini per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili da parte dei soggetti pubblici.

La conservazione dei dati di traffico

Importanza particolare assumono le modifiche legislative apportate all'art. 132 del Codice (prima della sua entrata in vigore) con riguardo alla materia, di rilevanza costituzionale, della conservazione dei dati relativi al traffico telefonico per finalità di accertamento e di repressione dei reati (decreto-legge 24 dicembre 2003, n. 354, come modificato dalla legge di conversione 26 febbraio 2004, n. 45). Questa tema-

tica si è riproposta anche nel contesto delle misure adottate per contrastare la diffusione telematica abusiva di materiale audiovisivo, nell'ambito del dibattito parlamentare relativo alla materia regolata nel decreto-legge 22 marzo 2004, n. 72 (convertito con legge 21 maggio 2004, n. 128).

Il profilo della conservazione dei dati di traffico telefonico e telematico è nuovamente riemerso, con tutte le criticità che lo caratterizzano, nel corso delle audizioni effettuate in sede d'esame del disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (AC 4599) (in merito si rinvia al par. 15.2).

Il trattamento di dati idonei a rivelare lo stato di salute in ambito sanitario

Alcune modifiche al Codice –a brevissima distanza di tempo dalla sua entrata in vigore– hanno riguardato altresì i trattamenti di dati personali effettuati in ambito sanitario. In merito a tali interventi il Garante aveva peraltro manifestato i propri dubbi al Senato, trattandosi di modifiche in alcuni casi non necessarie (ad esempio, in quanto volte ad esonerare i medici di base dall'adozione di misure alle quali essi non erano comunque tenuti) e in altri non opportune (in quanto suscettibili di incrinare gravemente l'armonia del quadro normativo).

Con tali innovazioni è stata esclusa l'applicabilità ai medici di base dell'obbligo di notificare al Garante alcuni trattamenti effettuati a fini sanitari (art. 37, comma 1-*bis*, del Codice) e di alcune disposizioni del Codice (v. ora l'art. 83, comma 2-*bis*) a garanzia dell'"anonimato" del paziente in sala d'attesa (già, peraltro, limitato sin dall'origine alle sole "strutture" sanitarie). Inoltre, si è subordinata l'omissione delle generalità del paziente in alcune ricette mediche ad un'esplicita richiesta dell'interessato (art. 89, comma 2-*bis*).

È stato poi soppresso l'art. 181, comma 1, lett. *e*), del Codice, che prevedeva il termine del 30 settembre 2004 per adottare modalità semplificate per l'acquisizione del consenso e il rilascio dell'informativa previste dall'art. 76, comma 2; con il risultato, quindi, di cancellare inopportunamente il termine transitorio che era stato previsto a favore dei soggetti contemplati nella disposizione (decreto-legge 29 marzo 2004, n. 81, convertito con modificazioni con legge 26 maggio 2004, n. 138; pochi mesi prima, un analogo provvedimento d'urgenza non era stato approvato alla Camera: decreto-legge 21 gennaio 2004, n. 10).

Nel corso dei lavori di conversione del decreto-legge è stato anche presentato, e poi ritirato, un emendamento parlamentare che prevedeva una sorta di "consenso presunto" del paziente al trattamento dei propri dati personali. L'Autorità ha evidenziato al Governo e al Parlamento il contrasto di tale disposizione con i principi normativi, anche comunitari, in materia di consenso –che deve essere comunque "esplicito", oltre che inequivoco–, soprattutto in relazione ai dati sensibili. Tuttavia, a conclusione dei lavori, il Governo ha accettato come raccomandazione una proposta di ordine del giorno in base alla quale dovrebbero essere adottate, in via transitoria, misure che consentano ai pazienti già in carico ai medici di base di esprimere il consenso mediante una procedura di silenzio-assenso.

Proroga dei termini

Nel pur breve lasso di tempo dall'entrata in vigore del Codice, ricorrendo alla decretazione d'urgenza, si sono differiti i termini per l'adempimento di taluni obblighi posti a garanzia dell'interessato, relativamente all'applicazione delle "nuove" misure minime di sicurezza (per l'introduzione delle quali il Codice aveva fissato il termine del 30 giugno 2004 all'art. 180, comma 1) e all'adozione dei regolamenti in materia di dati sensibili da parte dei soggetti pubblici (su entrambi gli argomenti si vedano pure, rispettivamente, i par. 16.1 e 2.2).

Adozione delle misure minime di sicurezza

Con specifico riguardo alle misure minime di sicurezza, malgrado la scadenza originariamente fissata potesse ritenersi congrua rispetto alle esigenze prospettate (tanto più che era previsto il più ampio termine del 1° gennaio 2005 per i soggetti che alla data di entrata in vigore del Codice non disponessero di strumenti elettronici tali da consentire l'immediata applicazione delle misure di sicurezza), essa ha subito, in appena un anno, un duplice rinvio: inizialmente al 31 dicembre 2004 e, quindi, al 30 giugno 2005. Analogamente, è stato prorogato anche il termine per l'adozione delle 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 e, da ultimo, al 30 settembre 2005 (art. 3, decreto-legge 24 giugno 2004, n. 158, convertito, con modificazioni, con legge 27 luglio 2004, n. 188; decreto-legge 9 novembre 2004, n. 266, convertito, con modificazioni, con legge 27 dicembre 2004 n. 306).

Adozione dei regolamenti sul trattamento dei dati sensibili e giudiziari

Il citato decreto-legge n. 158/2004 ha prorogato anche il termine previsto dal Codice per approvare i regolamenti delle pubbliche amministrazioni in materia di dati sensibili e giudiziari, originariamente fissato al 30 settembre 2004 (art. 181, comma 1, lett. *a*). Si tratta dell'ennesimo rinvio dell'attuazione di una disciplina (che riguarda un settore assai delicato), prevista ora dagli artt. 20 e 21 del Codice, ma introdotta già con il d.lg. n. 135/1999 e rimasta largamente inattuata, come più volte rilevato dal Garante che ha peraltro richiamato sul punto l'attenzione del Governo (v., fra l'altro, *Provv.* 17 gennaio 2002).

1.3. *Legge finanziaria 2005 e altre novità normative con riflessi in materia di protezione dei dati personali*

Nel corso dell'anno sono stati approvati altri provvedimenti normativi che riguardano la materia del trattamento dei dati personali e l'attività del Garante.

Si fa riferimento, in particolare, alla legge finanziaria per il 2005 (legge 30 dicembre 2004, n. 312, alla *G.U.* 31 dicembre 2004, n. 306, S.O. n. 193), che prevede la trasmissione per via telematica del certificato di diagnosi sull'inizio e sulla durata presunta della malattia da parte del medico curante all'Inps (art. 1, comma 149) ovvero dei cedolini per il pagamento delle competenze stipendiali del personale della pubblica amministrazione (art. 1, comma 197); presenta poi profili di sovrapposizione con alcune norme del Codice la disciplina, dettata a fini di contrasto di fenomeni di elusione fiscale, che mira a circoscrivere la riutilizzazione commerciale dei documenti e dei dati acquisiti dagli archivi catastali o da pubblici registri immobiliari (art. 1, commi 367-373). La predetta legge, infine, modificando l'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito dalla legge 24 novembre 2003, n. 326, prevede che la tessera sanitaria sia consegnata a tutti gli assistiti entro il 31 dicembre 2005.

La medesima legge finanziaria ha poi ridotto considerevolmente le risorse finanziarie a disposizione del Garante, comportando gravi difficoltà per il funzionamento dell'Ufficio, come ampiamente segnalato dal Garante al Governo e al Parlamento durante i lavori di approvazione del disegno di legge.

Di particolare interesse, inoltre, è una recente ordinanza del Presidente del Consiglio dei ministri, approvata previo parere del Garante, finalizzata alla localizzazione dei cittadini italiani presenti nelle aree colpite dai recenti eventi calamitosi che hanno investito il sud-est asiatico (ordinanza n. 3390 del 29 dicembre 2004, in *G.U.* 4 gennaio 2005, n. 2). Con tale provvedimento, i gestori di sistemi di telefonia sono stati autorizzati a fornire al Ministero degli affari esteri dati e informazioni utili per

rintracciare i titolari di utenze di telefonia mobile presenti nei luoghi del disastro.

In materia di Carta nazionale dei servizi si registra, infine, l'adozione del d.m. 6 dicembre 2004 (adottato dal Ministro dell'interno, di concerto con i Ministri dell'innovazione e le tecnologie, nonché dell'economia e delle finanze), recante regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della "Carta" medesima. Il decreto individua altresì i dati personali registrati nella memoria riscrivibile del microcircuito, le misure di sicurezza, i servizi e le infrastrutture delle pubbliche amministrazioni coinvolte nel circuito di emissione.

1.4. *Il monitoraggio delle leggi regionali*

Nel corso dell'anno si è proceduto, con riferimento alle disposizioni più rilevanti in materia di protezione dei dati personali, a monitorare le leggi regionali pubblicate sulla Gazzetta Ufficiale.

I testi sui quali è stata effettuata un'analisi più approfondita riguardano disposizioni relative ai settori più vari, in ragione del carattere ampio e trasversale della disciplina di protezione dei dati personali.

Tra le questioni più rilevanti esaminate vi è quella dei limiti della potestà legislativa nelle materie riservate alle regioni rispetto a quella esclusiva dello Stato in tema di protezione dei dati personali alla luce dell'art. 117 Cost. (così come novellato dalla legge costituzionale 18 ottobre 2001, n. 3). Trattasi, com'è noto, di un tema al centro del vivace dibattito al quale l'Autorità è stata chiamata a prendere parte in passato (per i profili di propria competenza), anche con l'audizione del Presidente del Garante alla Commissione affari costituzionali della Camera dei deputati, avvenuta il 30 ottobre 2001 (*Indagine conoscitiva sugli effetti nell'ordinamento delle revisioni del titolo V della parte II della Costituzione*).

Sotto tale profilo è stata in particolare registrata la crescente adozione di provvedimenti legislativi che, pur attenendo direttamente a materie di competenza regionale, contengono disposizioni anche in materia di protezione dei dati personali; si tratta, tuttavia, di discipline a volte ripetitive rispetto alla legislazione nazionale e quindi inidonee ad incidere sul livello di protezione dei diritti della persona garantito dalla legislazione comunitaria e da quella statale (salvo riproporne caratteri e problematiche).

A titolo esemplificativo, si menziona la normativa in materia di prestazioni sociali agevolate che, com'è noto, prevede il ricorso all'indicatore della situazione economica equivalente ai fini della redazione della graduatoria dei beneficiari (cfr. d.lg. 31 marzo 1998, n. 109 successivamente integrato dal d.lg. 3 maggio 2000, n. 130 e dai regolamenti applicativi). A questo proposito, è stato rilevato che la genericità e la frammentarietà della legislazione nazionale in materia di prestazioni sociali agevolate, a suo tempo evidenziate dall'Autorità (cfr. *Pareri* 27 marzo 1998, 26 maggio 1999 e 5 aprile 2000), si riflettono sulle legislazioni regionali in merito all'esatta individuazione delle medesime, degli enti erogatori e dei soggetti, anche privati, legittimati al trattamento dei dati, delle condizioni e dei limiti delle interconnessioni con gli archivi pubblici e privati.

Nell'evidenziare la sostanziale conformità a volte anche letterale tra le disposizioni regionali e quelle statali, è emersa anche, con riferimento alla normativa sugli enti locali –che riconosce ai consiglieri comunali e provinciali il diritto di ottenere dalle amministrazioni di appartenenza notizie ed informazioni connesse all'espletamento del proprio mandato (art. 43, comma 2, d.lg. 18 agosto 2000, n. 267)– la dibattuta questione dei limiti del predetto diritto di accesso; mentre alcune pronunce giuri-

sprudenziali (per esempio Cons. Stato, 4 maggio 2004, n. 2716) lo configurano in modo piuttosto ampio (ritenendo ad esempio che la motivazione relativa alla richiesta di accesso avanzata "per l'espletamento del mandato" basti a giustificarla, senza che occorra alcuna ulteriore precisazione circa le specifiche ragioni della richiesta), altre significative prese di posizione evidenziano, al contrario, una delimitazione dell'accesso ai soli dati personali comunque pertinenti e non eccedenti rispetto alle finalità perseguite nel caso specifico dal richiedente.

Anche con riferimento alla legislazione regionale, in più casi è emersa la mancata, o inadeguata specificazione dei dati sensibili oggetto di trattamento, che necessitano pertanto di un'ulteriore individuazione con atto regolamentare ai sensi dell'art. 20, comma 2, del Codice, nei pur più ampi termini temporali accordati dal menzionato decreto-legge n. 158/2004.

È allo studio dell'Autorità la questione se ipotesi di accordi tra Stato e regioni nonché, più specificamente, forme di intesa su materie che presentino riflessi rilevanti sulla riservatezza delle persone siano soggette al preventivo parere del Garante (cfr. art. 154, comma 4, del Codice).

1.5. *Lavori parlamentari*

Oltre ai provvedimenti normativi approvati, menzionati nel paragrafo precedente, vanno segnalati alcuni lavori parlamentari in corso, anch'essi di interesse per la materia della protezione dei dati personali. In proposito vanno ricordati, in particolare:

Costituzione

a) il disegno di legge costituzionale di modifica della Parte II della Costituzione (AC 4862), nell'ambito del quale la Camera, il 30 settembre 2004, ha approvato un emendamento che "inserisce" le autorità indipendenti nella Carta costituzionale. L'emendamento, presentato da esponenti della maggioranza e modificato da subemendamenti presentati da parlamentari dell'opposizione, è stato approvato quasi all'unanimità (352 sì e 10 no). Esso ha inserito nella Costituzione l'art. 98-*bis* ai sensi del quale, per lo svolgimento di attività di garanzia o di vigilanza in materia di diritti di libertà riconosciuti dalla Costituzione e su materie di competenza dello Stato, si possono istituire con legge apposite autorità indipendenti, stabilendo i requisiti di eleggibilità e le condizioni di indipendenza dei componenti e la durata del relativo mandato. Tali autorità riferiscono alle Camere sui risultati delle attività svolte;

Sfruttamento sessuale dei bambini e pedopornografia in Internet

b) il disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (AC 4599), che mira ad istituire, presso il Dipartimento della pubblica sicurezza, un ufficio centrale per il contrasto della pedopornografia sulla rete Internet. A tale unità organizzativa (Centro nazionale) verrebbe attribuita una pluralità di compiti: raccogliere dalle forze di polizia segnalazioni di siti che diffondono materiale pedopornografico; tenere un registro dei medesimi, dei loro gestori, dei soggetti beneficiari dei pagamenti connessi al commercio di materiale pedopornografico; raccogliere, inoltre, le segnalazioni dei fornitori di servizi di comunicazione elettronica relative a contratti con imprese o soggetti che diffondono o commerciano il predetto materiale. Il disegno di legge pone, poi, a carico dei fornitori di connettività ad Internet obblighi finalizzati ad impedire o a filtrare l'accesso ai siti segnalati e prevede scambi informativi fra il menzionato Centro nazionale, l'Ufficio italiano cambi e il sistema bancario e finanzia-

rio per l'individuazione delle persone che beneficiano dei pagamenti sopra menzionati. Per l'individuazione delle modalità di trasmissione in via telematica di tali informazioni riservate è prevista l'adozione di un regolamento, previo parere del Garante. Nell'ambito dei lavori in Commissione giustizia della Camera si sono tenute una serie di audizioni informali, che hanno interessato anche l'Autorità, nell'ambito delle quali è stato sollevato il problema della conservazione dei dati di traffico in Internet (sul quale si rinvia al par. 15.2), ritenuta utile dalle forze di polizia per finalità d'indagine e repressione dei reati commessi in via telematica;

Siti aventi natura editoriale e testate editoriali

c) il disegno di legge del Governo in materia di editoria e di diffusione della stampa (AC 4163), in discussione presso la Commissione cultura della Camera, che all'art. 1 reca disposizioni in materia di siti aventi natura editoriale e testate editoriali. In un'audizione informale tenuta il 4 novembre u.s., il Presidente del Garante ha richiamato l'attenzione della Commissione sulla necessità di coordinare le emanande disposizioni con le norme del Codice che disciplinano le responsabilità e i compiti del titolare e del responsabile del trattamento, in particolare quando i dati sono trattati mediante un sito Internet. Il Garante ha ritenuto inoltre opportuno un migliore coordinamento tra alcune disposizioni del disegno di legge, la normativa vigente in materia di registrazione delle testate giornalistiche e il progetto di legge recentemente approvato dalla Camera in materia di diffamazione a mezzo stampa, che ha esteso ai siti aventi natura editoriale l'intera disciplina della legge sulla stampa (AS 3176);

Dna dell'imputato o dell'indagato

d) due proposte di legge in materia di analisi del Dna dell'imputato o dell'indagato in ambito processuale, che prevedono un'integrazione del codice di procedura penale e, a certe condizioni, l'obbligo per tali soggetti di sottoporsi al prelievo di materiale biologico a fini di confronto con quello presente su materiale probatorio rinvenuto nel corso delle indagini (AC 4682 e AC 4161). Nelle ultime sedute è stato sollevato dal Presidente della Commissione giustizia della Camera e dal relatore il problema dell'eventuale istituzione di una banca dati in cui conservare i campioni di materiale genetico e i dati personali dei soggetti interessati. Ogni approfondimento al riguardo richiederà un'attenta valutazione delle implicazioni di rilievo costituzionale che ne deriverebbero per i diritti fondamentali della persona e, in particolare, per la riservatezza e la dignità degli interessati;

Accesso ai dati sanitari da parte dell'interessato

e) alcuni disegni di legge recanti disposizioni in materia di consenso informato e di dichiarazioni di volontà anticipate nei trattamenti sanitari (AASS 1437, 2279 e 2943) sono all'esame congiunto della Commissione sanità del Senato. Fra gli aspetti d'interesse in materia di protezione dei dati personali, i disegni di legge prevedono il diritto del paziente di "conoscere i dati sanitari" che lo riguardano, diritto che però dovrebbe essere opportunamente coordinato con il diritto di accesso ai dati personali già previsto dall'art. 7 del Codice (oltre che con la disposizione contenuta nell'art. 84 del Codice relativa alle modalità di comunicazione all'interessato dei dati idonei a rivelare lo stato di salute). Le proposte di legge introducono, poi, il "testamento di vita" e il "mandato in previsione dell'incapacità", definiti, rispettivamente, come l'atto scritto con cui si dispone in merito ai trattamenti sanitari, nonché in ordine all'uso del proprio corpo, e come il contratto con cui si attribuisce al mandatario il potere di compiere atti giuridici in nome e nell'interesse del rappresentato in caso di incapacità sopravvenuta. Sia il "testamento di vita", sia il "mandato in pre-

visione dell'incapacità" sarebbero conservati in un registro informatico istituito nell'ambito di un archivio unico nazionale presso il Consiglio nazionale del notariato, consultabili, in via telematica, da notai, autorità giudiziaria, dirigenti sanitari e medici responsabili del trattamento di soggetti ove ricorrano le condizioni di incapacità previste dal disegno di legge. Il contenuto del testamento di vita e le convenzioni oggetto del mandato non verrebbero considerati, ai fini dell'applicazione della norma, dati sensibili. Anche per questi aspetti, le disposizioni richiedono un diverso e adeguato coordinamento con la normativa in materia di protezione dei dati personali;

f) il disegno di legge comunitaria 2004 (AS 2742-B), il cui art. 8 conferisce delega al Governo per il recepimento della direttiva 2003/6/CE del Parlamento europeo e del Consiglio del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (cd. abusi di mercato). La disposizione, originariamente all'esame delle Commissioni VI e X della Camera nell'ambito del testo di riforma della normativa in materia di tutela del risparmio, attribuisce alla Consob poteri di informazione e di indagine in relazione ai quali l'Autorità ha suggerito alla Commissione per le politiche dell'Unione europea della Camera alcune proposte emendative volte ad armonizzarne il testo con le disposizioni del Codice, in particolare per quanto riguarda l'applicazione delle garanzie in materia di comunicazione o diffusione dei dati e di acquisizione di dati di traffico;

Cd. "abusi di mercato"

g) il disegno di legge di riforma della legge 7 agosto 1990, n. 241 (AS 1281-B) in relazione al quale l'Autorità ha segnalato alla Commissione affari costituzionali del Senato la necessità di alcune modifiche in vista di un opportuno coordinamento con le norme del Codice che disciplinano l'accesso ai dati personali, anche per quanto riguarda la prevista "collaborazione" fra il Garante e la Commissione per l'accesso ai documenti amministrativi, istituita presso la Presidenza del Consiglio, in procedimenti nei quali rilevino allo stesso tempo questioni concernenti l'accesso ai documenti e a dati personali. Solo due delle proposte suggerite dall'Autorità sono state, poi, approvate dal Senato;

Disciplina dell'accesso ai documenti amministrativi

h) il progetto di riforma della normativa in materia di fallimento (r.d. 16 marzo 1942, n. 267), predisposto da un comitato ristretto istituito nell'ambito della Commissione giustizia del Senato, che presenta alcuni aspetti di interesse in materia di protezione dei dati personali, sui quali la predetta Commissione ha richiesto, informalmente, un contributo all'Autorità per un più ampio approfondimento della materia;

Fallimento

i) nell'ambito dei lavori in Commissione giustizia del Senato per la modifica del codice di procedura civile (AS 2430, approvato dalla Camera), cui si è già fatto cenno nella *Relazione 2003*, l'Autorità ha segnalato l'opportunità di armonizzare alcune disposizioni del testo con le modifiche apportate dal Codice in materia di notifica di atti giudiziari e di pubblicazione degli avvisi di esecuzione immobiliare (art. 490 c.p.c., modificato dall'art. 174, comma 9, del Codice);

Modifiche al codice di procedura civile

l) sono stati seguiti i lavori relativi ad alcune indagini conoscitive riguardanti tematiche d'interesse, fra le quali, in particolare, l'indagine sull'armonizzazione dei sistemi di gestione dell'anagrafe tributaria, presso la competente Commissione parlamentare di vigilanza. In tale ambito, il 21 gennaio 2004 si è tenuta un'audizione del Presidente del Garante,

Anagrafi tributarie nell'Ue

nella quale si sono auspicate modalità armonizzate nella circolazione delle informazioni personali conservate nelle anagrafi tributarie dei vari Paesi europei, rispettose dei principi di protezione dei dati. Il documento conclusivo dell'indagine approvato il 6 aprile 2004, nel riportare le indicazioni del Garante, dà risalto al sistema delle garanzie e di tutela degli interessati, mettendo in luce l'importanza del rispetto delle disposizioni del Codice per assicurare un equilibrio fra le esigenze di riservatezza e quelle di conoscenza dei dati di tipo fiscale ed economico, anche in ambito europeo.

II - L'attività svolta dal Garante

Prologo

I compiti del Garante, in buona parte descritti all'art. 154 del Codice (ma non esauribili in questa disposizione) sono molteplici ed implicano attività dal contenuto composito.

Per renderne conto compiutamente, questa sezione della *Relazione* è idealmente strutturata in due corpi: il primo (compreso tra i paragrafi 2 e 16), è orientato sui macro-settori nei quali le norme contenute nel Codice incidono (semplificando: trattamenti in ambito pubblico, attività economiche e libertà fondamentali e tecnologie dell'informazione); il secondo (compreso tra i paragrafi 17 e 23), tralasciando il criterio della materia, mette in luce la multiforme tipologia di attività posta in essere dal Garante e dall'Ufficio, a livello nazionale e sovranazionale, finalizzata all'attuazione della disciplina di protezione dei dati.

2 Trattamenti effettuati in ambito pubblico

2.1. *Notazioni introduttive*

A otto anni dall'introduzione nel nostro ordinamento della disciplina di protezione dei dati personali, il settore pubblico manifesta (anche alla luce dei quesiti pervenuti al Garante nel 2004) una crescente consapevolezza dei valori sottesi al Codice.

Ciononostante, e malgrado l'impegno profuso in varie forme dall'Autorità (ad esempio, attraverso risposte a quesiti, attività di comunicazione, formazione ed informazione svolte; per queste ultime v. i par. 23.1. e ss.) nel sensibilizzare le amministrazioni pubbliche, permane in alcuni contesti una inattuazione (o parziale attuazione) delle disposizioni poste in materia di trattamento dei dati personali, soprattutto con riferimento a quelli sensibili (e giudiziari).

A testimoniare poi l'esistenza di flussi di informazioni personali diversi da quelli sensibili e giudiziari tra enti pubblici, anche in assenza di una norma di legge o di regolamento che li preveda (flussi pur necessari per lo svolgimento delle funzioni istituzionali di uno degli enti coinvolti), stanno le numerosissime comunicazioni pervenute all'Autorità ai sensi degli artt. 19, comma 2 e 39, comma 1, lett. *a*) del Codice (analiticamente menzionate nel successivo par. 2.2).

Il settore pubblico resta uno dei contesti nei quali, per i motivi più vari, persiste la difficoltà di una applicazione piena –che non si risolva nel mero assolvimento di adempimenti puramente formali– dei principi di protezione dei dati personali.

Se obiettivo prioritario del Garante è tuttora la "messa in sicurezza" dei trattamenti più delicati (quelli aventi ad oggetto il trattamento dei dati sensibili) o delle modalità più pericolose di trattamento delle informazioni (prime fra tutte le interconnessioni), le pagine a seguire renderanno conto dei mille rivoli nei quali l'Autorità, costantemente sollecitata e pur potendo disporre di risorse assai limitate, è chiamata ad intervenire.

2.2. *Regolamenti sui trattamenti di dati sensibili e giudiziari*

Come è noto, i soggetti pubblici possono trattare i dati sensibili esclusivamente in base ad un'espressa disposizione di legge nella quale siano specificati i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. In presenza di una disposizione primaria che si limiti unicamente a specificare solo la finalità di rilevante interesse pubblico, tali soggetti devono identificare e rendere pubblici i tipi di dati sensibili o giudiziari, nonché le operazioni eseguibili in relazione alle finalità perseguite nei singoli casi, al fine di rendere legittimo il trattamento: a tale scopo, sono tenuti ad adottare o a promuovere l'adozione di un atto di natura regolamentare che sia conforme al parere reso dal Garante sui relativi progetti (parere che, nell'ottica di garantire il principio di semplificazione nell'elevata tutela, può essere fornito anche su schemi-tipo).

Nonostante tale adempimento fosse già contemplato dalla legge n. 675/1996, il Codice, prevedendo un ulteriore periodo transitorio di adeguamento per le amministrazioni, aveva indicato, in un primo tempo, il 30 settembre 2004, termine successivamente prorogato al 31 dicembre 2005, quale scadenza perentoria per l'adozione dei predetti regolamenti previsti dagli artt. 20 e 21 (legge 27 luglio 2004, n. 188, di conversione del decreto-legge 24 giugno 2004, n. 158).

Collaborazioni con le p.a.

Al fine di agevolare l'adozione dei menzionati regolamenti, il Garante ha mantenuto e ampliato le forme di collaborazione con le pubbliche amministrazioni già avviate negli anni passati, finalizzate all'elaborazione dei menzionati schemi-tipo, prestando particolare attenzione ai contenuti delle schede che identificano la tipologia di dati sensibili trattati e le operazioni eseguibili in relazione alle finalità perseguite.

Nel corso dell'anno l'Autorità è stata interpellata sul punto anche da altri soggetti pubblici tra i quali, in particolare, si segnalano la Crui (Conferenza dei rettori delle università italiane), nonché l'Istituto nazionale di fisica nucleare.

Direttiva della Funzione pubblica

L'Autorità ha inoltre collaborato su richiesta alla predisposizione di una direttiva del Dipartimento della funzione pubblica, finalizzata a richiamare l'attenzione delle amministrazioni sulle prescrizioni del Codice che incidono maggiormente nel settore pubblico e che richiedono l'adozione di efficaci scelte organizzative per tradurre sul piano sostanziale le garanzie previste dal legislatore, nonché sulle conseguenze connesse alla loro mancata attuazione.

In chiave di semplificazione, con la direttiva in fase di definitiva formalizzazione, le amministrazioni sono state esortate ad avviare ogni iniziativa utile ad identificare settori di attività, comuni a più enti, per i quali si possa procedere ad un'elaborazione congiunta di schemi tipo da sottoporre all'attenzione del Garante, avvalendosi della collaborazione del Dipartimento della Funzione pubblica medesimo, che intraprenderà a tale scopo le necessarie attività di coordinamento.

In vista della scadenza del 31 dicembre 2005, l'Autorità si riserva di fornire ulte-

riori chiarimenti ed indicazioni di carattere generale in aggiunta a quelle, già dettagliate, del 17 gennaio 2002 (in *Bollettino* n. 24 del 2002, p. 40-45).

Enti locali

Anche la collaborazione avviata dall'Autorità con gli organismi rappresentativi delle autonomie locali (Anci, Upi e Uncem) ha ricevuto un ulteriore impulso nel corso del 2004. La fase della consultazione è altresì proseguita con le regioni, riunite nell'ambito della Segreteria della conferenza dei presidenti delle regioni e delle province autonome di Trento e Bolzano, sotto il coordinamento del Cisis (Centro interregionale per il sistema informatico e il sistema statistico).

Anci

Nel quadro della collaborazione instauratasi, è stata redatta una prima bozza di regolamento per i comuni e le comunità montane contenente la denominazione dei trattamenti effettuati, la fonte normativa, le rilevanti finalità di interesse pubblico perseguite, i tipi di dati trattati e di operazioni eseguibili, nonché la sintetica, ma esauriente, descrizione dei trattamenti e dei flussi informativi.

Lo schema di regolamento per il trattamento dei dati sensibili e giudiziari è stato messo a disposizione delle amministrazioni comunali e delle comunità montane, dal 25 maggio al 15 giugno 2004, sul sito dell'Ancitel (*http://www.ancitel.it/RegolamentoDatiSensibili/*), al fine di stimolare proposte di modifica, suggerimenti, integrazioni ed osservazioni e perfezionare ulteriormente il documento che, una volta approvato dall'Autorità, costituirà lo schema-tipo in conformità al quale gli enti citati potranno adottare –senza dover più richiedere il parere formale del Garante ai sensi dell'art. 20, comma 2, del Codice– i propri atti regolamentari, salvo che debbano procedere a specifici trattamenti non considerati nel contesto generale.

UPI

Analoghe forme di collaborazione sono intercorse con l'Unione delle Province d'Italia (UPI) per la stesura di corrispondenti schemi di regolamento utili per le amministrazioni provinciali: anche in questo caso, è imminente la pubblicazione del modello predisposto sul sito *web* dell'organo rappresentativo, per raccogliere pure in questo ambito, eventuali proposte di integrazione e suggerimenti prima che il Garante esprima il parere di competenza e lo ponga formalmente a disposizione delle province.

Regioni

Con riferimento, invece, alla collaborazione con le regioni, è stato istituito un gruppo di lavoro interregionale, con la partecipazione del Garante, del Ministero della salute, degli assessorati alla sanità e delle aziende sanitarie locali, in considerazione della necessità di includere nello schema di regolamento anche i trattamenti di dati relativi alla salute. Ciò, alla luce della nuova disciplina dettata in argomento dal Codice, che non prevede più una specifica competenza del Ministero della salute a regolamentare tali trattamenti (a differenza dell'art. 23, comma 1-*bis*, della legge n. 675/1996) e demanda tale incombenza all'iniziativa delle diverse amministrazioni.

In considerazione della peculiarità dei trattamenti da parte delle Asl, si è ritenuto opportuno istituire un sottogruppo di esperti, costituito dai rappresentanti degli assessorati in materia, che si è soffermato sui trattamenti di dati sanitari di competenza delle regioni predisponendo lo schema-tipo per i trattamenti di competenza delle aziende sanitarie da inserire nello schema di regolamento regionale.

Pur essendo stata redatta una prima bozza di regolamento nel corso del 2004, la già menzionata proroga al 31 dicembre 2005 del termine per l'adozione degli atti regolamentari (inizialmente prevista per il 30 settembre 2004) ha offerto la possibi-

lità di svolgere ulteriori approfondimenti, potendosi così tenere conto anche delle ulteriori proposte modificative o integrative e delle osservazioni pervenute recentemente al gruppo tecnico e sottoposte successivamente all'attenzione del Garante.

2.3. *Trasparenza dell'attività amministrativa e accesso ai documenti*

Il difficile equilibrio tra la trasparenza dell'attività amministrativa e la tutela della riservatezza ha costituito oggetto di attenta riflessione da parte del Garante che, al pari degli anni passati, è stato interpellato in più circostanze in merito.

Permessi di accesso a zone a traffico limitato

È stata sottoposta al vaglio del Garante la prassi, seguita da alcuni enti locali, di acquisire copia del documento di identità dei soggetti che, a diverso titolo (ad es. residenti e domiciliati in determinate zone), chiedono il rilascio del permesso di accesso/sosta nelle zone urbane a traffico limitato. Tale trattamento dei dati personali è stato ritenuto legittimo –anche in conformità al nuovo Codice della strada (art. 7 del d.lg. 30 aprile 1992, n. 285) e alla normativa in materia di documentazione amministrativa (art. 45 del d.P.R. 28 dicembre 2000, n. 445)– poiché rientra tra le finalità istituzionali dei comuni (art. 18, commi 2 e 3, del Codice) e non contrasta i principi di pertinenza e non eccedenza, di cui all'art. 11, comma 1, lett. *d*), del Codice (*Nota* 28 ottobre 2004).

Albo dei beneficiari di provvidenze economiche

Ulteriori problemi ha sollevato la compatibilità dello specifico regime di pubblicità dell'albo dei beneficiari di provvidenze economiche, istituito ai sensi dell'art. 1 del d.P.R. 7 aprile 2000, n. 118, con le disposizioni in materia di tutela della riservatezza; l'Autorità ha ritenuto lecita la diffusione indifferenziata dei nominativi dei beneficiari unitamente all'indicazione della normativa che autorizza l'erogazione (art. 1, comma 2, del citato d.P.R. n. 118/2000) escludendo, invece, l'indicazione in quella stessa sede di ulteriori dati personali (quali, ad esempio, l'indirizzo, il codice fiscale o l'importo dell'erogazione) ritenuti non pertinenti ed eccedenti rispetto alle finalità perseguite.

In considerazione del divieto di diffondere i dati sulla salute (artt. 22, comma 8, e 68, comma 3, del Codice), è stato precisato che eventuali elenchi di soggetti beneficiari di assegni di cura o di prestazioni sanitarie non devono contenere i nominativi o le iniziali degli interessati, né il puntuale riferimento a disposizioni di legge (come nel caso della legge 5 febbraio 1992, n. 104 in materia di assistenza, integrazione sociale e diritti delle persone handicappate) da cui possano desumersi le cause dell'erogazione: possono essere invece utilizzate, a fini di trasparenza, diciture generiche o codici numerici (*Nota* 2 novembre 2004).

Accesso ai documenti amministrativi

Aspetto importante della tematica relativa alla trasparenza è la conciliabilità del diritto di accesso con il diritto alla riservatezza: permangono in merito numerose le richieste di chiarimenti.

Ostensibilità delle retribuzioni

A tal proposito, tra le questioni maggiormente significative si segnala una richiesta di chiarimenti sull'ostensibilità di documenti amministrativi concernenti l'attività lavorativa dell'*ex* coniuge detenuti dal Servizio ispezione del lavoro (*Nota* 26 aprile 2004). Sul punto il Garante è stato consultato anche da una pubblica amministrazione con riferimento alla richiesta di accesso, presentata da parte dell'*ex* coniuge di un proprio dipendente, volta ad ottenere copia della documentazione contabile relativa alla situazione retributiva del dipendente medesimo al fine di

avviare un'azione giudiziaria per la rideterminazione di un assegno di mantenimento (*Nota* 20 luglio 2004).

In entrambe le occasioni l'Autorità ha evidenziato che la normativa in materia di protezione dei dati personali non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60 del Codice), le quali attribuiscono al cittadino che vi abbia interesse per la tutela di situazioni giuridicamente rilevanti il diritto di accedere ai documenti detenuti dalle amministrazioni pubbliche (artt. 22 e ss. legge 7 agosto 1990, n. 241). È stato quindi sottolineato che spetta all'amministrazione destinataria della richiesta di accesso verificare, caso per caso, l'interesse e i motivi sottesi alla relativa istanza, nonché valutare la sussistenza di una delle ragioni per le quali il documento può essere sottratto alla conoscibilità del richiedente, essendo la stessa in possesso di tutti i necessari elementi di ponderazione della istanza di accesso.

Con riferimento ad una richiesta di accesso ad un rapporto informativo concernente un dirigente scolastico, redatto in seguito ad un accertamento ispettivo, il Garante ha ricordato che il rispetto della normativa in materia di accesso ai documenti amministrativi è requisito di liceità del trattamento. Pertanto, l'Autorità ha ribadito che, qualora il documento sia stato illecitamente reso accessibile, come nel caso specifico, i dati ivi contenuti sono inutilizzabili stante la violazione di una disciplina rilevante in materia di protezione dei dati personali (art. 11, comma 2, del Codice) (*Nota* 16 luglio 2004).

Elenchi delle società concessionarie

L'Autorità è stata chiamata a precisare ulteriormente il rapporto tra il diritto di accesso e quello alla protezione dei dati personali con specifico riferimento alla possibilità per i comuni di accedere ad elenchi dettagliati detenuti dalle società concessionarie dell'erogazione di pubblici servizi contenenti i dati degli intestatari dei contratti di fornitura. In particolare il Garante ha chiarito che ai fini della comunicazione si può prescindere dal consenso dell'interessato nel caso in cui sussistano esigenze di istituzione o completamento del catasto degli impianti termici, alla luce dell'art. 17 del d.P.R. n. 551/1999, il quale ha espressamente previsto che le società distributrici di combustibile comunichino agli enti locali che ne facciano richiesta la titolarità degli impianti da esse riforniti nel corso degli ultimi dodici mesi (*Nota* 1° marzo 2004).

Consiglieri comunali e provinciali

È allo studio dell'Autorità la predisposizione di un documento sulla delicata questione del diritto di accesso dei consiglieri comunali e provinciali, già oggetto di talune pronunce in casi specifici nel corso dell'anno. Con riferimento alla possibilità di consentire ad alcuni consiglieri comunali l'acquisizione di informazioni sui cespiti relativi ad un piano di dismissione del patrimonio immobiliare di un comune, ivi inclusi i nominativi degli utenti assegnatari delle singole unità immobiliari, ed ulteriori dati di carattere sensibile, il Garante ha evidenziato che 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, comprese aziende ed enti collegati, informazioni utili all'espletamento del loro mandato, nel rispetto del segreto d'ufficio e del principio di pertinenza e non eccedenza, ai sensi dell'art. 43, comma 2, d.lg. 18 agosto 2000, n. 267 (*Nota* 13 settembre 2004).

Nell'ipotesi in cui l'accesso da parte dei consiglieri comunali riguardi dati sensibili, l'esercizio di tale diritto, ai sensi dell'art. 65, comma 4, lett. *b)*, del Codice, è consentito se indispensabile per lo svolgimento della funzione di controllo, di indirizzo politico, di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo.

Resta ferma la necessità, come già accennato nel par. 1.4., che i dati così acquisiti siano utilizzati per le sole finalità connesse all'esercizio del mandato, rispettando in particolare il divieto di divulgazione dei dati idonei a rivelare lo stato di salute. Spetta quindi all'amministrazione destinataria della richiesta accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* del consigliere comunale.

Il medesimo orientamento è stato espresso con riferimento alla possibilità di consentire a un consigliere comunale l'acquisizione di informazioni relative ad una comunità di nomadi Rom coinvolti in un progetto di assistenza ed integrazione sociale intrapreso in loro favore da un comune (*Nota* 10 novembre 2004).

Sindaco

Il Garante ha poi precisato, come in passato, che il diritto di accesso si configura in termini diversi con riferimento ad altri esponenti istituzionali del comune: tale è il caso del diniego opposto ad un sindaco di acquisire copia di tutti i ricorsi proposti dai trasgressori del Codice della strada, corredati dalle deduzioni tecniche redatte dal locale Comando di polizia municipale. Il d.lg. n. 267/2000 dispone, a differenza di quanto previsto per i consiglieri, che il sindaco e i singoli assessori per gli specifici settori ad essi delegati, debbano unicamente sovrintendere al funzionamento degli uffici e dei servizi, non con atti di diretta gestione, ma con direttive generali.

L'ordinamento degli enti locali, infatti, prevede il principio della distinzione tra le funzioni di indirizzo e controllo politico-amministrativo, che spettano agli organi di governo dell'ente, e l'attuazione e gestione amministrativa, che competono ai dirigenti.

Pertanto, nel solo caso in cui la richiesta di informazioni, anche di natura sensibile, sia indispensabile al sindaco per espletare la funzione di controllo politico-amministrativo sull'andamento dell'ufficio del personale, l'acquisizione dei dati può risultare conforme alle norme rilevanti in tema di protezione dei dati. Di contro, in assenza delle ricordate finalità di rilevante interesse pubblico, la comunicazione di questi dati, specie se non generalizzata, non è legittima e l'accesso da parte del sindaco non è consentito (*Nota* 22 ottobre 2004).

Difensore civico

Un ulteriore caso particolare è stato portato all'attenzione del Garante da un'associazione, in merito alla richiesta da parte di un difensore civico di conoscere eventuali provvedimenti adottati nei confronti di un educatore (a seguito del rinvio a giudizio di quest'ultimo per maltrattamenti a danno di soggetti disabili affidatigli). Sulla base degli elementi disponibili riguardo ai poteri informativi dello specifico difensore civico richiedente, l'Autorità non ha ravvisato una specifica funzione idonea a consentire l'acquisizione delle informazioni richieste all'associazione, in mancanza del consenso dell'interessato, necessario ai sensi dell'art. 24 del Codice (*Nota* 3 maggio 2004).

Tesserino di riconoscimento

Rispettoso del principio di pertinenza è stato giudicato anche il trattamento dei dati personali riportati nel tesserino di riconoscimento delle guardie ecologiche volontarie di una provincia: al riguardo, la normativa di settore (in particolare il regolamento della provincia in questione) indica espressamente gli elementi identificativi destinati ad essere riportati nel documento (le generalità, la fotografia, i connotati e gli estremi del decreto di guardia particolare giurata), disciplinandone, inoltre, l'uso in caso di esibizione per lo svolgimento dei particolari compiti attribuiti (*Nota* 9 settembre 2004).

2.4. *Il principio del cd. pari rango*

Profili particolari riguardano l'accesso ai documenti amministrativi contenenti dati idonei a rivelare lo stato di salute o la vita sessuale. Infatti, in tal caso il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (art. 60 del Codice).

In proposito, il Garante ha già chiarito che il destinatario della richiesta, al fine di stabilire se il diritto dedotto dal richiedente vada considerato "di pari rango" rispetto a quello della persona cui si riferiscono i dati, deve fare riferimento non al "diritto di azione e difesa" –che pure è costituzionalmente garantito– quanto alla situazione giuridica soggettiva sottostante che il terzo intende far valere (v. già *Provv.* 9 luglio 2003, in *Relazione 2003*, p. 64).

I predetti principi, affermati anche dalla giurisprudenza del Consiglio di Stato, sono stati posti all'attenzione dell'Autorità in varie circostanze. È in avanzato stadio di trattazione la richiesta di chiarimenti di un'amministrazione alla quale un Comando provinciale della Guardia di finanza aveva chiesto copia degli atti relativi al procedimento a carico di un finanziere per l'applicazione della sanzione amministrativa prevista per la fattispecie colposa del reato di atti osceni (art. 527, comma 2, c.p.). La documentazione oggetto della richiesta potrebbe contenere dati sensibili riconducibili, ad esempio, ad informazioni idonee a rivelare la vita sessuale dell'interessato. L'Autorità si è, invece, pronunciata in merito alla richiesta di chiarimenti avanzata da un comune circa la possibilità da parte delle strutture sanitarie di rilasciare ad un consigliere comunale, ai sensi dell'art. 43 del d.lg. n. 267/2000, copia di un referto medico riguardante un terzo (*Nota* 30 settembre 2004).

Ciò comporta, in sintesi, che nella prevalenza dei casi riguardanti solo diritti di credito non sia possibile accogliere l'istanza di accesso e di comunicazione, e che si possa invece valutare, sia pure con cautela e caso per caso, l'effettiva necessità di consentire l'accesso ad una cartella clinica –prima della sua probabile acquisizione su iniziativa del giudice– in caso di controversia risarcitoria per danni ascritti all'attività professionale medica documentata nella cartella stessa.

Dati sanitari

La questione dei limiti alla comunicazione di dati sulla salute e sulla vita sessuale a persone diverse dall'interessato ha assunto spesso rilevanza nel caso di richieste di accesso a cartelle cliniche detenute presso strutture sanitarie, a volte formulate da un difensore nell'ambito delle cd. indagini difensive (art. 391-*quater* c.p.p.).

Anche in tal caso l'Autorità ha ribadito che le pubbliche amministrazioni non necessitano di una specifica autorizzazione del Garante ai fini dell'accoglimento di richieste di accesso ai documenti o di comunicazione di dati personali formulate ai sensi della disciplina delle indagini difensive introdotta dalla legge 7 dicembre 2000, n. 397. Dal momento che il Codice, come già ricordato, non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (art. 59 del Codice), le disposizioni contenute nell'art. 391-*quater* del c.p.p. vanno ritenute un'idonea fonte normativa per la comunicazione all'esterno di dati personali che va comunque inquadrata sistematicamente (v., ad esempio, art. 71 del Codice). Spetta pertanto all'amministrazione destinataria della richiesta, che dispone di tutti gli elementi a ciò necessari, accertare, caso per caso, la sussistenza dei presupposti per l'esercizio di tale facoltà, compresa la legittimazione del soggetto che ha formulato l'istanza di accesso (*Nota* 15 ottobre 2004).

2.5. *Pubblici registri, elenchi, atti e documenti conoscibili da chiunque*

Nel corso dell'anno il Garante si è pronunciato su alcune questioni relative al trattamento dei dati contenuti in pubblici registri, elenchi, atti e documenti conoscibili da chiunque.

Registro quote-latte

In particolare, l'Autorità è stata chiamata a chiarire il regime di pubblicità del registro delle quote-latte tenuto dall'Agenzia per le erogazioni in agricoltura (AGEA) all'interno del Sistema informativo agricolo nazionale (SIAN). Al riguardo, è stata evidenziata la base normativa che consente l'integrale consultabilità (anche in via telematica attraverso il sito Internet del SIAN) del predetto registro da chiunque ne abbia interesse, lasciando invece all'Agenzia la valutazione circa la possibilità di estendere la piena conoscibilità anche alle informazioni relative al periodo antecedente all'istituzione del registro (*Nota* 27 settembre 2004).

ACI

Un'altra questione all'esame dell'Autorità riguarda la possibilità di divulgare tramite il sito *web* dell'ACI l'elenco dei demolitori autorizzati all'esercizio delle operazioni di "rottamazione" dei veicoli fuori uso: in proposito, il Garante ha ribadito le indicazioni già fornite in un'altra occasione (*Nota* 16 giugno 1999), facendo presente che la diffusione del predetto elenco è lecita solo se prevista da apposita disposizione di rango normativo primario o secondario, non essendo sufficiente in tal senso la sola previsione contenuta in un regolamento interno dell'ACI (*Nota* 29 dicembre 2004).

Ipoteche

In sede di ricorso è stata ritenuta infondata, allo stato della normativa all'epoca applicabile, la richiesta di cancellazione dei dati relativi ad un'ipoteca avanzata nei confronti di una società che fornisce informazioni commerciali. Tali dati, relativi alla proprietà immobiliare e detenuti dai competenti uffici dell'Agenzia del territorio competenti erano, infatti, pubblici e quindi accessibili a chiunque ed utilizzabili anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*). Pertanto, la loro estrazione e comunicazione a terzi da parte di società che operano nel settore dell'informazione societaria e commerciale erano, allo stato, lecite (*Provv.* 20 maggio 2004).

Sul punto, tuttavia, è intervenuto da ultimo il legislatore che, con la legge finanziaria 2005, al fine di contrastare fenomeni di elusione fiscale e di tutelare la fede pubblica, ha introdotto una disposizione che, di regola, vieta 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., legge 30 dicembre 2004, n. 311). L'eventuale possibilità di riutilizzare per fini commerciali tali informazioni verrebbe subordinata alla stipula di specifiche convenzioni con la stessa Agenzia, le quali dovrebbero disciplinare, a fronte del preventivo pagamento dei tributi dovuti, le modalità ed i termini della raccolta, della conservazione, dell'elaborazione dei dati, nonché il controllo del limite di riutilizzo consentito.

Va però rilevato che l'applicazione di tali disposizioni dovrà essere coordinata con le scelte normative già fatte da Governo e Parlamento nel Codice, anche in attuazione di raccomandazioni del Consiglio d'Europa, tenendo conto, in particolare, del principio di compatibilità con gli scopi per i quali i dati sono stati raccolti, e affidando al Garante la promozione di codici deontologici che dovranno regolare la materia (artt. 61 e 118 del Codice).

2.6. *Documentazione anagrafica e materia elettorale*

A seguito delle modifiche introdotte dal Codice nella materia anagrafica, dello stato civile e delle liste elettorali, sono pervenuti numerosi quesiti volti ad ottenere chiarimenti; più precisamente, il Codice ha integrato la disciplina sull'utilizzo degli elenchi anagrafici da parte delle pubbliche amministrazioni, prevedendo espressamente che rientrano tra gli scopi di pubblica utilità anche quelli relativi all'applicazione della disciplina in materia di comunicazione istituzionale e che può farne uso per tale finalità anche il comune presso il quale è istituita l'anagrafe.

Al riguardo, l'Autorità si è pronunciata su un ricorso relativo all'invio a cittadini minorenni, da parte di un comune, di un invito a partecipare alla sagra patronale ed alla festa di *Halloween* organizzate dall'ente. Il Garante non ha riscontrato, sulla base degli elementi forniti dalle parti, specifiche violazioni in quanto i dati trattati non erano conservati presso il comune e le comunicazioni erano state inviate direttamente dall'ente con la sola intenzione di fare conoscere ai bambini il contenuto delle iniziative ricreative organizzate (*Provv.* 30 gennaio 2004). Sono stati avviati però specifici accertamenti al fine di verificare la liceità del trattamento e la correttezza del comportamento del comune, soprattutto con riferimento all'acquisizione dei dati dei minori.

Scambio di dati Italia-Germania

Significativa è stata anche la collaborazione richiesta al Garante dal Ministero dell'interno per la definizione di una bozza di accordo tra la Repubblica federale tedesca e la Repubblica italiana sullo scambio reciproco di dati tra gli uffici anagrafici nell'ambito dei trasferimenti di domicilio degli abitanti (vale a dire delle persone fisiche sulle quali ricadono obblighi anagrafici ai sensi della normativa statale interna, indipendentemente dalla loro cittadinanza), da e verso i rispettivi territori nazionali.

In proposito il Garante ha evidenziato, con riferimento all'istituzione presso ciascuno Stato contraente di un "ufficio centrale" nazionale competente a gestire il flusso di dati tra i due Paesi, che la disciplina sulle modalità di utilizzazione anche esterna delle banche dati ed il connesso obbligo per gli uffici anagrafici di comunicare dati a tale ufficio centrale, devono essere previsti da norme di legge o di regolamento, in conformità all'art. 19 del Codice. Inoltre, l'Autorità ha rilevato il rischio di vanificare la disciplina anagrafica tramite la previsione contenuta nella bozza di accordo in questione, in quanto i flussi di comunicazioni anagrafiche che si intendono attivare modificano profondamente la specifica normativa di settore (cfr. d.P.R. 30 maggio 1989, n. 223; legge 15 maggio 1997, n. 127). Il Garante ha osservato che simili modifiche potrebbero essere introdotte solo sulla base di una previa disposizione legislativa che le preveda e ne determini i caratteri fondamentali, nel rispetto di necessarie cautele quali, in particolare, la non eccedenza delle informazioni trasmesse rispetto alle finalità perseguite (*Nota* 14 settembre 2004). Alla luce di tali considerazioni, su richiesta del Ministero dell'interno, si è aperto un tavolo di lavoro presso l'Autorità al fine di esaminare congiuntamente i profili più delicati dell'iniziativa ed individuare idonee soluzioni anche nell'ambito della disciplina vigente ed avvalendosi dell'Indice nazionale delle anagrafi (Ina).

Ina-Saia

La collaborazione proficuamente avviata con il Ministero dell'Interno ha trovato conferma anche in altri ambiti: il Garante, infatti, è stato chiamato a prendere parte, assieme ad altre istituzioni, al Comitato tecnico per la predisposizione di uno studio finalizzato alla revisione della normativa anagrafica, alla luce delle innovazioni riguardanti l'Ina ed il Sistema di accesso ed interscambio anagrafico (Saia).

Biografie

Una questione particolarmente delicata in materia è all'esame dell'Autorità, con riferimento alla possibilità di rilasciare ad un istituto enciclopedico privato informazioni sullo *status* di figlio adottivo di un noto imprenditore, al fine di completarne la biografia da inserire nel dizionario degli imprenditori italiani. La normativa fa espresso divieto dell'indicazione della paternità e della maternità nelle attestazioni di stato civile riferite all'adottato (cfr. artt. 26, comma 4, 28, comma 2, e 73, comma 1, della legge 4 maggio 1983, n. 184, in materia di adozioni), negli estratti per riassunto degli atti dello stato civile, nonché nei certificati relativi agli atti di nascita, di matrimonio, di cittadinanza, negli atti attestanti lo stato di famiglia e nelle pubblicazioni di matrimonio esposte al pubblico (art. 1 della legge 31 ottobre 1955, n. 1064, richiamata dall'art. 108, comma 3 del d.P.R. 3 novembre 2000, n. 396). Peraltro, la disciplina in materia di protezione dei dati personali se, da un lato, autorizza, in linea generale, il rilascio degli estratti degli atti dello stato civile una volta decorsi settanta anni dalla loro formazione (cfr. art. 177, comma 3, del Codice), dall'altro fa salve le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di "taluni" dati personali (art. 184, comma 3). Occorre quindi valutare il rilievo dei predetti divieti stabiliti dalla legge sull'adozione.

Ricerche genealogiche

L'Autorità è stata anche interpellata sulla fondatezza della richiesta formulata da uno studio di ricerche genealogiche, volta ad ottenere l'autorizzazione ad effettuare ricerche presso i servizi dello stato civile di alcuni comuni al fine di definire le devoluzioni successorie. Sul punto, il Garante ha ricordato che –a partire dal 1° gennaio 2004, secondo quanto disposto dall'art. 177, comma 3, del Codice– il rilascio degli estratti degli atti dello stato civile è consentito unicamente ai soggetti cui l'atto si riferisce, oppure su motivata istanza comprovante l'interesse personale e concreto del richiedente ai fini di tutela di una situazione giuridicamente rilevante, ovvero decorsi settanta anni dalla formazione dell'atto. Resta ferma la possibilità che l'ufficiale dello stato civile fornisca a richiesta singole notizie che possono essere comunicate ai sensi dell'art. 450 c.c. (*Nota* 12 maggio 2004).

Liste elettorali

Con riferimento, invece, al trattamento dei dati contenuti nelle liste elettorali, il Garante è stato impegnato a fornire chiarimenti alla luce della rilevante modifica introdotta dal Codice che, rispetto al previo regime di piena conoscibilità e pubblicità delle liste elettorali degli enti locali, ora prevede, in applicazione del principio di finalità, che le liste elettorali possano essere rilasciate in copia solo in favore di chi intende perseguire una finalità di attuazione della disciplina in materia di elettorato attivo o passivo, di studio, ricerca scientifica o storica o socio-assistenziale, oppure per perseguire un interesse collettivo o diffuso (art. 177, comma 5, del Codice).

L'Autorità è stata chiamata a pronunciarsi, tra l'altro, in merito al possibile rilascio, da parte delle amministrazioni comunali, di copia delle liste elettorali ai patronati per lo svolgimento delle loro funzioni istituzionali. Il Garante ha chiarito che spetta all'amministrazione destinataria dell'istanza entrare nel merito della richiesta e valutare se la specifica finalità del loro successivo utilizzo dichiarata da parte del richiedente sia conforme all'attività svolta dal soggetto medesimo, nonché se rientri effettivamente tra le ipotesi di cui al citato art. 177. In tale occasione è stato ricordato che il Codice consente agli istituti di patronato e di assistenza sociale, per lo svolgimento delle proprie attività, e solo nell'ambito di un mandato conferito dall'interessato, di accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso dell'interessato (art. 116 del Codice) (*Nota* 28 luglio 2004).

Sportello per il permesso di soggiorno

In materia di immigrazione, è stato adottato un regolamento per la razionalizzazione e l'interconnessione delle comunicazioni fra amministrazioni pubbliche ai fini, in particolare, del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (d.P.R. 27 luglio 2004, n. 242, di attuazione della legge 30 luglio 2002, n. 189), sul quale l'Autorità ha espresso parere il 4 marzo 2004.

Il Dipartimento per le libertà civili e l'immigrazione presso il Ministero dell'interno istituisce e detiene gli archivi automatizzati in materia di immigrazione e di asilo, ai quali accedono le pubbliche amministrazioni interessate, individuate con decreto del Ministro medesimo. Tali archivi sono interconnessi con i sistemi informativi delle pubbliche amministrazioni interessate e con quelli delle regioni, delle province autonome e degli enti locali.

Su richiesta dell'Autorità, i "controlli" sugli accessi al sistema informativo sono stati disciplinati in conformità al principio di proporzionalità, prevedendo che i dati personali concernenti l'identificazione degli utenti e le operazioni di accesso agli archivi possano essere utilizzati solo per finalità di sicurezza e di accertamento di eventuali illeciti.

2.7. *Istruzione*

Esiti scolastici

Anche in materia di pubblicità degli esiti scolastici l'Autorità ha dovuto recentemente ricordare che non è vietata la pubblicazione dei risultati degli scrutini; al contrario, essi devono essere pubblicati, come esplicitamente previsto dalla disciplina in materia (ordinanze ministeriali 13 febbraio 2001, n. 29; 4 aprile 2003, n. 35; 9 febbraio 2004, n. 21).

Voti e interrogazioni

Numerose sono state le richieste di chiarimenti in merito al trattamento dei dati personali nel settore dell'istruzione, con particolare riferimento alla conoscibilità di informazioni riguardanti gli studenti. L'Autorità ha dovuto ancora una volta precisare che non esiste alcuna disposizione del Codice o provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe o delle interrogazioni, né di consegnarli agli alunni in busta chiusa. Così come non esiste alcuna disposizione che proibisca ai medesimi di rendere nota la fede religiosa o che ostacoli le soluzioni da tempo in atto per la partecipazione o meno degli studenti all'ora di religione (*Comunicato stampa* 3 dicembre 2004).

Comunicazioni *ex* art. 39

Sono giunte al Garante numerose comunicazioni ai sensi dell'art. 39, comma 1, lett. *a*), del Codice da parte di istituti scolastici che intendevano comunicare dati personali degli alunni ad altri soggetti pubblici per lo svolgimento di finalità istituzionali, in particolare di natura socio-assistenziale.

In tali occasioni nel ricordare che il trattamento dei dati personali deve essere ispirato ai principi di pertinenza, proporzionalità e necessità, il Garante ha fissato alcuni limiti a tale flusso di dati personali degli alunni, di seguito sintetizzati:

- in merito alla richiesta di una Asl di ricevere dalle strutture scolastiche presenti nella provincia alcuni dati personali dei minori ivi iscritti al fine di realizzare un archivio informatizzato per contattare gli studenti in caso di denuncia di malattie infettive, l'Autorità ha precisato che, pur essendo attribuito a tali enti il compito di provvedere, tra l'altro, all'igiene e alla medicina scolastica negli istituti di istruzione pubblica e privata di ogni ordine e grado (cfr. art. 14, comma 3, lett. *e*), l. n. 833/1978), lo stesso può essere assolto con modalità meno invasive. Ad esempio, sarebbe pos-

sibile individuare un responsabile interno ad ogni istituto scolastico in grado di fornire, qualora si verifichi un evento infettivo, i dati strettamente necessari per assicurare l'opportuno intervento sanitario, senza creare una banca dati informatizzata relativa alla realtà scolastica minorile di un'intera provincia (*Nota* 28 dicembre 2004);

- analogamente, una Asl ha richiesto l'elenco dei nomi e degli indirizzi degli alunni iscritti nelle scuole presenti nel distretto sanitario dell'azienda, al fine di contattare gli stessi all'interno di una campagna contro il morbillo. Il Garante ha osservato che la finalità di promuovere la prevenzione delle malattie infettive attribuita alle Asl può essere utilmente raggiunta anche senza procedere all'invio sistematico alle stesse degli elenchi di tutti gli alunni iscritti agli istituti, mettendo a disposizione delle famiglie il materiale informativo distribuito dal Ministero della salute e dalle Asl presso gli istituti scolastici (*Nota* 17 novembre 2004);
- alcuni istituti scolastici presenti all'interno di uno stesso comune hanno comunicato di voler avviare un progetto di gestione integrato dell'anagrafe scolastica, contenente i dati personali degli alunni iscritti e delle loro famiglie. Da un esame dei dati personali richiesti è risultato che sarebbero state raccolte anche informazioni di carattere sensibile relative ad alunni (es. stato di handicap). In merito a tale progetto, ai sensi degli artt. 20 e ss. del Codice, il Garante sta valutando se –in mancanza di un'espressa previsione di legge o di regolamento che preveda l'interconnessione di banche dati per la gestione integrata dell'anagrafica scolastica comunale e tenendo conto dei principi di indispensabilità, pertinenza e proporzionalità– la finalità di migliorare il percorso formativo degli alunni possa essere raggiunta con altre modalità che non comportino la creazione di archivi contenenti dati sensibili relativi a minori, condivisi da più soggetti pubblici;
- un assessorato regionale alla sanità ha richiesto ad un'università pubblica alcuni dati personali degli iscritti alle facoltà di medicina e di scienze, per inviare agli studenti una lettera di sensibilizzazione in merito alla donazione di sangue e midollo osseo, nonché informazioni sull'autoemoteca dei volontari dell'AVIS. Al riguardo è stato osservato che, pur sussistendo in capo alle regioni ed ad altre amministrazioni pubbliche la funzione di promuovere la donazione del sangue e degli emoderivati (cfr. art. 11, comma 3, legge 4 maggio 1990, n. 107 e Dir. P.C.M. 6 giugno 2003), tale finalità può essere raggiunta con altre modalità, quali, ad esempio, la distribuzione di specifico materiale informativo presso le facoltà universitarie (*Nota* 29 dicembre 2004).

Atti e circolari del dirigente scolastico

L'Autorità ha ricordato che anche nella redazione di atti e circolari interne contenenti dati personali è necessario rispettare i principi di pertinenza e non eccedenza. In seguito ad una segnalazione di un'insegnante il Garante ha ravvisato la non conformità a tali principi del comportamento di un dirigente scolastico che, nell'informare il personale e gli studenti di alcune difficoltà organizzative causate dalla pendenza di procedimenti amministrativi e giudiziari contro l'istituto, aveva specificato anche i nominativi delle insegnanti che li avevano avviati (*Nota* 25 novembre 2004).

Controllo delle presenze

Sono in corso alcuni approfondimenti in merito al progetto di un istituto tecnico industriale volto al controllo elettronico della presenza degli studenti nell'edi-

ficio scolastico, rendendo possibile la verifica della presenza degli alunni da parte dei genitori degli stessi tramite il sito *web* della scuola.

Il Garante è in procinto di definire l'istruttoria in ordine ad un caso di monitoraggio della presenza di allievi stranieri nel territorio provinciale effettuato da un istituto scolastico. Tale attività, che prevede la raccolta di dati sugli alunni tramite questionari distribuiti agli istituti d'istruzione, può comportare il trattamento di dati sensibili dei medesimi (in particolare, di informazioni relative all'origine razziale o etnica), nonché di altre delicate informazioni di carattere personale, come quelle concernenti adozioni o affidamenti.

Comunicazione di dati a privati

A seguito di un ricorso (*Provv.* 29 dicembre 2003), il Garante ha avviato ulteriori accertamenti in merito all'avvenuta comunicazione ad una casa editrice, da parte di un'università statale, di alcuni dati personali dei propri studenti. Al riguardo, è stato rilevato che un determinato decreto rettorale non poteva ritenersi fonte idonea a consentire tale operazione, non individuando in modo puntuale i casi di comunicazione di dati personali degli studenti da parte dell'ateneo a soggetti privati. L'ateneo è stato invitato a sospendere di propria iniziativa il trattamento in questione, nonché ad individuare con esattezza nell'atto regolamentare le singole ipotesi di comunicazione di dati personali degli studenti a soggetti privati, in conformità ai principi di necessità, pertinenza e non eccedenza dei dati rispetto alle finalità perseguite.

L'Autorità in tale occasione ha anche accertato che la stessa università aveva fornito un'informativa incompleta agli studenti, senza individuare le finalità, le modalità del trattamento, nonché l'ambito di comunicazione dei dati personali degli studenti a soggetti privati. Il Garante ha, quindi, contestato all'università la sanzione amministrativa di cui all'art. 161 del Codice (contestazione del 19 novembre 2004, cui è seguito il pagamento in misura ridotta).

2.8. *Notificazioni di atti e comunicazioni*

Notificazioni

Già in passato l'Autorità ha più volte rappresentato alle pubbliche amministrazioni l'esigenza di tutelare in maniera adeguata la riservatezza delle persone alle quali sono notificati atti giudiziari, verbali di contravvenzione, avvisi fiscali o altri atti amministrativi (*Provv.* 22 ottobre 1998 e 26 ottobre 1999).

Molte esortazioni espresse dal Garante sono state tradotte in disposizioni normative dal nuovo Codice, il quale ha modificato le norme processuali interessate (art. 174) seguendo il principio secondo cui, qualora la notificazione non possa essere eseguita nelle mani del destinatario, la copia dell'atto deve essere consegnata in busta sigillata e su questa non devono essere apposte indicazioni da cui possa desumersi il contenuto dell'atto stesso. Tale principio si applica sia nel processo civile, sia in quello 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.

Consegna a mezzo del messo comunale

L'Ufficio del Garante ha inoltre risposto a quesiti relativi alla notifica di violazioni finanziarie o di sanzioni disciplinari, ribadendo che gli addetti al protocollo e il messo comunale tramite il quale viene effettuata la notifica vanno designati quali soggetti incaricati di svolgere le pertinenti operazioni del trattamento; essi possono pertanto accedere al contenuto del documento oggetto di notifica senza che ciò comporti la violazione delle disposizioni sulla comunicazione dei dati personali, essendo peraltro i medesimi incaricati tenuti al segreto d'ufficio in virtù del loro *sta-*

tus di dipendenti pubblici.

Utilizzo del fax

L'Autorità ha ricordato che l'utilizzo del fax come mezzo di comunicazione tra pubbliche amministrazioni è espressamente consentito dalla legge, ed ha fatto anche presente che i dipendenti incaricati dalle amministrazioni di inviare e ricevere comunicazioni tramite fax devono rivestire il ruolo di incaricati del trattamento e, in quanto tali, rispettare le misure di sicurezza e gli obblighi di riservatezza previsti dal Codice (*Nota* 29 dicembre 2004).

Comunicazione di dati sanitari

Il Garante ha precisato che, nel recapitare a mano documenti contenenti dati relativi allo stato di salute (anche qualora il destinatario sia un dipendente del medesimo ente), devono essere prescelte modalità rispettose della riservatezza degli interessati, eliminando ogni occasione di impropria conoscibilità dei dati anche da parte delle persone fisiche incaricate del trattamento, inclusi i messi notificatori (es., allegazione di dati sanitari in busta chiusa; inviti all'interessato a ritirare personalmente un documento presso l'ufficio competente; comunicazione o messa a disposizione telematica o informatica direttamente in favore del solo interessato) (*Provv.* 23 luglio 2004).

Vendite giudiziarie

L'Autorità ha evidenziato in più occasioni che il Codice ha apportato alcune modifiche anche alle disposizioni relative alla pubblicità degli avvisi di vendita giudiziaria. In particolare, con riferimento al processo esecutivo, il nuovo art. 490 c.p.c. prevede che debba essere omessa l'indicazione del debitore qualora l'annuncio sia inserito in quotidiani, oppure divulgato con le forme della pubblicità commerciale. Le informazioni relative al debitore possono essere però fornite dalla cancelleria del tribunale a chiunque vi abbia interesse, unitamente ad ogni altra ulteriore necessaria informazione.

2.9. *Attività fiscale, tributaria e doganale*

Dichiarazioni stragiudiziali

A seguito di numerosi quesiti, segnalazioni e ricorsi, l'Autorità ha giudicato illegittima la prassi delle società concessionarie del servizio per la riscossione dei tributi di chiedere informazioni personali a terzi per ottenerne una dichiarazione stragiudiziale che attesti l'esistenza di crediti del contribuente su cui rivalersi, in quanto nessuna previsione legislativa o regolamentare attribuiva alla stessa il potere di effettuare questo tipo di trattamento senza il consenso del contribuente medesimo (*Provv.* 12 gennaio 2004). Tale procedura, anche in contrasto con il principio di non eccedenza (art. 11 del Codice), poiché sproporzionata rispetto alla finalità di recupero del credito (che può essere comunque perseguita con altri strumenti), risultava, infatti, disciplinata solo da risoluzioni dell'Agenzia delle entrate e da mere circolari ministeriali.

Deve essere tuttavia segnalato che il quadro normativo è stato parzialmente modificato di recente con la legge 30 dicembre 2004, n. 312 (art.1, comma 425, della legge finanziaria 2005), che ha introdotto l'istituto della dichiarazione stragiudiziale. Il nuovo art. 75-*bis* del d.P.R. n. 602/1973 stabilisce, infatti, che il concessionario –anche prima di procedere al pignoramento presso terzi– possa chiedere ai debitori del soggetto che è iscritto a ruolo di indicare per iscritto le cose e le somme dovute al creditore. Poiché la norma prevede che l'indicazione possa avvenire anche solo in modo generico, dovrà essere nuovamente verificato il rapporto tra la novella e il predetto principio di pertinenza e non eccedenza.

Pubblicità elenco contribuenti

Per quanto riguarda il regime di pubblicità dell'elenco dei contribuenti, il Garante ha affermato più volte in passato che, in base al vigente quadro normativo, risultava legittima la pubblicazione presso gli uffici finanziari ed i comuni degli elenchi nominativi dei contribuenti che avevano presentato la dichiarazione dei redditi, unitamente all'indicazione del reddito imponibile. Merita al riguardo segnalare che, recentemente, l'Agenzia delle entrate –nel disporre la pubblicazione degli elenchi per gli anni 2001 e 2002– ha ritenuto, adducendo il rispetto dei principi di pertinenza e non eccedenza, di limitare tale pubblicità al dato relativo alla categoria reddituale prevalente (Provv. dell'Agenzia 29 settembre 2004).

Agenzia delle dogane

Sono stati avviati approfondimenti con l'Agenzia delle dogane in merito all'applicazione del Codice ai trattamenti effettuati da parte degli uffici centrali e territoriali antifrode che svolgono funzioni di prevenzione, accertamento e repressione delle violazioni della normativa tributaria ed extratributaria. In particolare, l'Autorità ha esaminato anche le collaborazioni avviate dall'Agenzia con gli operatori commerciali e le associazioni di categoria, quali ad esempio la Confindustria.

2.10. *Trattamenti svolti da regioni ed enti locali*

Comunicazioni *ex* art. 39

Numerosissimi sono stati i casi in cui le regioni e gli enti locali hanno sottoposto all'attenzione del Garante, ai sensi degli artt. 19, comma 2, e 39, comma 1, lett. *a*), del Codice, l'intenzione di trasmettere ad altri soggetti pubblici dati personali reputati necessari per lo svolgimento di funzioni istituzionali, anche in assenza di una norma di legge o di regolamento.

In seguito ad una richiesta di informazioni (*Nota* 15 giugno 2004), ad esempio, il Garante ha ritenuto legittimo il progetto di una regione volto a consentire ai singoli comandanti di polizia locale, in possesso di specifiche *password*, l'accesso all'archivio contenente i dati personali dei propri operatori di polizia locale partecipanti ai corsi di aggiornamento e qualificazione professionale organizzati dalla regione medesima, al fine di poter valutare la partecipazione ai predetti corsi per le esigenze di servizio delle rispettive amministrazioni.

Analogamente, non è stato interdetto alle province l'accesso in rete ai dati contenuti nell'anagrafe venatoria centrale della regione di appartenenza per consentire la vigilanza e la gestione delle opzioni sulle forme di caccia esercitate dagli interessati (*Nota* 30 agosto 2004).

Al contrario, l'Autorità ha precisato che il meccanismo previsto dall'art. 39 non è idoneo a consentire ad un comune di arricchire la propria banca dati sui soggetti che hanno manifestato la propria disponibilità all'affidamento temporaneo di minori con le informazioni relative ai nuclei familiari aspiranti all'adozione trattate dalla Asl. La reciproca comunicazione di dati tra il comune e la Asl avrebbe, infatti, coinvolto anche dati sensibili per i quali sono da osservare le più rigorose garanzie di cui agli artt. 20 e ss. del Codice (*Nota* 13 settembre 2004).

Analoghe problematiche ha sollevato la richiesta della Regione Lazio volta ad ottenere dall'Inps la comunicazione di alcuni dati personali, anche sensibili, per la concessione di benefici economici a favore degli anziani e degli invalidi civili. L'Autorità, interpellata sul punto, ha indicato alle amministrazioni coinvolte le modalità più idonee a garantire il rispetto della normativa in materia di protezione dei dati personali. L'INPS, pertanto, secondo i criteri stabiliti dalla regione, ha individuato direttamente i soggetti beneficiari delle provvidenze economiche. Successivamente, su indicazione della regione, ha consegnato a Poste Italiane S.p.A.,

designata responsabile del trattamento dall'Istituto, l'elenco dei nominativi ed il relativo domicilio dei beneficiari per l'erogazione delle provvidenze economiche.

È stato poi operato un doveroso distinguo tra le ipotesi in cui la comunicazione di dati sia indirizzata da un'amministrazione comunale ad un consorzio, a seconda della natura giuridica, pubblica o privata, di quest'ultimo. L'applicazione degli artt. 19, comma 2, e 39, comma 1, lett. *a*) del Codice è, infatti, ammissibile solo per la comunicazione di dati tra soggetti pubblici, non essendo invece possibile avvalersi della norma in questione ove il consorzio abbia, invece, natura privata. La comunicazione di dati da un soggetto pubblico ad un soggetto privato è ammessa, infatti, dall'art. 19, comma 3, unicamente quando è prevista da norme di legge o regolamento (*Nota* 22 novembre 2004).

Sulla base dei medesimi principi, è stata rappresentata ad un comune l'impossibilità di una trasmissione sistematica di dati relativi a deceduti alle parrocchie, non avendo queste ultime natura di soggetti pubblici (*Nota* 17 gennaio 2005).

Sistema interbibliotecario

Con riferimento allo scambio dei dati dei tesserati nell'ambito dei sistemi bibliotecari provinciali, è stato rilevato che la finalità di assicurare un adeguato servizio pubblico di lettura e di informazione tramite il servizio di prestito interbibliotecario potrebbe essere utilmente conseguita anche riducendo i flussi di dati personali. Ad esempio, nel rispetto dei principi di pertinenza e non eccedenza di cui all'art. 11 del Codice, potrebbero essere trasmesse alle biblioteche collegate le sole richieste dei volumi prive dei dati personali degli utenti, che sarebbero conservati solo presso la biblioteca richiedente (*Nota* 21 dicembre 2004).

Dati anagrafici

È stata ritenuta legittima la comunicazione di dati anagrafici da parte di un comune alla Asl al fine di addivenire, nell'ambito di un piano integrato per l'emergenza estiva, alla campionatura della popolazione anziana per monitorare e prevenire eventuali episodi di grave decadimento psico-fisico e di solitudine. La normativa sugli atti anagrafici prevede, infatti, la possibilità per l'ufficiale dell'anagrafe di rilasciare, anche periodicamente, elenchi degli iscritti nell'anagrafe della popolazione residente alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità, ai sensi dell'art. 34, comma 1, d.P.R. n. 223/1989 (*Nota* 19 luglio 2004).

Diffusione di dati sanitari

In materia di trattamento di dati sensibili da parte degli enti locali, è in istruttoria il caso nel quale un comune ha divulgato sul proprio sito Internet i nominativi di coloro che avevano richiesto la sostituzione nel pagamento della tariffa per la gestione dei rifiuti, affiancati dai motivi della richiesta. In base ad una deliberazione del locale consiglio comunale, la predetta sostituzione può avvenire per "*le utenze domestiche connesse a nuclei familiari ove sussiste la condizione di indigenza o sono presenti portatori di handicap*". La questione involge i diritti dei soggetti portatori di handicap che, sebbene non menzionati con le relative generalità, potrebbero essere indirettamente identificati.

Ausiliari del traffico

Un recente caso in fase di preliminare approfondimento attiene alla richiesta di collaborazione pervenuta da parte della Procura della Repubblica di Roma in relazione ad accertamenti avviati per controllare la liceità dei trattamenti di dati personali relativi alle contestazioni delle sanzioni previste dal Codice della strada effettuate da ausiliari del traffico.

La vicenda riguarda in particolare profili connessi alla verifica dei presupposti richiesti dalla legge in relazione a comunicazioni di dati personali eventualmente inter-

corse tra un ente locale e la società di cui l'ente si avvale per la gestione del servizio.

Censimento nella Provincia autonoma di Bolzano

Nel corso del 2004 è proseguita intensamente l'attività di collaborazione richiesta al Garante in relazione alle modalità di svolgimento del censimento etnico-linguistico nella Provincia di Bolzano. In seguito ad ampi approfondimenti, anche in collaborazione con le istituzioni europee, nazionali e locali, l'Autorità ha ribadito al Governo le considerazioni, già contenute nei due provvedimenti del 2001, in merito al contrasto tra alcuni profili della disciplina sulla "*proporzionale etnica*" e la normativa in materia di protezione dei dati personali sopravvenuta sul piano internazionale comunitario e nazionale. In particolare, è stata evidenziata la necessità di separare dalle operazioni di censimento decennale della popolazione le dichiarazioni individuali nominative di appartenenza o aggregazione linguistica e l'esigenza che le medesime dichiarazioni divengano facoltative, da esercitarsi *una tantum* solo dalle persone interessate ad usufruire dei previsti benefici, senza la necessità di periodici rinnovi. La conservazione di tali dichiarazioni deve avvenire presso un organo pubblico, escludendo la raccolta intermedia presso gli enti locali e, soprattutto, la creazione di banche dati centralizzate. Pur volendo legittimamente prevenire elusioni o utilizzi strumentali, la normativa deve prevedere che, trascorso un adeguato lasso temporale, comunque inferiore all'attuale decennio, l'interessato possa modificare la dichiarazione, semmai con effetti che si producono decorso un congruo periodo di tempo (*Nota* 2 luglio 2004).

Dopo un ampio e serrato confronto, le istituzioni coinvolte hanno siglato un accordo sulle modifiche da apportare alla normativa provinciale, sottoposto nei giorni scorsi al parere del Garante, il quale valuterà prontamente se –come ipotizzato– sono state recepite diverse sue indicazioni, tenendo peraltro conto di alcuni rilievi critici di recente formulati in una nuova segnalazione inviata da parte di associazioni locali.

2.11. *Attività giudiziaria e informatica giuridica*

Processo civile *on-line*

Il Ministero della giustizia ha chiesto all'Autorità un parere in merito allo schema di decreto ministeriale (successivamente approvato con il d.m. 14 ottobre 2004) finalizzato a rendere pienamente operativo il processo civile telematico.

Il decreto prevede che, tramite un complesso sistema informatico (SICI-Sistema informativo civile), magistrati, avvocati, parti e personale giudiziario, collegati in rete, possano intervenire direttamente nel processo, trasmettendo comunicazioni, notifiche, atti sottoscritti con firma digitale e consultando lo stato del procedimento, senza recarsi necessariamente in tribunale.

Nel parere adottato il 23 luglio 2004, l'Autorità, richiedendo maggiori garanzie per i cittadini, ha tra le altre cose invitato il Ministero ad effettuare una rigorosa individuazione dei soggetti abilitati all'accesso al sistema sulla base delle rispettive specifiche competenze. In considerazione della delicatezza della tematica e della complessità del sistema informativo, l'Autorità ha poi sottolineato l'esigenza che i dati e le informazioni trattati dai soggetti pubblici coinvolti nel funzionamento del sistema debbano essere usati solo per le finalità legate allo svolgimento del processo civile *on-line* e in base alle rispettive funzioni e competenze.

Il Garante ha inoltre richiesto un rafforzamento delle misure di sicurezza e l'individuazione di specifici e congrui termini di conservazione dei dati in ragione del tempo necessario a raggiungere gli scopi per i quali essi sono stati raccolti.

Il decreto (pubblicato in *G.U.* n. 272 del 19 novembre 2004) ha tuttavia recepito solo in minima parte le indicazioni fornite dal Garante.

Metodi alternativi di risoluzione delle controversie presso la camera di commercio

Precise garanzie per gli interessati sono state indicate in un progetto avviato da una camera di commercio, un tribunale ed un consiglio dell'ordine degli avvocati nell'ambito dello sviluppo di metodi alternativi di risoluzione delle controversie. Pur essendo il progetto basato sull'adesione libera e volontaria degli interessati, l'Autorità ha individuato alcune prescrizioni da rispettare nella definizione dei moduli operativi. In particolare, i dati personali contenuti nei fascicoli del tribunale non devono essere accessibili ai rappresentanti della camera di commercio e dell'ordine; le parti delle controversie interessate dal tentativo di conciliazione stragiudiziale devono essere preventivamente informate in sede giudiziaria che verranno contattate dagli addetti dello sportello della camera di commercio. L'informativa dovrà essere specifica, con particolare riferimento alle modalità di trattamento ed al periodo di eventuale temporanea conservazione dei dati presso la camera di commercio, anche in caso di insuccesso del tentativo di conciliazione.

Mediazione penale e giustizia riparativa

È in corso un tavolo di lavoro con il Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia nell'ambito dei lavori della Commissione di studio "Mediazione penale e giustizia riparativa". Il Ministero ha infatti avviato un progetto finalizzato all'adozione di modelli di giustizia riparativa nell'ambito dell'esecuzione penale, in particolare con la sperimentazione di percorsi di mediazione penale tra reo e vittima.

Le modalità di attuazione di tale progetto sono al vaglio del Garante nella parte in cui coinvolgono profili che attengono alla tutela della riservatezza, soprattutto per quanto riguarda le esigenze di tutela della vittima del reato.

Pubblicità di sentenze e provvedimenti

Come in passato, il Garante ha più volte ribadito che la normativa in materia di protezione dei dati personali non ha modificato il regime di pubblicità delle sentenze, le quali devono essere redatte secondo le regole ordinarie. Solamente in caso di riproduzione per attività di informazione giuridica il giudice, d'ufficio o su richiesta di parte per motivi legittimi, può disporre l'apposizione sul provvedimento di un'annotazione volta a precludere l'indicazione, nella versione pubblicata, delle generalità e di altri dati identificativi degli interessati. A prescindere dall'annotazione, le generalità e i dati identificativi devono essere comunque omessi nelle decisioni in materia di rapporti di famiglia e di stato delle persone o che coinvolgono minori (artt. 51 e 52 del Codice).

Una distinta questione è stata invece posta all'attenzione del Garante da un ricorso avverso l'Autorità garante per la concorrenza e il mercato, relativamente alla conoscibilità in rete mediante motori di ricerca dei provvedimenti che tale amministrazione deve pubblicare sul proprio bollettino, "riprodotto" anche sul sito *web* istituzionale.

Mezzi di prova

Infine, rispondendo ad alcuni quesiti e segnalazioni relativamente a particolari modalità di acquisizione di mezzi di prova nell'ambito di procedimenti giudiziari, il Garante ha ribadito che resta ferma la competenza del giudice per ogni valutazione circa l'ammissibilità e la rilevanza delle prove; il Codice, infatti, afferma chiaramente che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizione di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (art. 160, comma 6).

3 Sanità

3.1. *Trattamento di dati idonei a rivelare lo stato di salute*

Modifiche al Codice

Come segnalato, nel corso del 2004 sono intervenute alcune modifiche al Codice per quanto riguarda il trattamento dei dati personali in ambito sanitario. In particolare, in materia di trattamenti effettuati da parte dei medici di medicina generale e dei pediatri di libera scelta, il decreto-legge 29 marzo 2004, n. 81, convertito con legge 26 maggio 2004, n. 138, ha introdotto alcune disposizioni in favore di tali soggetti. È stato previsto che ad essi non si applichino le misure organizzative di cui all'art. 83 del Codice (ad es. la distanza di cortesia), purché vengano adottate nell'organizzazione delle prestazioni e dei servizi idonee misure per garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale (art. 83, comma 2-*bis*, del Codice).

Per effetto delle ulteriori modifiche apportate dal citato decreto all'art. 89 del Codice, l'obbligo del medico di medicina generale e del pediatra di libera scelta di apposizione sulla ricetta di un tagliando sopra le generalità e l'indirizzo dell'assistito è ora subordinato ad un'esplicita richiesta di quest'ultimo.

Documentazione clinica abbandonata

Il Garante si è occupato della vicenda, apparsa anche sui mezzi di informazione, del rinvenimento presso un *ex* ospedale psichiatrico in Calabria di documentazione sanitaria abbandonata. Dopo il sequestro della stessa da parte dei carabinieri, l'Autorità ha avviato autonomi accertamenti nei confronti degli enti titolari del trattamento, con particolare riferimento all'adozione delle misure di sicurezza previste dal Codice per la conservazione delle informazioni idonee a rivelare lo stato di salute degli interessati (artt. 11 e 31-35) (*Nota* 13 ottobre 2004). I profili penali della vicenda sono attualmente all'esame della Procura della Repubblica di Catanzaro.

Al di là di quanto più analiticamente segnalato nel par. 20.3, con riferimento ad una vicenda simile l'Autorità ha coordinato un'attività ispettiva in una struttura sanitaria presso cui erano state abbandonate numerose cartelle cliniche per garantire che il recupero e la conservazione della documentazione sanitaria avvenisse con modalità idonee ad evitare accessi non autorizzati ai dati personali in essa contenuti (ispezione presso una *ex* colonia di Santa Maria di Leuca del 12 febbraio 2004). Analogamente, l'Ufficio è intervenuto a seguito di notizie stampa per assicurare la rapida rimozione di numerose ricette e cartelle cliniche rinvenute nel cortile di una biblioteca comunale e nella zona antistante ad una azienda sanitaria in Roma (ispezioni del 10 e 12 gennaio 2004; v. *Comunicato stampa* 24 settembre 2004)

Dati personali dei pazienti

Riguardo alla possibilità di comunicare i dati personali dei pazienti a terzi, ivi compresi i familiari, l'Autorità ha ribadito che gli esercenti le professioni sanitarie sono tenuti ad informare preventivamente in modo adeguato l'interessato ed a richiedere uno specifico consenso scritto sul punto, in conformità a quanto previsto dall'autorizzazione generale del Garante (autorizzazione n. 2/2004, punto 5). Non è, infatti, possibile considerare di per sé equipollente ad una valida prestazione di consenso la presenza del familiare in occasione della visita medica.

Nel caso segnalato all'Autorità, il medico aveva rilasciato alla moglie, senza il con-

senso del marito, un certificato attestante la patologia riscontratagli in occasione di una visita medica. Successivamente, il certificato, che riportava informazioni incomplete ed estranee alle ordinarie esigenze di diagnosi clinica, relative al carattere dell'interessato, era stato prodotto dalla moglie nel procedimento civile di separazione.

Avendo accertato che i dati sulla salute del segnalante erano stati trattati con modalità non conformi alla normativa sulla protezione dei dati personali, il Garante ha intimato al medico di astenersi dall'ulteriore trattamento delle informazioni relative all'interessato; ha poi ricordato che i dati medesimi, essendo stati illecitamente acquisiti, non possono essere ulteriormente utilizzati (art. 11, comma 2, del Codice).

Copia della segnalazione è stata inviata al competente Consiglio dell'Ordine dei medici per le valutazioni del caso (*Nota* 12 agosto 2004).

Contrassegni invalidi

A seguito delle novità introdotte dal Codice, nel corso dell'ultimo anno sono pervenute numerose richieste di parere in merito ai contrassegni per la circolazione e la sosta di veicoli a servizio di persone invalide, regolate, in particolare, dall'art. 188 del Codice della strada (d.lg. 30 aprile 1992, n. 285), dall'art. 381 del relativo regolamento di attuazione (d.P.R. 16 dicembre 1992, n. 495) e, da ultimo, dall'art. 74 del Codice. In relazione al possibile conflitto tra le norme citate, il Garante ha chiarito che, configurandosi l'art. 74 del Codice norma specifica di rango primario, la stessa deve considerarsi prevalente.

Pertanto, i contrassegni da esporre su veicoli devono contenere i soli dati indispensabili ad individuare l'autorizzazione rilasciata e risultare privi di simboli o diciture dai quali possa desumersi la speciale natura dell'autorizzazione.

Per il controllo della regolarità del contrassegno è, quindi, sufficiente porre in evidenza l'indicazione del comune competente e del numero di autorizzazione, informazioni dalle quali si può agevolmente risalire al titolare del permesso, oltre a verificare la validità dello stesso e la correttezza del suo utilizzo (*Note* 21 maggio 2004).

Patologia psichiatrica

È all'attenzione dell'Autorità la richiesta avanzata dal dipartimento di salute mentale di una Ausl di acquisire dalle case di cura private operanti nel territorio di propria competenza i nominativi dei pazienti con patologia psichiatrica. Tale comunicazione avverrebbe in attuazione di quanto previsto da una deliberazione della Giunta della Regione Veneto, in virtù della quale le strutture sanitarie private operanti nella regione, che prendano in cura pazienti psichiatrici, devono comunicare tempestivamente, e comunque entro tre giorni dall'evento, l'avvenuto accoglimento degli stessi.

Al riguardo, il Garante ha precisato che il d.P.R. 10 novembre 1999 (Approvazione del progetto obiettivo "Tutela salute mentale 1998-2000") ha previsto che presso la direzione del Dipartimento di salute mentale (DSM) sia collocato il sistema informativo dipartimentale, il quale raccoglie, elabora ed archivia i dati di struttura, processo ed esito, anche al fine di rilevare il ricorso a strutture di ricovero private degli abitanti del proprio bacino di utenza e i costi relativi. Tuttavia, nessuna disposizione del citato decreto presidenziale impone alle strutture di ricovero private di fornire al DSM competente per territorio l'elenco nominativo dei soggetti che abbiano fatto ricorso alle stesse.

In conformità al citato decreto e al principio di indispensabilità dettato dal Codice, l'Ufficio sta verificando se debbano essere inviati al sistema informativo del DSM solo dati anonimi e aggregati che indichino il numero degli abitanti del bacino di utenza del dipartimento che si siano recati presso la relativa struttura privata e non anche i loro dati identificativi.

Benefici per l'acquisto di sussidi tecnici

Il Garante ha preso in esame la questione, segnalata da un quotidiano, relativa alla documentazione sanitaria da presentare ai rivenditori per beneficiare della riduzione dell'Iva all'atto dell'acquisto di sussidi tecnici e informativi utili a favorire l'autonomia delle persone disabili.

Secondo la disciplina di settore, per usufruire di questa agevolazione occorre presentare al rivenditore una specifica prescrizione rilasciata dal medico specialista della Asl, da cui risulti il collegamento funzionale tra la menomazione e il sussidio che si intende acquistare, insieme ad un certificato (rilasciato dalla Asl) che attesti l'esistenza di un'invalidità funzionale permanente.

L'applicazione di tali disposizioni deve avvenire, però, nel rispetto delle garanzie previste dal Codice per le informazioni sulla salute, secondo le quali è possibile trattare soltanto le informazioni "indispensabili", pertinenti e non eccedenti rispetto alle finalità di volta in volta perseguite, ferme restando ulteriori cautele più severe per il trattamento di talune categorie di dati, quali quelli relativi all'Aids, alla sieropositività o allo stato di disabilità.

Pertanto, è allo studio dell'Autorità la praticabilità di alcune soluzioni alternative rispettose della riservatezza e della dignità delle persone disabili, anche con riferimento alle disposizioni della legge n. 448/1998, che consentano di utilizzare lo strumento dell'autocertificazione per attestare le condizioni personali necessarie al fine di usufruire di una serie di benefici, tra cui le agevolazioni di carattere fiscale.

Sono in corso inoltre ulteriori approfondimenti in merito alle procedure adottate dalle aziende sanitarie locali per il rilascio della tessera di esenzione dal pagamento del *ticket* e dei certificati di invalidità.

Reclami alle Asl e qualità del servizio sanitario

Il Garante è intervenuto in merito ai trattamenti di dati relativi alla gestione dei reclami raccolti dalle Ausl e ai questionari telefonici a domicilio per il rilevamento della qualità sanitaria. Al riguardo, si è precisato che sia l'attività di gestione dei reclami, sia quella di rilevamento della qualità sanitaria, pur essendo considerate di rilevante interesse pubblico dal Codice (artt. 67, comma 1, lett. *b*), 73, comma 2, lett. *g*) e 85, comma 1, lett. *b*), non possono essere effettuate se non dopo aver individuato con atto di natura regolamentare i tipi di dati che possono essere trattati e le operazioni su di essi eseguibili, ai sensi dell'art. 20, comma 2, del Codice (*Nota* 5 ottobre 2004).

Con riferimento alla possibilità di svolgere tali interviste telefonicamente ovvero di contattare al telefono i soggetti che hanno effettuato una prenotazione di un esame clinico al fine di ottenere la conferma o la cancellazione della stessa prenotazione, il Garante ha sottolineato che tali iniziative, seppur lodevoli in quanto dirette ad offrire un servizio migliore agli utenti, presentano profili di criticità. Infatti, in occasione del contatto telefonico, soggetti diversi dall'interessato potrebbero venire a conoscenza di alcuni dati sulla salute di quest'ultimo o più in particolare della sua intenzione di effettuare un determinato esame clinico. Al fine di superare il rischio di tale indebita conoscenza di dati personali dell'interessato, è stato pertanto suggerito di attivare tali servizi solo a seguito di un esplicito assenso dell'utente, previa specifica informativa resa allo stesso ai sensi dell'art. 13 del Codice. Ulteriori, possibili accorgimenti sono stati ipotizzati per l'eventuale uso in occasione di chiamate di conferma da parte dell'azienda sanitaria, specie per ciò che attiene al tipo di indagine medica prenotata o ad altre informazioni di carattere sensibile. Analoghe cautele sono state suggerite in ordine all'attività di refertazione telefonica, effettuata da una casa di cura privata (*Note* 5 ottobre 2004 e 4 gennaio 2005).

Misure organizzative

In materia di consegna dei referti medici, l'Autorità ha appreso da alcune notizie stampa della prassi avviata da un'azienda sanitaria di trasmettere i referti ai pazienti tramite il fax di una tabaccheria. Al riguardo, l'Ufficio ha ricordato che l'art. 84 del Codice prevede che i dati personali inerenti allo stato di salute siano resi noti all'interessato solo per il tramite di un medico designato dallo stesso o dal titolare ed ha quindi invitato la Ausl ad interrompere spontaneamente tale modalità di consegna dei referti, ricevendo subito un positivo riscontro da parte dell'azienda sanitaria (*Nota* 19 ottobre 2004).

L'Autorità è stata interpellata più volte in merito alla possibilità che il personale infermieristico possa essere reso edotto da quello medico delle patologie sofferte dai pazienti in cura. Al riguardo, il Garante ha ricordato che gli organismi sanitari nell'organizzazione delle prestazioni e dei servizi, devono adottare idonee misure per garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati; sono altresì tenuti a sottoporre gli incaricati, che non siano tenuti per legge al segreto professionale, a regole di condotta analoghe (art. 83, comma 2, lett. *i*), del Codice). Il personale infermieristico e di assistenza sanitaria, debitamente designato quale incaricato del trattamento ai sensi dell'art. 30 del Codice, può venire a conoscenza delle informazioni sullo stato di salute dei pazienti strettamente necessarie ad assicurare agli interessati le cure ritenute più idonee e ad adottare le opportune cautele per la propria salute nello svolgimento della prestazione lavorativa. Tali soggetti dovranno, tuttavia, trattare le informazioni sanitarie nel pieno rispetto di quanto indicato nella designazione degli incaricati del trattamento, della normativa in materia di protezione dei dati personali, dell'autorizzazione generale n. 2/2004 e delle regole deontologiche (*Nota* 12 ottobre 2004).

Un'ulteriore problematica sottoposta al Garante riguarda la comunicazione di dati personali di soggetti affetti da una determinata patologia ad una società privata vincitrice di un pubblico appalto per la fornitura di ausili protesici, al fine di consentire alla stessa di provvedere alla consegna di detti ausili direttamente al domicilio dei pazienti.

Carta sanitaria

Il decreto-legge 30 settembre 2003, n. 269, convertito con legge 24 novembre 2003, n. 326, prevede all'art. 50 (*Disposizioni in materia di monitoraggio della spesa nel settore sanitario e di appropriatezza delle prescrizioni sanitarie*) l'introduzione di un modello di ricetta medica a lettura ottica e la costituzione di una banca dati centralizzata (contenente il codice fiscale degli assistiti) in cui confluiscono i dati riguardanti le prescrizioni di farmaci e di prestazioni specialistiche.

Già nel corso dei lavori di conversione del decreto legge, il Garante ha richiamato l'attenzione del legislatore sui delicati problemi sollevati da tale disposizione che, seppur ispirata dall'esigenza di incentivare il monitoraggio della spesa pubblica, è però, allo stato, perseguita attraverso soluzioni che rischiano di compromettere il diritto alla protezione dei dati e, in particolare, di quelli riguardanti lo stato di salute, salvaguardati da particolari garanzie. Attraverso i farmaci prescritti e le prestazioni specialistiche ottenute può essere infatti ricostruita analiticamente la storia sanitaria di ciascun soggetto.

In tale occasione è stato poi rappresentato che le necessarie finalità di controllo della spesa sanitaria potrebbero essere raggiunte anche attraverso altre modalità che non consentano l'identificazione dei soggetti cui si riferiscono le informazioni sanitarie.

Al riguardo, la Camera dei deputati, nella seduta del 19 novembre 2003, ha impegnato il Governo ad intraprendere adeguate iniziative normative al fine di escludere il trattamento dei dati degli assistiti per le finalità sopra descritte.

Tuttavia, in attuazione di quanto previsto dall'art. 50 del decreto-legge

n. 269/2003, sono stati adottati, senza la necessaria consultazione dell'Autorità (prevista dall'art. 154 del Codice), sei atti amministrativi, tra decreti ministeriali e provvedimenti dirigenziali, che individuano con un maggior grado di dettaglio gli aspetti applicativi di tale norma.

Già dal mese di luglio 2004 è stato evidenziato al Governo che per l'adozione di tali atti è mancata la necessaria consultazione del Garante. Il rilievo è stato mosso, tra gli altri, soprattutto nei confronti di un decreto del 30 giugno del 2004, che ha previsto un obbligo –per tutti i cittadini aventi diritto– di dotarsi della tessera sanitaria; obbligo che, per il suo impatto sui diritti delle persone interessate e per le sue caratteristiche, può essere peraltro introdotto solo da una disposizione legislativa e non da un atto amministrativo. Ancora, la connessa sostanziale trasformazione del codice fiscale in un identificativo generale, inserito nella predetta tessera sanitaria, non è allo stato compatibile con la disciplina prevista dalla direttiva 95/46/CE (e con il Codice) nella parte in cui questa dispone che gli Stati membri determinano in base a quali garanzie e condizioni un numero nazionale di identificazione o qualsiasi altro mezzo identificativo di portata generale può essere oggetto di trattamento.

Recentemente, il Garante ha nuovamente rappresentato al Governo le ampie riserve in merito alla circostanza che sia stato adottato, con particolare riferimento alla materia sanitaria, un intero pacchetto di atti amministrativi suscettibili di incidere in maniera significativa sui diritti fondamentali garantiti dal Codice, senza il necessario coinvolgimento dell'Autorità in relazione alle proprie specifiche attribuzioni previste dal medesimo Codice, con atti quindi viziati sul piano amministrativo.

Il Ministero della salute ha recentemente sottoposto all'attenzione dell'Autorità l'intenzione di inviare a tutte le famiglie italiane un opuscolo divulgativo dal titolo *"Pensiamo alla salute"*, attraverso Poste italiane S.p.A., designata responsabile del trattamento. L'Autorità, nel prendere atto dell'iniziativa, ha richiamato i criteri indicati nelle precedenti pronunce relative ad importanti casi di comunicazione istituzionale (v., ad esempio, *Provv.* 11 aprile 2002, sull'"euroconvertitore", in *Bollettino* n. 27 del 2002, p. 56), specificando che il titolare di tale trattamento di dati personali, deve essere considerato il Ministero quale entità nel suo complesso, anziché una sua singola articolazione.

3.2. *Trattamento di dati personali in occasione dell'accertamento dell'infezione da Hiv*

L'Autorità è stata più volte sollecitata dalle strutture sanitarie a pronunciarsi in merito alla possibilità di comunicare ai familiari la notizia dello stato di sieropositività di un paziente ricoverato con prognosi grave (anche in caso di decesso). Al riguardo, si è rilevato che il Codice non contiene deroghe alle disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali e ciò anche per quanto riguarda la legge 5 giugno 1990, n. 135 in tema di Aids e Hiv. In tale legge figura, in particolare, l'obbligo di comunicare i risultati di accertamenti diagnostici diretti o indiretti per l'infezione da Hiv alla sola persona cui tali esami si riferiscono (art. 5, comma 4).

Pertanto, deve ritenersi che la comunicazione ai familiari dello stato di sieropositività del paziente non possa prescindere dal consenso dell'interessato. È stata anche valutata l'opportunità che il medico provveda a sensibilizzare la persona sieropositiva e cerchi di persuaderla a comunicare al coniuge la propria sieropositività oppure a manifestare il proprio consenso alla rivelazione da parte dello stesso medico.

Restano infatti da valutare le possibili responsabilità penali del soggetto che, consapevole del proprio stato patologico, ometta di informare il coniuge

(cfr. Cass. pen. n. 30425/2001), nonché le riflessioni in ambito giuridico e scientifico circa i presupposti per l'eventuale applicazione dell'esimente penale dello stato di necessità (art. 54 c.p.) nel caso in cui la sieropositività sia resa nota dal medico senza consenso ad un familiare dell'interessato.

Deve ritenersi peraltro che il difficile bilanciamento dei diversi interessi non possa essere risolto nel senso dell'applicazione –nella fase temporanea in cui il paziente è momentaneamente incosciente– delle recenti disposizioni che prevedono, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, che il consenso possa essere validamente prestato anche da persone diverse da quest'ultimo (art. 82, comma 2, lett. *a*), del Codice), dovendosi considerare anche questa norma in termini sistematici ed omogenei rispetto a tutto il quadro normativo.

Va invece valutato se possa invece giungersi, almeno in parte, a diversa conclusione qualora, in caso di decesso del paziente sieropositivo, il coniuge chieda di accedere alle informazioni che riguardano la persona deceduta. Il diritto di accesso ai dati personali concernenti persone decedute può essere, infatti, esercitato da chiunque abbia un interesse proprio o agisca a tutela dell'interessato o per ragioni familiari meritevoli di protezione (art. 9, comma 3, del Codice).

Sono in corso alcune verifiche volte a controllare se, in occasione del prelievo di sangue per l'accertamento dell'infezione da Hiv, sia fornita al soggetto che si sottopone al test un'idonea informativa, se sia acquisito il suo consenso al trattamento dei dati sensibili, nonché le tipologie di dati raccolti. Dovrà inoltre essere appurato il rispetto delle disposizioni di legge che impongono all'operatore sanitario e ad ogni altro soggetto che viene a conoscenza di un caso di Aids, ovvero di un caso di infezione da Hiv, di adottare in particolare ogni misura o accorgimento necessari alla tutela dei diritti, della dignità e delle libertà fondamentali dell'interessato.

In particolare, l'Autorità si è occupata del caso in cui una paziente era stata sottoposta al test per l'accertamento dell'infezione da Hiv in occasione di un intervento oculistico, senza aver prestato previamente il suo consenso informato. Sebbene la struttura abbia in seguito provveduto alla cancellazione dei dati riguardanti l'interessata, l'Ufficio ha comunque avviato accertamenti sulle modalità con cui vengono generalmente eseguite le analisi in occasione di analoghe prestazioni sanitarie (*Nota* 22 ottobre 2004).

Sono stati, inoltre, avviati alcuni accertamenti volti a verificare la pertinenza e non eccedenza dei dati idonei a rivelare le condizioni di salute dell'interessato (affezione da Aids) contenuti in un verbale di sommarie informazioni assunte *ex* art. 351 c.p.p. dalla Guardia di finanza e successivamente inserito nel fascicolo delle indagini preliminari.

Per quanto concerne la ricerca medica, è avanzato lo studio della questione relativa all'attuazione di un sistema di sorveglianza epidemiologica delle infezioni da Hiv, secondo un progetto della Commissione nazionale per la lotta contro l'Aids e le altre malattie infettive emergenti e riemergenti, sottoposto all'attenzione del Garante, tematica che si collega a precedenti segnalazioni, di cui è ormai ultimata l'istruttoria.

Sull'argomento è stato costituito un gruppo di lavoro in cui, oltre all'Autorità ed alla citata Commissione, sono rappresentate le regioni, la Presidenza del Consiglio dei ministri, l'Istituto superiore di sanità e le associazioni che tutelano l'interesse delle persone affette da Hiv. Nell'ambito di questo gruppo sono stati inizialmente esaminati i presupposti che rendono lecito il trattamento dei dati personali dei sieropositivi, i dati utilizzati, i loro flussi, le modalità con le quali rendere l'informativa agli interessati, nonché le misure di sicurezza da adottare.

L'Ufficio ha poi svolto ulteriori approfondimenti sulla composizione del "codice

identificativo" da assegnare alle segnalazioni delle nuove infezioni e sulla grandezza dell'unità territoriale di rilevazione. Occorre assicurare, infatti, che tale codice sia composto in modo tale, da un lato, da minimizzare il rischio che siano registrate due o più segnalazioni relative ad uno stesso soggetto, e dall'altro, da rispettare l'esigenza, espressa dalla legge 5 giugno 1990, n. 135 e ribadita dal d.m. del 13 ottobre 1995, di non consentire l'identificabilità delle persone cui si riferiscono le singole segnalazioni (artt. 5, l. n. 135/1990 e 178 del Codice, artt. 1 e 2 del decreto citato). Va inoltre individuata la grandezza dell'unità territoriale di rilevazione (macro regioni, regioni, province, macro aree, ecc.) in modo da assicurare l'impossibilità di risalire all'identità degli interessati, in relazione ai tempi e agli strumenti che possono essere ragionevolmente impiegati per compiere tale operazione (v. punto 1, Raccomandazioni del Consiglio d'Europa nn. R (97) 5 e (97) 18).

In proposto, l'Autorità ha anche acquisito un parere tecnico dal Dipartimento per la produzione statistica e il coordinamento tecnico-scientifico dell'Istat, per disporre di idonei elementi di valutazione al fine di formulare le proprie determinazioni all'interno del gruppo di lavoro (*Nota* 19 luglio 2004).

3.3. *Notificazioni in ambito sanitario*

In materia di trattamenti di dati personali in ambito sanitario, il Garante ha adottato un provvedimento nel quale sono individuati i trattamenti di dati idonei a rivelare lo stato di salute esonerati dall'obbligo di notificazione di cui all'art. 37 del Codice (*Deliberazione* n. 1, del 31 marzo 2004).

L'Autorità ha anche chiarito che sono esonerati (dall'obbligo di notificazione) esclusivamente i trattamenti effettuati dai singoli professionisti e dagli altri medici che, in forma associata, condividono il trattamento con altri professionisti, specie all'interno di uno stesso studio medico (*Parere* 26 aprile 2004).

L'esenzione riguarda solo tali soggetti e si riferisce unicamente al trattamento di dati genetici e biometrici, di dati relativi alla procreazione assistita, ai trapianti, alle indagini epidemiologiche, alla rilevazione di malattie mentali, infettive, diffusive e alla sieropositività che siano effettuati nell'ambito degli ordinari rapporti con il paziente. L'esonero non opera, invece, se il trattamento è sistematico ed assume il carattere di costante e prevalente attività del medico come, ad esempio, quello di dati genetici effettuato da un genetista.

Non è previsto esonero neppure per i trattamenti di dati genetici e biometrici effettuati da strutture sanitarie pubbliche o private (ospedali, case di cura e di riposo, aziende sanitarie, laboratori di analisi cliniche, associazioni sportive). Detta misura è stata, infatti, disposta solo in favore di persone fisiche esercenti le professioni sanitarie e non per i trattamenti in quanto tali.

Al riguardo, il Garante ha avviato, con la collaborazione della Guardia di finanza, un ciclo di ispezioni nei confronti di aziende sanitarie locali e di laboratori di analisi privati. Tali accertamenti hanno condotto alla contestazione diretta delle sanzioni amministrative per omessa o ritardata notificazione nei confronti di 14 soggetti sui 15 controllati.

Servizi sanitari *on-line*

Con riferimento alle prestazioni di servizi sanitari per via telematica, il Garante ha precisato che devono essere notificati solo i trattamenti relativi ad una banca dati, ovvero alla fornitura di beni.

Non vanno quindi notificati i trattamenti di dati sanitari nell'ambito della teleassistenza (consultazione di specialisti per via telefonica) e quelli organizzati in banche

dati trattati manualmente (archivi cartacei), ovvero informatizzate ma non collegate ad una rete telematica. Non devono, infine, notificare i medici che usano unicamente un *computer* nel proprio ufficio utilizzando la posta elettronica per dialogare con i pazienti e per effettuare prenotazioni per gli assistiti.

In merito all'attività di monitoraggio della spesa sanitaria è stato precisato che non sono soggetti a notificazione i trattamenti di dati sanitari effettuati da strutture convenzionate con il Servizio sanitario nazionale al solo fine di ottenere il rimborso delle prestazioni specialistiche erogate.

3.4. *Protezione dei dati e procreazione medicalmente assistita*

Per quanto riguarda la materia della procreazione medicalmente assistita, come segnalato nella *Relazione 2003*, l'Autorità è intervenuta in collaborazione col Ministero della salute in ordine alle modalità di attuazione dell'art. 17 della legge n. 40/2004, nella parte in cui prevede che le strutture e i centri in cui si praticano tecniche di procreazione medicalmente assistita trasmettano al Ministero della salute *"un elenco contenente l'indicazione numerica degli embrioni prodotti ... nonché, nel rispetto delle vigenti disposizioni sulla tutela della riservatezza dei dati personali, l'indicazione nominativa di coloro che hanno fatto ricorso alle tecniche medesime a seguito delle quali sono stati formati gli embrioni"*.

Il Ministero ha poi specificato che non si sarebbe più sollecitata una comunicazione nominativa di tutti gli interessati che avevano fatto ricorso alla procreazione assistita presso i centri e che, al contrario, si sarebbe proceduto alla sola richiesta di inviare al Ministero una serie di codici numerici indicanti il centro, la regione di riferimento e un numero sequenziale per ogni embrione congelato, in collegamento con i dati identificativi (che rimarranno in possesso dei soli centri).

Nella stessa materia, l'Autorità ha espresso un parere sullo schema di regolamento che disciplina le modalità di manifestazione della volontà degli interessati di accedere alle tecniche di procreazione medicalmente assistita (art. 6, legge 19 febbraio 2004, n. 40). Sebbene la tematica del consenso informato al trattamento medico, oggetto del regolamento, deve ritenersi distinta rispetto a quella del consenso al trattamento dei dati personali, tenuto conto della delicatezza della materia, si è invitato ad adottare la medesima soluzione prevista dal cd. "decreto Di Bella", ovvero quella di acquisire contestualmente entrambe le manifestazioni di volontà, in modo da agevolare l'attività delle strutture e dei centri interessati (*Parere* del 23 luglio 2004).

4 Dati genetici

4.1. *Le informazioni genetiche*

Autorizzazione

Il Garante è in procinto di rilasciare l'autorizzazione generale prevista dal Codice per il trattamento dei dati genetici sentito il Ministero della salute, il quale provvederà una volta acquisito il parere del Consiglio superiore di sanità (art. 90).

Con la nuova autorizzazione si intende precisare la nozione di "dato genetico" e individuare le cautele da adottare 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, nonché 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, nonché di indagini medico-legali (come i test di paternità e/o maternità), soprattutto in relazione al contenuto e alle modalità dell'informativa, alla necessità di fornire all'interessato un'appropriata consulenza genetica e psicologica, al diritto di quest'ultimo di non conoscere i risultati dell'esame (comprese eventuali notizie inattese che lo riguardano), alle modalità di manifestazione del consenso ed al periodo di conservazione dei dati e dei campioni biologici.

Le ricerche dovrebbero essere effettuate secondo 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 potranno essere attuati soltanto se preceduti da un'ampia attività di informazione volta ad illustrare alle comunità interessate le caratteristiche fondamentali della ricerca.

Particolari limitazioni si applicano, infine, al trattamento di dati genetici da parte di datori di lavoro e di imprese assicurative.

Ricerche genetiche

In risposta ad alcune richieste di autorizzazione al trattamento di dati genetici, l'Ufficio ha precisato che, nel breve periodo che precede il rilascio di tale nuova autorizzazione, il trattamento di queste informazioni resta disciplinato in via transitori 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 es. il divieto di comunicare le informazioni genetiche a terzi (punto 1.4, dell'autorizzazione generale n. 2/2004, che rinvia al punto 2, lett. *b*), dell'autorizzazione generale n. 2/2002) (*Note* 2 agosto 2004 e 31 agosto 2004).

Sempre in tema di dati genetici, il Garante è intervenuto, a seguito di una segnalazione proveniente dall'estero, rispetto ad una vicenda relativa ad un'articolata ricerca genetica su popolazioni isolate in Alto Adige. L'Autorità, sulla base delle informazioni e dei documenti acquisiti con accertamenti ispettivi *in loco*, anche grazie alla collaborazione dei professionisti preposti alla ricerca, ha accertato la violazione, pur in presenza del rispetto di larga parte dei principi di protezione dei dati, di alcune norme in materia di misure di sicurezza e ha adottato un provvedimento di prescrizione di misure idonee ai sensi dell'art. 169 del Codice.

Su richiesta di una società di ricerca che ha sede in Sardegna, l'Ufficio si è anche

espresso in ordine a un complesso progetto di studio del genoma della popolazione italiana, sottolineando la necessità di tenere conto, nei progetti di medio-lungo periodo come quello esaminato, di alcune garanzie ipotizzate per la autorizzazione.

Sono state quindi anticipate alcune considerazioni in merito alla titolarità del trattamento (la cui individuazione è necessaria anche per determinare il soggetto tenuto ad effettuare la notificazione al Garante ai sensi dell'art. 37 del Codice), alle finalità perseguite, alle modalità di informativa e di manifestazione del consenso, ai diritti che devono essere garantiti agli interessati rispetto alle informazioni che li riguardano, nonché all'ambito di comunicazione dei dati e all'impiego di detti dati per scopi ulteriori rispetto a quelli originari.

In particolare, l'informativa resa deve porre in evidenza il diritto dell'interessato di opporsi per motivi legittimi al trattamento dei dati che lo riguardano e di non conoscere i risultati della ricerca o degli esami genetici effettuati, comprese eventuali notizie inattese.

Nel ricordare che soltanto il perseguimento di altre eventuali legittime finalità di carattere storico, statistico o scientifico, può giustificare una conservazione che si protragga oltre il periodo di tempo necessario al conseguimento degli scopi per i quali i dati sono raccolti o successivamente trattati, l'Ufficio ha segnalato la necessità di individuare con chiarezza le ulteriori finalità scientifica eventualmente perseguite, in modo da determinare un periodo di conservazione dei dati e dei campioni biologici realmente proporzionato rispetto ai medesimi scopi (*Nota* 20 ottobre 2004).

Ricongiungimento familiare

L'Autorità è stata inoltre interpellata dal Ministero degli affari esteri e dal Ministero dell'interno in relazione alla possibilità di utilizzare, nell'ambito delle procedure relative al ricongiungimento familiare dei cittadini dei paesi nei quali non esiste un'autorità statale riconosciuta, l'esame del Dna, già impiegato nei confronti dei cittadini somali, quale strumento di accertamento dell'identità delle persone interessate. In considerazione dei delicati profili incidenti sulla dignità e sulla riservatezza degli interessati, l'Ufficio ha avviato alcuni approfondimenti, anche in collaborazione con i competenti uffici dei predetti dicasteri, per valutare la liceità della procedura impiegata ed, eventualmente, concordare soluzioni idonee a realizzare l'iniziativa prospettata nel pieno rispetto delle garanzie previste dal Codice e dalla nuova autorizzazione sul trattamento dei dati genetici, a tutela dei diritti e delle libertà fondamentali delle persone.

5 Ricerca statistica e scientifica

5.1. *Ricerca statistica*

Dal 1° ottobre 2004 trova applicazione il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici effettuati al di fuori del Sistema statistico nazionale (pubblicato in *G.U.* il 19 agosto 2004 a cura del Garante, e riportato con decreto del Ministro della giustizia del 14 gennaio 2005 nell'allegato A) del Codice).

Tale codice (previsto inizialmente dall'art. 10 del d.lg. 30 luglio 1999, n. 281, e successivamente dall'art. 106, comma 1, del Codice) è il risultato di un lungo lavoro che ha coinvolto, oltre al Garante, la Conferenza dei rettori delle università italiane e numerose associazioni e società scientifiche italiane.

Le norme contenute nel codice deontologico, il cui rispetto è condizione di liceità e correttezza del trattamento, si applicano ai trattamenti di dati personali per scopi statistici e scientifici effettuati da università, altri enti o istituti di ricerca e società scientifiche.

Il codice si ricollega alle garanzie previste dalla normativa che regola i trattamenti effettuati nell'ambito del Sistema statistico nazionale, assicurando particolari cautele per i dati sensibili e giudiziari e per la ricerca medica, biomedica ed epidemiologica, nonché per le ricerche di mercato che non siano connesse alle attività commerciali e di informazione commerciale. Sono previste specifiche regole di condotta e misure di sicurezza soprattutto in relazione alla conservazione dei dati identificativi.

Le ricerche dovranno essere effettuate conformemente agli *standard* metodologici del pertinente settore disciplinare e sulla base di un progetto consultabile per verificare la corretta applicazione della normativa sulla protezione dei dati personali. Le università, gli altri istituti o enti di ricerca e le società scientifiche devono assicurare la diffusione e il rispetto del codice deontologico e segnalano al Garante le violazioni di cui vengono a conoscenza.

Dati reddituali

Per quanto riguarda la concreta applicazione della normativa in materia statistica, il Garante è stato interpellato dall'Agenzia delle entrate in merito alla trasmissione ad una provincia (che aveva avviato un'indagine statistica finalizzata all'individuazione delle differenze socio-economiche tra uomini e donne) dei dati reddituali relativi alla popolazione residente in un comune.

L'Autorità ha specificato in proposito che non devono essere comunicati i dati identificativi diretti degli interessati. I dati possono essere trasmessi, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite dall'indagine, solo a seguito del rilascio di un'idonea informativa agli interessati (*Nota* 1° ottobre 2004).

Ricerca sociologica

Nell'ambito della ricerca sociologica, un'università pubblica ha richiesto ad una scuola i dati personali degli alunni e delle loro famiglie per lo svolgimento di uno studio sull'influenza dell'ambiente scolastico nella valorizzazione del capitale sociale delle famiglie e dei ragazzi. L'Autorità, nell'evidenziare che a tali trattamenti si applica il codice deontologico di recente approvazione, ha precisato che le fina-

lità di ricerca perseguite dall'università potevano essere raggiunte con altre modalità, limitando l'utilizzo di dati personali (art. 12, comma 3, del codice deontologico) (*Nota* 1° dicembre 2004).

Istat

Nel rendere all'Istat il prescritto parere relativo al Programma statistico nazionale per gli anni 2005-2007, l'Autorità ha valutato positivamente l'inserimento nel documento programmatico delle schede relative alle rilevazioni ed elaborazioni che trattano dati personali. Tali schede consentono, infatti, di informare in maniera più chiara gli interessati qualora i dati non siano stati raccolti direttamente presso di loro e il conferimento dell'informativa a ciascuno richieda uno sforzo sproporzionato rispetto al diritto tutelato.

In tale occasione l'Autorità, con riferimento alle cosiddette indagini "multiscopo", ha invitato l'Istat a prestare particolare attenzione nella scelta degli organismi esterni ai quali affidare le fasi di rilevazione, assicurandosi che possiedano requisiti di esperienza, capacità ed affidabilità tali da fornire idonee garanzie del pieno rispetto delle istruzioni ricevute e tenendo conto della delicatezza delle rilevazioni loro affidate. Sono state inoltre fornite indicazioni in relazione a rilevazioni che, seppur non concernenti dati sensibili, riguardino tuttavia informazioni suscettibili di ledere la dignità di chi è chiamato a rispondere.

Per quanto riguarda il quattordicesimo censimento generale della popolazione, sono state sottoposte all'esame dell'Autorità le modalità di diffusione e comunicazione dei dati censuari in favore degli enti della rete di rilevazione, con particolare riferimento ai comuni sprovvisti dell'ufficio di statistica, al fine di contemperare il fabbisogno informativo statistico locale con le disposizioni stabilite a tutela del segreto statistico e della riservatezza dei dati personali.

5.2. *Ricerca medica, biomedica ed epidemiologica*

Nell'ambito della ricerca medica, biomedica ed epidemiologica, oltre all'entrata in vigore del codice deontologico sulla ricerca statistica e scientifica (1° ottobre 2004), occorre più in generale ricordare la disciplina di favore del Codice (art. 110).

Sperimentazioni cliniche

In proposito, con riferimento alla richiesta di una Asl volta ad ottenere l'autorizzazione per l'avvio di una sperimentazione, l'Ufficio ha ricordato che i trattamenti di dati sulla salute effettuati per scopi di ricerca scientifica finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico sono consentiti previa acquisizione del consenso informato delle persone interessate e nel rispetto delle prescrizioni dell'autorizzazione generale n. 2/2004 (*Nota* 30 agosto 2004). Non occorre pertanto un'apposita autorizzazione dell'Autorità laddove il trattamento di queste informazioni venga effettuato in presenza dei presupposti di liceità sopra richiamati e sia altresì conforme alla disciplina sulle sperimentazioni cliniche di medicinali (v. in particolare, il d.lg. 24 giugno 2003, n. 211, ove applicabile).

Comunicazioni *ex* art. 39

Nel corso del 2004 sono pervenute all'Autorità numerose comunicazioni, inoltrate ai sensi dell'art. 39, comma 1, lett. *b*), del Codice. Al riguardo, l'Ufficio ha dovuto precisare in più occasioni che la possibilità di trattare dati sulla salute a prescindere dal consenso degli interessati per scopi di ricerca medica, biomedica ed epidemiologica, è un'ipotesi residuale prevista dal Codice nel caso in cui la ricerca rientri in uno dei programmi di ricerca biomedica o sanitaria. Soltanto in questa evenienza il titolare è

tenuto ad informarne preventivamente il Garante ai sensi dell'art. 39, comma 1, lett. *b*), specificando quali trattamenti intende effettuare senza il consenso degli interessati e la correlazione della ricerca con un programma previsto dall'art. 12-*bis*, d.lg n. 502/1992. Il trattamento potrà poi essere avviato trascorsi 45 giorni da tale comunicazione, a meno che l'Autorità si opponga entro il medesimo termine oppure con successiva determinazione (v., ad esempio, *Nota* 28 ottobre 2004).

In occasione di una comunicazione, ai sensi del medesimo art. 39, comma 1, lett. *b*), concernente la realizzazione di un progetto di ricerca sulla congruità delle prescrizioni farmaceutiche nell'ambito di un programma di ricerca biomedica e sanitaria, l'Autorità ha ricordato che, nel caso in cui le modalità di trattamento previste dal progetto implichino la possibilità di identificare gli interessati, sia pure indirettamente (ad esempio, mediante il riferimento al numero identificativo della cartella detenuta dal medico aderente alla ricerca o anche solo al numero identificativo dello stesso medico), i dati oggetto di trattamento non hanno la natura di "dati anonimi", trattandosi piuttosto di dati personali non direttamente identificativi (art. 4, comma 1, lett. *b*) del Codice).

Quando le informazioni trattate sono idonee a rivelare lo stato di salute degli interessati (poiché, ad esempio, si riferiscono alle patologie che hanno giustificato le prescrizioni mediche), è necessario altresì limitare il trattamento, nelle fasi sia della raccolta sia dell'utilizzo, ai soli dati strettamente indispensabili al raggiungimento delle finalità perseguite, in armonia con i principi di indispensabilità, necessità, pertinenza e non eccedenza dei dati (artt. 3, 11 e 22 del Codice) (*Nota* 28 ottobre 2004).

In un'altra vicenda sottoposta all'esame dell'Autorità, l'Ufficio ha specificato che, nel caso in cui siano coinvolti nella ricerca vari soggetti, occorre indicare nella comunicazione inoltrata all'Autorità ai sensi dell'art. 39 del Codice quali, tra questi, è il titolare del trattamento. Il titolare e, se designato, il responsabile del trattamento devono essere inoltre indicati nell'informativa specifica resa agli interessati ai sensi degli artt. 13, 78, comma 5, e 79 del Codice (*Nota* 14 dicembre 2004).

Registri tumori

Prosegue l'esame delle questioni relative al trattamento dei dati effettuato per la tenuta e la gestione dei registri tumori. Al riguardo, sono stati curati ulteriori approfondimenti al fine di verificare in quale misura le operazioni connesse alla tenuta ed alla gestione di tali banche dati possano considerarsi comprese tra le attività di rilevante interesse pubblico individuate dal Codice (in particolare, dall'art. 98).

In un caso riguardante il trattamento dei dati sulla salute dei pazienti coinvolti in un programma di prevenzione dei tumori sono stati avviati accertamenti nei confronti di una Asl e dell'associazione che, per suo conto, ha svolto le attività di gestione delle visite mediche e delle schede dei pazienti, con particolare riferimento al rispetto delle cautele poste dal Codice in materia di informativa, consenso e adozione delle misure di sicurezza (*Nota* 24 novembre 2004).

Sorveglianza epidemiologica

L'Autorità ha avviato anche approfondimenti volti a verificare l'idoneità delle disposizioni di una legge della Regione Piemonte a legittimare, ai sensi dell'art. 20 del Codice, il trattamento dei dati sulla salute necessario per la gestione di un sistema di sorveglianza epidemiologica delle malattie sessualmente trasmissibili, anche in considerazione della mancanza di attribuzioni regionali a disciplinare, sia pure indirettamente, la materia della protezione dei dati personali e tenuto conto che, per alcune delle patologie interessate dal sistema di sorveglianza regionale, è già operativo un sistema nazionale di sorveglianza epidemiologica sulle malattie infettive e diffusive che prevede soltanto la rilevazione di dati anonimi (artt. 253 e 254, r.d. n. 1265/1934; d.m. 5 luglio 1975 e 15 dicembre 1990).

Su richiesta del Ministero della difesa, l'Autorità si è pronunciata sul flusso di dati necessario all'attuazione delle disposizioni legislative che hanno previsto la realizzazione di una "campagna di monitoraggio" sulle condizioni sanitarie dei cittadini italiani operanti a qualunque titolo in Bosnia-Herzegovina e in Kosovo (art. 4-*bis*, decreto-legge 29 dicembre 2000, n. 393, convertito, con modificazioni, dalla legge 28 febbraio 2001, n. 27). La questione concerne profili particolarmente delicati attinenti ai diritti della personalità dei soggetti inclusi nel monitoraggio sui quali l'Autorità non è stata coinvolta in sede di emanazione del d.m. 22 ottobre 2002 del Ministro della salute che dà attuazione alle citate disposizioni legislative.

Al riguardo, pur comprendendo la rilevanza delle finalità perseguite dall'iniziativa, il Garante ha rilevato che, in considerazione dei delicati aspetti su cui essa incide, il quadro normativo deve essere perfezionato al fine di garantire i diritti delle persone interessate.

La norma di legge che ha previsto il monitoraggio non individua, infatti, gli obiettivi dell'iniziativa, né fissa i criteri generali sulle relative modalità di attuazione. In base a tale previsione sarebbe consentita una semplice rilevazione dei dati numerici dei casi eventualmente accertati, senza alcun riferimento ai dati personali. Laddove, invece, l'utilizzo di dati sulla salute sia ritenuto indispensabile per svolgere l'attività di monitoraggio, non essendo sufficiente il trattamento di dati anonimi o di dati personali di natura diversa (art. 22, comma 3, del Codice), è necessario tenere presente il sistema di garanzie previsto dal Codice per il trattamento dei dati sensibili da parte dei soggetti pubblici (attraverso i regolamenti di cui all'art. 20 del medesimo Codice). Inoltre, devono essere introdotte specifiche cautele volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, avendo cura, in particolare, di fornire un'idonea informativa agli interessati e di conservare i dati nel rispetto delle rigorose misure di sicurezza previste per il trattamento dei dati sanitari.

6 Attività di polizia

6.1. *Il controllo sul Centro elaborazione dati del Dipartimento di p.s.*

Anche nel 2004 l'Autorità ha ricevuto alcune segnalazioni, talvolta presentate direttamente al Garante o adesso a seguito di istanze di accesso rivolte al Dipartimento della pubblica sicurezza, con le quali gli interessati hanno fatto presente la registrazione nel Centro elaborazioni dati (C.e.d.) di dati inesatti, incompleti ovvero non aggiornati, per lo più in riferimento a provvedimenti giudiziari o amministrativi adottati e non registrati (art. 10, legge 1° aprile 1981, n. 121, modificato dall'art. 42, l. n. 675/1996 e, da ultimo, dall'art. 175, comma 3, del Codice).

In più occasioni l'Autorità ha sottolineato che anche i trattamenti effettuati da organi o uffici di polizia concernenti dati memorizzati nel predetto C.e.d. ovvero trattati per finalità di prevenzione, accertamento o repressione dei reati devono essere effettuati nel rispetto dei principi di liceità, pertinenza e non eccedenza. L'Autorità ha richiamato l'attenzione degli uffici sulla necessità di verificare con cadenza periodica la rispondenza dei dati trattati a tali principi, apportandovi le modifiche richieste e necessarie o cancellando i dati detenuti, specie in ragione degli esiti processuali a volte documentati dagli stessi interessati.

Dal 1° gennaio 2004, con l'entrata in vigore del Codice, tali indicazioni hanno trovato ulteriore rafforzamento, in linea con quelle fornite dal Garante.

Interrogazioni di altre banche dati

Il Codice ha previsto che il C.e.d. del Dipartimento della pubblica sicurezza debba assicurare, in misura più incisiva rispetto al passato, l'aggiornamento periodico e la pertinenza e non eccedenza dei dati trattati anche attraverso interrogazioni di altre banche dati, come il casellario giudiziale e quello dei carichi pendenti del Ministero della giustizia, al fine di garantire il costante "allineamento" delle informazioni registrate nel C.e.d. con quelle conservate in altri archivi (art. 54, comma 3, del Codice).

L'obbligo di verificare periodicamente il rispetto dei principi descritti nell'art. 11 del Codice è previsto anche per i singoli organi e uffici di polizia, i quali potranno avvalersi delle risultanze del C.e.d. e dovranno, in caso di trattamenti di dati effettuati con mezzi diversi da quelli elettronici, annotare o integrare i documenti cartacei che li contengono (art. 54, comma 4, del Codice).

L'importanza attribuita dal Codice a tali garanzie è testimoniata dalla previsione di un regolamento governativo che dovrà sviluppare l'applicazione dei descritti principi ai trattamenti effettuati per finalità di polizia, prevedendo, fra l'altro, più precisi termini di conservazione dei dati e specifiche modalità di aggiornamento periodico e di verifica della pertinenza dei dati stessi rispetto alla finalità perseguita (art. 57 del Codice).

In considerazione della particolare importanza che assume la corretta applicazione dei principi di protezione dei dati personali in tale settore, l'Autorità intende fornire in materia altre utili indicazioni al Governo, anche in occasione del rilascio del parere sullo schema di regolamento che dovrà essere richiesto al Garante ai sensi dell'art. 154, comma 4 del Codice.

Accesso ai dati conservati nel C.e.d.

Il Codice ha ulteriormente valorizzato le garanzie per l'interessato in materia di accesso ai dati personali che lo riguardano, in riferimento alla circostanza che la disciplina vigente per l'accesso ai dati conservati nel C.e.d. si applica anche ai dati comunque trattati da organi o uffici di polizia con l'ausilio di strumenti elettronici, nonché a quelli –già espressamente considerati in passato– destinati a confluire nel C.e.d. medesimo (art. 10, commi 3, 4 e 5, l. n. 121/1981 e art. 56 del Codice).

A fronte dell'accresciuto quadro di garanzie, il Garante, nell'esaminare alcune segnalazioni pervenute, ha non di rado constatato l'inadeguatezza del riscontro fornito dal competente ufficio della pubblica sicurezza alle richieste di accesso, di rettifica o di cancellazione dei dati registrati nel C.e.d. presentate dall'interessato.

In alcuni casi, infatti, contrariamente a quanto chiaramente previsto dallo stesso art. 10 della l. n. 121/1981, l'ufficio competente non ha fornito all'interessato la "comunicazione in forma intellegibile" dei dati registrati nel C.e.d.; in altri, la richiesta di modifica o di cancellazione dei dati, benché supportata da documentati esiti processuali, è stata riscontrata con la sola, generica comunicazione che la posizione dell'interessato nella banca di dati risultava aggiornata o che erano state apportate le richieste modifiche ai dati. L'Autorità intende avviare un ciclo generale di accertamenti e verifiche presso gli archivi del C.e.d. tenendo conto del numero ingente di casi per i quali il riscontro fornito dal Dipartimento non è risultato soddisfacente, al fine di verificare l'effettiva corrispondenza delle operazioni compiute dal Dipartimento della pubblica sicurezza alle richieste di rettifica o di cancellazione dei dati presentate dagli interessati e, più in generale, affinché i trattamenti effettuati nell'ambito del C.e.d. si svolgano nel tempestivo e sostanziale rispetto delle garanzie previste dal Codice.

Particolari tecnologie

Sempre nel quadro delle più ampie garanzie previste dal Codice, deve essere prestata particolare attenzione a taluni trattamenti effettuati per finalità di polizia che presentano maggiori rischi per l'interessato in quanto riferiti a dati genetici, biometrici o effettuati mediante tecniche basate su dati relativi all'ubicazione.

Per tali trattamenti l'Autorità intende prescrivere, anche su comunicazione degli organi interessati, particolari misure ed accorgimenti a garanzia dell'interessato (artt. 55 e 17, del Codice) ed ha già segnalato la necessità di individuare tali misure in relazione alla raccolta dei rilievi dattiloscopici effettuata in occasione del rilascio o del rinnovo del permesso di soggiorno agli stranieri e all'eventuale inserimento dei dati biometrici nel documento di soggiorno elettronico.

6.2. *Controllo sui trattamenti effettuati dai servizi di informazione e di sicurezza*

Il Garante ha svolto anche nel periodo di riferimento l'attività di verifica su specifici trattamenti di dati personali effettuati presso gli organismi competenti in materia di informazioni e di sicurezza (SISMI, SISDE e CESIS), disciplinati ora dall'art. 58 del Codice.

Questa disposizione, oltre a specificare quali regole del Codice sono applicabili a tali trattamenti, stabilisce che, con decreto del Presidente del Consiglio, si provveda ad individuare le misure minime di sicurezza e le modalità di applicazione a tali trattamenti delle pertinenti disposizioni del Codice. La previsione di tali decreti assume particolare importanza per assicurare, anche in sintonia con orientamenti giurisprudenziali internazionali in materia di tutela dei diritti dell'uomo, trasparenza ai trattamenti effettuati per tali finalità, in relazione ai tipi di operazioni e di dati trattati, l'aggiornamento e la corretta conservazione dei dati mede-

simi. L'Autorità si accinge quindi a prestare la propria collaborazione a partire dai profili relativi alle misure di sicurezza.

Il Garante ha effettuato gli accertamenti rispetto alle segnalazioni presentate dai soggetti interessati, in conformità a quanto previsto dal Codice (art. 160) e con le modalità già osservate nel corso dei precedenti anni.

I controlli, che hanno fatto seguito a quelli effettuati nel marzo 2003, sono stati concentrati nel quinto gruppo di verifiche effettuate dal Garante a decorrere dalla sua istituzione (per un totale di circa 40 persone che hanno chiesto accertamenti) e si sono svolti con la piena collaborazione dei predetti organismi, permettendo di fornire un riscontro dell'attività svolta agli interessati nei particolari termini previsti dal Codice all'esito degli accertamenti.

6.3. *Il controllo sul Sistema di informazione Schengen*

Il Codice ha introdotto importanti modifiche alle modalità di esercizio del diritto di accesso al Sistema di informazione Schengen (SIS) e degli altri diritti connessi (rettifica, integrazione o cancellazione), che possono ora essere esercitati direttamente nei confronti dell'autorità di polizia (c.d. accesso "diretto") e non più solo "per il tramite" del Garante (c.d. accesso "indiretto").

Accesso diretto

Come riportato più diffusamente nella *Relazione 2003*, il Codice ha stabilito (in linea con le scelte effettuate da gran parte dei paesi di "area Schengen") che l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del Sis, ossia il Dipartimento della pubblica sicurezza, fermo restando il diritto di proporre una segnalazione o un reclamo al Garante in caso di mancata o incompleta risposta.

In vista dell'entrata in vigore della nuova normativa il Garante, sulla base dell'esperienza, ha suggerito al Ministero dell'interno e all'Ufficio visti del Ministero degli affari esteri accorgimenti idonei ad assicurare ai richiedenti l'accesso un riscontro completo e tempestivo, anche attraverso il ricorso a moduli prestampati. A seguito delle indicazioni fornite dall'Autorità, il Dipartimento della pubblica sicurezza ha designato la Divisione N-SIS dell'Ufficio coordinamento e pianificazione delle forze di polizia quale ufficio preposto a ricevere le richieste di accesso, mentre il Ministero degli affari esteri ha comunicato alle ambasciate e alle cancellerie le necessarie misure operative, riformulando l'informativa da inserire sui provvedimenti di diniego di visto in modo da orientare più correttamente l'esercizio del diritto di verifica delle segnalazioni.

Il Garante ha reso nota al pubblico la nuova procedura (anche mediante *Newsletter*) pubblicando sul proprio sito *web*, in italiano e in inglese, una breve informativa con alcune indicazioni volte ad agevolare l'inoltro delle richieste di verifica, consultabile nella *home-page* del sito dell'Autorità (*www.garanteprivacy.it*); ad essa ha fatto riferimento anche il Ministero degli affari esteri nell'ambito delle direttive impartite agli uffici consolari.

Delle novità introdotte dal Codice l'Autorità ha poi informato le autorità nazionali di controllo sulla protezione dei dati, con le quali è stata instaurata una significativa collaborazione nell'ambito della procedura di coordinamento prevista dall'art. 114 della Convenzione di Schengen al fine di definire le indicazioni che tali autorità possono fornire agli interessati che richiedano assistenza per l'inoltro di richieste di accesso al SIS.

In proposito, l'Autorità ha registrato la fattiva collaborazione della Divisione N-SIS

del Dipartimento della pubblica sicurezza nell'applicazione della nuova normativa.

Su specifica indicazione fornita dall'Autorità, la Divisione N-SIS informa per conoscenza il Garante su ogni richiesta di accesso ricevuta e sul relativo riscontro fornito, in modo da consentire all'Autorità un efficace monitoraggio e controllo di tutte le richieste di accesso presentate. Quest'ultima, a sua volta, trasmette al predetto ufficio le richieste di semplice verifica dei dati che continuano a pervenire assai numerose probabilmente a causa di una ancora incompleta conoscenza (specie in paesi terzi) delle nuove modalità di accesso "diretto" introdotte dal Codice (dal 1° gennaio 2004 al 31 dicembre 2004 risultano pervenute al Garante circa 300 richieste).

Si tratta in gran parte di domande presentate a seguito di diniego del rilascio di visti, per lo più in conseguenza di segnalazioni dovute alla non ammissione nei Paesi Schengen di persone nei cui confronti sono stati emessi provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno (espulsione, respingimento alla frontiera). In altri casi si tratta di asserite usurpazioni d'identità o di omonimie in relazione alle quali è stata ulteriormente rafforzata la collaborazione con il Centro visti del Ministero degli affari esteri e con la Direzione centrale per l'immigrazione e la polizia delle frontiere del Dipartimento della pubblica sicurezza.

Valutazione Schengen in Italia

Nei mesi di settembre e ottobre, l'Italia è stata oggetto della visita di valutazione da parte di gruppi di esperti del Consiglio dell'Unione europea. Il Consiglio ha infatti costituito da alcuni anni un gruppo per la valutazione Schengen che sta procedendo ad un esame, paese per paese, del funzionamento di tutti gli elementi che compongono il sistema: visti, frontiere esterne, SIS e SIRENE.

Una delle visite era espressamente dedicata alla verifica del rispetto delle norme italiane in materia di protezione dei dati personali; in particolare, ha riguardato le modalità di inserimento dei dati nel SIS nazionale, quelle di accesso ai dati contenuti nel sistema, le misure di protezione da accessi indesiderati e le misure di sicurezza dei sistemi e delle reti.

Attenzione è stata anche dedicata all'incontro con il Garante nella sua qualità di autorità nazionale di controllo sul SIS; dopo la presentazione svolta dal segretario generale dell'Autorità, sono state soddisfatte diverse domande tese a verificare il grado di effettiva indipendenza dell'Autorità (come, ad esempio, in merito a: disponibilità di una sede idonea, adeguatezza delle risorse finanziarie, possibilità di scelta del proprio personale e numero di persone in servizio) e le modalità di esercizio del suo ruolo di controllo sulla correttezza dei trattamenti.

Il rapporto redatto dagli esperti al termine della visita esprime una valutazione positiva pur contenendo alcuni inviti agli uffici di polizia che gestiscono il sistema informativo a migliorare la protezione dei dati da accessi non autorizzati e a controllare, in particolare, i dati inseriti dall'Italia nel SIS, numericamente superiori a quelli di qualsiasi altro paese Schengen, verificando la necessità del loro mantenimento nel sistema. Su questo aspetto il Garante stà eseguendo un dettagliato lavoro di verifica concordato con l'Autorità comune di controllo Schengen.

6.4. *Altri casi di intervento del Garante in relazione a diverse attività svolte dalle forze di polizia*

Foto segnaletiche

L'Autorità è nuovamente intervenuta in merito alla diffusione da parte di organi di polizia di immagini e, specialmente, di foto segnaletiche di persone coinvolte in attività di polizia (in particolare con riferimento ad una vicenda giudiziaria che ha coinvolto anche alcuni personaggi del mondo dello spettacolo). Il Garante ha sot-

tolineato –in linea con quanto già avvenuto in precedenti occasioni– che la diffusione di immagini di persone coinvolte in indagini o altri accertamenti è consentita agli organi di polizia solo per finalità di giustizia o di polizia e comunque nel rispetto della dignità della persona arrestata o altrimenti detenuta (cfr. art. 97, legge 22 aprile 1941, n. 633 sul diritto d'autore e art. 42-*bis*, legge 26 luglio 1975, n. 354). A seguito dell'intervento del Garante, le amministrazioni interessate hanno nuovamente richiamato il personale di polizia al rispetto della normativa vigente e delle cautele indicate dall'Autorità.

L'orientamento dell'Autorità ha trovato da ultimo conferma in una pronuncia della Corte europea dei diritti dell'uomo.

Trasmettere agli organi di stampa fotografie di una persona accusata in un procedimento penale costituisce infatti una violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo.

Il principio è stato affermato in una recente sentenza della Corte europea (50774/99, 11 gennaio 2005) originata dal ricorso di un'insegnante italiana –fermata e posta agli arresti domiciliari con l'accusa di associazione a delinquere, evasione fiscale e falso in bilancio– la cui fotografia, scattata durante le indagini, era stata diffusa nel corso di una conferenza stampa delle forze dell'ordine e quindi pubblicata su diverse edizioni di due quotidiani locali.

I giudici hanno messo in evidenza che, rispetto ad altri casi oggetto di precedenti pronunce della Corte (cfr. von Hannover/Germania, 59320/00, 24 giugno 2004), la fattispecie in esame presentava alcune peculiarità: essa, in primo luogo, non riguardava un personaggio pubblico; inoltre, la foto pubblicata proveniente dal fascicolo d'inchiesta era stata fornita ai giornali da agenti della Guardia di finanza.

Il fatto che nel caso di specie la ricorrente non fosse un personaggio pubblico giustifica –secondo la Corte– una contrazione della legittima "zona di interazione tra l'individuo e i terzi" (più ampia, evidentemente, nel caso di persone note) che non può espandersi in ragione del coinvolgimento della donna in un procedimento penale.

I giudici, inoltre, ravvisando l'inapplicabilità al caso di specie dell'art. 329 c.p.p. (obbligo del segreto per gli atti d'indagine), non hanno riscontrato la presenza di previsioni normative nell'ordinamento italiano che nella fattispecie in esame giustificassero, ai sensi del secondo comma dell'art. 8 della Convenzione, l'ingerenza nella vita privata della ricorrente.

Osservatorio appalti nel Mezzogiorno

Nell'ambito dei trattamenti svolti per finalità di polizia, il Ministero dell'interno ha sottoposto all'esame dell'Autorità la realizzazione di un sistema automatizzato di supporto alle decisioni per garantire trasparenza e sicurezza degli appalti nel Mezzogiorno che comporta l'acquisizione di dati da numerose altre pubbliche amministrazioni. Il Garante ha proposto l'avvio di un tavolo di lavoro finalizzato all'individuazione di una soluzione idonea a realizzare tale iniziativa nel pieno rispetto delle garanzie previste dal Codice (*Nota* 4 ottobre 2004).

L'Autorità ha altresì avviato specifici accertamenti in merito ad un progetto finanziato dall'Unione europea volto alla prevenzione ed alla repressione da parte delle forze di polizia del traffico di stupefacenti tra alcuni porti dell'Adriatico attraverso l'utilizzo di tecnologie informatiche di ultima generazione.

Cessione di fabbricati

Il Ministero dell'interno e la Questura di Genova hanno chiesto al Garante se i dati contenuti nelle comunicazioni di cessione di fabbricati di cui al decreto-legge 21 marzo 1978, n. 59, convertito in legge, con modificazioni, dalla legge 18 maggio 1978, n. 191, delle quali il sindaco è destinatario ai sensi dell'art. 15, comma 2, della l. n. 121/1981, potessero essere utilizzati dal comune per lo svol-

gimento di controlli di natura fiscale e tributaria.

L'Autorità ha chiarito che la disciplina da ultimo menzionata consente l'utilizzo delle informazioni contenute nel C.e.d. del Dipartimento di pubblica sicurezza esclusivamente per finalità di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità e ne vieta la circolazione all'interno della pubblica amministrazione (*Nota* 5 ottobre 2004).

Collaborazione con il Ministero dell'interno

L'Autorità è stata contattata dal Ministero dell'interno per approfondire le modalità di attuazione della normativa in materia protezione dei dati personali nell'ambito delle prefetture, con particolare riferimento ai trattamenti non finalizzati alla tutela della sicurezza e dell'ordine pubblico ovvero alla prevenzione, accertamento e repressione dei reati e, quindi, soggetti all'integrale applicazione del Codice.

Accesso ai dati anagrafici

Alcuni quesiti riguardano ancora le richieste delle autorità di pubblica sicurezza e delle forze di polizia volte ad acquisire informazioni e documenti riguardanti cittadini detenuti dagli uffici comunali. In proposito è stato in più occasioni ricordato che, fermo restando il divieto per le persone estranee all'ufficio di anagrafe di accedere all'ufficio stesso e, quindi, di procedere alla consultazione diretta degli atti anagrafici, le persone appositamente incaricate dall'autorità giudiziaria e gli appartenenti alle forze dell'ordine ed al Corpo della Guardia di finanza possono legittimamente consultare tali informazioni. In tal caso, tuttavia, i nominativi delle persone autorizzate ad effettuare la consultazione diretta degli atti anagrafici devono figurare in apposite richieste dell'ufficio o del comando di appartenenza, da esibire all'ufficiale di anagrafe unitamente ad un documento di riconoscimento (art. 37, d.P.R. 30 maggio 1989, n. 223).

Inoltre, il Codice prevede che, in conformità alla legge ed ai regolamenti, tale acquisizione possa altresì essere realizzata per via telematica attraverso convenzioni, anche con schemi tipo adottati dal Ministero dell'interno su conforme parere del Garante, a condizione che le modalità di collegamento previste assicurino un accesso selettivo ai soli dati necessari al perseguimento delle finalità di sicurezza ed ordine pubblico, nonché di prevenzione, accertamento e repressione dei reati (artt. 3, 11 e 54, del Codice).

Monitoraggio della spesa sanitaria

Prosegue, infine, l'attività di verifica dell'Autorità sui protocolli di intesa sottoscritti tra le regioni, le Asl e la Guardia di finanza ai fini del coordinamento dei controlli e dello scambio di informazioni in materia di spesa sanitaria che presentano diversi elementi critici sul piano della proporzionalità e liceità delle modalità di trattamento previste.

7 Attività giornalistica e mezzi di informazione

7.1. *Profili generali*

Il Codice in materia di protezione dei dati personali ha confermato il principio in base al quale chi esercita l'attività giornalistica o altra attività comunque riconducibile alla libera manifestazione del pensiero (inclusa l'espressione artistica e letteraria, come ora precisato dall'art. 136 del Codice) può trattare dati personali anche prescindendo dal consenso dell'interessato e, con riferimento ai dati sensibili e giudiziari, senza una preventiva autorizzazione di legge o del Garante. A fronte di queste esenzioni e deroghe si pone, tuttavia, l'obbligo di rispettare alcune condizioni: i limiti al diritto di cronaca già individuati in passato da una consolidata giurisprudenza; il requisito dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice); i principi previsti dal codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (adottato con provvedimento del Garante del 29 luglio 1998, all. A1 al Codice).

A distanza di sei anni dall'entrata in vigore del codice deontologico è stato costituito un gruppo di lavoro tra l'Autorità e l'Ordine nazionale dei giornalisti che si è occupato di analizzarne i principali profili applicativi. Per rispondere ai quesiti posti in quella sede, il 6 maggio 2004 il Garante ha approvato un documento *("Privacy e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti")* con il quale sono state fornite ulteriori precisazioni in merito al corretto utilizzo dei dati personali da parte dei giornalisti, specie in riferimento ad aspetti di particolare problematicità, quali la diffusione di fotografie, la pubblicazione dei nomi delle persone coinvolte in vicende giudiziarie, la diffusione di dati relativi allo stato di salute e alla vita sessuale, i margini di accessibilità da parte dei giornalisti alle informazioni detenute dalle pubbliche amministrazioni.

7.2. *Tutela dei minori*

La particolare tutela accordata ai minori dal Codice è stata richiamata dal Garante con interventi incisivi anche nel corso del 2004.

Si tratta di un settore in cui la vigente normativa in materia di tutela dei dati individua più chiaramente le coordinate entro cui il giornalista (o un soggetto ad esso equiparato ai sensi dell'art. 136 del Codice) è tenuto ad operare.

Il codice deontologico e la Carta di Treviso (da questo richiamata) stabiliscono con nettezza che il diritto del minore (anche quando si trovi coinvolto in fatti di cronaca che non costituiscono reato) alla riservatezza prevale sul diritto di critica e di cronaca. Il Codice ha rafforzato tali garanzie estendendo il divieto di pubblicare con qualsiasi mezzo notizie e immagini idonee a consentire l'identificazione di un minore (già affermato con l'art. 13, d.P.R. 22 settembre 1988, n. 448) anche nel caso in cui esso sia coinvolto a qualunque titolo in procedimenti giudiziari in materie diverse da quella penale (art. 50).

Il Garante ha adottato in proposito specifici provvedimenti di divieto della diffusione di dati idonei a rendere il minore, anche solo indirettamente, identificabile

(si pensi al caso, ad esempio, della pubblicazione di informazioni idonee ad identificare i genitori o afferenti al contesto ambientale e sociale in cui vive). Il divieto di diffusione del resto è posto, in caso di abusi sessuali subiti dal minore, anche da altre norme dell'ordinamento (*Provv.* 12 marzo 2004 e 6 aprile 2004).

Può inoltre rivelarsi necessaria l'adozione di cautele anche nella divulgazione dei dati identificativi di soggetti che risultano indagati per reati di siffatta natura pur quando non operino in tal senso specifiche limitazioni di legge (*Newsletter* 8-11 novembre 2004).

Come è stato chiarito nel documento del 6 maggio 2004, i limiti posti alla diffusione dei dati e delle immagini riguardanti i minori non sono assoluti; essa, infatti, può avvenire in casi particolari in cui un servizio giornalistico ritrae il minore in momenti di svago e di gioco o dà comunque positivo risalto a sue qualità e/o al contesto familiare in cui va formandosi, sempre che i dati siano stati raccolti nel rispetto del principio di correttezza. In linea con i principi generali della normativa in materia di tutela dei dati, il giornalista dovrà tuttavia valutare, anche in queste specifiche ipotesi, l'eventuale opposizione al trattamento manifestata dal minore o da chi ne esercita la potestà genitoriale.

7.3. *Cronache giudiziarie*

Come è noto, i dati giudiziari possono formare oggetto di trattamento per finalità di giornalismo (art. 137, comma 1, lett. *b*) del Codice), anche se nei limiti indicati dall'art. 12 del codice deontologico il quale, a sua volta, rinvia al principio di essenzialità dell'informazione. Tale disposizione va letta alla luce del Codice che estende ora la nozione di dati giudiziari, includendovi anche i dati idonei a rivelare la qualità di imputato e di indagato (art. 4, comma 1, lett. *e*), del Codice.

Continuano ad essere numerosi i reclami e le segnalazioni in relazione al trattamento di tali informazioni da parte degli organi di informazione. In questo ambito, indicazioni utili sono state fornite dal citato documento del 6 maggio 2004 che ha fornito chiarimenti sulle condizioni di liceità della diffusione di dati identificativi di persone arrestate o indagate, di foto segnaletiche e di altre immagini che documentano operazioni di arresto o altre attività processuali (ad es., la traduzione degli imputati), anche alla luce di norme diverse da quelle contenute nella normativa sulla protezione dei dati. Entro questi limiti è affidata alla responsabilità del giornalista la valutazione, caso per caso, dell'essenzialità della notizia (contenente il dato personale) in relazione all'interesse pubblico, ferma restando la completezza della medesima con riferimento alla corretta indicazione della fase del procedimento giudiziario di cui si dà notizia.

Non di rado i profili sollevati dai segnalanti in questo settore attengono alle modalità con cui vengono riportate le notizie, evidenziando possibili lesioni dell'onore e della reputazione dell'interessato piuttosto che problematiche attinenti alla protezione dei dati personali. Merita di essere segnalato a tal proposito il caso sottoposto all'attenzione del Garante (e in corso di accertamento) relativo alla diffusione del contenuto di intercettazioni telefoniche che consentivano l'accostamento del nome dell'interessato a quello dei componenti di un'organizzazione criminale. L'Autorità, ravvisata la liceità della raccolta dei dati dell'interessato in quanto desunti da atti conoscibili (ordinanza regolarmente depositata), ha ricordato nelle more che, fermo restando il diritto di chiedere la pubblicazione di una rettifica nei casi previsti dalla legge, la valutazione del carattere diffamatorio della notizia e dell'eventuale richiesta di risarcimento dei danni rimane di competenza dell'autorità giudiziaria ordinaria.

7.4. *Dati idonei a rivelare lo stato di salute*

Anche quest'anno l'Autorità ha richiamato i mezzi di informazione al rispetto della dignità e della libertà di autodeterminazione delle persone malate. In particolare, nel comunicato del 3 febbraio 2004 è stato stigmatizzato l'accanimento dei giornali sulla vicenda della donna che aveva espresso un rifiuto all'operazione di amputazione della gamba, ritenuta dai medici necessaria per salvarle la vita.

I medesimi principi sono alla base di un recente provvedimento con cui il Garante –al fine di prevenire il rischio di un possibile pregiudizio per l'interessato e in attesa di procedere ad ulteriori approfondimenti sul caso (art. 154, comma 1, lett. *d*), del Codice)– ha disposto il blocco temporaneo dell'ulteriore diffusione televisiva di immagini particolarmente invasive relative ad un uomo indigente, senza dimora, la cui identità sembrava corrispondere a quella di uno straniero assente da diversi anni dal proprio paese e di cui alcuni familiari avevano di recente intrapreso nuove ricerche (*Provv.* 8 novembre 2004).

7.5. *Libertà di informazione e personaggi pubblici*

Come più volte ricordato in passato, esistono alcuni margini più ampi per la diffusione di dati personali relativi a persone che godono di particolare notorietà (eventualmente anche in ambito locale), in ragione del ruolo o della funzione ricoperti. Questo diverso approccio opera solo quando l'informazione si riferisce al ruolo e alla vita pubblica di tali personaggi e non vengano diffuse informazioni relative a terzi. Tali principi, consolidatisi negli anni di applicazione del codice deontologico (artt. 10 e 11), sono stati ripresi nel documento del 6 maggio 2004, anche alla luce di quanto precisato dal Consiglio d'Europa (Dichiarazione del 12 febbraio 2004).

Questa "giurisprudenza" del Garante va ora misurata sulla recente sentenza della Corte europea dei diritti dell'uomo (von Hannover/Germania del 24 giugno 2004, citata nel par. 6.4) che si è pronunciata sulla controversa pubblicazione di una foto della principessa di Monaco ritratta in un momento della sua vita privata. La pronuncia conferma per un verso alcuni principi già espressi nella normativa italiana e ribaditi dal Garante in varie occasioni in merito ai presupposti di liceità per la raccolta (correttezza e trasparenza) e la diffusione delle fotografie nell'ambito di servizi giornalistici (tutela della dignità della persona; pertinenza e non eccedenza di eventuali dettagli fotografici). La decisione della Corte introduce però un'inedita distinzione tra trattamenti concernenti personaggi politici nell'esercizio delle loro funzioni e individui che, pur essendo figure pubbliche, non esercitano tali funzioni, invitando gli organi di informazione ad una maggiore cautela con riferimento alla diffusione di immagini e altri particolari che riguardano la vita privata di questi ultimi.

7.6. *Esercizio dei diritti e diritto all'oblio*

I diritti riconosciuti all'interessato dall'art. 7 del Codice trovano applicazione anche con riferimento ai trattamenti effettuati nell'ambito dell'attività giornalistica: al riguardo il Garante ha accolto due ricorsi presentati *ex* art. 145 del Codice in relazione a istanze di opposizione per motivi legittimi al trattamento rimaste insoddisfatte. La prima concerne la pubblicazione, da parte di un giornale locale, di dati idonei a rendere indirettamente identificabile una minore, vittima di reati sessuali

(*Provv.* 6 aprile 2004 sopra citato con cui, alla luce della speciale tutela accordata ai minori, è stato disposto il divieto di ulteriore trattamento dei dati). La seconda riguarda la ripetuta rievocazione, da parte di giornali a diffusione locale, di un episodio di grave aggressione subita in passato da una donna, ponendolo in connessione ad altri simili e più recenti fatti di cronaca. Il Garante, reputata fondata l'istanza dell'interessata, ha ritenuto ingiustificata la pubblicazione dei dati che la riguardavano (dati identificativi, residenza, particolari relativi allo stato di salute, fotografie) in ragione della loro eccedenza nonché dell'ampio lasso di tempo trascorso dall'episodio che aveva portato l'interessata all'attenzione della cronaca. L'Autorità ha così disposto il divieto di ulteriore trattamento dei dati della ricorrente e la cancellazione dei medesimi dalle pagine *web* delle relative testate giornalistiche (*Provv.* 15 aprile 2004).

Quest'ultima decisione ha riproposto la delicata tematica del cosiddetto "diritto all'oblio" su cui pure diversi quesiti, segnalazioni e reclami pervenuti al Garante hanno sollecitato un'ulteriore riflessione: in questo quadro giova ricordare le indicazioni contenute nel più volte citato documento del 6 maggio volte a sollecitare, da parte del giornalista, un'attenta ponderazione dell'essenzialità dell'informazione e del (rinnovato) interesse pubblico con riferimento a cronache di casi giudiziari risalenti nel tempo, con riguardo a persone condannate o assolte e, a maggior ragione, a soggetti estranei al processo rievocato (in questo senso possono segnalarsi alcuni accertamenti avviati dal Garante con riferimento a casi riproposti a distanza di tempo da una trasmissione televisiva).

Questo tema non può essere disgiunto dall'analisi dell'incidenza sul punto delle nuove tecnologie dell'informazione, in particolare nel caso di diffusione di informazioni tramite la rete Internet e conseguente utilizzo di motori di ricerca. Il nodo è venuto al pettine a proposito del ricorso proposto nei confronti dell'Autorità garante della concorrenza e del mercato cui si è già fatto cenno (v. par. 2.11).

8 Associazioni, movimenti politici e partiti

8.1. *Associazioni*

Con riferimento alle strutture associative, il trattamento dei dati personali non sensibili degli altri associati, o di soggetti che hanno contatti regolari con le associazioni, è consentito anche senza il consenso dell'interessato qualora riguardi il perseguimento di finalità lecite e sulla base di quanto previsto dall'atto costitutivo o dallo statuto dell'associazione, o in presenza di uno degli ulteriori presupposti di liceità previsti dalla normativa sul trattamento dei dati personali (ad es., per obblighi di legge o per esigenze di difesa in sede giudiziaria).

Sindacati, patronati e Caaf

Nell'ambito delle diverse iniziative dell'Autorità sul tema del trattamento di dati personali da parte delle realtà associative è da ricordare, tra l'altro, l'incontro avuto con i rappresentanti delle principali organizzazioni sindacali, e degli enti di patronato e dei "Centri autorizzati assistenza fiscale" (Caaf) ad essi collegati, finalizzato alla revisione dei testi di informativa e consenso inseriti nelle tessere di adesione al sindacato. I soggetti intervenuti hanno chiesto il supporto dell'Ufficio del Garante allo scopo di sciogliere alcuni nodi interpretativi circa l'applicazione delle norme del Codice, con particolare riferimento alla possibilità di adottare un'informativa semplificata e di trattare in alcuni casi (in presenza di idonee garanzie) i dati senza il consenso degli interessati.

Con riferimento al trattamento dei dati all'interno delle strutture territoriali in cui si articolano le organizzazioni sindacali, il Garante ha richiamato la novità introdotta dal Codice riguardo alla facoltà di designare gli incaricati non solo nominativamente, ma anche mediante atti di preposizione a specifiche funzioni interne o unità organizzative che effettuano particolari trattamenti di dati, nell'ambito e a cura di titolari di strutture organizzative complesse che abbiano però chiarito per iscritto quali trattamenti di dati possono essere effettuati presso le singole articolazioni.

L'Autorità ha inoltre confermato l'obbligo, per i sindacati e per gli enti cd. collaterali (patronati e Caaf) di adottare le misure minime di sicurezza previste dal Codice e dal disciplinare tecnico, incluso il Documento programmatico per la sicurezza.

CONI

L'Ufficio ha anche reso un parere in ordine alla possibilità per il CONI di richiedere ad un ente di promozione sportiva riconosciuto a livello nazionale i dati relativi agli iscritti delle società affiliate all'ente. In proposito, nel richiamare le previsioni in materia di trattamento dei dati personali degli aderenti da parte delle associazioni, si è precisato che i soggetti pubblici, quale è il CONI, non devono richiedere il consenso degli interessati per il trattamento di dati personali effettuato nello svolgimento delle proprie funzioni istituzionali (*Nota* 24 maggio 2004).

Consorzi

È peculiare il caso esaminato dall'Autorità, su richiesta di un consorzio al fine di fornire alcuni chiarimenti in merito alle modalità di trattamento di taluni dati personali: si trattava di informazioni relative alla denominazione e alla sede del macello e delle aziende dove è avvenuto l'ingrasso, da riportare nell'etichettatura cd. facoltativa delle carni bovine, la quale contiene informazioni ulteriori rispetto a quelle

obbligatoriamente prescritte, allo scopo di migliorare la trasparenza delle condizioni di produzione e di commercializzazione delle carni bovine. In proposito, l'Autorità ha fatto presente che l'adesione al consorzio da parte delle singole imprese era avvenuta su base contrattuale e che, pertanto, la diffusione dei dati riprodotti nelle etichette (facoltativi rispetto alla normativa, ma obbligatori per gli aderenti al consorzio) non richiede il consenso degli interessati in quanto necessaria per eseguire obblighi derivanti dal contratto (qui consortile) (art. 24, comma 1, lett. *b*), del Codice) (*Nota* 1° luglio 2004).

8.2. *Movimenti politici e propaganda elettorale*

Il Garante –specie in prossimità di tornate di consultazioni elettorali– ha analizzato diverse questioni legate al trattamento dei dati personali effettuato da partiti e singoli candidati nell'ambito della propaganda politica.

In particolare, con un provvedimento di carattere generale (*Provv.* 12 febbraio 2004, pubblicato in *G.U.* 24 febbraio 2004, n. 45 e riprodotto anche in *Documentazione* par. 38) adottato in vista delle elezioni europee ed amministrative indette per il 12 e 13 giugno 2004, l'Autorità ha indicato i casi in cui partiti, movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare dati personali a fini di propaganda informando gli interessati, ma senza richiedere il loro consenso, e i casi in cui, al contrario, il consenso è necessario.

In tale occasione il Garante ha sottolineato che si può prescindere dal consenso nelle ipotesi in cui i dati utilizzati siano estratti da registri, elenchi, atti o documenti detenuti da un soggetto pubblico e accessibili liberamente in base ad un'espressa disposizione di legge o di regolamento.

Il candidato o l'organismo politico, sia quando acquisisca direttamente i dati sia allorché si avvalga dei servizi offerti da un privato, rivestendo comunque la qualifica di "titolare del trattamento", ha l'onere di verificare che gli interessati siano stati adeguatamente informati e abbiano prestato un consenso idoneo, validamente espresso solo se manifestato specificamente e se è stata resa all'interessato una previa informativa.

A tal proposito, merita di essere altresì ricordato il più recente provvedimento del 12 ottobre 2004, relativo all'invio di messaggi a contenuto propagandistico effettuato da una società per conto di una formazione politica. In tal caso l'Autorità ha sottolineato che, anche se l'invio di messaggi è avvenuto a nome di quest'ultima ad opera di un terzo, è la formazione politica medesima che è, e rimane, titolare del trattamento in questione; ciò in quanto essa assume le decisioni di fondo su finalità e modalità del trattamento preordinato all'invio del messaggio propagandistico.

Alla luce di tale principio, il Garante ha quindi prescritto alla formazione politica, a nome della quale la società aveva inviato *e-mail* per finalità promozionali senza aver acquisito il previo consenso dell'interessato, di fornire un idoneo riscontro alle richieste presentate ai sensi degli artt. 7 ed 8 del Codice.

Il Garante è stato anche interpellato in ordine alla liceità dell'invio di messaggi di posta elettronica a fini di propaganda elettorale da parte di società concessionarie di pubblicità ad utenti che avevano invece precedentemente conferito il loro esplicito consenso a ricevere solo comunicazioni di carattere commerciale e informativo. A tal proposito è stato rilevato che l'inserzione di messaggi di propaganda, in particolare nelle *Newsletter* tematiche richieste da soggetti cui è stata fornita una specifica informativa collegata al solo fine commerciale, non permette di considerare autorizzata anche la propaganda politica elettorale, poiché ciò contrasterebbe

con le particolari garanzie che il Codice prevede in tema di posta elettronica, differenti da quelle previste per la propaganda cartacea basata sull'utilizzo di registri ed elenchi pubblici accessibili a chiunque. È comunque praticabile (in luogo dell'inserzione di messaggi di propaganda all'interno di *Newsletter* tematiche) richiedere agli abbonati una manifestazione integrativa del consenso basata su un supplemento di informativa riferito alla propaganda politico-elettorale (*Nota* 25 marzo 2004).

Sempre a tale riguardo, e in linea con il predetto orientamento, in una successiva nota è stato precisato che non è sostenibile un accostamento tra le inserzioni pubblicitarie su quotidiani acquistati in modo anonimo presso un'edicola e i contenuti dei messaggi inviati nominativamente ad indirizzi di posta elettronica ad utenti che abbiano ricevuto un'informativa specifica riguardante solo attività commerciali o specifiche attività informative che nulla hanno a che vedere con la sfera politico-elettorale (*Nota* 7 aprile 2004).

9 Attività economiche

9.1. *Trattamenti in ambito bancario e finanziario*

Accesso ai dati personali in ambito bancario

Gli strumenti di tutela offerti dal Codice vengono utilizzati sempre più ampiamente nel settore bancario e finanziario: una problematica ricorrente è rappresentata dal rapporto tra il diritto di accesso ai dati personali detenuti da istituti di credito, specificamente disciplinato dagli artt. 7 e seguenti del Codice, ed il (diverso) diritto di ottenere copia della documentazione relativa ad operazioni bancarie, riconosciuto dall'art. 119, comma 4, d.lg. n. 385/1993 (T.U. in materia bancaria e creditizia).

In proposito, rispondendo anche ad alcune segnalazioni pervenute, nonché, in particolare, ad un quesito della Banca d'Italia, l'Autorità ha confermato l'alterità delle due figure in quanto il diritto di accesso previsto dal Codice si riferisce solo ai dati personali e non agli atti o documenti che li contengono, diversamente dal diritto, accordato dal menzionato art. 119, comma 4, d.lg. n. 385/1993, in base al quale il cliente, o colui che gli succede a qualunque titolo o colui che subentra nell'amministrazione dei suoi beni, possono *"ottenere, a proprie spese, entro un congruo termine e comunque non oltre novanta giorni, copia della documentazione inerente a singole operazioni poste in essere negli ultimi dieci anni"* (*Nota* 6 agosto 2004).

Si è così ribadita la posizione consolidata dell'Autorità, precisando anche che il diritto di accesso ai dati personali comporta l'obbligo per il titolare del trattamento (in questi casi, le banche) di estrarre i dati e di trasporli, se vi è richiesta, su un supporto cartaceo o informatico, ma non l'obbligo di esibire o consegnare, anche in copia, gli atti e documenti che li contengono (a meno che risulti particolarmente difficoltosa l'estrazione dei dati dai medesimi atti o documenti e non sia parimenti possibile la loro trasmissione per via telematica: art. 10, comma 4, del Codice).

Il diritto di accesso riguarda, di norma, unicamente i dati riferiti all'interessato. Soltanto in casi particolari, nei quali risulti impossibile per la banca estrarre o trasporre singoli dati, può rendersi necessario far visionare o trasmettere, in tutto o in parte, atti o documenti che possono riguardare anche terzi: si tratta però di ipotesi eccezionali, ricorrenti solo quando i dati relativi al richiedente e ai terzi siano tra loro collegati in maniera tale che la scomposizione degli stessi o la privazione di alcuni elementi ne renderebbe incomprensibile la lettura (v. art. 10, comma 5, del Codice).

In base a tali disposizioni l'Autorità ha definito, ad esempio, il procedimento con il quale si è segnalata l'avvenuta consegna, da parte di un istituto di credito, della documentazione relativa ad estratti di un conto corrente, cointestato anche alla segnalante, agli eredi legittimi del genitore deceduto (contitolare di quel conto) che ne avevano fatto richiesta (*Nota* 24 marzo 2004).

Al di là dei più consueti rapporti di conto corrente, al diritto di accesso si fa ricorso anche in funzione prodromica a possibili azioni di responsabilità nei confronti degli istituti di credito: il Garante ha esaminato, ad esempio, il ricorso presentato da un cliente di una banca colpito da un'ingente perdita finanziaria dopo aver sottoscritto un investimento erroneamente reputato a basso rischio; il ricorrente intendeva accedere ai dati personali che lo riguardavano e, in particolare, a quelli contenuti nei documenti che ne evidenziavano obiettivi e propensione al rischio. Nel definire il procedimento, l'Autorità ha ribadito che il cliente può cono-

scere tutti i dati personali che lo riguardano detenuti da un istituto di credito e, in caso di operazioni finanziarie, può conoscere anche le informazioni eventualmente riportate nei documenti in cui sono indicati i rischi dell'investimento (*Provv.* 12 marzo 2004, v. *Newsletter* n. 209 del 5-25 aprile 2004). Come già riconosciuto in passato, le informazioni personali devono essere comunque comunicate in modo chiaro e intellegibile, fornendo altresì i criteri e i parametri per la comprensione dei codici eventualmente utilizzati.

Nella nozione di dato personale rientra *"ogni informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"* (art. 4, comma 1, lett. *b*), del Codice). Il Garante ha pertanto accolto un ricorso (*Provv.* 23 luglio 2004) avente ad oggetto l'accesso ai dati relativi alle registrazioni telefoniche degli ordini di negoziazione effettuati dal ricorrente, secondo le disposizioni di cui al regolamento Consob n. 11522/1998. Anche in tali fattispecie viene infatti effettuato un trattamento di dati personali (qui la voce del cliente) e sono pertanto proponibili le istanze *ex* art. 7 del Codice.

In ordine ai trattamenti effettuati da società emittenti carte di credito è stata poi esaminata una vicenda nella quale l'interessato aveva espressamente chiesto di conoscere anche i "criteri di selezione" adottati per valutare la richiesta della carta (*Provv.* del 10 giugno 2004); al riguardo l'Autorità ha sottolineato l'obbligo per il titolare del trattamento di comunicare all'interessato tutti i dati che lo riguardano, eventualmente detenuti anche in forma di punteggi negativi. Si sono ritenute inammissibili, invece, le richieste volte a conoscere alcune notizie attinenti a criteri organizzativi e gestionali del titolare del trattamento.

Accesso ai dati da parte di eredi dell'interessato

Un particolare profilo applicativo del diritto di accesso ai dati personali, che si presenta di frequente specialmente in ambito bancario e assicurativo, riguarda la possibilità che, nel caso di dati concernenti persone decedute, i diritti dell'interessato siano esercitati anche *"da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione"* (art. 9, comma 3, del Codice).

Si tratta di tematica delicata e complessa rispetto alla quale si è più volte richiamata la necessità di distinguere fra richieste, inammissibili dal punto di vista della protezione dei dati, volte ad ottenere specificamente e direttamente dati personali relativi a terzi (ad esempio, i nominativi dei beneficiari di contratti di assicurazione a favore di terzo o di destinatari di rimesse bancarie: v. già il *Provv.* 3 aprile 2002, in *Bollettino* n. 27 del 2002, p. 20 e ss.) ed istanze, fondate, dirette invece a conoscere dati e informazioni riferite al defunto: la banca è quindi tenuta a comunicare agli eredi in modo chiaro e comprensibile i dati relativi alla consistenza patrimoniale del defunto, a movimentazioni bancarie, saldi, depositi "al portatore", anche se estinti da terzi dopo la data del decesso, usando però l'accortezza di oscurare eventuali informazioni personali riferite a terzi (*Provv.* 20 maggio 2004; v. *Newsletter* 21-27 giugno 2004).

Nelle diverse decisioni assunte in tema di accesso, il Garante ha ribadito la natura essenzialmente gratuita dell'esercizio dei diritti previsti dall'art. 7 del Codice. Peraltro, la complessità e l'estensione di alcune richieste di accesso in ambito bancario, sottolineata da diversi titolari, potrebbe portare in futuro l'Autorità, all'esito di un'adeguata istruttoria, ad adottare un provvedimento generale in tema di eventuali contributi spese forfettari a carico dell'interessato (contributo che, secondo quanto disposto dall'art. 10, comma 8, del Codice e in base ad una previa decisione generale del Garante, può essere chiesto dal titolare del trattamento, ad esempio qualora il riscontro alle richieste di accesso degli interessati comporti un notevole impiego

di mezzi in relazione all'entità o complessità delle istanze o comunque sia fatta richiesta della riproduzione dei dati cui si richiede l'accesso su speciali supporti).

Profili di liceità e correttezza

Attenzione particolare merita di essere attribuita ad un fenomeno relativo a modalità improprie di comunicazione talora adottate da banche, società finanziarie o società di recupero crediti, e consistenti nel contattare telefonicamente soggetti terzi –ad esempio abitanti nello stesso stabile– affinché riferiscano agli interessati di rivolgersi all'istituto per comunicazioni urgenti che li riguardano.

Si tratta di modalità di comunicazione che possono risultare lesive della riservatezza e della dignità degli interessati; l'Autorità ha pertanto richiamato l'attenzione di alcune banche sulla necessità di conformare le operazioni di trattamento ai principi di liceità e correttezza (art. 11, comma 1, lett. *a*), del Codice). In applicazione di tali principi, non dovranno essere effettuate comunicazioni alla clientela (relative anche a semplici richieste a terzi di riferire all'interessato di contattare la banca) per il tramite di condomini dello stesso stabile o vicini di casa, recando peraltro disturbo alla tranquillità di soggetti estranei al rapporto tra la banca e l'interessato; le banche e le società interessate, inoltre, sono state invitate a fornire apposite istruzioni in tal senso alle proprie strutture e dipendenti (*Note* 30 marzo 2004 e 25 ottobre 2004).

In un altro caso, l'Autorità ha rilevato un trattamento non corretto di dati personali da parte di una banca e di una società finanziaria, in occasione dell'addebito della rimessa interbancaria diretta (Rid) su un conto corrente diverso da quello indicato dal segnalante nell'ambito di una operazione di finanziamento (*Nota* 28 settembre 2004). La società finanziaria aveva infatti comunicato all'istituto di credito i dati indicati dal segnalante per la domiciliazione del Rid in modo inesatto ed incompleto, non fornendo né il numero di conto corrente prescelto per l'addebito, né il nominativo del terzo effettivamente intestatario di tale conto corrente (coobbligato per lo stesso rapporto di finanziamento). La banca, pur rilevando un'incompletezza dei dati comunicati, ha poi autonomamente proceduto, senza interpellare l'interessato, a domiciliare il Rid su un altro conto corrente non indicato a tal fine (cointestato al segnalante e ad un suo familiare), salvo poi sospendere l'addebito delle somme a seguito delle contestazioni del cliente.

Anche in questo caso, l'Autorità ha richiamato l'attenzione delle due società sulla necessità di impartire adeguate istruzioni al personale incaricato del trattamento per ridurre la probabilità che si verifichino errori analoghi e, comunque, per assicurare il pieno rispetto dei principi sanciti dal Codice in tema di correttezza del trattamento, di esattezza e di completezza dei dati.

9.2. *Trattamenti effettuati nell'ambito dei sistemi di informazione creditizia*

Conclusisi i lunghi e complessi lavori per la redazione del codice di deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti, il testo preliminare del codice è stato dapprima sottoposto ad una consultazione pubblica e all'attenzione delle associazioni dei consumatori riunite nel Consiglio nazionale dei consumatori e utenti (Cncu) (recependone poi varie osservazioni) e, quindi, approvato dal Garante il 16 novembre 2004. Suscettibile di applicazione dal 1° gennaio 2005 (con d.m. 14 gennaio 2005 il Ministro della giustizia ha disposto l'allegazione al Codice), il codice è stato sottoscritto dalle associazioni rappresentative del settore creditizio e introduce un quadro articolato di garanzie per i soggetti che chiedono prestiti, mutui, dilazioni di pagamento, *leasing* e carte di credito.

Tra le novità, al di là della (significativa) nuova dizione –abbandonandosi la tradizionale denominazione *"centrali rischi private"* a vantaggio della locuzione *"sistemi di informazioni creditizie"* (Sic)–, merita segnalare le principali regole di comportamento che costituiscono condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali da parte delle società che li gestiscono e che li consultano (banche, società finanziarie e società di *leasing*), precisando che il codice deontologico non riguarda nella sua interezza i sistemi informativi gestiti da soggetti pubblici e, in particolare, il servizio di centralizzazione dei rischi gestito dalla Banca d'Italia (al quale continua ad applicarsi la specifica normativa di settore).

Per quanto riguarda, invece, il sistema centralizzato di rilevazione dei rischi di importo contenuto istituito con deliberazione Cicr del 3 maggio 1999 e attualmente gestito da Sia S.p.A. (Società interbancaria per l'automazione), relativo agli affidamenti di importo inferiore al limite minimo di censimento previsto per la Centrale della Banca d'Italia e superiore al limite massimo fissato per le operazioni di credito al consumo (cd."centralina"), con esclusione dei crediti in sofferenza, trovano applicazione, in quanto compatibili, alcuni principi stabiliti dal codice. Al riguardo, l'Autorità ha già avuto occasione di pronunciarsi precisando che quest'ultimo sistema (e il relativo trattamento di dati personali) non rientra nel campo di applicazione dell'art. 8, comma 2, lett. *d*), del Codice, per cui gli interessati possono esercitare i diritti di cui al precedente art. 7 (*Provv.* 27 luglio 2004).

Questi i principi basilari contenuti nel codice di deontologia:

- la fissazione delle finalità esclusive per le quali i sistemi di informazioni creditizie potranno essere utilizzati e consultati (tutela del credito e contenimento dei relativi rischi), con la contestuale preclusione del perseguimento di scopi ulteriori (ad esempio, relativi all'attività di *marketing* o ricerche di mercato);
- la precisazione delle categorie di dati che potranno essere trattate in questi sistemi; in particolare, si conferma la distinzione tra i sistemi, più diffusi, che registrano e forniscono informazioni su richieste e rapporti di finanziamento (ossia informazioni "di tipo positivo-negativo") e quelli che raccolgono solo dati "di tipo negativo", come i ritardi nei pagamenti (le cd. morosità) o situazioni più gravi di mancato rimborso del credito;
- la necessità di fornire idoneo preavviso al cliente prima di effettuare una segnalazione a contenuto negativo al sistema d'informazione creditizia;
- l'individuazione di precise regole per la segnalazione delle morosità;
- maggiore trasparenza nei confronti dei consumatori attraverso una completa informativa inserita in una modulistica più chiara: in allegato al codice deontologico vi è un modello unico per l'informativa –predisposto dal Garante ai sensi dell'art. 154, comma 1, lett. *c*), del Codice– basato su espressioni che aspirano ad essere chiare, semplici e di agevole comprensione, e che dovrà essere adottato da tutti gli operatori economici;
- la fissazione di tempi massimi di conservazione, distinti a seconda della natura della segnalazione effettuata. In particolare, per i dati di tipo "negativo": un anno per gli inadempimenti, poi regolarizzati, relativi a ritardi fino a due rate; due anni per ritardi superiori poi sanati; tre anni per inadempimenti non regolarizzati. Per i dati "positivi": ventiquattro mesi dalla cessazione del rapporto o dalla scadenza del contratto;
- la previsione che, in caso di ritardo nel fornire la risposta al consumatore che abbia esercitato il diritto d'accesso, la visualizzazione dei dati sia sospesa e che, in caso di controversie relative al rapporto sottostante la richiesta di finanziamento (riguardanti ad esempio inadempimenti del

venditore/fornitore dei beni o servizi oggetto del contratto), ne verrà fatta opportuna annotazione.

Tra i partecipanti ai sistemi non figurano le società di telefonia, che avevano iniziato a collaborare con le centrali rischi in termini che il Garante aveva già considerato illegittimi. Il principio è stato ribadito anche in un provvedimento a seguito di ricorso (v. *Newsletter* 20-26 dicembre 2004), nel quale è stato precisato che nei sistemi di informazioni creditizie (Sic) potranno figurare solo dati relativi al vero e proprio rischio creditizio e non informazioni relative a bollette telefoniche non pagate e contratti di telefonia.

Il bilanciamento di interessi

Il trattamento dei dati personali nei sistemi di informazione creditizia richiede, secondo le previsioni del Codice, il consenso libero e informato degli interessati (art. 23) o la sussistenza degli altri presupposti di liceità alternativi rispetto ad esso (art. 24).

In proposito, l'Autorità ha ritenuto opportuno dare attuazione all'istituto del bilanciamento di interessi (previsto all'art. 24, comma 1, lett. *g*), del Codice), individuando i casi in cui il predetto trattamento potrà avvenire anche a prescindere dal consenso dell'interessato ed al solo fine di perseguire i legittimi interessi del titolare del trattamento o dei terzi destinatari dei dati (*Provv.* 16 novembre 2004, in *Documentazione* par. 40).

Il provvedimento del Garante riguarda in particolare i trattamenti relativi a:

- ritardi nel pagamento di un credito (che possono essere conservati, a seconda dei casi, per dodici o ventiquattro mesi dalla loro regolarizzazione);
- rapporti di credito per i quali si sono verificati ritardi o inadempimenti non regolarizzati (che possono essere conservati per non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto, o comunque dalla data di cessazione del rapporto). In quest'ultimo caso, possono essere conservati ulteriormente anche i dati personali relativi ad informazioni creditizie di tipo positivo eventualmente presenti nel sistema informativo, anche se riferiti ad altri rapporti di credito riguardanti il medesimo interessato.

In questi casi, il trattamento dei dati personali da parte dei soggetti che gestiscono o consultano sistemi di informazioni creditizie, è lecito ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, anche in assenza del consenso degli interessati.

Dati provenienti da fonti pubbliche

Secondo un principio recepito anche nel nuovo codice di deontologia, i dati trattati nell'ambito dei sistemi di informazioni creditizie devono essere in ogni caso di tipo obiettivo, strettamente pertinenti e non eccedenti rispetto alle finalità perseguite, oltre che relativi ad una richiesta/rapporto di credito. Non è sufficiente, a tal riguardo, che le informazioni vengano acquisite da fonti pubbliche (che comunque, se registrate, dovranno figurare in banche dati separate dal sistema di informazioni creditizie).

Al riguardo, si segnala un ricorso presentato da un cittadino relativamente alla mancata cancellazione, da parte del gestore del sistema di informazioni creditizie, di dati personali relativi alla trascrizione di una sentenza di divisione ereditaria e contenuti nella banca dati denominata "Atti pubblici". Il gestore giustificava il proprio diniego adducendo la perfetta coincidenza tra le informazioni censite nella propria banca dati e quelle risultanti dalla conservatoria dalla quale erano tratte, non ritenendo quindi di poter procedere alla cancellazione perché si era limitato a *"veicolare quanto contenuto nelle banche dati pubbliche consultate"* (*Provv.* 18 ottobre 2004). L'Autorità ha ritenuto il ricorso fondato in quanto, pur non contestandosi l'esattezza dell'informazione, il suo inserimento in una banca dati relativa a "dati pregiudizievoli" ha dato luogo ad un trattamento non corretto ai sensi dell'art. 11, comma 1,

lett. *a*), del Codice, per il fatto di aver descritto arbitrariamente come dato negativo un'informazione neutra quale quella connessa ad un'ordinaria operazione di scioglimento di una comunione ereditaria.

È stato al contrario ritenuto lecito il trattamento relativo ad un pignoramento immobiliare in quanto l'informazione, ancora presente nel pubblico registro dal quale era stata tratta, risultava pertinente e necessaria, trovando applicazione nel caso di specie la disposizione del Codice per cui, nel caso di informazioni provenienti da pubblici registri, i soggetti privati possono effettuare il relativo trattamento anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*), *Provv.* 29 aprile 2004).

Contributo spese

Nel quadro dei lavori relativi ai sistemi di informazione creditizia l'Autorità ha poi adottato il 23 dicembre 2004 una prima deliberazione di applicazione dell'art. 10, comma 8, del Codice, per il solo 2005, su istanza di una società che ha chiesto di riconoscere la facoltà di esigere dagli interessati un contributo spese per l'esercizio di alcuni diritti, in relazione alla situazione straordinaria che, presso quella società (Crif S.p.A.), si è temporaneamente determinata in ragione del notevole impiego di mezzi connessi alla complessità ed entità delle ricerche conseguenti alla richieste (*Deliberazione* 23 dicembre 2004, n. 15).

9.3. *Archivio degli assegni bancari e postali e delle carte di pagamento irregolari*

Anche il contenzioso relativo alle segnalazioni effettuate da soggetti pubblici (autorità giudiziaria e Ministero dell'interno) e privati (banche, uffici postali, società emittenti carte di credito) all'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento (Cai-Centrale d'allarme interbancaria) ha registrato un notevole incremento, con la proposizione di numerosi ricorsi da parte di privati cittadini concernenti la mancata cancellazione o rettifica dei dati.

Come ricordato nelle precedenti relazioni, l'archivio risponde alla finalità di interesse generale di assicurare il regolare funzionamento del sistema dei pagamenti e in esso vengono segnalati i provvedimenti o le segnalazioni riguardanti persone che hanno emesso assegni senza autorizzazione o provvista, titolari di carte di pagamento revocate (per mancato pagamento o costituzione di fondi), nonché assegni o carte di pagamento sottratti, smarriti o bloccati. Gli enti che effettuano tali segnalazioni vi sono obbligati da precise norme di legge (v. legge 15 dicembre 1990, n. 386, legge 25 giugno 199, n. 205, d.lg. 30 dicembre 1999, n. 507) che non consentono ai segnalanti alcuno spazio di valutazione personale.

Con alcune decisioni il Garante ha esaminato taluni profili relativi al trattamento dei dati effettuato presso tale archivio, riconoscendo la possibilità di esercitare il complesso dei diritti previsti dall'art. 7 del Codice sia nei confronti degli intermediari segnalanti sia della Banca d'Italia, soggetti che agiscono entrambi in qualità di titolari dei trattamenti rispettivamente effettuati (*Provv.* 27 settembre 2004 e 4 ottobre 2004).

L'Autorità ha altresì dichiarato l'infondatezza di diverse richieste volte ad ottenere la cancellazione di alcuni dati personali dall'archivio Cai relativi alla revoca di carte di credito o dell'autorizzazione ad emettere assegni, in quanto tali segnalazioni risultavano essere state effettuate nel rispetto della vigente normativa che disciplina il funzionamento del Cai (art. 10-*bis*, l. n. 386/1990; v. *Provv.* 4 e 12 ottobre 2004).

Anche un pagamento tardivo ritenuto satisfattivo dal creditore, ma non documentato nelle forme puntualmente previste dalla legge (art. 8, l. n. 386/1990), deve essere infatti segnalato nell'archivio una volta decorso il termine di legge indicato nel preavviso di revoca dell'autorizzazione ad emettere assegni a causa del mancato

pagamento per difetto di provvista. Resta in ogni caso salva, per effetto del Codice, la possibilità per gli interessati di richiedere ed ottenere la rettifica della segnalazione a loro carico, allorché siano in grado di dimostrare l'avvenuto pagamento nelle forme idonee, attraverso, ad esempio, un'integrazione della documentazione richiesta dalla legge (*Provv.* 4 ottobre 2004).

In applicazione di questi principi, è stato ritenuto fondato il ricorso di un imprenditore che era stato privato dell'autorizzazione ad emettere assegni per non essere riuscito a dimostrare alla banca, seguendo le prescritte formalità, di aver pagato un assegno. L'Autorità, pur riconoscendo la sussistenza dei presupposti per l'inserimento del nominativo dell'imprenditore nell'archivio informatizzato, ha tuttavia ordinato la cancellazione dei dati inseriti nell'archivio, in quanto gli stessi documentavano una situazione non più corrispondente alla realtà: l'interessato figurava infatti come un soggetto che non aveva provveduto al pagamento, neppure tardivo, dell'assegno, mentre lo stesso era stato effettuato per intero, anche se la documentazione in grado di dimostrarlo non era stata inizialmente accettata e, infine, era giunta con lieve ritardo (*Provv.* 27 settembre 2004). Non si è ritenuta, quindi, giustificata la tesi sostenuta dai titolari del trattamento di dover conservare i dati nella Cai per il periodo di efficacia del provvedimento di revoca dell'autorizzazione ad emettere assegni (sei mesi) sulla base di un regolamento (d.m. n. 458/2001), normativa peraltro di rango secondario rispetto al Codice, che disciplina in termini generali la conservazione dei dati.

9.4. *Trattamenti in ambito assicurativo*

Accesso alle perizie medico-legali

Nel contesto assicurativo il tema delle perizie medico-legali è da tempo al centro di un intenso contenzioso e continua ad essere oggetto di numerose decisioni del Garante.

La questione dell'accesso ai dati personali contenuti in perizie medico-legali redatte da professionisti incaricati dalle compagnie assicurative di stimare i danni denunciati dagli assicurati –rispetto alla quale in passato si erano registrate alcune difformità di posizioni tra Garante e taluna giurisprudenza di merito– è ora oggetto di una apposita e dettagliata disposizione del Codice (art. 8, comma 4) in base alla quale *"l'esercizio dei diritti di cui all'art. 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"*.

In alcune decisioni su ricorsi, il Garante ha ricordato che, come molti altri documenti, anche le perizie medico-legali in ambito assicurativo contengono di regola dati personali del paziente interessato, sia nella parte nella quale sono riportati dati identificativi dello stesso, nonché riscontri di visite mediche e dei cd. esami obiettivi, sia all'interno della parte che comprende valutazioni e giudizi del perito fiduciario. Informazioni personali riferite all'interessato possono essere ugualmente presenti nelle relazioni investigative eventualmente predisposte su incarico delle imprese di assicurazione. Si tratta infatti di informazioni comunque relative all'interessato che devono essere considerate "dati personali" ai sensi dell'art. 4, comma 1, lett. *d*), del Codice.

È possibile comunque che il titolare del trattamento invochi il temporaneo differimento dell'esercizio dei diritti di cui all'art. 7 del Codice, per il solo periodo durante il quale potrebbe derivarne un pregiudizio per lo svolgimento di cd. "inda-

gini difensive" o, più in generale, per far valere o difendere un diritto in sede giudiziaria (art. 8, comma 2, lett. *e*) del Codice); la valutazione dell'esistenza del pregiudizio deve essere effettuata caso per caso e sulla base di elementi concreti. Cessate tali circostanze, il diritto di accesso ai dati personali può essere nuovamente esercitato (*Provv.* 19 aprile 2004).

Per quanto riguarda le modalità del riscontro alle richieste di accesso relative ai dati inerenti allo stato di salute, contenuti nella perizia medico-legale, esso deve essere fornito direttamente agli interessati (a differenza di quanto previsto dalla normativa precedente, in base alla quale il riscontro doveva invece provenire da un medico di fiducia designato dal titolare o dall'interessato: v. l'art. 23, comma 2, della legge n. 675/1996, abrogato). L'art. 84 del Codice prevede ora l'obbligo del loro inoltro per il tramite del medico di fiducia solo a carico di esercenti le professioni sanitarie e di organismi sanitari.

Liceità e correttezza del trattamento in ambito assicurativo

Sempre in ambito assicurativo, ulteriori interventi dell'Autorità hanno riguardato alcuni profili relativi al trattamento di dati sensibili degli assicurati o di terzi.

In particolare, valutando la modulistica predisposta da una compagnia assicurativa, è stato affrontato il profilo dell'informativa. In tale occasione, il Garante, oltre a ribadire che la disciplina sulla protezione dei dati personali rende comunque necessaria la raccolta da parte dell'impresa di assicurazione del consenso scritto dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute (v. art. 26, del Codice, nonché le autorizzazioni del Garante nn. 2 e 5 del 2004), ha richiamato l'attenzione della società sulla necessità che il modello di informativa sottoposto ai clienti, e più in generale agli interessati, specifichi con chiarezza le caratteristiche del trattamento. In particolare, anche in considerazione del fatto che il consenso dell'interessato deve essere prestato *"specificamente in riferimento ad un trattamento chiaramente individuato"* (art. 23, comma 3, del Codice), l'informativa deve contenere un'indicazione puntuale e non esemplificativa dei titolari in favore dei quali il consenso potrebbe valere, eventualmente allegando un elenco, nonché delle principali caratteristiche degli ulteriori trattamenti effettuati (finalità, modalità e ambito di comunicazione dei dati).

La società è stata inoltre invitata a valutare la praticabilità di una designazione del professionista che effettua le visite medico-legali su incarico della stessa, in qualità di "responsabile del trattamento" ai sensi dell'art. 29 del Codice, specificando analiticamente per iscritto i compiti e le istruzioni cui attenersi. In tal modo il professionista potrebbe rendere l'informativa all'interessato precisando che i dati rientreranno nell'ambito del più generale trattamento effettuato dall'impresa di assicurazioni. In mancanza di tale designazione il professionista deve essere considerato un autonomo titolare del trattamento, anche relativamente ai dati sensibili rilevati nel contesto della visita medico-legale, e deve pertanto effettuare una autonoma informativa all'interessato e riceverne il consenso formulato per iscritto.

L'Autorità ha esaminato, inoltre, una segnalazione relativa ad un contratto di assicurazione riguardante il rimborso della penale prevista per l'annullamento di un viaggio; nel caso di specie, la compagnia di assicurazioni non ha proceduto al rimborso perché non ha reputato sufficiente il certificato medico inviato dal segnalante e riferito ad un congiunto impossibilitato a partecipare al viaggio, richiedendo, invece, copia della cartella clinica attestante la ragione dell'addotta impossibilità.

In tale occasione, il Garante non ha ritenuto ammissibile l'acquisizione, da parte del segnalante o di altri soggetti (la compagnia assicuratrice), della cartella clinica detenuta dalla struttura ospedaliera presso cui la persona interessata era stata ricove-

rata. Si è infatti rilevato che, quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il medesimo è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale o inviolabile (art. 60 del Codice; si vedano anche i chiarimenti sul concetto di "diritto di pari rango" forniti dal Garante con provvedimento del 9 luglio 2003, con cui è stato precisato che, quantomeno "nella prevalenza dei casi", i diritti di credito non rientrano tra i "diritti di rango almeno pari" a quello della persona cui si riferiscono i dati).

Preso atto che il diritto fatto valere dal segnalante nei confronti della società assicuratrice aveva natura di mero diritto di credito (rimborso della penale pagata al *tour operator* in seguito all'annullamento del viaggio), l'Autorità ha concluso per l'impossibilità per la struttura ospedaliera di accogliere una sua eventuale richiesta di ottenere, a scopo di tutela di tale diritto, un accesso ai dati sanitari contenuti nella cartella clinica del terzo ricoverato.

Già in precedenti occasioni il Garante aveva considerato giustificati i trattamenti di dati relativi alla salute degli assicurati effettuati da imprese di assicurazione al fine della gestione e dell'esecuzione di polizze infortuni e malattie, previa acquisizione del consenso scritto dell'interessato (nel caso di specie, peraltro, estraneo al contratto). Tra questi trattamenti può rientrare anche la raccolta di dati sanitari contenuti in cartelle cliniche degli assicurati, quando tali dati siano strettamente necessari per fornire le specifiche prestazioni richieste dagli interessati con questa tipologia di contratti, in relazione –ad esempio– ad attività di accertamento dei sinistri denunciati e di rimborso delle spese mediche sostenute dall'assicurato (cfr. *Provv.* 12 aprile 1999, in *Bollettino* n. 8 del 1999, p. 42).

È stato sottolineato, anzi, che anche per il trattamento dei dati contenuti nella certificazione sanitaria già inviata dal segnalante la società assicuratrice avrebbe dovuto comunque acquisire il consenso scritto della persona interessata. Inoltre, la raccolta ed il trattamento dei dati sanitari devono comunque essere effettuati in conformità ai principi di indispensabilità, di pertinenza e di non eccedenza dei dati rispetto alle finalità perseguite (v. l'art. 11 del Codice) oltre che ai requisiti indicati dalle citate autorizzazioni generali, con particolare riguardo alla stretta necessità per la società di assicurazione di acquisire copia integrale di una cartella clinica ai fini della liquidazione di un sinistro. L'acquisizione dell'intera cartella clinica può infatti rivelarsi non rispettosa dei principi ora richiamati poiché tale documento, insieme ad elementi strettamente necessari ai fini delle verifiche effettuate dall'impresa di assicurazione per procedere al rimborso (riguardo, ad esempio, ad informazioni che permettono di stabilire la natura della malattia), contiene ulteriori dati di carattere sanitario che possono non avere alcuna rilevanza ai fini delle suddette verifiche e che devono essere quindi omesse.

Oltre ad aver rilasciato nuove autorizzazioni generali, alcune delle quali di diretto rilievo per il settore assicurativo (v. in particolare le autorizzazioni nn. 2 e 5 del 2004), il Garante ha autorizzato con un provvedimento *ad hoc* una società cooperativa di assicurazioni che ne aveva fatto richiesta, a trattare i dati relativi alla convinzione religiosa dei propri soci (*Newsletter* 4-10 ottobre 2004). L'autorizzazione riguarda i dati e le operazioni strettamente indispensabili per l'applicazione di una specifica norma dello statuto della compagnia di assicurazioni, alle stesse condizioni previste dalla citata autorizzazione generale n. 5/2004 (che la società deve già rispettare per il trattamento degli altri dati personali dei propri assicurati).

Nell'accogliere la richiesta dell'assicurazione, il Garante ha tenuto conto anche dello scopo mutualistico della società che offre ai propri soci contratti di assicura-

zione a condizioni economiche particolari. La società cooperativa di assicurazioni si trova, secondo quanto stabilito dallo statuto, nella condizione di raccogliere e conservare anche dati dei soci che dichiarano di professare la religione cattolica e manifestano sentimenti di adesione alle opere cattoliche. A differenza degli altri clienti, tali soci possono essere assicurati a particolari condizioni di favore.

Nel caso in esame, l'intervento specifico a tutela del dato "religioso" dei soci si è reso necessario, non essendo prevista nelle autorizzazioni generali una disposizione che regoli espressamente il trattamento di questo tipo di informazioni da parte delle imprese di assicurazioni.

9.5. Marketing

Il settore del *marketing* è stato oggetto di costante attenzione da parte del Garante, in special modo a seguito dei numerosi ricorsi, segnalazioni e reclami relativi ad episodi di ricezione di lettere, telefonate, fax ed altre comunicazioni indesiderate effettuate da operatori del settore.

Una parte cospicua del contenzioso ha riguardato, ad esempio, l'invio di corrispondenza pubblicitaria relativa a proposte di abbonamento a riviste o all'acquisito di alcuni prodotti editoriali.

In proposito, il Garante ha valutato il ricorso di un cittadino che, avendo ricevuto un invito ad abbonarsi ad una rivista pubblicata da una casa editrice italiana (tra l'altro in collaborazione con un editore straniero), non aveva ricevuto riscontro alla richiesta di sapere in che modo la società avesse ottenuto i suoi dati personali, con quali modalità essi venissero utilizzati e per quali scopi. L'Autorità ha pertanto ordinato alla casa editrice di dare completo riscontro alle richieste del ricorrente (*Provv.* 25 maggio 2004; v. *Newsletter* 21-27 giugno 2004).

L'Autorità ha altresì avviato accertamenti nei confronti di una società che offre alcuni servizi aggiuntivi ai clienti che si registrano nel proprio sito *web*. Il Garante, in particolare, intende accertare se gli utenti, al momento della registrazione *on-line*, ricevano un'informativa idonea e se il consenso, che la società chiede di manifestare obbligatoriamente, sia espresso liberamente dagli utenti; ulteriore profilo che l'Autorità intende valutare è se il consenso richiesto faccia riferimento ad un trattamento ben individuato di dati personali o sia, invece, un consenso "*omnibus*" che autorizzi anche l'invio di materiale pubblicitario, vendita diretta, ricerche di mercato o comunicazioni commerciali.

Al vaglio del Garante è altresì la prassi, ormai diffusa fra gli istituti bancari, di raccogliere e trattare dati personali ai fini di *marketing* diretto per la promozione di carte di credito. In merito a tale vicenda l'Autorità ha compiuto accertamenti sulle modalità dei trattamenti effettuati, al fine di verificare la loro conformità al Codice. In particolare, sono state acquisite notizie sull'adempimento degli obblighi di informativa e la raccolta dell'eventuale consenso dell'interessato, nonché sull'origine dei dati personali utilizzati per la promozione delle predette carte.

Al riguardo, tenuto conto della tendenza degli operatori commerciali ad attingere dati personali da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per intraprendere operazioni di *marketing*, il Garante ha ribadito nuovamente, nell'ambito dei menzionati accertamenti, il divieto dell'ulteriore utilizzo per finalità pubblicitarie dei dati estratti dalle liste elettorali, in relazione a quanto previsto dall'art. 177, comma 5 del Codice (che ha modificato l'art. 51 del d.P.R. n. 223/1967). Alla luce di tale quadro legislativo, infatti, le liste elettorali, pur avendo natura di elenchi pubblici, non possono essere più utilizzate da terzi per scopi commerciali o

pubblicitari, a differenza della previgente disciplina che consentiva a chiunque di copiare, stampare o mettere in vendita tali liste.

Con parere del 15 luglio 2004, l'Autorità ha inoltre stabilito che a partire dalla seconda metà del 2005 non potranno più essere adoperati i nominativi contenuti negli elenchi telefonici per realizzare operazioni di *marketing* diretto nei confronti di chi non lo abbia espressamente consentito. Sono state così individuate le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati (ed ai titolari di carte prepagate) negli elenchi cartacei o elettronici disponibili al pubblico, anche con riferimento al diritto dell'interessato di decidere se ricevere o meno pubblicità per corrispondenza o per telefono. Infatti, sarà possibile inviare pubblicità soltanto a chi avrà scelto liberamente, in forma specifica e documentata per iscritto (tramite la compilazione del modello messo a punto dal Garante ed allegato al provvedimento menzionato), di ricevere informazioni commerciali o promozionali; la scelta da parte dell'utente di voler ricevere tali comunicazioni sarà evidenziata da un simbolo associato, a seconda dei casi, all'indirizzo e/o al numero telefonico (cfr. ulteriori considerazioni in merito nel par. 15.3).

L'attività dell'Autorità nella tematica in questione ha riguardato anche l'illecito utilizzo, per finalità pubblicitarie, di fax inviati da altri Stati dell'Unione europea. Grazie ad un sistema di cooperazione tra le istituzioni competenti nei vari stati membri, il quale prevede una procedura di trasmissione delle segnalazioni e dei reclami riguardanti la possibile violazione dell'art. 13 della direttiva 2002/58/CE, è stato possibile intervenire, per il tramite della omologa autorità britannica, anche nei confronti di una società che effettuava dal Regno Unito un invio massivo di fax pubblicitari nel nostro paese.

Infine, nel più ampio contesto dell'autoregolamentazione promossa dall'Autorità, particolare rilevanza riveste per il settore in esame la definizione del codice di deontologia relativo al trattamento dei dati personali a scopo di *marketing* diretto e di invio di materiale pubblicitario, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale. Il codice dovrà tra l'altro prevedere, anche per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale opposizione all'invio di determinate comunicazioni commerciali.

Sono già pervenute all'Autorità alcune richieste di partecipazione ai prossimi lavori preparatori per l'adozione del predetto codice. Il Garante sta valutando tali richieste al fine di individuare i soggetti rappresentativi del settore in esame che prenderanno parte ai lavori.

9.6. *Carte di fidelizzazione*

Già in passato l'Autorità è stata chiamata a pronunciarsi sul tema delle cd. "carte di fedeltà" o tessere di "fidelizzazione" della clientela: si tratta di tessere, spesso rilasciate gratuitamente presso punti di vendita, centri o esercizi commerciali, che consentono ai consumatori di usufruire di sconti o premi. Il rilascio delle predette carte è di regola subordinato alla compilazione di questionari sulle abitudini e le scelte di consumo dei clienti e delle loro famiglie e alla raccolta di ulteriori dati personali in ordine ai volumi di spesa e alle tipologie di prodotti acquistati dal consumatore al fine di consentire alle società titolari del trattamento di compiere operazione di cd. profilazione della clientela. Dalla documentazione acquisita è emerso che spesso gli interessati non hanno una piena consapevolezza di tali operazioni e dei rischi implicati, in quanto non ricevono preventivamente idonee informazioni sulle caratteristi-

che del trattamento dei dati che si accingono a fornire e sugli strumenti posti a difesa dei loro diritti.

L'Autorità ha ritenuto opportuno avviare una consultazione pubblica sul tema volta ad acquisire ulteriori elementi di informazione e documentazione da parte degli operatori dei settori della grande distribuzione e del *marketing*, degli organismi rappresentativi degli operatori dei predetti settori, delle associazioni dei consumatori e di ogni altro soggetto interessato. I quesiti che hanno formato oggetto della consultazione hanno riguardato in particolare: l'individuazione delle prassi seguite in sede di rilascio delle carte, con particolare riferimento alla (necessaria) richiesta del consenso della clientela al trattamento dei dati per la fruizione di benefici di varia natura (premi, sconti o buoni, speditezza e dilazione nei pagamenti ecc.); le modalità e finalità del trattamento dei dati dei clienti e l'individuazione della loro tipologia; gli adempimenti degli obblighi di informativa e consenso; l'eventuale uso in tale ambito delle tecniche di profilazione e classificazione della clientela; i tempi di conservazione delle informazioni raccolte; le misure adottate per agevolare l'esercizio dei diritti degli interessati, nonché l'ambito di comunicazione di tali dati.

9.7. *Flussi transfrontalieri*

Il trasferimento all'estero di dati personali da parte di una società o di una pubblica amministrazione è consentito dalla normativa comunitaria ed italiana solo se il livello di protezione garantito dal Paese di destinazione è adeguato. Si possono, invece, trasferire i dati verso Paesi che non garantiscono tale livello di protezione solo con il consenso degli interessati o sulla base di altri presupposti di liceità indicati all'art. 43 del Codice (esecuzione di obblighi derivanti da un contratto di cui è parte l'interessato, esigenza di salvaguardia della vita e dell'incolumità di un terzo, investigazioni difensive ecc.) oppure con l'autorizzazione del Garante. Al di fuori di questi casi il trasferimento verso Paesi terzi di dati personali è vietato.

Questi principi sono stati ribaditi anche in occasione di una richiesta di intervento urgente del Garante, trasmessa da alcune associazioni a tutela dei diritti dei consumatori, relativamente al trasferimento in Argentina di dati personali di soggetti intestatari di titoli obbligazionari (nell'ambito di una Offerta pubblica di scambio volontaria promossa dalla Repubblica Argentina). Si è precisato, in particolare, che il trasferimento dei dati personali degli investitori che intendono aderire all'offerta della Repubblica Argentina –paese che la Commissione europea ritiene fornisca un adeguato livello di tutela dei dati personali (Decisione 30 giugno 2003, in *G.U.C.E.* 5 luglio 2003)– è lecito solo se necessario per l'esecuzione di obblighi contrattuali o in presenza di uno specifico consenso informato che individui le istituzioni argentine come destinatarie dei dati (art. 43 del Codice).

L'Autorità, a seguito dell'esame della documentazione relativa alla predetta operazione, ha ritenuto che il trasferimento di dati personali degli investitori sia consentito solo in base ai requisiti sopra indicati, fermo restando che i dati, una volta trasferiti, potranno essere poi utilizzati soltanto per le finalità specificate nel rapporto contrattuale (e che potranno essere trasferiti, altresì, solo i dati pertinenti e non eccedenti rispetto a tale rapporto).

Il Garante ha svolto un attento monitoraggio in relazione ad operazioni di "esportazioni" di dati da parte di operatori italiani e al tipo di garanzie e strumenti adottati per tutelare i diritti degli interessati. Nel 2004 è stata portata a conclusione l'indagine (v. *Relazione 2003*, p. 96) presso cinquanta tra le principali società e gruppi industriali che operano in Italia, incentrata sull'analisi dei presupposti, delle

finalità e modalità del trasferimento di dati all'estero, delle categorie di dati trasferiti e delle persone interessate (cittadini, lavoratori, professionisti, imprenditori ed altre società), delle attività dei soggetti importatori, nonché degli strumenti utilizzati per la tutela dei dati personali in rapporto a ciascuna tipologia di trasferimento.

Dall'indagine svolta è emerso che l'oggetto prevalente dei trasferimenti di dati all'estero effettuati dalle società è rappresentato dai dati personali dei dipendenti ed in misura minore, ma sempre rilevante, dalle informazioni relative a clienti, società concorrenti e fornitori. Di regola i flussi di dati sono effettuati dopo aver acquisito lo specifico consenso degli interessati. In alcune limitate ipotesi, quando la gestione delle risorse umane avviene negli Stati Uniti, le società che "importano" i dati personali hanno aderito all'accordo del cosiddetto "*Safe Harbor*". È emersa, inoltre, una diffusa tendenza a predisporre contratti, anche "multilaterali" nel caso di gruppi societari, da sottoporre al parere preventivo del Garante, e a fare uso delle clausole contrattuali *standard* indicate dalla Commissione europea (cfr. *Newsletter* 17 maggio 2004).

Nel corso del 2004 si è assistito, altresì, ad un aumento di richieste di pareri ed informazioni da parte di imprese e gruppi societari, operanti a livello internazionale, in merito alla corretta applicazione della normativa in materia di trasferimento dei dati personali.

In particolare, è attualmente all'esame dell'Autorità una richiesta di parere relativa ad un sistema informativo costituito da una banca dati elettronica e centralizzata –allo stato non più aggiornata, in attesa di verificare appunto la compatibilità del sistema con la normativa sulla protezione dei dati personali– la cui gestione e manutenzione è affidata ad una società che ha sede nel Regno Unito e nella quale confluiscono informazioni trasmesse da istituti di credito, relative a presunte condotte fraudolente tenute da esercenti commerciali convenzionati con un circuito internazionale.

Il *server* che ospita la predetta banca dati è fisicamente collocato al di fuori dell'Ue, in particolare negli Stati Uniti, mentre la consultazione del sistema da parte degli istituti di credito aderenti al circuito avviene su base nazionale.

Da una prima analisi dei quesiti formulati dalla società richiedente, l'Autorità ha potuto rilevare che il trattamento di dati personali effettuato da parte di quest'ultima nell'ambito del sistema descritto potrebbe non essere soggetto alla normativa italiana sulla protezione dei dati personali, trattandosi di un sistema gestito direttamente da un titolare del trattamento stabilito fuori dal territorio dello Stato. In tal caso, infatti, in base al principio di stabilimento previsto dal Codice (art. 5), il trattamento dei dati non ricadrebbe nell'ambito di applicazione della legge italiana. Per quanto riguarda, invece, la trasmissione dei dati al sistema da parte degli istituti bancari italiani, nonché il successivo trasferimento degli stessi al *database* situato negli Usa, il Garante si è riservato di esaminare i profili inerenti la materia di trasferimento dei relativi dati personali all'estero al fine di individuare la disciplina applicabile.

Sempre nel settore dei flussi transfrontalieri di dati riguardanti presunte condotte irregolari connesse all'uso di carte di credito, il Garante ha partecipato attivamente ad un gruppo di lavoro istituito presso il *Working Group* di cui all'art. 29 della direttiva 95/46/CE, insieme a rappresentanti di altre autorità nazionali di protezione dei dati, della Commissione europea, e dell'industria delle carte di credito, con l'obiettivo di individuare alcune linee-guida affinché questi flussi di dati –talvolta limitati all'interno dello spazio comune europeo, talaltra invece su base globale– avvengano nel rispetto dei diritti e delle libertà delle persone interessate. Il documento, in versione non ancora definitiva, è adesso al vaglio del *Working Group* che dovrà tenere conto delle osservazioni formulate in merito da alcune autorità nazionali (tra queste, il Garante).

Sono inoltre giunte all'attenzione dell'Autorità alcune richieste di autorizzazione al trasferimento dei dati all'estero da parte di società di revisione contabile che, in base alla normativa di settore vigente negli Usa (in particolare il recente *Sarbanes-Oxley Act*), per svolgere prestazioni professionali a favore di società quotate nei listini americani sono tenute a registrarsi presso un apposito elenco, detenuto da un organismo americano istituito per monitorare le società che operano nel mercato finanziario. Le società richiedenti hanno infatti evidenziato che, ai fini della relativa registrazione, devono raccogliere e trasmettere all'organismo menzionato informazioni personali relative alle stesse società, ai soci e ai dipendenti, nonché ai consulenti che assistono le società di revisione nello svolgimento dei relativi incarichi. Tali informazioni, peraltro, includono dati giudiziari e fanno altresì riferimento a procedimenti civili, amministrativi e disciplinari o arbitrati in cui sono stati coinvolti i predetti soggetti.

Al riguardo, il Garante sta valutando se siano applicabili al caso descritto i presupposti di liceità richiesti dall'art. 43 del Codice e, più in generale, la compatibilità di tali trattamenti di dati con la normativa italiana e comunitaria.

Con riferimento all'attività svolta dall'Autorità al fine di dare attuazione ad alcune decisioni comunitarie relative al settore in esame, come anticipato nella *Relazione 2003*, è in procinto di essere resa operativa in Italia anche la decisione della Commissione europea n. 2003/490/CE del 30 giugno 2003, pubblicata sulla *G.U.C.E.* L 168 del 5 luglio 2003, riguardante l'adeguatezza del livello di tutela dei dati personali esistente in Argentina. Va specificato, inoltre, che il 28 aprile 2004 la Commissione europea, con decisione 2004/411/CE, ha stabilito che il livello di protezione dei dati personali esistente nell'Isola di Man, su cui si era già espresso in senso favorevole, con il parere n. 6 del 21 novembre 2003, il Gruppo art. 29, è parimenti "adeguato" ai fini del trasferimento di dati personali dall'Ue verso soggetti ivi residenti. È, infine, in fase di pubblicazione sulla Gazzetta Ufficiale la deliberazione con la quale il Garante ha dato attuazione alla Decisione comunitaria del 21 novembre 2003, n. 2003/821/CE recante il riconoscimento del Baliato del Guernsey tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali.

10 Libere professioni

10.1. *Ordini e collegi professionali*

Anche nel corso del 2004 sono pervenuti quesiti sul trattamento dei dati personali relativi a soggetti iscritti ad albi e collegi professionali. Rispondendo ad essi, il Garante ha avuto occasione di ribadire le significative innovazioni introdotte in questa materia dal Codice e di fornire alcune precisazioni in merito alla divulgazione delle informazioni relative a provvedimenti disciplinari.

Al riguardo, si ricorda che, ai sensi dell'art. 61 del Codice, in armonia con le disposizioni sulla comunicazione e diffusione di dati personali da parte dei soggetti pubblici, gli ordini e i collegi professionali possono ora più agevolmente comunicare pure a privati e diffondere, anche mediante reti di comunicazione elettronica, i dati (diversi da quelli sensibili e giudiziari) che, secondo le disposizioni legislative o regolamentari di settore, devono essere necessariamente inseriti nei rispettivi albi per legge o regolamento.

In merito alla divulgazione delle informazioni relative a provvedimenti atti ad incidere sull'attività dell'iscritto all'albo, su richiesta del Consiglio nazionale degli ingegneri, è stato specificato che nelle comunicazioni a soggetti pubblici o privati, o in sede di diffusione, anche per via telematica, di dati inseriti nell'albo professionale, può essere resa nota l'esistenza di provvedimenti disciplinari che dispongono la sospensione dalla professione, ma non il provvedimento nella sua integralità, fermo restando il dovere di porre in circolazione informazioni corrette, complete ed aggiornate, specie con riguardo ad eventuali sviluppi favorevoli per gli interessati.

D'altra parte, in base alla nuova disciplina (art. 61, comma 3, del Codice) gli ordini ed i collegi professionali possono integrare i dati contenuti negli albi con ulteriori informazioni che l'iscritto richieda di aggiungere, purché pertinenti e non eccedenti in relazione alla sua attività professionale (*Nota* 17 agosto 2004).

In risposta ad un quesito di un consiglio notarile distrettuale, l'Ufficio ha poi precisato che, ai sensi dell'art. 61 del Codice, l'esistenza e l'esito del provvedimento di sospensione possono essere comunicati a soggetti privati che abbiano presentato un esposto, ferma restando, peraltro, l'applicazione nel caso concreto delle disposizioni della legge n. 241/1990 in tema di accesso ai documenti amministrativi (*Nota* 17 agosto 2004).

10.2. *Liberi professionisti*

In ossequio ai principi di semplificazione ed efficacia, il Garante, in un articolato parere indirizzato al Consiglio nazionale forense, ha fornito alcuni chiarimenti per una corretta applicazione della disciplina sulla protezione dei dati nell'esercizio dell'attività forense che, per alcuni aspetti, possono valere anche per altri liberi professionisti (*Nota* 3 giugno 2004).

In relazione alla titolarità del trattamento è stato chiarito che, quando l'attività è svolta individualmente, titolare del trattamento è lo stesso avvocato, cui spettano quindi le decisioni sull'uso dei dati, sugli strumenti impiegati e sul profilo della sicu-

rezza, mentre sono contitolari del medesimo trattamento due professionisti che operino congiuntamente. Se l'attività è invece svolta in forma societaria o associata, il titolare è l'entità nel suo complesso e gli adempimenti previsti dal Codice devono essere attuati unitariamente per evitare frammentazioni o ripetizioni da parte dei singoli professionisti. La designazione del responsabile del trattamento è facoltativa e nelle grandi organizzazioni ne possono essere designati anche diversi. Chiunque abbia accesso interno ai dati (praticanti, personale amministrativo ecc.), deve essere designato quale incaricato del trattamento, indicando per iscritto i compiti affidatigli.

Per quanto riguarda gli adempimenti, la maggior parte dei trattamenti effettuati dagli avvocati non sono soggetti a notificazione, mentre resta fermo l'obbligo di informativa all'interessato, che può essere resa anche oralmente e in forma sintetica, purché completa.

Il titolare deve inoltre adottare le misure di sicurezza idonee e preventive per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta. Contrariamente a quanto ipotizzato in alcuni quesiti formulati da singoli professionisti, il Garante ha precisato che, per quanto riguarda l'organizzazione del lavoro quotidiano di studio, non si deve affatto eliminare il nome delle parti dalla copertina dei fascicoli cartacei. È invece sufficiente seguire adeguate modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti.

I dati comuni e sensibili possono essere trattati senza il consenso degli interessati solo se il loro uso è necessario per svolgere indagini difensive o far valere un diritto in sede giudiziaria. Se tra i dati sensibili vi sono anche informazioni relative a salute e vita sessuale, è necessario seguire il cd. principio del pari rango, in ragione del quale il diritto difeso o fatto valere in giudizio deve essere un diritto della personalità o un altro diritto o libertà fondamentale o inviolabile (art. 26, comma 4, lett. *c*), del Codice).

Per quanto riguarda il trattamento dei dati giudiziari, purché esso avvenga nel rispetto dell'autorizzazione generale n. 4/2004, non è richiesto il consenso dell'interessato.

L'esercizio dell'attività stragiudiziale (arbitrati, conciliazioni, ricorsi amministrativi) è soggetto, invece, a regole differenti, in base alle quali il trattamento dei dati comuni di soggetti diversi dal cliente deve generalmente avvenire con il consenso dell'interessato, a meno che sia applicabile uno dei presupposti indicati dall'art. 24 del Codice (ad esempio, nel caso di trattamento di dati "pubblici"). Nel caso di dati sensibili, il consenso, sempre necessario, deve essere scritto.

Notai

Nel corso dell'anno, con un parere reso al Consiglio nazionale del notariato, l'Autorità ha precisato le modalità con le quali i notai, in qualità di titolari del trattamento, devono dare applicazione alla normativa in materia di protezione dei dati personali, assumendo un formale impegno a redigere a breve un agevole e sintetico "decalogo", in cooperazione con il Consiglio.

L'Ufficio ha nel frattempo ribadito che la disciplina sulla protezione dei dati personali non pone in discussione la peculiarità della funzione notarile e si affianca alle regole generali sul segreto professionale per assicurare l'integrità e la disponibilità dei dati, indicando come gli stessi debbano essere custoditi e trattati in concreto.

Analogamente a quanto previsto per gli avvocati, il Garante ha chiarito le modalità di applicazione delle misure minime di sicurezza e degli obblighi di informativa all'interessato. Tuttavia, è stato precisato che, data la peculiarità e gli obblighi della funzione notarile, il dare conoscenza o pubblicità ad alcuni dati e documenti trat-

tati dal notaio non concreta la fattispecie della "diffusione" prevista dal Codice.

È stato ricordato, ferme restando le particolari garanzie per i dati sensibili, che il consenso è solo uno dei presupposti del trattamento dei dati comuni: si può, infatti, fare riferimento agli altri presupposti indicati nell'art. 24 del Codice, come, ad esempio, l'adempimento di obblighi di legge o l'esecuzione di obblighi contrattuali (*Nota* 3 dicembre 2004).

11 Rapporto di lavoro e previdenza

11.1. *Dati trattati nel corso del rapporto di lavoro*

Il Garante ha proseguito la valutazione, già iniziata nel 2003, degli effetti delle disposizioni di attuazione della cd. riforma Biagi del mercato del lavoro (l. n. 30/2003 e d.lg. n. 276/2003) con riguardo al trattamento dei dati personali in ambito lavorativo.

L'Autorità, anche con le autorizzazioni generali al trattamento dei dati sensibili, ha ribadito la necessità che il trattamento di taluni dati sensibili sia effettuato nel rispetto delle regole e dei principi generali dettati dal Codice ed entro i limiti fissati dall'art. 8 dello Statuto dei lavoratori (legge 20 maggio 1970, n. 300, che vieta indagini sulle opinioni e trattamenti discriminatori).

La Borsa continua nazionale del lavoro

Il principio è stato altresì indicato in un parere reso il 3 settembre 2004 sullo schema di decreto interministeriale di attuazione della Borsa continua nazionale del lavoro, nel quale il Garante ha sottolineato l'esigenza che il richiamo all'art. 10 del d.lg. n. 276/2003 ivi contenuto sia interpretato in armonia con l'art. 8 della legge n. 300/1970.

Con il citato parere, le cui indicazioni sono state solo in parte recepite nel testo definitivo del decreto del 13 ottobre 2004, sono stati affrontati ulteriori importanti profili in materia di protezione dei dati personali nel sistema della Borsa continua nazionale del lavoro: in particolare, su specifica richiesta dell'Autorità, il regolamento reca ora l'indicazione dei titolari dei trattamenti, al fine di definirne compiutamente le relative responsabilità. Per assicurare il rispetto del principio di proporzionalità del trattamento dei dati, l'indicazione dei dati da far confluire nella Borsa (in particolare, delle informazioni minime ed essenziali relative alle candidature e alle richieste di personale), contenuta negli allegati, è ora esaustiva e si prevede che eventuali ulteriori dati possano essere inseriti solo su base volontaria e non possano essere oggetto, in ogni caso, di utilizzazione a fini discriminatori, specie qualora abbiano natura di dati sensibili, come l'"appartenenza a liste speciali"; è stato altresì precisato nel regolamento che i soggetti che fruiscono della Borsa possono trattare solo i dati pertinenti all'instaurazione del rapporto di lavoro.

Videosorveglianza in ambito lavorativo

Sono stati definiti alcuni procedimenti già istruiti in materia di controllo a distanza dei lavoratori a mezzo di apparecchiature di videosorveglianza e sono state fornite prescrizioni ai titolari del trattamento con particolare riferimento al rispetto dell'art. 4 della legge n. 300/1970, oltre che dei principi generali posti dal Codice a garanzia degli interessati.

Il controllo del lavoratore attraverso videocamere è stato oggetto anche di alcuni ricorsi sottoposti al Garante.

I casi affrontati nel corso dell'anno (concernenti impianti di ripresa video installati da soggetti privati) hanno permesso di dare applicazione ai precetti di legge ed alle indicazioni specifiche contenute nel provvedimento generale del Garante del 29 aprile 2004 (v. par. 12.1).

In particolare, nelle decisioni del 16 giugno 2004 e dell'11 ottobre 2004, è stato sottolineato che i trattamenti in questione violavano i presupposti di liceità, propor-

zionalità, correttezza e trasparenza in relazione, tra l'altro, all'angolo di ripresa delle telecamere, all'assenza di idonea informativa o all'invasività dell'impianto stesso di videosorveglianza, nonché alle finalità perseguite che potevano essere raggiunte anche con accorgimenti diversi (nel caso di specie, installazione di cancelli o provvedimenti per regolare gli accessi).

Profili di liceità e correttezza del trattamento in ambito lavorativo

L'Autorità è poi intervenuta su ulteriori temi specifici, tra i quali: adeguatezza della modulistica di informativa e richiesta del consenso dei lavoratori predisposta dai datori di lavoro; accesso dei lavoratori ai dati personali che li riguardano; modalità di conservazione e custodia dei dati dei dipendenti a cura dei datori di lavoro.

È stato esaminato il caso di un dipendente di banca che ha contestato la formula di manifestazione del consenso al trattamento dei dati personali riportati nell'estratto conto certificativo della sua posizione contributiva (cd. "Ecocert") inserita dal datore di lavoro in un modulo con il quale chiedeva all'interessato la delega all'acquisizione di tali dati presso l'ente previdenziale. L'Autorità (*Nota* 7 luglio 2004) ha rilevato che, nel caso di specie, la richiesta del consenso era superflua, in quanto i dati non sensibili erano trattati per adempiere a specifici obblighi fissati dalla normativa vigente (artt. 4 e 24, legge 23 luglio 1991, n. 223) e dagli accordi contrattuali al fine di avvalersi di procedure di riduzione collettiva del personale.

Anche con riferimento agli eventuali dati sensibili contenuti nel modulo "Ecocert", l'acquisizione del consenso dell'interessato è stata ritenuta superflua, dal momento che il segnalante aveva già manifestato alla banca il consenso al trattamento dei dati personali, anche sensibili, per le finalità e nei termini indicati nelle informative già fornite a suo tempo dalla banca e nel cui ambito potevano essere ricomprese anche le operazioni necessarie per adempiere agli obblighi appena richiamati. Si è poi fatto presente che, in base alle nuove disposizioni del Codice, non è più necessario il consenso scritto dell'interessato quando il trattamento dei dati sensibili occorra in rapporto a specifici obblighi o compiti previsti dalla legge per la gestione del rapporto di lavoro, nel rispetto dell'autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro e delle regole che saranno individuate mediante il codice di deontologia in materia di lavoro e previdenza (art. 26, comma 4, lett. *d*), del Codice).

L'Autorità ha pertanto prescritto alla banca di precisare agli interessati, ad integrazione delle informative fornite in passato, che il conferimento dei dati contenuti nel modulo "Ecocert" è necessario per l'adempimento dei predetti obblighi, con l'indicazione delle conseguenze in caso di mancato rilascio di tali dati, e di invitare i lavoratori a produrre direttamente l'estratto conto della propria posizione contributiva in alternativa al rilascio di una delega a tal fine alla banca, tenuto conto che comunque è loro facoltà accedere personalmente ai dati in questione presso gli enti previdenziali (art. 54, legge 9 marzo 1989, n. 88).

Rapporto di lavoro e tutela della dignità e della riservatezza del lavoratore

In numerose ipotesi il Garante è dovuto intervenire a tutela della dignità e della riservatezza dei lavoratori, specialmente se interessati da delicate vicende personali e familiari attinenti allo stato di salute e alla vita sessuale.

Si segnala, al riguardo, l'accoglimento del ricorso della dipendente di una società per una seria violazione della propria riservatezza personale e familiare (*Provv.* 27 luglio 2004, v. *Newsletter* 11-17 ottobre 2004). La dipendente, che occupava temporaneamente la scrivania di un collega, aveva trovato la fotocopia di una lettera da lei stessa inviata al direttore dell'ufficio, nella quale erano riportate anche delicate informazioni sulla condizione di salute della figlia minore disabile.

L'Autorità ha rilevato che la presenza di tale fotocopia contenente dati sensibili

della dipendente e della figlia minore, al di fuori del fascicolo personale e comunque in un contesto inappropriato, contrastava con le prescrizioni e le cautele indicate nell'autorizzazione generale che disciplina il trattamento dei dati sensibili nei rapporti di lavoro, nonchè con le disposizioni del Codice in materia di misure di sicurezza; ha ricordato che i dati sensibili devono essere conservati in una sezione separata del fascicolo personale ed essere accessibili solo al personale autorizzato.

Il Garante, riconosciute le ragioni della dipendente, ha imposto alla società di adottare tutte le misure di sicurezza idonee a prevenire il ripetersi di eventi del genere, comunicandone il contenuto all'Autorità.

La società, che non ha contestato la ricostruzione della vicenda fatta dalla dipendente, ha avviato una indagine interna i cui esiti dovranno essere comunicati al Garante per la valutazione di altre eventuali violazioni o responsabilità.

Cartellini identificativi e mutamento del sesso

L'Autorità ha inoltre affrontato la delicata questione relativa alla possibilità di ottenere la rettificazione degli atti dello stato civile solo a seguito di una sentenza del tribunale passata in giudicato che attribuisca alla persona un sesso diverso da quello enunciato nell'atto di nascita, in ragione delle intervenute modificazioni esteriori dei suoi caratteri sessuali. Tale previsione, pur corrispondendo ad una scelta normativa specifica, che solo il Parlamento ha il potere di modificare, mostra alcuni elementi di criticità in merito alla difesa dei diritti dei soggetti coinvolti nel procedimento di rettificazione del sesso, specie nella fase transitoria di tale procedimento. La lunga durata dei procedimenti di rettificazione di attribuzione di sesso ha reso quindi necessario richiamare l'attenzione sull'esigenza di porre allo studio la possibilità di introdurre nell'ordinamento specifiche misure provvisorie volte a tutelare l'identità personale e la dignità dell'interessato nel periodo preliminare al passaggio in giudicato della sentenza. Spetta al Governo e al Parlamento valutare anche la possibile applicazione di tali misure in eventuali altri procedimenti giudiziari in cui si presentino analoghe esigenze (*Nota* 11 agosto 2004).

Con riferimento all'uso sul luogo di lavoro del nome di battesimo, nell'intervallo di tempo necessario al passaggio in giudicato della sentenza di rettificazione di sesso, l'Autorità ha avuto modo di precisare che, in applicazione dei principi di pertinenza e non eccedenza, sui cartellini identificativi dei dipendenti devono essere presenti unicamente i dati sufficienti ad assicurare la trasparenza dei rapporti tra il personale e tra questi e gli utenti (ad es. l'immagine fotografica, la definizione del ruolo ricoperto ed eventualmente un numero o una sigla) e non anche altri dati non necessari per perseguire tale finalità (es. dati anagrafici). Analogamente, con riferimento alla prassi di indicare il nome di battesimo nell'indirizzo di posta elettronica, nei moduli di richiesta di ferie e/o permessi e nelle comunicazioni personali e domiciliari, l'Autorità ha ricordato che l'interessato che non desidera che su tali atti compaia il suo dato anagrafico non ancora rettificato ha il diritto di richiedere, per motivi legittimi, l'adozione di specifiche misure che, in armonia con la disciplina dettata dal Codice, tengano conto della sua delicata posizione meritevole di tutela (art. 7, comma 4, del Codice). Il datore di lavoro ha l'obbligo di valutarle tempestivamente; l'interessato che ritenga di aver ricevuto una risposta insoddisfacente ha il diritto di adire l'autorità giudiziaria ordinaria o, in alternativa, il Garante con gli strumenti di tutela previsti dal Codice.

Accesso in ambito lavorativo

Diverse ipotesi esaminate hanno avuto origine da richieste da parte del lavoratore di accedere ai dati che lo riguardano detenuti dal datore di lavoro, richieste talvolta estese alla conoscenza di tutte le informazioni utilizzate dallo stesso datore di lavoro in relazione alla carriera professionale dell'interessato (comprese relazioni

valutative periodiche, documentazione relativa a ferie, permessi e malattie, o tabulati contenenti le registrazioni delle presenze in servizio) (*Provv.* 12 maggio 2004).

Il Garante ha ribadito che il riscontro alle richieste di accesso deve essere completo e deve comprendere tutti i dati relativi all'interessato comunque trattati dal titolare, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali (art. 10, comma 3, del Codice). Ciò, anche nel caso in cui il conferimento all'interessato di determinate qualifiche e ruoli sia ricavabile da atti societari custoditi in archivi aziendali diversi da quelli contenenti i dati connessi alla gestione del rapporto. L'Autorità, nel caso esaminato, ha rilevato che l'interessato aveva dapprima formulato un'istanza in termini tali da potersi ritenere riferita esclusivamente ai dati conservati nel suo fascicolo personale, mentre una richiesta successiva comprendeva, di fatto, tutti i dati personali che lo riguardavano trattati dall'*ex* datore di lavoro. A fronte di questa seconda richiesta, la società era comunque tenuta a individuare tutti i dati personali del lavoratore, a prescindere dalla circostanza che fossero custoditi nel fascicolo personale del lavoratore stesso (*Nota* 9 agosto 2004).

In risposta ad una richiesta di parere presentata da una società, il Garante ha per altro verso sottolineato che, in linea di principio, non può escludersi la necessità di esibire o consegnare al richiedente copia di interi atti o documenti, o parte di essi, riguardanti anche terzi, purché ciò avvenga nel solo caso in cui i dati relativi al richiedente e ai terzi siano intrecciati al punto da risultare incomprensibili o snaturati nel loro contenuto, se privati di alcuni elementi o scomposti rispetto alla loro originaria collocazione (*Nota* 23 novembre 2004).

In merito all'ammissibilità della richiesta dell'interessato di accedere a dati già in suo possesso, l'Autorità ha ricordato che alla richiesta di accesso ai dati deve essere fornito riscontro anche nell'ipotesi in cui le medesime informazioni, in tutto o in parte, siano state comunicate all'interessato o siano comunque dallo stesso detenute. Ciò, al fine di consentire all'interessato di poterne controllare l'esattezza e di chiederne, se del caso, l'aggiornamento, l'integrazione o la correzione. Si è inoltre fatto presente che il diritto di accesso è a volte esercitato chiedendo legittimamente di conoscere anche origine dei dati, finalità, modalità e logica del trattamento, ovvero gli estremi identificativi del titolare e del responsabile del trattamento, ove nominato, nonché 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 (art. 7, comma 2, lett. *e*), del Codice).

Sempre sul tema dell'accesso ai dati personali relativi a dipendenti (in particolare, dati valutativi o contenuti in note di qualifica, dati relativi ad assenze dal servizio per malattia ed altri dati contenuti nei fascicoli personali), sono state numerose anche le decisioni adottate a seguito di ricorso. Unitamente a tali richieste di accesso è stata talvolta manifestata l'opposizione per motivi legittimi al trattamento dei dati: in particolare, in un caso l'istanza era motivata dall'illecita comunicazione di dati riferiti alla carriera professionale del lavoratore ad altre società, in assenza del consenso informato dell'interessato (*Provv.* 3 giugno 2004).

Al termine del 2004 il Garante ha avviato un ciclo di ispezioni per accertare la posizione di alcune *ex* società di fornitura di lavoro interinale e società di ricerca e selezione del personale in materia di notificazione dei trattamenti di taluni dati personali (cfr. par. 20.3)

11.2. *Rapporto di lavoro in ambito pubblico*

Dati sensibili

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

Non è stata così ritenuta rispondente al principio di necessità l'indicazione, nelle comunicazioni indirizzate alle sedi interessate, dei gravi motivi di salute su cui era fondato il provvedimento di trasferimento di un dipendente. Il trasferimento, infatti, avrebbe potuto essere comunicato a tali uffici mediante una nota contenente, in sintesi, il testo del provvedimento originario e gli estremi di riferimento del provvedimento. Tale accorgimento, peraltro, non pregiudica l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, l. n. 241/1990), né la facoltà delle persone a ciò legittimate di accedere ad eventuali altri dati, anche di tipo sensibile, contenuti in tali atti, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa.

In materia di trattamento di dati sensibili, l'Autorità ha ritenuto che la disciplina sulla protezione dei dati personali non ponesse ostacoli di fondo ad un'iniziativa del Ministero degli affari esteri consistente nell'identificare i dipendenti portatori di handicap ai fini di esercitazione per evacuazioni antincendio in conformità alla disciplina sull'igiene e la sicurezza del lavoro. Tale attività rientra infatti tra quelle che, sulla base del Codice, possono giustificare il trattamento di dati sensibili (artt. 86, comma 1, lett. *c*) e 112, comma 2, lett. *e*) del Codice).

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

Test psico-attitudinali

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

Si è precisato, in primo luogo, che il divieto di trattare informazioni sensibili nell'ambito di test psico-attitudinali previsto dal Codice (art. 22, comma 10) si riferisce anche alla raccolta di questi dati mediante questionari volti a costruire il profilo o la personalità dell'interessato. Va pertanto espunta dai questionari utilizzati sia per gli esami psico-attitudinali, sia per quelli psichiatrici, ogni domanda idonea a rivelare profili particolarmente delicati della sfera privata dell'interessato, quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere.

A seconda degli esiti di tali esami è invece possibile procedere ad ulteriori accer-

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

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

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

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

Visite medico-legali

Non è risultata, invece, contraria alla disciplina sul trattamento dei dati personali la trasmissione alla questura e alla prefettura da parte di un comune (finalizzata all'adozione dei provvedimenti di competenza) dell'esito di alcune visite medico-legali cui era stato sottoposto un dipendente, essendo l'interessato, un agente di pubblica sicurezza, abilitato al porto di pistola, nonché in possesso del porto d'armi per uso di caccia (*Provv.* 22 gennaio 2004). Il caso va visto in connessione con un altro, esaminato da questa Autorità, oggetto di una valutazione parzialmente difforme dell'autorità giudiziaria presso cui è stato impugnato il provvedimento del Garante, in considerazione dell'ulteriore documentazione prodotta dall'interessato, invece non presentata in sede di ricorso all'Autorità (v. par. 19.4). Nel ricorso, il dipendente di una questura aveva lamentato che i dati relativi al proprio stato di salute, accertati nel corso di una visita medica cui era stato sottoposto per verificare la sua idoneità al servizio, erano stati comunicati ad altri soggetti al fine del ritiro cautelativo dell'arma in dotazione e del tesserino di servizio. Nella decisione del ricorso, sulla base degli elementi prodotti dalle parti, il Garante aveva ritenuto che tali comunicazioni fossero avvenute lecitamente, in quanto effettuate in conformità alle norme sulle autorizzazioni di polizia per la detenzione ed il porto d'armi e finalizzate all'adozione dei relativi provvedimenti (*Provv.* 15 gennaio 2004). L'Ufficio, invece, ha avviato specifici accertamenti per verificare se all'interessato sia stata fornita un'idonea informativa anche in relazione ai flussi di dati necessari ai fini dell'adozione dei provvedimenti sull'arma di servizio.

Sempre in materia di trattamento di dati del personale in servizio presso le questure, è stato oggetto di una decisione su ricorso il trattamento di dati sensibili di un funzionario amministrativo. In proposito, il Garante ha segnalato alla questura

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

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

L'utilizzo del fax come mezzo di comunicazione tra amministrazioni è consentito dalla legge e, in linea generale, non è in contrasto con i principi in materia di protezione dei dati personali. Il Garante ha tuttavia evidenziato che per talune circostanze occorre rispettare le specifiche modalità eventualmente previste dalla normativa di settore. Ad esempio, è all'attenzione dell'Autorità una questione relativa alle modalità di trasmissione delle comunicazioni nell'ambito del procedimento disciplinare, per alcune delle quali la normativa prevede la consegna personale all'interessato o, qualora questa non sia possibile, l'invio di una raccomandata (artt. 111 e 104, d.P.R. n. 3/1957). Nel caso in esame, il fax era stato utilizzato anche per le convocazioni dei componenti del Consiglio di disciplina che contenevano il nominativo della persona sottoposta al procedimento, anche se, in ossequio ai principi di pertinenza e non eccedenza, sarebbe stato probabilmente sufficiente anticipare soltanto il tipo di intervento per il quale si richiedeva la presenza del consigliere.

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

Diritto al lavoro dei disabili

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

Anche a tale proposito occorre sottolineare che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti.

Un'amministrazione provinciale ha poi informato il Garante, nell'ambito di una comunicazione ai sensi dell'art. 39 del Codice, dell'intenzione di trasmettere ad un comune i dati identificativi degli iscritti ad una lista del collocamento obbligatorio per consentire lo svolgimento di un'indagine sui bisogni dei cittadini disabili. In proposito, l'Autorità ha precisato che, trattandosi di informazioni idonee a rivelare lo stato di disabilità degli interessati, occorre far riferimento alla distinta e più stringente disciplina prevista per il trattamento dei dati sensibili (artt. 20 e 22 del Codice) (*Nota* 21 settembre 2004). Nel corso degli ulteriori approfondimenti, avviati in collaborazione con gli enti pubblici coinvolti, sono state poi fornite indicazioni idonee a realizzare l'iniziativa nel pieno rispetto delle garanzie poste dal Codice a tutela della riservatezza e degli altri diritti dei disabili interessati dall'indagine.

Sciopero nei servizi pubblici essenziali

Con riferimento alla disciplina sullo sciopero nei servizi pubblici essenziali, l'Autorità si è occupata della prassi, seguita da alcune amministrazioni pubbliche, di comunicare al Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e all'apposita Commissione di garanzia gli elenchi nominativi di dipendenti che hanno esercitato, in specifici casi, il diritto di sciopero.

In proposito, considerando la chiarezza del dettato normativo della legge n. 146/1990, che pone in capo alle amministrazioni e alle imprese erogatrici di detti servizi l'obbligo di rendere pubblico "il numero dei lavoratori che hanno partecipato allo sciopero, la durata dello stesso e la misura della trattenuta effettuata secondo la disciplina vigente" (art. 5), si è rilevato che talune amministrazioni potevano essere state indotte ad effettuare siffatte comunicazioni da una espressione utilizzata nella circolare del 18 giugno 2002 del Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, con riferimento alle rilevazioni delle adesioni allo sciopero.

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

Concorsi

Il Ministero degli affari esteri ha sottoposto all'attenzione del Garante l'intenzione di consentire ai candidati interessati a partecipare ai concorsi banditi dall'amministrazione di inviare direttamente *on-line* all'ufficio competente la domanda di partecipazione, corredata di dati personali. Poiché la questione attiene alla più generale tematica dell'informatizzazione dell'amministrazione pubblica, il Garante, nelrilevare che l'iniziativa in esame di per sé non era in contrasto con i principi del Codice, ha evidenziato al Ministero che, tuttavia, la disciplina dell'accesso agli impieghi nelle pubbliche amministrazioni e dello svolgimento dei concorsi pubblici (art. 4, d.P.R. n. 487/1994) esclude espressamente l'utilizzo di strumenti diversi dalla diretta presentazione all'ufficio competente delle domande di ammissione al concorso o dal loro invio tramite raccomandata con avviso di ricevimento (*Nota* 25 agosto 2004).

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

Sempre in tema di trattamento di dati personali nell'ambito di concorsi pubblici, si è precisato che non costituisce violazione della disciplina sulla riservatezza la richiesta, rivolta dalle amministrazioni pubbliche agli aspiranti, di una dichiarazione sostitutiva dei carichi pendenti. Tale procedura tiene conto dell'esigenza dell'amministrazione di verificare l'eventuale presenza di cause ostative all'accesso al pubblico impiego (art. 85, d.P.R. 10 gennaio 1957, n. 3 e art. 2, d.P.R. 9 maggio 1994, n. 487); esigenza quest'ultima espressamente riconosciuta dall'art. 71 del d.P.R. n. 445/2000 e dalla recente riforma del casellario giudiziale, che prevede anche una forma di accesso diretto alla banca dati da parte delle amministrazioni (d.P.R. 14 novembre 2002, n. 313).

11.3. *Previdenza*

Su richiesta di un'associazione di difesa dei diritti dei cittadini, sono all'esame del Garante alcuni moduli adottati dall'Inps con la circolare n. 103 dell'11 maggio 2001, utilizzabili dai lavoratori per presentare le domande di congedo per maternità e di congedo parentale.

In proposito, è necessario valutare alla luce dei principi di indispensabilità, pertinenza e non eccedenza dei dati trattati, la raccolta di informazioni ulteriori rispetto a quelle che, secondo la disciplina sulla tutela delle lavoratrici madri, devono essere necessariamente riportate nel certificato medico di gravidanza (art. 14 d.P.R. 25 novembre 1976, n. 1026).

Maggiori garanzie nelle modalità di raccolta, peraltro, non pregiudicano l'eventuale successiva acquisizione di ulteriori informazioni, anche sensibili, da parte dell'istituto previdenziale o dei medici dei servizi ispettivi del Ministero del lavoro e delle politiche sociali, qualora emerga la reale necessità di svolgere gli accertamenti amministrativi e i controlli previsti (artt. 76 e 77, d.lg. n. 151/2001).

Non è invece in contrasto con i principi di pertinenza e non eccedenza la raccolta, sul modulo di domanda per congedo parentale, dei dati relativi all'altro genitore o affidatario (dati anagrafici, periodi di congedo eventualmente fruiti, tipologia dell'attività lavorativa svolta, ecc.). Tali informazioni sono infatti pertinenti rispetto alla necessità di quantificare il periodo di congedo e la relativa indennità che il datore di lavoro e l'istituto previdenziale devono accordare al genitore richiedente (artt. 32, 33 e 34, d.lg. n. 151/2001) e non risultano eccedenti rispetto alla medesima finalità, non facendo alcun riferimento specifico al tipo di rapporto che intercorre tra i soggetti beneficiari.

L'Autorità, pertanto, è in procinto di definire la questione al fine di invitare l'Inps a riesaminare i moduli per la presentazione delle domande di congedo per maternità, in modo da garantire la riservatezza delle lavoratrici che intendono usufruire dei benefici previsti dalla legge a tutela della maternità.

A seguito di una segnalazione relativa al trattamento dei dati sanitari, l'Autorità si è pronunciata circa le informazioni che devono essere contenute nelle denunce di malattia professionale che i datori di lavoro sono tenuti a trasmettere all'Inail. In tali atti devono essere indicate solo informazioni sanitarie relative o collegate alla patologia denunciata, anziché dati sulla salute inerenti a semplici malesseri accusati o ad assenze registrate nel corso del rapporto di lavoro, non rilevanti per la malattia professionale.

Dati sanitari dei dipendenti

Con un provvedimento del 15 aprile 2004, il Garante ha così vietato all'Inail di utilizzare i dati sanitari di un'assicurata ed ha disposto il blocco di alcune informazioni relative allo stato di salute presenti negli archivi del datore di lavoro e ricavabili dalle diagnosi contenute nei certificati dei lavoratori. All'amministrazione è stato, inoltre, imposto di adottare opportuni accorgimenti per non rendere visibili le diagnosi sulle certificazioni sanitarie detenute.

L'attuale disciplina in materia prevede che il lavoratore assente per malattia sia tenuto a presentare al datore di lavoro solo l'attestazione della prognosi. Può capitare, però, che il certificato contenga un'indicazione non necessaria della diagnosi: in questo caso l'amministrazione non è legittimata a trattare ulteriormente questi dati, e deve adottare opportune misure affinché lavoratori e medici rispettino tali cautele nella redazione dei certificati.

Nel 2004 è stata allo studio dell'Autorità la questione relativa alla trasmissione per via telematica all'Inps dei certificati di malattia predisposti da medici di medi-

cina generale. Al riguardo, il Garante aveva avviato un tavolo di lavoro con i rappresentanti dell'Istituto, al fine di evidenziare gli aspetti relativi alla tutela dei dati personali degli assistiti coinvolti da tale progetto. In particolare, l'Ufficio aveva rappresentato che tale modalità di trasmissione doveva essere prevista da norma di legge o di regolamento essendo difforme da quella prevista dalla disciplina vigente.

Da ultimo, con la legge finanziaria 2005 (art. 1, comma 149, l. n. 311/2004), è stato però stabilito che, a decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante trasmetta 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 sul quale l'Autorità dovrà fornire il proprio parere ai sensi dell'art. 154, comma 4, del Codice per garantire, in particolare, il rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati trattati.

12 Videosorveglianza

12.1. *Protezione dei dati e videosorveglianza*

Nel corso degli ultimi anni si è constatato un forte incremento dell'impiego di sistemi a circuito chiuso, di telecamere e di altri sofisticati strumenti di rilevazione di immagini da parte sia di soggetti pubblici, sia di soggetti privati. Nel corso del 2004 il Garante è ripetutamente intervenuto, intensificando altresì la propria attività ispettiva, a fronte delle sempre più frequenti segnalazioni di cittadini per presunte violazioni della normativa sulla protezione dei dati determinate dall'installazione di impianti di videosorveglianza.

Nel periodo in esame sono stati anche ribaditi i chiarimenti, a più riprese forniti in passato, relativi all'uso privato di telecamere. In particolare, in occasione di un ricorso, l'Autorità ha constatato la mancanza dei presupposti di applicazione del Codice al trattamento dei dati personali effettuato per mezzo di un impianto di videosorveglianza installato da alcuni soggetti presso il cancello di ingresso della propria abitazione (*Provv.* 25 febbraio 2004). Le telecamere così attivate, infatti, configuravano un trattamento effettuato per fini esclusivamente personali. Su questo tipo di trattamenti occorre peraltro verificare quanto richiamato nel citato provvedimento del 29 aprile 2004, sia in relazione alle finalità perseguite, sia in riferimento alla necessità che i dati personali così registrati non siano destinati alla comunicazione sistematica o alla diffusione (in merito v. pure par. 13.1).

Il provvedimento generale sulla videosorveglianza: i principi

Alla luce dell'evoluzione tecnologica, dei nuovi documenti elaborati in sede comunitaria ed internazionale (in particolare, il parere n. 4/2004 dell'11 febbraio 2004 fornito dai Garanti europei, nonché le linee guida espresse dal Consiglio d'Europa il 20-23 maggio 2003) e, soprattutto, delle innovazioni contenute nel Codice, si è reso necessario aggiornare ed integrare il "decalogo" sulla videosorveglianza del novembre 2000, adottando un nuovo provvedimento di carattere generale che stabilisce regole più precise a garanzia dei cittadini (*Provv.* 29 aprile 2004).

Con tale provvedimento sono stati richiamati i principi generali enucleati dal Codice (validi in ambito pubblico e privato) il cui rispetto assicura un equo contemperamento tra le esigenze di sicurezza ed il rispetto della normativa sulla protezione dei dati personali nella rilevazione di immagini e suoni.

Il trattamento deve ovviamente avvenire nel rispetto, oltre che della citata normativa, anche delle prescrizioni contenuti in altre disposizioni di legge che possono interessare l'installazione di apparecchi audiovisivi (come, ad es., in materia di interferenze illecite nella vita privata, tutela della dignità, dell'immagine e del domicilio, tutela dei lavoratori e intercettazioni di comunicazioni e conversazioni).

Con riferimento al principio di necessità, i sistemi di videosorveglianza e il relativi programmi informatici non possono utilizzare dati riferiti a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

Viene inoltre ribadito che, nel rispetto del principio di proporzionalità, il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare se il suo impiego sia realmente proporzionato agli scopi perseguiti; l'utilizzo di tali

strumenti può essere giustificato, allora, solo quando altre misure (sistemi d'allarme, altri controlli fisici o logistici, misure di protezione agli ingressi ecc.) siano insufficienti o inattuabili.

In applicazione del principio di finalità, il titolare che attiva telecamere deve perseguire scopi determinati, espliciti e legittimi e, non ultimo, di sua pertinenza. È invece emerso che finalità di pubblica sicurezza, prevenzione e accertamento dei reati, pur competendo solo ad organi giudiziari o a forze armate o di polizia, sono state indicate quali finalità perseguite da parte di soggetti pubblici e privati.

Attività dei comuni

È stata ritenuta in contrasto con il principio di finalità l'attivazione da parte di un comune di impianti di videosorveglianza per propaganda turistica, nonché per rendere visibili le condizioni meteorologiche di porti e spiagge. In particolare, l'Autorità ha considerato del tutto ingiustificata l'attività di rilevazione di immagini con finalità promozionali e pubblicitarie, peraltro realizzata attraverso *web cam* dotate di *zoom*, successivamente diffuse sul sito *web* del comune, se in grado di rendere identificabili i cittadini ripresi (*Nota* 15 giugno 2004).

Non sono invece stati rilevati profili di illiceità nell'installazione, da parte di alcuni comuni, di apparecchi in grado di scattare fotografie in prossimità di semafori, al fine di monitorare il traffico e rilevare infrazioni. L'installazione di tali apparecchi che, peraltro, se hanno la finalità di controllare gli accessi ai centri storici, sono disciplinati da un apposito regolamento che ha recepito alcune indicazioni del Garante, non deve essere autorizzata caso per caso dall'Autorità.

Nel recente provvedimento generale sono stati confermati anche gli adempimenti cui sono soggetti tutti i titolari di impianti di videosorveglianza pubblici e privati.

Informativa

I cittadini che si trovano o che transitano in una zona videosorvegliata devono poter essere resi edotti dell'esistenza di sistemi di videosorveglianza, anche attraverso un modello semplificato di informativa "minima", messo a disposizione dal Garante (art. 13, comma 3, del Codice), consistente in un cartello con un simbolo che rappresenta una telecamera, valido per la videosorveglianza posta in essere in aree esterne. In tutte le altre ipotesi, devono essere altresì indicati gli elementi di cui all'art. 13 con particolare riguardo alle finalità e all'eventuale conservazione dei dati.

Prior checking

Nel citato provvedimento generale, il Garante ha anche ricordato che, di regola, l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo dell'Autorità e che non si applica il principio del silenzio-assenso. Pertanto, non può desumersi alcuna approvazione implicita dalla semplice trasmissione al Garante di progetti relativi alla intenzione di installare sistemi di videosorveglianza, peraltro spesso incompleti o comunque privi di quegli elementi che consentirebbero di valutare il rispetto del principio di proporzionalità.

La verifica preventiva da parte dell'Autorità è invece obbligatoria per le tecnologie particolarmente invasive, come quelle che prevedono intrecci, interconnessioni, collegamenti delle immagini con altri particolari dati personali (ad es. biometrici) o in caso di digitalizzazione o indicizzazione delle immagini o di videosorveglianza cd. dinamico-preventiva, che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi, caratteristiche fisionomiche o eventi improvvisi.

Bilanciamento

Per quanto riguarda il settore privato, con il provvedimento in questione ha trovato applicazione anche la disciplina che prevede il bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice) individuando i casi in cui è possibile effet-

tuare la rilevazione di immagini anche senza il consenso dell'interessato, ritenendosi prevalente il legittimo interesse del titolare, con un impiego circoscritto dei sistemi di videosorveglianza nei limiti previsti dal provvedimento.

Notificazione

I trattamenti di dati nell'ambito di un'attività di videosorveglianza devono essere notificati al Garante solo se rientrano in una delle ipotesi previste dall'art. 37 del Codice; in ogni caso, non devono essere notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio (v. *Provv.* 31 marzo 2004, relativo ai casi da sottrarre all'obbligo di notificazione, nonché il *Parere* 23 aprile 2004, recante chiarimenti sui trattamenti da notificare al Garante).

Numerose segnalazioni e reclami sul trattamento di dati effettuato tramite sistemi di videosorveglianza installati da studi professionali, esercizi commerciali, società, enti *no-profit*, hanno reso necessario effettuare accertamenti *in loco* spesso in collaborazione con la Guardia di finanza. In alcuni di questi casi, precedenti all'adozione del nuovo provvedimento generale, è stato necessario contestare gli illeciti di omessa notificazione al Garante del trattamento effettuato mediante impianti di videosorveglianza e/o di mancata adozione di un'idonea informativa agli interessati circa la presenza dei predetti sistemi, comprovata dall'assenza di avvisi o cartelli recanti le indicazioni prescritte dalla vigente normativa in materia di protezione dei dati personali. I relativi titolari del trattamento sono stati, inoltre, richiamati al rispetto delle precise garanzie fissate nel provvedimento del 29 aprile e a fornire un riscontro al riguardo (*Note* 27 ottobre 2004). Anche a seguito dell'adozione del predetto provvedimento del 29 aprile, sono state accertate *in loco* e contestate alcune violazioni dell'obbligo di informativa, che i titolari del trattamento non hanno reso neanche nella forma semplificata suggerita dal Garante con il modulo allegato al provvedimento (v., al riguardo, par. 20.3). In altri casi in cui gli elementi acquisiti in sede ispettiva hanno consentito di escludere la commissione di illeciti da sanzionare, l'Autorità ha comunque richiamato i titolari al rispetto delle prescrizioni contenute nel provvedimento medesimo (*Nota* 29 novembre 2004).

Impianti di videosorveglianza su treni e stazioni

In relazione ad un progetto sperimentale di Trenitalia S.p.A., relativo all'installazione di sistemi di videosorveglianza su taluni vagoni dei treni che transitano su specifiche tratte ferroviarie oggetto di ripetuti atti vandalici e di episodi di microcriminalità a danno dei passeggeri, l'Autorità (v. *Note* 11 novembre 2003 e 25 novembre 2004), preso atto di taluni accorgimenti adottati spontaneamente dalla società a protezione dei dati (effettuazione delle riprese con modalità volte ad escludere l'ingrandimento dell'immagine e la ripresa degli scompartimenti dei passeggeri; memorizzazione delle immagini riprese in forma criptata; predisposizione di un'informativa agli interessati), ha prescritto l'adozione di alcune misure: in particolare, individuare i responsabili e gli incaricati del trattamento; ridurre al minimo, ove tecnicamente possibile, i tempi di conservazione giornaliera delle immagini prima della loro cancellazione; adottare idonee misure di sicurezza dei sistemi e dei dati raccolti. Trenitalia S.p.A. ha recentemente comunicato al Garante che, per ragioni tecnico-organizzative, la sperimentazione non avrebbe avuto inizio prima della fine del 2004, impegnandosi a fornire, entro il primo semestre del 2005, una relazione dettagliata sullo stato di avanzamento del progetto.

Sempre in relazione all'impiego di impianti di videosorveglianza nel settore del trasporto ferroviario, va segnalato un parere che il Garante ha reso ad una società del gruppo Ferrovie dello Stato circa un'iniziativa sperimentale da avviare con la colla-

borazione di una società telefonica (v. *Nota* 29 ottobre 2004). Il progetto consiste nell'installazione presso tre stazioni (Roma Fiumicino, Anzio, Taormina) di alcune telecamere con inquadratura panoramica e rilevazione di immagini a bassa definizione da trasmettere via Internet attraverso il portale *web* della società per finalità di carattere pubblicitario. Gli impianti, inoltre, permettono la visualizzazione delle immagini solo in presa diretta, senza possibilità per l'utente di accedere a registrazioni, né di scaricare le informazioni sul proprio *computer*, o di effettuare variazioni di inquadratura o di dimensioni dell'immagine visualizzata. Il Garante, confermando quanto aveva già precisato con un provvedimento del 14 giugno 2001, ha fatto presente che questo tipo di sistema di videosorveglianza non si pone in contrasto con quanto affermato nel provvedimento del 29 aprile 2004, poiché le telecamere installate non consentono di identificare (neanche indirettamente) gli interessati, in ragione della distanza dal luogo ripreso o delle altre caratteristiche tecniche.

La società ha inoltre sommariamente descritto le caratteristiche di un diverso sistema di videosorveglianza, costituito da telecamere ad alta risoluzione e utilizzato dalla Polizia ferroviaria per finalità di tutela dell'ordine e della sicurezza pubblica. Con lo stesso parere, quindi, l'Autorità ha precisato che quest'ultimo sistema rientra invece nell'ambito applicativo del Codice; e ha altresì sottolineato che il trattamento di dati personali effettuato attraverso l'impianto deve essere pienamente conforme ai principi di necessità, finalità e proporzionalità richiamati nel citato provvedimento generale, e che occorre rispettare, pur in presenza di pericoli concreti o dell'esigenza di prevenzione di specifici reati, le competenze che le leggi assegnano a tali scopi solo ad organi giudiziari e di polizia giudiziaria.

Recentemente l'Autorità ha avuto comunicazione da Trenitalia S.p.A. della messa in servizio, dal 9 settembre 2004, dei treni regionali "Minuetto", dotati di particolari sistemi di videosorveglianza. Si tratta di un'iniziativa scaturita da indicazioni emerse nel corso dei lavoro del Comitato interministeriale sulla sicurezza dei trasporti (Cist) che, ai fini di tutela dell'ordine e sicurezza pubblica, ritiene che tra le misure prioritarie da adottare vi sia anche la videosoveglianza sui treni. L'Autorità è in procinto di definire i termini della propria eventuale attivazione.

12.2. *Videosorveglianza in ambito pubblico*

Frequenti sono stati gli interventi del Garante con riferimento a sistemi di videosorveglianza posti in essere da comuni, da istituti scolastici o da luoghi di cura pubblici.

Ambiti sanitari

A questo riguardo, l'Autorità ha espresso il proprio avviso in ordine alla liceità dell'uso di telecamere presso alcune Asl al fine di assicurare un livello adeguato di sicurezza all'interno dei locali e fronteggiare episodi di aggressione a danno di guardie mediche (*Note* 15 luglio 2004).

L'Autorità ha così precisato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti od ambienti, stante la natura sensibile di alcuni dati che possono essere in tal modo raccolti, devono essere circoscritti ai soli casi di stretta indispensabilità e limitando le riprese a determinati locali e a precise fasce orarie. Deve inoltre essere adottato ogni ulteriore accorgimento necessario per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione delle misure che il Codice prescrive per le strutture sanitarie.

È stato ribadito, inoltre, che il titolare deve assicurare che l'accesso alle immagini sia limitato solo ai soggetti specificamente autorizzati, evitando che siano visionate

da estranei. Rigorose cautele sono state indicate anche in relazione alla possibilità di accedere alle riprese da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione). In tali ipotesi, i familiari possono comunque visionare, con gli adeguati accorgimenti tecnici, l'immagine del proprio congiunto. Stante il divieto di divulgazione dei dati idonei a rivelare lo stato di salute, deve essere prevenuto il rischio di diffondere immagini di persone malate su *monitor* accessibili al pubblico.

Esigenze di sicurezza

L'Autorità ha fornito ancora chiarimenti in risposta a quesiti posti da alcuni comandi provinciali dei vigili del fuoco e dall'Istat circa la possibilità di installare sistemi di videosorveglianza presso l'ingresso, l'atrio e il vano scala della sede degli edifici, per ragioni di sicurezza e tutela del patrimonio dell'ente (*Nota* 30 novembre 2004), nonchè per controllare l'accesso del pubblico, onde evitare che utenti esterni possano accedere ad aree vietate (*Note* 15 luglio 2004).

In particolare è stato evidenziato, sulla scorta di precedenti provvedimenti dell'Autorità, che le riprese potrebbero riguardare anche i lavoratori dipendenti e configurare, pertanto, un controllo a distanza nei confronti dei medesimi. A tal proposito, si è richiamata nuovamente l'attenzione sulle garanzie da osservare nell'ambito dei rapporti di lavoro anche quando gli impianti siano utilizzati per esigenze organizzative e dei processi produttivi, ovvero siano richiesti per la sicurezza del lavoro, con particolare riguardo al principio contenuto nell'art. 4 della l. n. 300/1970 che sancisce il divieto di controllo a distanza dell'attività dei lavoratori.

Istituti scolastici

Con riferimento agli istituti scolastici, è stata sottoposta all'attenzione dell'Autorità la questione riguardante l'installazione di telecamere presso alcuni istituti (*Note* 18 agosto 2004 e 24 dicembre 2004) al fine di controllare gli accessi all'edificio e dissuadere dal compimento di atti di vandalismo.

Al riguardo, è stato evidenziato che l'installazione di sistemi di videosorveglianza può essere giustificata nelle sole aree interessate, soltanto se strettamente indispensabile (ad esempio in caso di ripetuti atti vandalici) e, comunque, al di fuori dell'orario scolastico, quando gli edifici sono chiusi.

È necessario, in ogni caso, rispettare il diritto alla riservatezza dello studente (art. 2, comma 2, d.P.R. n. 249/1998), anche in considerazione del fatto che, frequentemente, lo studente è un minore.

In applicazione di questi principi, l'Autorità è intervenuta a proposito dell'installazione, secondo quanto segnalato da alcune notizie di stampa, di numerose telecamere all'interno e all'esterno di un edificio scolastico. L'Ufficio ha invitato l'istituto a conformarsi alle citate prescrizioni e a produrre ogni documento utile a sostegno delle iniziative assunte (*Nota* 10 settembre 2004), ricevendo un tempestivo riscontro sul quale sono stati però attivati ulteriori accertamenti.

Luoghi di culto

Il Garante è altresì intervenuto al fine di assicurare l'intimità di chi accede a luoghi di culto, quali chiese od altri luoghi di ritrovo dei fedeli, invitando i titolari ad un uso particolarmente prudente dei mezzi di ripresa in ragione del potenziale discriminatorio dei trattamenti riguardanti tali informazioni sensibili, relative alla sfera religiosa dell'individuo, e a limitare l'utilizzo di telecamere nei luoghi di sepoltura ai casi in cui via sia concreto rischio di atti vandalici.

Camere ardenti

Ciononostante, a seguito di un ciclo ispettivo, è stata rilevata l'installazione da parte di un comune di un sistema di videosorveglianza presso un edificio all'interno del quale vengono allestite camere ardenti per la veglia dei defunti. Tali telecamere

non erano segnalate mediante le necessarie informative previste dal Codice, ed anzi erano celate alla vista del pubblico. A seguito di un invito da parte dell'Autorità ad effettuare il blocco spontaneo del trattamento, gli uffici comunali hanno sospeso le attività di videosorveglianza, sulla cui complessiva liceità e sull'eventuale applicazione di sanzioni l'Autorità si esprimerà a breve.

13 Condomìni e multiproprietà

13.1. *Protezione dei dati e condomìni*

Diversi profili di protezione dei dati personali in ambito condominiale, approfonditi negli anni precedenti, sono stati ripresi nel corso del 2004 per rispondere al rilevante numero di segnalazioni e quesiti pervenuti in materia all'Autorità.

In particolare, sono stati posti –sia da parte degli interessati, sia da amministratori di condominio– numerosi quesiti in merito alla diffusione di dati personali riguardanti eventuali situazioni di morosità di singoli condòmini. Ciò, allo scopo di verificare se le modalità di volta in volta utilizzate in concreto, in quanto potenzialmente idonee a rendere tali informazioni accessibili ad un numero indeterminato di soggetti esterni al condominio, fossero compatibili, ed in quali limiti, con le disposizioni contenute nella normativa sulla tutela dei dati personali. Su tale argomento, l'Autorità ha confermato la posizione già assunta in provvedimenti e decisioni adottate nel corso degli anni precedenti.

Il Garante ha avuto modo di precisare che il singolo condòmino può avere conoscenza dei dati disponibili presso l'amministratore, relativi anche agli indirizzi degli altri condòmini, poiché gli indirizzi, così come i nominativi degli interessati, oltre a rendere possibile l'individuazione di ciascun proprietario, sono utili per consentire il regolare svolgimento della vita condominiale (ad esempio, in caso di convocazione dell'assemblea da parte dei condomini o per la comunicazione di avvisi).

L'Autorità ha specificato, inoltre, che i principi in materia di condominio sono applicabili anche nei confronti della gestione di edifici in multiproprietà a scopo residenziale e, con riferimento agli indirizzi di comproprietari che abbiano domicilio o residenza diversi dall'immobile in multiproprietà, qualora ciò sia necessario per particolari e reali esigenze collegate alla gestione della cosa e interessi comuni (*Nota* 11 agosto 2004).

Per contro, in un altro caso sottoposto alla sua attenzione, il Garante ha ribadito che il condominio deve adottare, anche tramite l'amministratore, tutte le cautele necessarie per evitare che terzi non legittimati vengano indebitamente a conoscenza dei dati relativi ai condomini (*Nota* 20 ottobre 2004).

Impianti di videosorveglianza nei condomìni

In relazione al frequente impiego di sistemi di videosorveglianza nei condomìni, il provvedimento del 29 aprile 2004 ha precisato che i videocitofoni sono utilizzabili per identificare coloro che si accingono ad entrare in luoghi privati e che la loro installazione, quando non sono predisposti da persone fisiche per fini esclusivamente personali (art. 5, comma 3, del Codice), deve essere resa nota attraverso un'informativa agevolmente rilevabile.

Quanto all'installazione di vere e proprie telecamere ad iniziativa di singoli condòmini all'interno di edifici in condominio e loro pertinenze (es. posti auto, *box*), il Garante ha precisato che l'impiego di tali sistemi, pur non rientrando nell'ambito di applicazione delle disposizioni del Codice, a meno che i dati siano comunicati sistematicamente o diffusi (art. 5, comma 3, del Codice), richiede comunque l'adozione di cautele a tutela dei terzi. In particolare, l'angolo visuale delle riprese deve essere rigorosamente limitato ai soli spazi di propria esclusiva per-

tinenza, ad esempio antistanti l'accesso alla propria abitazione, escludendo ogni forma di ripresa anche senza registrazione di immagini relative ad aree comuni (cortili, pianerottoli, corridoi, scale, garage comuni) o antistanti l'abitazione di altri condomini; ciò, anche al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.).

Il Codice si applica, invece, in caso di installazione di sistemi di ripresa di aree condominiali da parte di più proprietari o condòmini oppure ad iniziativa di un condominio o della relativa amministrazione (comprese le amministrazioni di *residence* o multiproprietà). In questi casi, l'installazione di impianti è ammissibile a condizione che ricorrano determinate finalità, quali l'esigenza di preservare la sicurezza di persone e la tutela di beni in presenza di concrete situazioni di pericolo (di regola costituite da illeciti già verificatisi); la valutazione di proporzionalità, da effettuare anche nei casi di utilizzazione di sistemi di videosorveglianza che non prevedano la registrazione dei dati, va effettuata in rapporto ad altre misure già adottate o che è possibile adottare (es. sistemi comuni di allarme, blindatura o protezione rinforzata di porte e portoni, cancelli automatici).

Un caso particolarmente delicato ha riguardato l'installazione da parte di un condominio di un impianto di videosorveglianza finalizzato a garantire la sicurezza dei condòmini in seguito ad un grave delitto verificatosi in uno stabile vicino. L'Autorità ha ritenuto che, nel caso di specie, trovassero applicazione le prescrizioni e i principi richiamati nel citato provvedimento del 29 aprile, ed ha invitato l'amministrazione del condominio a fornire un riscontro dettagliato su finalità e proporzionalità del trattamento, tempi di conservazione delle immagini registrate, nonché sull'eventuale designazione del responsabile dell'impianto come "responsabile" o "incaricato" del trattamento delle immagini, il quale potrebbe accedere ai dati solo attenendosi alle istruzioni del condominio (*Nota* 5 ottobre 2004).

14 Dati biometrici

14.1. *Protezione dei dati e biometria*

L'impiego di sistemi di rilevazione di impronte digitali comporta chiaramente un trattamento di dati personali, intendendosi in tal senso "*ogni informazione relativa a persona fisica,..., identificat[a] o identificabil[e], anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" (art. 4, comma 1, lett. *b*), del Codice). Tale trattamento di dati personali può avvenire solo se proporzionato rispetto alle finalità che si vogliono perseguire: il titolare, prima ancora di dare inizio al trattamento, deve quindi valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione di un sistema di rilevazione delle impronte digitali sia in concreto realmente proporzionata, anche nelle modalità prescelte, rispetto agli scopi prefissi e legittimamente perseguibili.

In questo ambito, sono pervenute all'Ufficio numerose richieste di cittadini relative all'installazione, da parte di alcune banche, di sistemi di rilevazione biometrica per l'accesso alle filiali associati ad apparecchiature di videosorveglianza. In un caso del tutto particolare, originato dalla segnalazione relativa all'utilizzo di un sistema di rilevazione dell'impronta digitale per l'accesso ad una banca, l'Autorità (*Nota* 29 ottobre 2004), ribadendo il chiaro orientamento già espresso che delimita l'uso a casi del tutto eccezionali, valuterà quanto dichiarato dalla banca circa le specifiche e concrete esigenze di sicurezza che hanno giustificato l'installazione dell'impianto (nell'Agenzia segnalata si erano verificati due episodi di rapina). Nel frattempo, ha segnalato interlocutoriamente alla banca la necessità di adottare talune misure: predisporre meccanismi che, in caso di libera indisponibilità dell'utente al rilascio dei propri dati biometrici, gli permettano comunque di accedere alla banca; abbinare il sistema di rilevazione ai comuni dispositivi d'ingresso già in uso, evitando il ricorso a meccanismi complicati ed ulteriori rispetto a quelli già comunemente utilizzati per l'ingresso in banca.

Sul tema dell'impiego da parte delle banche di dati biometrici, eventualmente in associazione a sistemi di videosorveglianza, è in corso un approfondimento con l'Associazione bancaria italiana che, anche a seguito di alcuni incontri con l'Ufficio, si è impegnata a far pervenire gli elementi necessari per consentire all'Autorità di esprimersi nuovamente in materia a seguito di una completa valutazione dell'entità e rilevanza del fenomeno. Uno specifico approfondimento si è avuto, inoltre, in occasione di un convegno organizzato presso la Confindustria.

Il Garante, infine, sta effettuando accertamenti specifici a seguito di alcune segnalazioni circa l'impiego, da parte di talune società, di tecniche di autenticazione biometrica (impronta palmare o facciale) per la rilevazione delle presenze del personale dipendente, in considerazione del fatto che il trattamento di dati biometrici in tale ambito è in molti casi eccedente e ingiustificato alla luce dei principi di necessità e proporzionalità.

Dati biometrici in ambito pubblico

Ulteriori interventi hanno riguardato l'installazione di impianti di rilevazione delle impronte digitali per il controllo degli accessi ai luoghi di lavoro o a servizi di mensa universitaria.

In merito all'iniziativa di un ente regionale per il diritto allo studio, volta ad

installare lettori di impronte digitali in ristoranti e pizzerie convenzionati al fine di controllare che l'accesso al servizio di ristorazione avvenisse esclusivamente da parte degli aventi diritto, l'Autorità aveva già avuto modo di chiarire nei primi mesi del 2004 che tale sistema era sproporzionato rispetto alle finalità di controllo della spesa perseguite (*Newsletter* 12-18 gennaio 2004).

In seguito, il Garante ha accertato che tale ente regionale per il diritto allo studio ha nuovamente manifestato la concreta volontà di installare tali sistemi di rilevazione delle impronte digitali per l'accesso ai servizi di ristorazione convenzionati, avendo riscontrato un aumento degli ingressi a tali esercizi di ristorazione da parte di soggetti non autorizzati. L'Autorità ha quindi disposto il blocco del trattamento di dati personali degli studenti effettuato tramite tale sistema di rilevazione delle impronte digitali, riaffermando il principio secondo cui la raccolta generalizzata di dati biometrici di un gruppo selezionato di individui (tutti gli studenti universitari iscritti ad un ateneo) risulta sproporzionata rispetto ad un generico bisogno di "regolare l'utilizzo del servizio ristorazione" in assenza di reali esigenze di sicurezza determinate da concrete e gravi situazioni di rischio (*Provv.* 16 dicembre 2004).

In tale occasione, è stato anche ribadito che i sistemi di rilevazione di impronte digitali rappresentano una *extrema ratio,* potendo essere attivati solo quando, dopo matura riflessione, altre misure (nel caso esaminato, la vigilanza all'ingresso delle mense, ovvero l'esibizione del tesserino di riconoscimento da parte degli studenti) siano valutate del tutto insufficienti o inattuabili, e non quando tale scelta risulti semplicemente meno costosa o di più rapida attuazione ovvero risponda a mere esigenze di apparenza o di "prestigio".

Sono in corso, inoltre, vari approfondimenti in merito a diversi progetti attivati da enti pubblici diretti a sostituire il normale controllo degli accessi al luogo di lavoro (foglio firme, *badge* magnetico) con sistemi di rilevazione delle impronte digitali o di altri dati biometrici come la geometria della mano.

15 Reti di comunicazione elettronica

15.1. *Notazioni introduttive*

Il rapido sviluppo tecnologico degli ultimi anni ha reso sempre più urgente l'individuazione a favore degli utenti dei servizi di comunicazione elettronica di un elevato livello di protezione dei diritti della personalità, con particolare riguardo alla protezione dei dati e del segreto nelle comunicazioni.

Anche in considerazione della crescente convergenza fra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione, l'Autorità è intervenuta, cooperando talora con altri soggetti istituzionali (come riferito nel par. 21.4) e con i diversi operatori del settore, svolgendo un'ampia serie di attività: adozione di provvedimenti, attività istruttorie ed ispettive (in taluni casi a seguito di ricorsi decisi dall'Autorità); intense, inoltre, le attività di studio e monitoraggio che in alcuni casi, come si vedrà più avanti, sono giunte ad uno stadio avanzato, con l'apertura di procedure di consultazione pubblica.

15.2. *Dati di traffico*

Si è già dato conto (v. *Relazione 2003*) delle modifiche apportate all'art. 132 del Codice, in materia di conservazione di dati di traffico per finalità di accertamento e repressione di reati (*ex* art. 3, decreto-legge 24 dicembre 2003 n. 354, convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45). Si può qui brevemente ricordare che, nella sua formulazione originaria, l'art. 132 prevedeva che, per le predette finalità, i fornitori di servizi di comunicazione elettronica dovessero conservare i dati relativi al traffico telefonico per trenta mesi; il citato decreto legge, approvato a ridosso dell'entrata in vigore del Codice, aveva prolungato il periodo di conservazione ad un periodo massimo di cinque anni, estendendolo anche al traffico su Internet.

Tale soluzione suscitò forti preoccupazioni anche al di fuori del circuito istituzionale; il Garante manifestò forti riserve, soprattutto alla luce della prevista estensione delle nuove regole al traffico su Internet, che avrebbe determinato una forte compressione delle garanzie della persona, anche in relazione ai principi costituzionali in materia di libertà delle comunicazioni e segretezza della corrispondenza.

La soluzione adottata in sede di conversione del decreto-legge ha portato a sopprimere ogni riferimento ai dati di traffico diversi da quello telefonico (in particolare Internet), determinando in complessivi quattro anni i tempi di conservazione dei soli dati di traffico telefonico.

Analoghe preoccupazioni, con espresso riferimento all'ipotesi di conservazione dei dati di traffico telematico, sono state ribadite dall'Autorità –nell'audizione in Commissione giustizia della Camera dei Deputati il 24 novembre 2004– in sede di esame del disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (del quale si è riferito nel par. 1.2).

In questa occasione sono stati richiamati, oltre al quadro normativo europeo e nazionale e alla giurisprudenza costituzionale in materia di segretezza delle comuni-

cazioni, anche le conclusioni cui è pervenuto lo stesso Parlamento, in particolare nel corso della discussione del decreto-legge n. 354/2003 (cfr. par. 1.2). Nell'ambito dei dati di traffico telematico è stata altresì sottolineata la difficoltà di distinguere, anche sul piano tecnico, i dati "esteriori" (tutelati anch'essi dalla garanzia costituzionale, ma acquisibili sulla base di un ordine di esibizione da parte dell'autorità giudiziaria, senza le garanzie previste dal codice di procedura penale in materia di intercettazioni) da quelli di "contenuto". Infatti, vi sono diversi casi in cui dati apparentemente "esteriori" sono idonei a rivelare il contenuto della comunicazione (ad esempio, i messaggi allegati alle *e-mail*, i contenuti di *chat* e *newsgroup*), le scelte della persona e, in alcuni casi, anche dati sensibili (è il caso di dati di accesso ai siti *web*).

Fermo restando il potere-dovere dell'autorità giudiziaria e di polizia di accedere a fonti di prova eventualmente disponibili in base alla legge (ad es. i dati di traffico telefonico), è stato evidenziato il rischio che un eventuale obbligo di (indiscriminata) conservazione di tutti i dati di traffico telematico configuri già, esso stesso, una sostanziale limitazione della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione.

Con riferimento alla conservazione dei dati di traffico telefonico, il Garante, conformemente alla previsione dell'art. 132, comma 5, del Codice, ha avviato i lavori necessari a individuare le misure e gli accorgimenti al cui rispetto è subordinato il trattamento per le finalità di accertamento e repressione dei reati. A tale scopo sono stati acquisiti elementi utili nel corso di incontri con diversi operatori telefonici, al fine della verifica preliminare dei sistemi attualmente utilizzati, in conformità con quanto stabilito dall'art. 17, comma 2, del Codice, cui l'art. 132, comma 5, fa espresso richiamo.

Accesso ai dati di traffico

Per quanto concerne l'accesso ai dati personali relativi alle comunicazioni telefoniche "in entrata", l'Autorità ha più volte sottolineato (v., da ultimo, *Provv.* 18 febbraio 2004) come il Codice realizzi al riguardo un primo bilanciamento tra il diritto dell'interessato di conoscere i dati che lo riguardano e il diritto alla riservatezza di terzi (utenti chiamanti e soggetti chiamati diversi dall'abbonato), circoscrivendo il diritto del chiamato di accedere ai dati identificativi di telefonate in entrata alle sole informazioni la cui mancata conoscenza possa comportare "*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).

L'Autorità ha ricordato che l'interessato può presentare la propria richiesta di accesso anche prima che sia instaurato un procedimento penale: l'attività investigativa può essere svolta, ai sensi dell'art. 391-*nonies* c.p.p., anche dal difensore che ha ricevuto apposito mandato dalla persona offesa dal reato, per l'eventualità che si instauri un procedimento penale (*Provv.* 15 aprile 2004). Il Garante, pertanto, ha accolto una richiesta di accesso a dati personali relativi al traffico telefonico "in entrata", avendo ritenuto che sussistesse un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive che poteva derivare al ricorrente dalla mancata identificazione del numero telefonico chiamante.

Come evidenziato già nella *Relazione* 2003, il diritto d'accesso ai dati relativi al traffico telefonico può essere esercitato dall'interessato soltanto nei confronti dei dati che lo riguardano, risultando inammissibile la richiesta volta a identificare utenze diverse da quella dell'interessato medesimo.

In relazione a ciò, e in particolare all'accesso ai dati relativi alle chiamate nella telefonia mobile, l'Autorità ha valutato con esito positivo la risposta fornita da un operatore ad una richiesta formulata ai sensi dell'art. 157 del Codice. Il Garante, in particolare, aveva chiesto di conoscere la procedura predisposta dalla società e le

misure di sicurezza adottate al fine di identificare i soggetti che richiedono l'accesso stesso utilizzando il telefono mobile o i servizi *on-line*.

15.3. *I nuovi elenchi telefonici*

La disciplina degli elenchi è stata oggetto di significative modifiche. Scopo peculiare degli elenchi è di consentire la ricerca degli abbonati per le comunicazioni interpersonali; ciò è ora previsto espressamente dall'art. 129, comma 2, del Codice che sancisce, in relazione a tale finalità, il principio della massima semplificazione per l'inserimento degli abbonati negli elenchi e, per le finalità ulteriori, la necessità del preventivo consenso specifico ed espresso degli interessati.

In applicazione di tale principio, e in esito ad un'intensa attività svolta anche in collaborazione con l'Autorità per le garanzie nelle comunicazioni, il Garante ha individuato le modalità da osservare per il corretto inserimento e successivo utilizzo dei dati personali degli abbonati nei nuovi elenchi telefonici (*Provv.* 15 luglio 2004).

Nei nuovi elenchi telefonici possono essere pubblicati anche i dati relativi alle utenze mobili, nonché informazioni ulteriori quali l'indirizzo di posta elettronica, la professione e il titolo di studio. Nel caso in cui l'interessato abbia manifestato il proprio consenso a ricevere informazioni commerciali o promozionali, l'indirizzo o il numero telefonico saranno contrassegnati da uno speciale simbolo: in tal modo l'abbonato potrà ricevere pubblicità telefonica tramite operatore o materiale pubblicitario a domicilio. Diversamente, nel caso di iniziative pubblicitarie realizzate mediante sistemi automatizzati (fax, chiamate senza operatore, messaggi *sms* o di posta elettronica), è comunque necessario raccogliere a parte il consenso specifico dell'interessato. Le scelte espresse dagli interessati possono essere modificate in ogni momento e senza alcun onere.

Il Garante ha altresì predisposto, con la cooperazione dell'Autorità per le garanzie nelle comunicazioni e la collaborazione delle associazioni dei consumatori, un modulo di informativa e richiesta di consenso che gli operatori telefonici devono inviare ai propri clienti entro il 31 gennaio 2005.

Successivamente all'adozione del provvedimento, si sono svolti presso l'Autorità ulteriori incontri con rappresentanti degli operatori telefonici e delle associazioni di consumatori. Nel corso di tali incontri, e principalmente dall'esame dei primi moduli predisposti dalle diverse compagnie, sono emersi alcuni elementi che hanno reso necessario un nuovo intervento del Garante, volto a fornire agli operatori stessi prescrizioni integrative di quelle già impartite, nonché a dare l'avvio alla campagna informativa prevista nel provvedimento stesso.

L'Autorità ha curato una prima campagna di informazione attraverso un apposito *depliant*, che, su sua autorizzazione, verrà inviato dai gestori al domicilio degli abbonati. Un'apposita conferenza stampa si è tenuta il 26 gennaio 2005.

15.4. Spam

È costantemente all'attenzione dell'Autorità il fenomeno dell'invio ad indirizzi di posta elettronica di comunicazioni non sollecitate, non solo di contenuto commerciale, ma anche riconducibili all'ambito del cd. *marketing* politico (cfr. *Provv.* 12 febbraio 2004, oltre al più recente provvedimento del 12 ottobre 2004, presi in considerazione nel par. 8.2).

Gli utenti della Rete hanno manifestato un'accresciuta sensibilità in relazione al

fenomeno *spam*, desumibile dall'intenso contenzioso che ha investito l'Autorità anche nel 2004 (come ricordato nel par. 18.3), oltre che dalle azioni proposte dinanzi all'autorità giudiziaria ordinaria.

Sono proseguite le attività di controllo e verifica effettuate presso i fornitori di servizi di comunicazione elettronica (individuati grazie alle segnalazioni pervenute) al fine di accertare eventuali violazioni dell'art. 130 del Codice e delle prescrizioni contenute nel provvedimento di carattere generale emanato dal Garante il 29 maggio 2003.

Per arginare il fenomeno, il Garante ha partecipato ad alcuni incontri tenuti presso il Ministero delle comunicazioni, cui sono intervenuti operatori di telefonia fissa e mobile, e associazioni di fornitori dei servizi Internet e dei consumatori.

In tali incontri si è lavorato alla possibile stesura di un codice di autoregolamentazione in relazione al quale è stata chiesta la collaborazione di questa Autorità, che fornirà il proprio contributo tenendo però presente il valore cogente delle norme che saranno contenute nel codice di deontologia e di buona condotta per Internet (v. par. 15.8).

Proprio in questo settore, grande rilievo sugli organi di informazione ha avuto la vicenda relativa all'indagine giudiziaria curata dalla Guardia di finanza nei confronti di una società quotata in borsa in relazione all'utilizzo di migliaia di indirizzi *e-mail* per finalità di *marketing*, in assenza del consenso informato degli interessati.

Sulla vicenda, per la quale sono indagati due responsabili della società per reati che vanno dall'illecito trattamento dei dati personali alla frode informatica ed all'accesso abusivo a sistemi informatici, il Garante ha ricevuto di recente copia di alcuni atti e valuterà a breve l'eventuale adozione dei provvedimenti di competenza.

15.5. Sms *istituzionali*

In occasione delle elezioni del 12 e 13 giugno 2004, gli utenti di telefonia mobile hanno ricevuto *Sms* "firmati" dalla Presidenza del Consiglio dei ministri con i quali si comunicavano orari e modalità di voto delle imminenti consultazioni elettorali.

A seguito di più di 4500 reclami e segnalazioni il Garante, al fine di acquisire ogni elemento idoneo a valutare la questione, ha richiesto informazioni al Ministero dell'interno (che aveva disposto l'invio degli *Sms* con proprio d.m. del 9 marzo 2004) ed agli operatori di telefonia mobile.

Pur prendendo atto dell'esistenza nel caso specifico di un formale provvedimento del Ministro che ravvisava ragioni contingibili e urgenti, l'Autorità ha sottolineato in termini generali il rischio che impropri riferimenti all'eccezionalità, all'emergenza e alle calamità possano condurre ad una "banalizzazione" dell'invio di messaggi *Sms* da parte di diversi soggetti istituzionali, anche a livello locale (*Provv.* 7 luglio 2004).

Il Garante aveva peraltro già individuato nella eccezionalità e straordinarietà delle circostanze le condizioni per l'invio di comunicazioni via *Sms*, anche in mancanza di previo consenso dell'interessato (*Provv.* 12 marzo 2003).

In relazione alla decisione del Ministero dell'interno di indicare la Presidenza del Consiglio dei ministri come firmataria del messaggio, l'Autorità ha rilevato come nel caso di specie non operasse una disposizione della legge n. 150/2000 sulla comunicazione istituzionale, che riguarda l'invio di messaggi da parte della concessionaria del servizio pubblico radiotelevisivo (art. 3). Con riferimento all'invio di *Sms* in caso di disastri o calamità naturali o per ragioni di tutela dell'ordine pubblico, il soggetto istituzionale "mittente" delle comunicazioni deve poi essere sempre identificabile.

Nel medesimo provvedimento è stata altresì evidenziata la necessità per gli operatori telefonici di integrare l'informativa fornita ai cittadini inserendo la previsione dell'eventualità che, tra i vari trattamenti di dati legati alle utenze, vi sia quello dell'invio di *Sms* istituzionali per effetto di provvedimenti d'urgenza. Tutte le compagnie telefoniche interessate hanno integrato il modello di informativa come richiesto dal Garante.

È stata da ultimo richiesta la cooperazione del Garante da parte della Presidenza del Consiglio dei ministri e del Ministero degli affari esteri ai fini dell'acquisizione dalle compagnie di telefonia di alcuni dati relativi all'utenza mobile di cittadini italiani che si trovavano nelle zone colpite dal maremoto in Asia del 26 dicembre 2004; ciò, in particolare, al fine di consentire al Ministero di inviare un *Sms* agli interessati, invitandoli a dare notizie di sé (cfr. anche par. 1.3 e 15.10).

15.6. *Videochiamate*

Ha formato oggetto di esame da parte dell'Autorità il fenomeno delle cd. videochiamate, ossia le chiamate –realizzate attualmente tramite la rete *Umts*– nel corso delle quali vengono trasmesse, oltre ai suoni, anche immagini dei soggetti coinvolti nella conversazione. La caratteristica peculiare dei trattamenti realizzati in occasione delle videochiamate consiste nel fatto che, a differenza di quanto accade con l'invio degli *Mms* (in relazione al quale si veda il *Provv.* 12 marzo 2003), le immagini vengono trasmesse contestualmente all'effettuazione della chiamata e coinvolgono il chiamante, il chiamato ed eventuali persone situate nelle loro vicinanze.

Ferma restando la generale liceità dell'utilizzo di tali nuove applicazioni tecnologiche, sono di tutta evidenza anche i potenziali pericoli insiti nelle stesse: le videocamere, infatti, oltre ad essere normalmente di dimensioni assai ridotte, il più delle volte non sono dotate di dispositivi acustici o visivi atti a rivelarne il funzionamento all'esterno.

Al fine di acquisire ulteriori elementi di valutazione, il Garante ha attivato una consultazione pubblica preordinata ad un provvedimento che fornirà indicazioni di carattere generale sul corretto utilizzo dei nuovi telefoni mobili c.d. di terza generazione.

15.7. *Servizi di comunicazione elettronica offerti a titolo gratuito*

Non di rado viene rappresentata da parte di utenti dei servizi gratuiti di accesso ad Internet ed alla posta elettronica l'impossibilità di esprimere un consenso specifico e differenziato con riferimento alle diverse finalità del trattamento operato dai fornitori dei medesimi servizi. In particolare, viene talvolta negata la stessa opportunità di usufruire dei predetti servizi nel caso in cui l'utente non presti il consenso al trattamento dei dati per finalità pubblicitarie e commerciali.

In occasione della trattazione di uno specifico ricorso (*Provv.* 12 ottobre 2004) il Garante ha chiarito che è improprio richiedere un ampio e generalizzato consenso –peraltro anche quando lo stesso Codice permette di prescindere da esso, come, ad esempio, per l'eventuale comunicazione dei dati all'autorità giudiziaria (cfr. art. 24, comma 1, lett. *a*), del Codice)– associandovi finalità pubblicitarie e di profilazione per le quali non è lasciata all'utente alcuna libertà nella manifestazione di volontà. La mancata richiesta di consensi differenziati (e limitatamente ai casi in cui sono necessari) determina un quadro confuso che non permette all'utente di esprimere scelte libere, consapevoli e non contraddittorie fra loro.

In questa prospettiva, l'Autorità ha riaffermato la necessità che il consenso sia realmente espresso senza condizionamenti che ne influenzino sotto vari profili la libera manifestazione (art. 23, comma 3, del Codice).

Quanto all'eventuale trattamento dei dati dell'interessato per finalità di profilazione, è stato precisato che tale trattamento potrebbe risultare lecito in determinate circostanze qualora, per i rapporti contrattuali, la società preveda l'assegnazione di un accesso gratuito ad Internet dietro "corrispettivo" di una profilazione lecita, corretta e proporzionata dell'interessato medesimo.

15.8. *Il codice deontologico*

Nell'ambito delle iniziative promosse in vista della predisposizione del codice deontologico e di buona condotta sui trattamenti dei dati personali effettuati dai fornitori dei servizi di comunicazione ed informazione offerti per via telematica (art. 133 del Codice), è stata avviata la consultazione delle organizzazioni rappresentative degli operatori del settore e dei consumatori che hanno aderito all'invito a partecipare formulato in precedenza dall'Autorità. Ciò è stato ritenuto opportuno al fine di identificare, congiuntamente ai soggetti a vario titolo interessati, gli aspetti che presentano particolari criticità sotto il profilo della protezione dei dati.

Alla luce dei primi contributi pervenuti, nonché degli studi da tempo avviati dalla stessa Autorità, sono state individuate alcune specifiche questioni che potranno essere oggetto di disciplina nell'adottando codice. Tra queste si ricordano, ad esempio, le modalità ed i contenuti dell'informativa; i profili relativi all'acquisizione del consenso ed ai diritti degli interessati; l'adozione di particolari misure di sicurezza; gli strumenti tecnici e giuridici di contrasto del fenomeno dello *spamming*, ivi compresa l'adozione di procedure di filtraggio o altre misure praticabili; l'individuazione di bollini di qualità per il trattamento dei dati posti in essere dagli operatori del settore; i problemi relativi alla registrazione dei nomi a dominio.

La definizione del codice in questione potrà fornire, sia agli operatori, sia agli utenti delle reti di comunicazione elettronica, riferimenti più precisi per assicurare il rispetto della normativa sulla protezione dei dati personali e, in particolare, dei principi generali di cui all'art. 11 del Codice.

15.9. *La televisione digitale: i servizi interattivi*

L'Autorità ha ultimato uno specifico studio sulle caratteristiche della televisione satellitare e interattiva individuando alcuni primi aspetti di rilevanza per la normativa sulla protezione dei dati personali.

Grazie allo sfruttamento delle potenzialità offerte dalla tecnologia digitale, è possibile offrire attraverso la televisione anche servizi caratterizzati dall'interattività: attraverso il collegamento di un apposito apparecchio (*decoder*) alla linea telefonica, l'utente può, ad esempio, partecipare a sondaggi, giochi, test o usufruire di particolari servizi di pubblica utilità erogati dalle amministrazioni pubbliche (cd. *T-government*), o ancora, usufruire di servizi cd. transattivi, previa identificazione ed autorizzazione, grazie all'inserimento nel *decoder* medesimo di particolari "carte identificative" (*smart card*).

Agli indubbi vantaggi derivanti da questa tecnologia, si affiancano, tuttavia, alcune criticità con riguardo alla tutela della sfera privata degli utenti: l'uso dei servizi e programmi interattivi può determinare un'esposizione, anche inconsapevole,

dei gusti, delle abitudini ed in generale della personalità dell'utente. Questi dati, opportunamente raccolti e trattati, potrebbero dare luogo al monitoraggio delle preferenze e dell'attività dell'utente medesimo. La circostanza che la raccolta dei dati avvenga in un ambito tipicamente "privato" (come quello familiare, nel quale l'individuo nutre la ragionevole aspettativa di essere al riparo da forme di controllo esterne) suscita ulteriori preoccupazioni. Inoltre, ad uno stesso apparecchio televisivo corrispondono di regola più fruitori (appartenenti o estranei al nucleo familiare dell'abbonato), i quali debbono essere messi in grado di compiere liberamente le proprie scelte in merito al trattamento dei dati personali che li riguardano.

Proprio al fine di approntare idonee cautele onde evitare che siano svolte illecite operazioni di profilazione ed invasive forme di controllo sulle abitudini delle persone, l'Autorità ha avviato una consultazione pubblica in vista della predisposizione di un provvedimento a carattere generale.

15.10. *Dati relativi all'ubicazione*

Negli ultimi anni si è assistito ad una rapida diffusione dei servizi basati sull'ubicazione. Tali servizi, pur presentando aspetti di indubbia utilità, possono comportare seri rischi per le libertà civili dell'interessato, potendo determinare un'esposizione, anche inconsapevole, dello stesso ad un controllo sistematico dei suoi spostamenti ovvero dei gusti e delle abitudini manifestati in occasione di specifiche richieste.

In questa prospettiva assume una particolare importanza il fatto che l'interessato sia pienamente a conoscenza delle caratteristiche del trattamento di dati che lo riguarda, nonché dei soggetti che svolgono il trattamento medesimo; ciò, anche al fine di prestare un consenso libero, specifico ed informato.

Proprio in ragione della particolare delicatezza di tali trattamenti, l'Autorità intende offrire indicazioni e chiarimenti ai soggetti che vogliano fornire tali tipologie di servizi. Al riguardo si segnala che il Garante sta ultimando la predisposizione di un provvedimento di carattere generale a completamento di quanto già disposto in materia dall'art. 126 del Codice.

Uno sviluppo di queste problematiche si è avuto con la menzionata richiesta della Presidenza del Consiglio dei ministri di acquisire dai vari gestori di telefonia mobile i dati di cittadini italiani che, in relazione alle informazioni sull'ubicazione dell'apparecchio disponibili presso i gestori stessi, risultavano trovarsi negli stati colpiti dal maremoto in Asia (v. par. 1.3 e 15.5).

Ferma restando la necessità di bilanciare la tutela della riservatezza con esigenze di salvaguardia della vita e dell'incolumità delle persone, questa vicenda pone (su un piano più generale) l'interrogativo se i dati relativi all'ubicazione degli apparecchi di telefonia mobile (e quindi, indirettamente, delle persone che li detengono), allorché siano diversi dai dati relativi al traffico telefonico –assistiti, questi ultimi, dalle garanzie costituzionali di libertà e segretezza della corrispondenza– godano comunque di una tutela costituzionale, e quale, anche alla luce del principio della libertà di circolazione (art. 16 Cost.).

15.11. Radio Frequency Identification

Il Garante ha seguito con grande attenzione lo sviluppo delle tecniche di identificazione via radiofrequenze (*Radio Frequency Identification-Rfid*).

Tali tecnologie si fondano sull'utilizzo di micro-processori che, collegati ad

un'antenna ed impiegati come etichette di riconoscimento (*cd. etichette intelligenti*), sono in grado di trasmettere –attraverso onde radio– segnali leggibili da appositi lettori dotati di un'antenna di attivazione/ricezione.

La *Rfid* rappresenta uno strumento utile in numerosi settori e per diverse finalità: essa può essere impiegata, ad esempio, per il "tracciamento" di singole unità di prodotto nella catena di distribuzione dell'industria; per la prevenzione di furti e di contraffazioni dei prodotti; per garantire una maggiore rapidità nelle operazioni commerciali; per il controllo degli accessi ad aree riservate. L'utilizzo di questa tecnologia può, in alcuni casi, comportare un trattamento di dati personali rendendo necessaria l'applicazione della relativa normativa. Attraverso le cd. "etichette intelligenti" si possono trattare, anche senza che l'interessato ne sia a conoscenza, innumerevoli dati personali che lo riguardano, compresi quelli di natura sensibile; raccogliere dati sulle abitudini del medesimo ai fini di profilazione attraverso l'aggregazione con altre informazioni di carattere personale; verificare prodotti (vestiti, accessori, medicine, ecc.) indossati o trasportati; tracciare i percorsi effettuati.

Il Garante ha svolto una prima attività di approfondimento della materia in questione, rivolgendo l'attenzione al possibile impatto che le tecniche di identificazione via radio possono già avere sulle condizioni di esercizio delle libertà delle persone e alle problematiche che la loro introduzione è destinata a sollevare relativamente all'applicazione della normativa sulla tutela dei dati personali.

Tutto questo anche in vista del fatto che, se attualmente il terreno di elezione della *Rfid* appare ancora il settore industriale (soprattutto all'interno della catena di distribuzione, dove però la sua applicazione non comporta, il più delle volte, un trattamento di dati personali), tale tecnologia presenta enormi potenzialità: in prospettiva, anche in vista dell'ulteriore sviluppo tecnologico, dell'abbattimento dei costi di produzione, della possibilità di integrazione con altre infrastrutture di rete (telefonia, Internet, ecc.), le tecniche di identificazione via radio-frequenza potranno avere un impiego sempre maggiore e nei più diversi settori.

Occorre tenere altresì presente che più gravi pericoli per gli interessati possono derivare dal prevedibile incremento della potenza dei sistemi di *Rfid* (i quali potrebbero rendere fattibile una "lettura" delle etichette a maggiori distanze) nonché –specie in ragione dell'adozione di *standard* tecnici comuni– dalla possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, "riscrittura").

L'attività istruttoria compiuta dall'Autorità in merito al trattamento dei dati nell'ambito della *Rfid* si è svolta anche attraverso contatti in Italia e all'estero con alcuni operatori del settore, che hanno portato ad un proficuo scambio di informazioni.

Consultazione pubblica

Al medesimo scopo è stata indetta una specifica consultazione pubblica cui è stata data ampia visibilità anche attraverso il sito *web www.garanteprivacy.it*. A completamento delle informazioni già acquisite, l'Autorità si è così potuta avvalere degli ulteriori elementi di valutazione provenienti da osservazioni e commenti inviati dalle associazioni di utenti, consumatori, operatori dei settori interessati e singoli cittadini.

Impianto sottocutaneo di etichette *Rfid*

Uno dei più recenti ambiti di utilizzo di questa tecnologia riguarda l'impianto sottocutaneo di dispositivi *Rfid* anche su persone. Si ha già notizia dell'avvio, anche in Italia, di tecniche di inserimento di *microchip* nel corpo umano per diverse finalità: ad esempio, allo scopo, di conservare e rendere all'occorrenza disponibili informazioni sullo stato di salute del paziente; al fine di verificare l'accesso a determinati luoghi riservati; ancora, per garantire pagamenti rapidi in transazioni commerciali di vario tipo.

La delicatezza di tali interventi è di tutta evidenza, sì da sollevare interrogativi circa le ripercussioni che i relativi trattamenti possono avere sulla dignità della persona (art. 2, comma 1, del Codice).

16 Sicurezza dei dati e dei sistemi

16.1. *Le misure minime di sicurezza*

L'Autorità –a seguito di numerose richieste di proroga e di chiarimenti pervenute circa il nuovo quadro normativo in materia di misure minime di sicurezza introdotto dal Codice– ha precisato che l'applicazione delle misure minime (artt. 33-35 del Codice e allegato B), la cui omessa adozione costituisce reato (art. 169 del Codice), va graduata a seconda che i trattamenti di dati personali, sensibili e giudiziari, siano effettuati con o senza l'ausilio di strumenti elettronici. Queste misure rappresentano, però, solo i requisiti minimi ai quali tutti i titolari del trattamento (anche a mezzo del responsabile, ove designato) devono attenersi nella protezione dei dati. Vi è, infatti, il dovere più generale di adottare misure preventive idonee (art. 31 del Codice), la cui mancata predisposizione può esporre il titolare a responsabilità civile per eventuali danni cagionati a terzi (*Nota* 22 marzo 2004).

Nella stessa sede il Garante ha ricordato anche che la redazione del Documento programmatico sulla sicurezza (Dps) rientra tra le misure minime di sicurezza e che qualsiasi titolare pubblico o privato deve redigerlo se effettua un trattamento di dati sensibili e/o giudiziari con strumenti elettronici.

Inoltre, le misure minime già previste dal d.P.R. n. 318/1999 e riprodotte nell'allegato B) restano obbligatorie senza differimenti. Il termine transitorio, di recente nuovamente prorogato al 30 giugno 2005 (decreto-legge 9 novembre 2004, n. 266, convertito, con modificazioni, con legge 27 dicembre 2004, n. 306; salva l'ulteriore proroga al 30 settembre 2005, da riferire al solo caso in cui obiettive ragioni tecniche non consentano di adottare subito alcune misure) riguarda, infatti, solo le "*nuove*" misure minime che non erano già previste dal citato d.P.R. n. 318/1999 (art. 180, comma 1 e 3, del Codice).

L'Autorità ha inoltre precisato che è sostenibile ipotizzare che la redazione del Dps sia una "nuova" misura minima, con la conseguenza che, anche per questo adempimento, vale il termine del 30 giugno 2005. Il Garante ha poi messo a disposizione degli operatori, sul proprio sito *web*, una guida utilizzabile per agevolarne la redazione soprattutto presso le realtà medio-piccole.

Gli stessi principi sono stati tra l'altro confermati dall'Autorità nel già richiamato parere reso al Consiglio nazionale forense (*Nota* 3 giugno 2004) sui principali adempimenti in materia di protezione di dati personali nello svolgimento dell'attività forense, con il quale si è anche precisato che, per quanto riguarda l'organizzazione del lavoro quotidiano di studio, non occorre affatto depennare il nome delle parti dalla copertina dei fascicoli cartacei ed utilizzare solo numeri identificativi. Resta invece necessario seguire opportune modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti.

L'orientamento del Garante è stato inoltre ribadito con un recente parere, anch'esso già menzionato (*Nota* 3 dicembre 2004), in materia di trattamento dei dati personali da parte dei notai rilasciato al Consiglio nazionale del notariato (v. pure par. 10.2).

Profili applicativi

Su richiesta di un dipendente di un ufficio legale comunale, l'Autorità ha rilevato i limiti entro i quali un dirigente può utilizzare la *password* del dipendente per accedere ai dati contenuti nel suo *computer* in caso di assenza di quest'ultimo.

L'adozione di un sistema di "autenticazione informatica" per gli incaricati del trattamento effettuato con strumenti elettronici rientra tra le misure "minime" di sicurezza aggiornate dal Codice. Secondo le modalità tecniche specificate nell'allegato B) del Codice, tale sistema deve basarsi sull'attribuzione all'incaricato di credenziali di autenticazione che possono consistere anche in un codice per l'identificazione associato ad una parola chiave riservata conosciuta solamente a quest'ultimo (regole nn. 1 e 2).

In particolare, quando i dati sono accessibili soltanto attraverso l'uso di parole chiave è possibile rendere disponibili le medesime informazioni solo in caso di prolungata assenza o impedimento dell'incaricato, sempre che l'intervento si rilevi indispensabile e indifferibile e sia altresì esclusivamente motivato da esigenze di operatività o di sicurezza del sistema. Proprio in vista di tali evenienze, è necessario individuare con chiarezza le modalità attraverso le quali il titolare può assicurare la disponibilità dei dati mediante idonee e preventive indicazioni fornite per iscritto. In tal caso, l'incaricato deve essere tempestivamente informato dell'intervento effettuato (regola n. 10 dell'allegato B).

Tali accorgimenti, oltre a consentire di proteggere i dati personali contenuti nella memoria dell'elaboratore dalla possibile intrusione di soggetti non autorizzati –specie se si tratta di dati giudiziari, come del caso sottoposto all'esame dell'Autorità–, permettono contestualmente di renderli disponibili in particolari casi di necessità e urgenza per trattamenti consentiti ed effettuati secondo modalità predeterminate chiaramente per iscritto dal titolare (*Nota* 16 luglio 2004).

A conclusione degli accertamenti svolti in seguito ad alcune segnalazioni relative alla raccolta e al trattamento di dati personali di clienti effettuato da una società nell'ambito di un servizio sperimentale di gestione *on-line* di polizze assicurative, l'Autorità ha ritenuto soddisfacente il riscontro fornito circa le misure tecniche ed organizzative adottate a protezione delle transazioni effettuate sul proprio *server web*. Gli accessi alle banche di dati personali relativi alle polizze assicurative, consentiti solo ad utenti registrati in apposite aree riservate del sito *web* della società, sono risultati protetti tramite specifiche misure di sicurezza (cd. protocollo *https*).

Si è comunque ricordato alla società che, per il trattamento di dati personali sensibili e/o giudiziari effettuato con strumenti elettronici, devono essere comunque adottate preventivamente idonee misure di sicurezza (art. 31 del Codice), oltre a quelle minime prescritte dal Codice (*Nota* 22 ottobre 2004).

L'Autorità sta concludendo accertamenti a seguito di un reclamo con il quale si è segnalata la diffusione di dati personali causata dall'asserito abbandono di documenti, da parte di una filiale della banca, in occasione del rilascio dei locali ove si svolgeva la sua attività (*Nota* 29 luglio 2004).

Il Garante si è inoltre pronunciato sul reclamo di un lavoratore che contestava le modalità di consegna di una lettera di sanzione disciplinare da parte del datore di lavoro (*Nota* 23 novembre 2004). Il dipendente aveva ricevuto una comunicazione di sanzione disciplinare contenuta in un foglio non spillato, né racchiuso in busta sigillata, consegnatogli a mano e recante la chiara indicazione dell'oggetto della lettera e della sanzione comminata. Dando attuazione ai principi di proporzionalità, pertinenza e non eccedenza dei dati, è stato chiesto alla società di prevedere che la comunicazione della sanzione all'interessato venga in ogni caso inserita in busta chiusa e sigillata; è stato inoltre prescritto di impartire precise istruzioni a tutti gli uffici e dipendenti formalmente incaricati di tali trattamenti di dati, volte all'ado-

zione di modalità e misure idonee a garantire la sicurezza e la riservatezza di comunicazioni contenenti dati relativi ai lavoratori interessati e ad evitare un accesso, anche casuale, da parte di terzi non autorizzati ai dati riportati al loro interno.

Ricevuta la segnalazione di un dipendente di una società che, alla ripresa del servizio dopo un prolungato periodo di assenza dal lavoro, non aveva trovato alcuni documenti personali lasciati in un armadio aziendale, l'Autorità dovrà valutare se sussistono o meno profili di violazione della normativa di protezione dei dati, anche in relazione alla circostanza che i documenti in questione siano relativi a trattamenti effettuati per ragioni di servizio.

17 Registro dei trattamenti

17.1. *La notificazione*

Linee normative

La nuova modalità di notificazione del trattamento dei dati personali al Garante (disciplinata dagli artt. 37, 38, 181, comma 1, lett. *c*), del Codice) presenta profondi cambiamenti sia nei contenuti, sia nelle modalità di compilazione, rispetto alla precedente normativa (artt. 7, 16 e 28, l. n. 675/1996): basti qui ricordare che, mentre quest'ultima prescriveva un obbligo di carattere generale di notificazione per un numero consistente di trattamenti –salve, comunque, le varie eccezioni previste dalla legge–, il Codice reca ora un più ristretto "elenco positivo" di trattamenti soggetti ad obbligo di notificazione, che il Garante può peraltro sviluppare attraverso un proprio provvedimento, il che attesta la conformità della soluzione innovativa ora prescelta dal legislatore italiano alla direttiva europea.

Il provvedimento di esonero

Il Garante si è già avvalso del potere di esonerare dal predetto obbligo alcuni trattamenti rientranti nelle generali previsioni di cui all'art. 37, ma in concreto ritenuti non suscettibili di recare specifico pregiudizio ai diritti e alle libertà dell'interessato (art. 37, comma 2). In base a tale disposizione con il provvedimento n. 1 del 31 marzo 2004 (v. *Documentazione* par. 39), l'Autorità ha individuato diverse ipotesi di trattamento sottratte all'obbligo di notificazione: è stato previsto, ad esempio, un esonero per il trattamento di dati genetici e biometrici trattati in maniera non sistematica da esercenti la professione sanitaria, purché non organizzati in banche dati accessibili da terzi; o, ancora, per il trattamento dei medesimi dati da parte degli avvocati, purché necessario a condurre investigazioni difensive o a far valere o difendere un diritto anche da parte di terzi in sede giudiziaria. È altresì possibile che, all'esito di questa prima fase di applicazione del Codice, si possano individuare, anche in collaborazione con le categorie interessate, ulteriori esoneri dall'obbligo di notificazione.

Il Garante ha poi ritenuto, allo stato, di non individuare ulteriori trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in aggiunta alla lista figurante nell'art. 37, comma 1, e pertanto da sottoporre all'obbligo di notificazione.

Ulteriori chiarimenti del Garante

Dopo il provvedimento che ha espressamente escluso la notificazione per alcuni trattamenti di dati personali, l'Autorità ha fornito numerosi chiarimenti per il settore privato (imprese, banche, assicurazioni, professionisti, enti *no-profit*) su alcuni trattamenti che devono ritenersi comunque sottratti all'obbligo di notificazione in base ad una corretta interpretazione delle disposizioni del Codice (*Nota* 23 aprile 2004; v. anche *Newsletter* n. 209 del 5-25 aprile 2004); ulteriori chiarimenti sono stati forniti in risposta a quesiti presentati dalla FnomCeo, dalla Fimmg e dall'Anisap, circa l'esatta individuazione dei trattamenti da notificare al Garante in ambito sanitario (*Nota* 26 aprile 2004; v. anche *Newsletter* n. 210 del 26 aprile-2 maggio 2004, consultabili sul sito *web* dell'Autorità).

La nuova notificazione

Accanto alla forte riduzione del numero dei trattamenti, è stata operata contemporaneamente, alla luce dell'esperienza, una drastica semplificazione dei contenuti e delle

modalità di compilazione del modello informatico. La nuova notificazione può avvenire anzitutto solo in via telematica e accompagnata dalla firma digitale; gli elementi richiesti sono pochi, ma significativi, di immediata comprensione e di facile redazione.

Il nuovo sistema ha così prodotto solo un numero limitato di notificazioni (circa 10.000 rispetto alle oltre 330.000 pervenute precedentemente ai sensi della legge n. 675/1996), circoscrivendo l'istituto alle sole ipotesi di trattamento "rischioso" per gli interessati, come prescritto dalla normativa comunitaria, e azzerando i casi di notificazione irregolare che avevano comportato in passato un onere assai rilevante per l'Ufficio del Garante.

Risoluzione di inconvenienti tecnici

Alcune temporanee e iniziali difficoltà tecniche dovute all'enorme traffico telematico registrato a ridosso della scadenza del termine per adempiere all'obbligo di notificazione fissato per il 30 aprile 2004 hanno indotto il Garante, avvalendosi delle facoltà previste dall'art. 38 del Codice, a riconoscere ulteriori quindici giorni a coloro che avevano tempestivamente intrapreso le operazioni di notificazione e che, per impossibilità tecniche a loro non imputabili, non erano riusciti a concludere la procedura. Alcuni interventi sulla stampa di dirigenti dell'Ufficio hanno ricostruito i punti estremamente interessanti di questo primo riuscito esperimento generalizzato nella p.a. di utilizzo della firma digitale per la produzione di un atto a rilevanza giuridica anche penale.

Il consistente potenziamento della banda trasmissiva utilizzata anche da molti visitatori interessati ad analizzare la procedura pur non dovendo notificare in concreto, e il breve differimento al 15 maggio 2004 del termine per concludere la notificazione hanno offerto agli utenti idonee opportunità di completare le operazioni di notificazione senza ulteriori problemi.

I vantaggi della procedura telematica

La procedura per la notificazione in via telematica ha dato ottima prova anche sotto l'aspetto della facilità d'uso. Il fatto che la medesima possa essere avviata e portata a termine nella sua interezza da una qualsiasi postazione, in qualunque momento e con l'assistenza *on-line* da parte del personale dell'Autorità durante l'orario d'ufficio, costituisce un indubbio vantaggio per l'utente.

Le procedure telematiche di notificazione si sono rivelate di qualità elevata per celerità nell'effettuare adempimenti e ricerche, affidabilità del programma di gestione, correttezza dei dati inseriti e puntualità nei riscontri.

Ulteriori prospettive

Permane tra gli obiettivi del Garante quello di mantenere alta la qualità del sistema di notificazione arricchendolo nel tempo di ulteriori elementi e procedure anche al fine di tenerlo al passo con lo sviluppo tecnologico e le prospettive di miglioramento complessivo delle attività dell'Autorità.

Accanto al perfezionamento dell'attuale versione, non va esclusa nel medio periodo la possibilità che, in conformità a quanto verrà deciso a livello europeo sulla standardizzazione della notificazione nei vari paesi, siano apportate modifiche al registro dei trattamenti e ai contenuti della notificazione. Una delle modifiche potrebbe, ad esempio, riguardare la redazione del modello anche in lingua inglese.

Nel corso dell'anno 2005 il Dipartimento registro dei trattamenti sarà comunque impegnato già nella predisposizione e messa a disposizione del modello di notificazione in lingua tedesca (come già avvenuto per la provincia di Bolzano con il vecchio modello di notificazione su carta).

Doppia notificazione

Nonostante il sistema di notificazione risulti agevole anche a fronte delle istruzioni esaustive e replicate in diversi passaggi della procedura, si sono riscontrati

pochi casi (limitati a qualche decina) di doppia notificazione da parte dello stesso titolare o di richiesta di annullamento di quella già inviata in quanto non dovuta.

L'orientamento dell'Ufficio è stato quello di restituire l'importo dei diritti di segreteria a coloro che, pur avendo iniziato la notificazione, non avevano ancora proceduto all'invio della medesima al Garante. Nei casi di doppia notificazione, invece, su dichiarazione del titolare, l'Ufficio ha provveduto ad "oscurare" una delle due, restituendo i diritti di segreteria pagati in eccesso.

Annullamento di notificazione inviata

Non sono state accolte, invece, le richieste di semplice "annullamento" della notificazione da parte di coloro che l'avevano validamente inviata, nonostante fosse a posteriori ritenuta non dovuta secondo il giudizio sopravvenuto del (solo) titolare del trattamento. Questo diverso orientamento si giustifica con il fatto che in tali casi la notificazione è regolarmente inserita nel registro (pubblico) dei trattamenti e ha dispiegato i suoi effetti (tenuto conto, tra l'altro, che l'inserimento nel registro non produce conseguenze negative sul titolare).

Assistenza agli utenti

Come già detto, il Garante ha fornito –e continua a fornire– ai soggetti tenuti alla notificazione un'attività di assistenza che si sostanzia in diverse forme: risposta ai numerosi quesiti e dubbi sulla notificazione, comunque formulati; controlli costanti dei messaggi inoltrati via *web* dagli utenti in caso di sospensione della notificazione e immediato riscontro via posta elettronica; effettuazione di controlli richiesti dai vari dipartimenti del Garante in occasione di istruttorie, attività ispettive e ricorsi.

17.2. *Il registro dei trattamenti e futuri sviluppi*

Le notificazioni regolarmente presentate sono confluite nel registro dei trattamenti.

Tale registro si è rivelato di maggiore utilità ed efficacia rispetto al precedente, non solo al fine di predisporre interventi ispettivi nei confronti di soggetti tenuti alla notificazione. Ulteriori benefici provenienti dal *database* riguardano, infatti, la possibilità di elaborare più efficacemente varie statistiche: esse costituiscono un importante strumento di comprensione dei fenomeni che ruotano intorno a trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà degli interessati; forniscono, inoltre, al Garante un significativo quadro di insieme in merito ai trattamenti effettuati; danno impulso, infine, alle attività di controllo assistite dal nucleo della Guardia di finanza.

In tale prospettiva, il Garante intende procedere all'affinamento di specifiche statistiche e alla creazione di sistemi che prevedano l'invio di una segnalazione automatica nel caso in cui la notificazione contenga elementi che si ritiene debbano essere sottoposti ad approfondimento.

Particolare cura verrà posta nel riscontro automatico dei pagamenti dei diritti di segreteria effettuati mediante banca e uffici postali, con la collaborazione della banca tesoriera e di Poste S.p.A.

Controlli a campione e audizioni in caso di contestazioni amministrative

Esaurita la fase di immissione della maggior parte delle notificazioni alla scadenza del 30 aprile 2004, sono stati effettuati diversi controlli a campione sulla congruenza dei dati dichiarati, sul ritardo o l'omissione della notificazione. A richiesta, il notificante viene ammesso ad un'audizione nella quale un funzionario del dipartimento stila una relazione sullo stato della notificazione.

Notificazione dei trattamenti e direttiva 95/46/CE

Nell'ambito dell'attività del Gruppo dei Garanti europei istituito dall'art. 29 della direttiva 95/46/CE, l'istituto della notificazione si avvia ad una possibile fase di revisione in chiave europea che ne conferma tuttavia l'utilità e la persistente necessità, soprattutto nell'innovativa connotazione che assume quella italiana.

In ragione del margine di discrezionalità che ciascuno Stato membro ha nel dare attuazione alla direttiva, nei diversi paesi sono stati infatti realizzati nel tempo sistemi (in parte) differenti con riferimento a taluni aspetti attinenti ai contenuti, alle modalità, ai provvedimenti di esonero e al diverso utilizzo delle tecnologie. Tali peculiarità non agevolano un pronto confronto tra le applicazioni nei vari Stati e possono comportare qualche difficoltà applicativa nel caso in cui il trattamento sia effettuato da aziende con stabilimenti in più paesi.

Si è pertanto proceduto ad uno studio congiunto con le autorità degli altri 24 paesi per omogeneizzare l'istituto e semplificare gli adempimenti. Ciò dovrebbe portare, per quanto possibile, all'eliminazione di notizie ritenute meno utili e ad elaborare un insieme condiviso di informazioni.

L'Italia, che tra gli ordinamenti europei dispone di una modalità esecutiva della notificazione progredita, ha svolto la funzione di relatore sugli aspetti di semplificazione ed omogeneizzazione dell'istituto e ha assunto un ruolo attivo nella predisposizione di un *vademecum* illustrativo delle diverse modalità di notificazione da pubblicare sul sito *web* della Commissione europea.

Il precedente registro generale dei trattamenti

Il precedente registro generale dei trattamenti viene temporaneamente utilizzato per alcuni riscontri, confrontando quanto il titolare abbia dichiarato all'epoca e quanto contenuto nella nuova notificazione.

Come evidenziato nella *Relazione 2003*, gran parte dell'attività del Dipartimento registro dei trattamenti ha riguardato in passato la regolarizzazione delle numerose notificazioni pervenute su modello cartaceo; operazione, questa, risultata piuttosto lunga e faticosa, nonostante l'utilizzo di strumenti a scansione ottica dell'intero archivio.

Il complesso archivio cartaceo è stato distrutto e memorizzato in dischi Dvd.

17.3. *Alcuni dati statistici*

Al 31 dicembre 2004 risultano pervenute poco più di 10.000 notificazioni.

Rinviando, per quanto riguarda la rappresentazione grafica alle tabelle riprodotte al par. 25 –nel quale sono rinvenibili i dati statistici relativi alla tipologia di trattamento notificato (tabella e grafico 14), alla distribuzione delle notificazioni per aree geografiche (grafico 15) o per tipologia di soggetto notificante, pubblico o privato (tabella e grafico 16); da ultimo si rappresentano le modalità di invio della notificazione (grafico 17)– si segnala qui che per il versamento dei diritti di segreteria, gli utenti si sono avvalsi, per il 80% circa dei casi, di forme tradizionali di pagamento (mediante conto corrente postale o bonifico bancario); una percentuale significativa (20%) ha preferito, tuttavia, il pagamento *on-line* mediante carta di credito.

Notificazioni pervenute tramite intermediari

Oltre il 46% delle notificazioni è pervenuto tramite intermediari, il che conferma l'utilità dell'iniziativa di stipulare convenzioni con organismi privati e pubblici per l'invio della notificazione con firma digitale.

Dei quattro intermediari con i quali il Garante ha stipulato la convenzione, Poste S.p.A. è stato quello più utilizzato dagli utenti privi di dispositivo di firma digitale.

18 Esercizio dei diritti e trattazione dei ricorsi

18.1. *Considerazioni generali*

Il ricorso al Garante come "*passepartout*". Questa immagine può dar conto in modo efficace del ruolo e del significato che lo strumento di tutela disciplinato negli artt. 145 e ss. del Codice è andato assumendo nel pur ampio spettro di quelli offerti dall'ordinamento.

A sei anni dall'entrata in vigore delle disposizioni applicative contenute nel d.P.R. 31 marzo 1998, n. 501 che, nel febbraio 1999, hanno dato concretezza e piena possibilità di esplicazione a questo meccanismo di tutela (originariamente previsto dall'art. 29 della legge n. 675/1996), il bilancio relativo al suo concreto utilizzo è senza dubbio positivo.

Dopo una necessaria fase di "rodaggio", la riflessione sulla portata e sull'estensione della nozione "dato personale", definita ora all'art. 4, comma 1, lett. *b*), del Codice (e sulle connesse possibilità di tutela) ha fatto sì che venissero pienamente apprezzate le potenzialità contenute nell'elenco di diritti di cui all'art. 7 del Codice (i soli in ordine ai quali può essere proposto un ricorso).

Di conseguenza, al più consueto esercizio del diritto di accesso ai dati personali (che, peraltro, si è andato estendendo dalla sfera dei comuni dati oggettivi, ai dati personali contenuti in giudizi ed alle informazioni di tipo valutativo: si vedano i provvedimenti del 19 aprile 2004 e 29 aprile 2004), si è affiancato l'utilizzo delle altre situazioni giuridiche soggettive contemplate dal medesimo art. 7: in particolare, per menzionare le ipotesi presentatesi più di frequente, il diritto di conoscere l'origine dei dati, le finalità e le modalità del trattamento come pure la logica applicata alle operazioni effettuate con strumenti elettronici; il diritto di ottenere l'aggiornamento, la rettificazione o l'integrazione dei dati, oltre alla possibilità di ottenere la cancellazione dei dati trattati in violazione di legge o di opporsi per motivi legittimi al loro trattamento, ancorché pertinenti allo scopo della raccolta.

Ma il vero punto di svolta, del quale la casistica dell'ultimo anno offre ampia prova, è l'utilizzo sempre più esteso dei diritti previsti dal Codice nell'ambito di più ampie e complesse vicende giudiziarie. Il ricorso tende quindi a trasformarsi da isolato (per quanto significativo) meccanismo di tutela, a strumento propedeutico o complementare (a volte anche strumentale) per rafforzarne altri già offerti dall'ordinamento ad ogni interessato. Ecco quindi che sempre più spesso si affaccia, nell'ambito della complessiva strategia processuale, l'utilizzo del ricorso in procedimenti giudiziari di tipo risarcitorio, in controversie di lavoro (volte alla ricostruzione di lunghi periodi di vita professionale) o relative al consapevole utilizzo di strumenti finanziari (v. *Provv.* 16 settembre 2004).

I dati statistici sono la migliore prova degli assunti precedenti: nell'anno solare 2004, con un incremento ancora più sensibile rispetto agli anni passati, sono stati esaminati e decisi dall'Autorità più di 700 formali ricorsi spesso piuttosto complessi. (cfr. par. 25.2).

Contributo spese per l'accesso ai dati

Con riferimento all'esercizio dei diritti dell'interessato, non sussistono differenze di fondo rispetto a quanto messo in evidenza in passato, avendo il Codice sostanzialmente riprodotto le previsioni normative in materia già contenute nelle previ-

gente disciplina, pur integrate con alcuni principi fissati dalla "giurisprudenza" del Garante in merito alle modalità di esercizio.

Al riguardo, occorre tuttavia sottolineare che l'Autorità, con il provvedimento del 23 dicembre 2004 (v. *Documentazione* par. 41), ha determinato i criteri per la fissazione del contributo spese relativo all'esercizio del diritto di accesso dell'interessato ai dati che lo riguardano; ciò, tenendo conto della tendenziale gratuità –confermata dal Codice, (art. 10, comma 8)– dell'esercizio di tale diritto, della normativa e della situazione in ambito comunitario e internazionale.

18.2. *Profili procedurali*

Novità introdotte dal Codice

Il 2004 ha visto la prima applicazione delle nuove disposizioni del Codice relative alle modalità di esercizio dei diritti di cui all'art. 7 e alla proposizione dei ricorsi: si tratta, in particolare, della possibilità di proporre ricorso dopo quindici giorni dalla ricezione dell'interpello preventivo da parte del titolare del trattamento; della durata del procedimento per la decisione del ricorso (ora di sessanta giorni); della possibilità di proroga di quaranta giorni di tale termine, anche su decisione dell'Ufficio; della previsione (contenuta nell'art. 150, comma 6, del Codice) secondo cui, in caso di mancata opposizione, il provvedimento, nella parte relativa all'ammontare delle spese e dei diritti, costituisce titolo esecutivo ai sensi degli artt. 474 e 475 del c.p.c.

Tali interventi, sia in ragione della loro limitata portata innovativa, sia in quanto rispondenti ad esigenze di razionalizzazione e di migliore gestione del procedimento, non hanno generato particolari problemi. Al contrario, la maggiore durata del procedimento (pur sempre assai contenuta) ha consentito di seguire in modo più accurato l'istruttoria dei ricorsi: sotto questo profilo, l'Ufficio e, in particolare, l'Unità ricorsi, ha potuto esercitare un ruolo più attivo, con frequenti richieste di integrazione della documentazione, preordinate ad assicurare il corretto svolgersi del contraddittorio, procedendo altresì all'assunzione di informazioni anche presso terzi.

Nei limitati casi in cui è stato segnalato un iniziale ritardo nella corresponsione della somma liquidata dal Garante a titolo di rimborso spese, l'Ufficio si è attivato al fine di accertare che il provvedimento non fosse stato impugnato ai sensi dell'art. 152 del Codice, con il conseguente pagamento da parte del soccombente.

Regolarizzazione e profili di inammissibilità

Negli ultimi mesi del 2004 è diminuito il numero dei ricorsi che formano oggetto di richiesta di regolarizzazione da parte dell'Ufficio per irregolarità o carenze sotto il profilo formale (con riferimento ai requisiti prescritti dall'art. 147 del Codice). A parte le informazioni quotidianamente fornite dall'Autorità attraverso l'Ufficio relazioni con il pubblico o il sito Internet *www.garanteprivacy.it*, si riscontra il diffondersi di moduli ed istruzioni (veicolate anche dalle associazioni dei consumatori) che facilitano l'accesso a questo strumento di tutela –e il suo corretto utilizzo– anche da parte dei singoli interessati (che, come noto, possono proporre il ricorso senza l'assistenza di un legale). Un nuovo modello per l'esercizio dei diritti è stato predisposto dall'Ufficio e pubblicato sul sito *web*, anche al fine di indurre gli interessati a concentrare l'attenzione sulle specifiche richieste di loro concreto interesse, caso per caso, nell'ambito della vasta gamma prevista dall'art. 7, semplificando anche i tempi per il riscontro e per la successiva tutela.

Continuano a pervenire, seppure in numero sempre più limitato, richieste di informazioni in ordine alla necessità di autenticazione della firma del ricorrente in calce al ricorso. In proposito si conferma l'obbligatorietà di tale requisito –ora spe-

cificamente previsto dall'art. 147, comma 4, del Codice– che non può essere sostituito dall'autocertificazione dell'interessato. L'Autorità ha recentemente ribadito tale necessità, rispondendo ad una richiesta di parere formulata dal Ministero dell'interno, Dipartimento per gli affari interni e territoriali.

Va infine ricordato che il Garante ha adottato, il 23 dicembre 2004 (e disposto la sua pubblicazione sulla Gazzetta Ufficiale), una nuova deliberazione concernente i casi di regolarizzazione dei ricorsi (art. 148, comma 2, del Codice), in sostituzione della delibera del 1° marzo 1999 adottata in occasione dell'entrata in vigore delle disposizioni del citato d.P.R. n. 501/1998.

In due occasioni, l'Autorità si è pronunciata in ordine a quanto disposto dall'art. 145, comma 2, del Codice in base al quale *"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"*. Con decisione del 4 ottobre 2004, è stato dichiarato inammissibile il ricorso proposto da un soggetto che aveva precedentemente prospettato la medesima questione innanzi ad una commissione tributaria provinciale. Al contrario, non si è ritenuta sussistente la fattispecie di cui all'art. 145, comma 2, in una decisione adottata il 21 ottobre 2004, ritenendosi ammissibile un ricorso al Garante avanzato a seguito del diniego opposto ad un'istanza di accesso ai dati formulata da un lavoratore già coinvolto in una controversia dinanzi al giudice del lavoro. Nel corso del procedimento giudiziario era stata avanzata una richiesta di esibizione di documenti (sulla quale il giudice si era riservato di decidere) ai sensi dell'art. 210 c.p.c. che, almeno in parte, potevano contenere alcuni dei dati personali poi richiesti con l'istanza *ex* art. 7. In proposito, l'Autorità ha rilevato l'ammissibilità del ricorso dal momento che –nonostante l'ipotetica coincidenza di alcuni documenti oggetto della domanda giudiziale rivolta al giudice con quelli contenenti le informazioni richieste ai sensi della normativa sulla protezione dei dati personali– i presupposti (*petitum, causa petendi*) sulla base dei quali il ricorrente aveva agito nel corso del giudizio erano diversi rispetto a quelli fatti valere innanzi al Garante.

Diritti di segreteria e determinazione delle spese del procedimento

A far data dal 15 gennaio 2005 è stata adeguata la misura dei diritti di segreteria che devono essere corrisposti per la presentazione di un ricorso all'Autorità.

I motivi di tale adeguamento, oltre al lungo tempo trascorso dalla prima deliberazione che li prevedeva (*Deliberazione* n. 1 del 18 febbraio 1999), sono solo in parte legati alla valutazione (ed alla connessa esigenza di parziale recupero) delle spese che l'Ufficio affronta per l'ordinaria gestione di tali procedimenti; procedimenti che comunque, come si è visto, presentano istruttorie maggiormente articolate, determinando oneri economici più elevati per l'Autorità e non compensati da correlativi aumenti di bilancio.

Da tale esborso, peraltro, l'interessato può essere tenuto indenne: va infatti ricordato che, su istanza di parte, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso posti a carico della parte soccombente (art. 150, comma 3).

18.3. *Brevi cenni sulla casistica*

Al di là dei riferimenti alle singole decisioni del Garante assunte in sede di ricorso e rinvenibili nell'intera *Relazione* in ragione della materia sulla quale sono andate ad incidere, si ritiene utile fornire qui un quadro d'insieme delle tematiche affrontate con i provvedimenti resi *ex* art. 150 del Codice, con particolare riguardo a quelle che sono state oggetto del maggior numero di ricorsi (rinviando, per la sintetica trat-

tazione del loro contenuto, alle diverse sezioni della presente *Relazione*).

Se gli ambiti interessati dai ricorsi sono stati i più vari –solo a fini esemplificativi, si menzionano qui le materie delle perizie medico-legali in ambito assicurativo, del rapporto di lavoro (pubblico e privato) e della videosorveglianza– non di rado le decisioni che ne sono scaturite hanno delineato un primo quadro di riferimento per provvedimenti più organici o rappresentato il punto di partenza per lo svolgimento di attività ispettive.

Settore bancario e finanziario

Dal punto di vista tipologico, si è registrato un elevato numero di decisioni nel settore bancario e finanziario, specie in riferimento a richieste di accesso riferite a tutti i dati e le informazioni di carattere personale detenute da un istituto di credito. Ad esso deve essere aggiunto il settore dei sistemi di informazione creditizia (Sic), già noti con la locuzione *"centrali rischi (private)"*, che ha registrato nel corso del 2004 una vera e propria esplosione del contenzioso. Ciò, anche a seguito della più ampia conoscenza del provvedimento generale adottato in materia dal Garante il 31 luglio 2002 (che ha costituito il primo tentativo di articolare i principi di protezione dei dati personali in un settore, quello appunto dei sistemi di informazione creditizia, sviluppatosi in Italia in assenza di uno specifico quadro normativo di riferimento) ed in relazione allo sviluppo dei lavori che hanno portato alla redazione ed all'adozione del codice deontologico di settore (pubblicato in *G.U.* 23 dicembre 2004, n. 300 in merito al quale v. par. 9.2.).

Nei numerosi provvedimenti adottati –oltre a rilevarsi l'esistenza di dati errati, incompleti o non aggiornati, o di constatare l'esistenza di dati comunicati ai Sic in assenza dei requisiti di liceità del trattamento (informativa e consenso espresso dell'interessato)– sono stati messi a fuoco tutti i principali problemi che la prassi operativa delle banche e delle società finanziarie (che consultano quotidianamente i predetti archivi) ha sollevato.

Si sono invece nettamente distinte dai dati trattati in riferimento alle operazioni di credito al consumo (oggetto di specifica tutela nel menzionato codice di deontologia) le informazioni (generalmente riferite a mutui ipotecari) presenti in altri archivi (cd. banche dati "Atti pubblici") che, parimenti, sono rese disponibili dai soggetti che gestiscono i sistemi di informazioni creditizie: si tratta di dati desunti dai pubblici registri immobiliari che i soggetti privati possono trattare anche senza il consenso degli interessati (art. 24, comma 1, lett. *c*), del Codice). Sono trattamenti, questi ultimi, che allo stato non possono ritenersi illeciti, ma rispetto ai quali (con particolare riguardo alla pertinenza e alla completezza delle informazioni e alla conservazione dei dati stessi) saranno fornite a breve più specifiche indicazioni in sede di adozione dei codici di deontologia di cui agli artt. 61 e 119 del Codice.

Va infine ricordato il provvedimento del 16 settembre 2004 nel quale, per la prima volta, il Garante ha accolto la richiesta di cancellazione dall'archivio di un sistema di informazioni creditizie di dati riferiti ad una richiesta di abbonamento telefonico. Tali trattamenti sono stati infatti ritenuti incompatibili e non pertinenti con le funzioni specifiche delle centrali rischi volte, come detto, alla tutela del credito e al contenimento dei relativi rischi nel solo settore del credito al consumo.

Trattamenti effettuati da pubbliche amministrazioni

Fra gli altri profili affrontati nel corso dell'anno vanno sinteticamente ricordate, tra le tante, la decisione del 27 settembre 2004 relativa alla possibilità del ricorrente di accedere ai dati personali che lo riguardano contenuti in un esposto presentato a suo carico presso l'ente locale titolare del trattamento (ente presso il quale il ricorrente aveva prestato servizio) ed il provvedimento del 21 ottobre 2004, concernente la rettificazione dei dati di un insegnante detenuti da un istituto scolastico, con par-

ticolare riferimento a quelli contenuti nei certificati relativi al servizio prestato nei precedenti anni scolastici.

Trattamenti in rete

Al di là di singoli interventi nel settore delle comunicazioni elettroniche –si pensi, fra le altre, alla decisione del 24 marzo 2004 concernente la divulgazione a mezzo degli elenchi cartacei e *on-line* dei dati dell'interessato riferiti ad un'utenza telefonica che doveva rimanere "riservata"– merita segnalare la persistenza di un intenso contenzioso in ordine all'invio di comunicazioni pubblicitarie non sollecitate dirette a indirizzi di posta elettronica senza che risulti acquisito il previo consenso dell'interessato.

Trattamenti degli operatori telefonici

Va sottolineato anche il provvedimento del 25 maggio 2004 con il quale è stata accolta la richiesta dell'interessato di conoscere i dati personali relativi alle numerose carte telefoniche illecitamente attribuite al ricorrente per la dolosa condotta di un *dealer.*

19 Contenzioso giurisdizionale

19.1. *Considerazioni generali*

L'entrata in vigore del Codice ha avuto ripercussioni sull'attività dell'Autorità anche riguardo al contenzioso giurisdizionale, sia quello direttamente concernente provvedimenti del Garante, sia, più in generale, quello relativo all'applicazione del Codice stesso.

Quest'ultimo infatti, all'art. 152, da un lato, ha confermato l'originaria impostazione della legge n. 675/1996 relativamente alla procedura per l'impugnazione degli atti del Garante (specificando alcuni aspetti che avevano dato luogo ad incertezze negli anni passati) e, dall'altro, ha previsto un'apposita procedura per il coinvolgimento dell'Autorità in tutte le cause in materia di protezione dei dati personali.

In particolare, sotto il primo profilo, ribadito che tutte le controversie riguardanti l'applicazione del Codice sono devolute all'autorità giudiziaria ordinaria, l'art. 152, comma 2, precisa che l'azione deve proporsi con ricorso da depositarsi *"nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento"*.

Con tale formulazione si è confermata la scelta della giurisdizione e del foro competente, superandosi, fra l'altro, definitivamente il dubbio circa la possibilità di adire il giudice di pace, che risulta ora evidentemente esclusa.

I commi da 7 a 11 dell'art. 152 descrivono poi le fasi processuali, in buona parte mutuate da quelle previste in materia di depenalizzazione dall'art. 23 della legge n. 689/1981.

Nel definire tale procedura, il legislatore delegato ha previsto (art. 152, comma 7) che i ricorsi presentati all'autorità giudiziaria vengano notificati anche al Garante. Tale disposizione non riguarda solo i casi in cui sia proposta opposizione avverso i provvedimenti dell'Autorità, ma tutte le controversie concernenti l'applicazione del Codice.

Per tale secondo aspetto la modifica legislativa è di sicuro rilievo in quanto consente all'Autorità, da un lato, di essere utilmente informata per intervenire anche in quei procedimenti nei quali, pur non essendo essa direttamente coinvolta, sono in discussione profili di carattere generale; dall'altro, di venire a conoscenza, comunque, di controversie concernenti l'applicazione della disciplina in materia di protezione dei dati personali.

Quest'ultima attività d'informazione, di primaria importanza anche in relazione all'adozione di eventuali provvedimenti amministrativi e all'attività di segnalazione al Parlamento ed al Governo degli interventi normativi necessari per la tutela del diritto alla protezione dei dati (art. 154, comma 1, lett. *f*), è formalizzata nell'ultimo comma del citato art. 154, il quale, riproducendo quanto originariamente previsto dall'art. 40 della legge n. 675/1996, stabilisce che copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica sia trasmessa, a cura della cancelleria, al Garante.

Le modifiche introdotte, nell'ottica di un maggior coinvolgimento dell'Autorità nel contenzioso giudiziario, hanno indotto il Garante ad istituire, con decorrenza 1° gennaio 2004, un'unità temporanea di primo livello per gli "Affari legali", ai fini di un approccio più strutturato ed organico nell'enucleazione delle linee di difesa e intervento dell'Autorità e nei rapporti con le competenti avvocature dello Stato.

19.2. *Profili procedurali*

Con riferimento al contenzioso giurisdizionale, appare opportuno ricordare almeno i più significativi interventi in materia, sotto il profilo procedurale e di merito, richiamando anche alcuni utili precedenti che, seppur relativi ad anni passati, spiegano ancora rilievo.

Riguardo al primo aspetto, vanno senz'altro segnalate le pronunce in tema di giurisdizione che già la legge n. 675/1996 (art. 29, comma 8) aveva individuato nel giudice ordinario e che ora il Codice –come si è detto– indica specificamente nel tribunale.

Sulla base della formulazione del 1996, il Tribunale amministrativo del Lazio ha dovuto dichiarare la propria carenza di giurisdizione in merito ad un ricorso ad esso presentato dalla Congregazione cristiana dei Testimoni di Geova che aveva impugnato l'autorizzazione n. 3/1999 del Garante.

Per analoghe ragioni, nel 2004, nel fornire alla Presidenza del Consiglio dei ministri –Dipartimento per il coordinamento amministrativo– gli elementi necessari a predisporre le valutazioni su due ricorsi straordinari al Capo dello Stato, l'Autorità ha dovuto eccepire il difetto di giurisdizione.

Il Garante ha rivolto ulteriori osservazioni relativamente alla possibilità di adire il giudice di pace anziché il tribunale ordinario; tema, questo, che si è posto in particolare evidenza nel 2004 anche a seguito di più decisioni del Giudice di pace di Napoli che, investito di alcune azioni contro lo *spamming*, ha condannato, nel caso più noto, una società a cancellare i dati dell'interessato dai propri archivi e a pagare allo stesso 1.000,00 euro (oltre interessi legali e spese di giudizio) a titolo di risarcimento del danno.

La decisione da parte di tale giudice si è resa possibile solo in quanto la causa era stata instaurata prima dell'entrata in vigore del Codice, sebbene sul piano mediatico sia stata erroneamente commentata da alcuni come sentenza-pilota per (improprie) azioni dinanzi al giudice di pace.

In merito al foro competente, non sono mancate decisioni volte a far valere quanto disposto dall'art. 29, comma 6, della legge n. 675/1996 (prima) e dell'art. 152 del Codice (ora), che individuano nel tribunale del luogo ove risiede il titolare del trattamento la sede presso la quale proporre l'azione per tutte le controversie riguardanti l'applicazione del Codice.

In tal senso, con riguardo all'art. 29 della legge, si era espresso già nel passato il Tribunale di Firenze con decisione depositata in cancelleria il 15 aprile 2003; analogamente, il Tribunale di Napoli, con ordinanza del 29 luglio 2004, ha dichiarato la propria incompetenza su un ricorso proposto contro un titolare del trattamento avente sede legale in Bologna, con la contestuale dichiarazione di manifesta infondatezza della questione di legittimità costituzionale sollevata dal ricorrente sulla scelta effettuata dal legislatore con il citato art. 152.

Sulla stessa linea il Tribunale di Barcellona Pozzo di Gotto, con ordinanza n. 3694 del 31 luglio 2004, ha dichiarato manifestamente infondata la questione di legittimità costituzionale connessa alla mancata previsione della competenza del giudice del luogo di residenza del ricorrente quale foro alternativo a quello del luogo ove ha sede il titolare del trattamento.

Sempre in tema di competenza territoriale, ma sotto un diverso profilo, può essere ricordata la decisione con la quale il Giudice di pace di Amantea, cui un titolare si era rivolto opponendosi ad un'ordinanza di applicazione di sanzione amministrativa comminata dal Garante (ai sensi di quanto previsto dalla l. n. 689/1981), si è dichiarato incompetente, ma qui con riferimento all'ambito territoriale. Nel caso di specie, infatti, si doveva far riferimento al *"luogo in cui è stata commessa la*

violazione" (art. 22, comma 1, l. n. 689/1981), coincidente, secondo quanto affermato della giurisprudenza costituzionale e di legittimità, con quello nel quale la violazione era stata accertata (Roma).

Ancora, con riferimento agli aspetti procedurali, la giurisprudenza ha consentito di chiarire il dubbio relativo alla legittimazione passiva del Garante e, quindi, alla possibilità per esso di costituirsi innanzi ai tribunali o alla Corte di cassazione per difendere le ragioni giuridiche dei provvedimenti oggetto di impugnazione.

Su tale questione il Garante aveva chiesto in passato l'avviso dell'Avvocatura generale dello Stato, la quale, con parere del 29 ottobre 1999, si era espressa in termini favorevoli, ritenendo essenziale che l'Autorità potesse far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni.

A questo indirizzo l'Autorità stessa si è attenuta costantemente nel corso degli anni, intervenendo a difesa di decisioni il cui rilievo, andando ben oltre il singolo caso di specie, aveva riflessi su un'ampia platea di interessati e coinvolgeva rilevanti profili interpretativi della disciplina sulla protezione dei dati.

Sul punto la giurisprudenza –dopo la sentenza della Corte di cassazione (Sez. I Civ. 30 giugno 2001, n. 8889) che, dichiarando inammissibile un ricorso incidentale proposto dal Garante, non aveva affermato principi contrastanti con la sua prospettata legittimazione passiva– ha registrato un netto chiarimento con la sentenza n. 7341/2002 della prima sezione civile della Corte di cassazione.

Con tale pronuncia la Suprema Corte ha precisato che *"il ricorso al giudice ordinario in opposizione al provvedimento del Garante non può essere inteso che come primo rimedio giurisdizionale a disposizione del soggetto che si pretende leso dall'atto del Garante"*. Pertanto, l'Autorità può partecipare al giudizio di impugnativa di un proprio atto quale che sia stato il procedimento che lo ha preceduto per far valere davanti al giudice lo stesso interesse pubblico a tutela del quale il Garante agisce.

A seguito di tale pronuncia, il Tribunale di Roma, cui erano stati nuovamente trasmessi gli atti per l'esame della controversia, si è dovuto anche esprimere sulla questione di costituzionalità sollevata dal ricorrente in merito alla possibile violazione della regola del "giusto processo". La parte, infatti, sosteneva che la possibilità di impugnare la decisione del giudice di primo grado sull'opposizione al provvedimento del Garante solo tramite ricorso per cassazione sarebbe stata in contrasto con la regola del doppio grado di giudizio. Il Tribunale, con sentenza del 17 luglio 2003, dichiarando la questione manifestamente infondata ha riconosciuto che ragioni di speditezza possono giustificare l'esistenza di procedimenti giurisdizionali semplificati in cui è previsto un unico sindacato di merito, in quanto nella Costituzione non è contenuta alcuna norma che garantisca espressamente il doppio grado di giudizio.

Sempre con riferimento alla legittimazione passiva dell'Autorità, nel corso del 2004, la Suprema Corte (Sez. I Civ., sent. 22 marzo-25 giugno 2004, n. 11864), nel rigettare un'opposizione proposta contro una decisione del Garante, ha ritenuto quest'ultimo (sollevando con ciò qualche perplessità in dottrina) privo di interesse ad impugnare, nel caso di specie, il provvedimento giurisdizionale che, sebbene avesse ingiustamente negato la sua legittimazione processuale, aveva però confermato la decisione adottata dall'Autorità.

19.3. *Profili di merito*

Relativamente agli aspetti di merito, i primi anni di applicazione della disciplina sulla protezione dei dati personali hanno visto un numero assai esiguo di giudizi di

impugnazione dei provvedimenti del Garante; giudizi che, comunque, si sono risolti in una generale conferma dei principi di diritto affermati dall'Autorità. L'ingresso ormai consolidato della protezione dei dati personali nel circuito giudiziario rende opportuno compiere, come nei paragrafi precedenti, una sintetica ricognizione di alcune decisioni giurisprudenziali che hanno finora riguardato l'applicazione della normativa sulla tutela dei dati.

Al riguardo (omettendo una panoramica integrale anche di casi particolarmente significativi come quelli all'esame, all'epoca, del Tribunale di Bergamo in materia di investigazione privata), giova ricordare, tra l'altro, le vicende relative alla riconducibilità delle valutazioni alla nozione di "dato personale" fornita dalla legge n. 675/1996 e confermata dal Codice.

In tal senso già il Tribunale di Bologna, con decreto del 2 luglio 2002, concluse nel senso che anche i giudizi valutativi riferiti ai dipendenti contengono di regola dati personali.

Sulla medesima linea e discostandosi da alcuni circoscritti precedenti (Tribunale di Fermo, 26 ottobre 1999), il Tribunale di Roma ha riconosciuto che, anche con riferimento a dati valutativi (e in particolare sulle valutazioni espresse nelle perizie medico-legali), l'interessato può esercitare il diritto di accesso e alcuni altri diritti previsti dalla normativa in materia di protezione dei dati, ad esclusione di quelli di rettificazione o integrazione. Al riguardo, merita di essere sottolineato che della questione della riconducibilità delle valutazioni alla nozione di "dato personale" si è infine fatto carico il legislatore adottando un'equilibrata soluzione nell'art. 8, comma 4, del Codice.

Con riferimento alla possibilità di ottenere l'integrazione dei dati personali, il Tribunale di Padova, con decisione del 26 maggio 2000, aveva confermato il provvedimento con il quale il Garante, respingendo il ricorso dell'interessato che chiedeva la cancellazione dei propri dati personali dal registro dei battesimi di una parrocchia, aveva affermato comunque il suo diritto a veder aggiornato il medesimo dato.

Sempre in materia di esercizio dei diritti ora disciplinati dagli artt. 7 e ss. del Codice, restano attuali i principi affermati dalla già citata sentenza della Corte di cassazione (Sez. I Civ. 30 giugno 2001, n. 8889) che, ribadendo la piena applicazione delle disposizioni della legge n. 675/1996 anche agli archivi ed ai trattamenti svolti in ambito giornalistico, ha riconosciuto la possibilità di esercitare detti diritti (con particolare riguardo al diritto di accesso, integrazione ed eventuale correzione di dati inesatti) anche nei confronti di dati personali trattati a tal fine.

19.4. *Opposizione ai provvedimenti del Garante*

Il 2004 ha registrato dodici opposizioni ad altrettanti provvedimenti del Garante (tutte decisioni adottate su ricorso).

Tale numero può essere considerato in linea con quello degli anni precedenti, sia in relazione all'aumentata attività decisoria dell'Autorità, sia in considerazione del fatto che ben sette di queste opposizioni sono state presentate da un unico titolare (Crif S.p.A.) nelle more dell'approvazione del codice deontologico sui sistemi di informazioni creditizie, successivamente alla quale, per le medesime opposizioni, è stata chiesta la cessazione della materia del contendere.

Per quanto riguarda le ulteriori opposizioni presentate nel corso del 2004 e quelle pendenti degli anni precedenti, si è registrata la conferma di due decisioni relative alla produzione in giudizio (rispettivamente, in una causa civile ed in una

penale) di documenti contenenti dati personali, con le quali il Garante aveva ricordato i limiti di applicazione della disciplina in materia di tutela della riservatezza nei casi di trattamenti svolti per fini di giustizia.

Hanno avuto invece esito favorevole ai ricorrenti due opposizioni ad altrettante decisioni dell'Autorità relative, rispettivamente, ad una comunicazione di una relazione medica fra uffici periferici della stessa amministrazione ed alla pubblicazione di fotografie di persone arrestate.

Relativamente alla prima, considerato che la diversa valutazione del giudice si è basata soprattutto su una documentazione non prodotta dall'interessato in sede di ricorso all'Autorità e che la stessa è apparsa condivisibile nella sostanza, il Garante, su conforme avviso dell'Avvocatura generale, ha deciso di prestare acquiescenza.

Decisione diversa è stata invece stata assunta con riferimento alla seconda decisione, la quale, annullando il provvedimento dell'Autorità che aveva ritenuto illegittima la pubblicazione di fotografie di persone in stato di arresto, è invece apparsa censurabile sotto diversi profili. Relativamente ad essa è stato pertanto proposto ricorso per cassazione.

Sono ancora alle prime fasi del giudizio due ulteriori opposizioni presentate nel corso del 2004 da altrettante amministrazioni locali contro le decisioni con le quali l'Autorità ha censurato, in termini di mancato rispetto del principio di pertinenza, la pubblicazione di notizie relative all'attività istituzionale e coinvolgenti direttamente i ricorrenti.

Allo stesso stadio processuale si trovano anche l'opposizione presentata dalla RCS S.p.A. contro il provvedimento del 26 novembre 2003, con cui il Garante ha vietato l'ulteriore diffusione di fotografie di persone sottoposte a misure restrittive della libertà personale, e quella proposta da un interessato avverso la decisione con cui l'Autorità ha dichiarato infondato il ricorso in materia di rilascio di certificati del casellario giudiziale.

Sono parimenti in attesa di decisione due ricorsi straordinari al Capo dello Stato, relativamente ai quali il Garante ha chiesto di far valere in primo luogo il difetto di giurisdizione; si è conclusa la fase istruttoria e dovrebbe essere imminente la decisione in merito alle opposizioni a suo tempo proposte da RAI S.p.A. e dall'Agenzia per le entrate contro il provvedimento del 5 dicembre 2001 in materia di canone televisivo.

19.5. *Intervento del Garante in giudizi relativi all'applicazione del Codice*

Nel corso del 2004 si è registrata la notifica al Garante, ai sensi di quanto ora prescritto dall'art. 152, comma 7, del Codice, di trentadue ricorsi all'autorità giudiziaria non coinvolgenti direttamente pronunce dell'Autorità.

A tal proposito, occorre evidenziare che il Garante, conformemente agli indirizzi giurisprudenziali ed al già riferito parere dell'Avvocatura generale dello Stato, ha deciso di delimitare la propria attiva presenza ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto, pur continuando a seguire con attenzione tutti questi contenziosi.

In questo quadro, il Garante, laddove non ha ritenuto opportuno intervenire, ha pregato le avvocature distrettuali dello Stato di seguire periodicamente le vicende, provvedendo invece direttamente per le questioni sollevate presso il foro della Capitale.

Per sette dei ricorsi notificatile, l'Autorità ha ritenuto opportuno costituirsi. Si è trattato, in particolare, di due casi concernenti l'applicazione delle regole in materia di trattamento dei dati da parte delle cd. "centrali rischi", per i quali l'intervento è stato ritenuto essenziale alla luce dei lavori allora in corso di svolgimento per il codice deontologico.

Due ulteriori costituzioni del Garante si sono avute in cause riguardanti la violazione della riservatezza in ambito condominiale (nella specie, si trattava dell'affissione nella bacheca di un condominio di vari atti relativi al ricorrente) e per una notificazione, senza busta ed in mani di terzi, di atti contenenti dati sensibili, entrambe questioni sulle quali l'Autorità è intervenuta in passato con proprie pronunce di carattere generale.

L'Autorità ha poi ritenuto necessario costituirsi, in ragione della questione di diritto sottostante, in una causa relativa al rifiuto di consegna di una perizia medica per una vicenda giudiziaria in corso, nonché in due ulteriori casi, per far valere l'incompetenza territoriale del foro prescelto dal ricorrente.

In questo primo anno di attività la nuova unità Affari legali ha coordinato gli interventi dell'Autorità alla luce anche del suo aumentato, e probabilmente crescente, coinvolgimento nei procedimenti innanzi all'autorità giudiziaria, anche in relazione alle controversie che un'aumentata attività ispettiva e, soprattutto, sanzionatoria del Garante potrà comportare.

20 Attività ispettive e applicazione di sanzioni amministrative

20.1. *Profili generali*

Al fine di dare concreta attuazione al diritto alla protezione dei dati personali, la legge ha dotato il Garante di veri e propri poteri ispettivi, tramite i quali è possibile richiedere informazioni e documenti al titolare, ai responsabili ed incaricati del trattamento, agli interessati ed a terzi (art. 157 del Codice), anche inviando personale per rilevare le informazioni e i documenti, acquisendole *in loco*. L'Autorità può, inoltre, accedere a banche dati e archivi ed effettuare ispezioni e verifiche nei luoghi in cui si svolge il trattamento o dove occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento di dati personali (art. 158). Nel solo caso in cui tali attività debbano svolgersi in abitazioni, in altri luoghi di privata dimora o nelle relative appartenenze, l'accesso è subordinato all'autorizzazione dell'autorità giudiziaria o, in alternativa, all'assenso informato del titolare o del responsabile del trattamento dei dati.

In generale, le ispezioni possono originare da segnalazioni o reclami ricevuti dal Garante, nonché da esigenze di approfondimenti ulteriori emerse nell'ambito dell'esame di ricorsi. L'Autorità ha un potere di iniziativa autonomo in relazione, ad esempio, all'esigenza di verificare gli adempimenti di determinate categorie di titolari di trattamenti, ovvero sulla base di notizie comunque direttamente acquisite dal Garante. Talvolta vengono effettuati controlli a campione per verificare lo stato di attuazione della legge in determinati settori, spesso in concomitanza con scadenze imposte dal Codice (quali, per esempio, quelle previste per le notificazioni e per il Documento programmatico di sicurezza).

La scelta dello strumento potestativo da utilizzare per l'esercizio dell'attività di controllo è informata a principi di proporzionalità, adeguatezza e gradualità, tenendo presente di volta in volta il contesto operativo di riferimento (rischio di dispersione o alterazione degli elementi di prova), nonché la disponibilità e la collaborazione del soggetto controllato per lo svolgimento delle verifiche.

Nell'ambito degli accertamenti ispettivi, il personale del Dipartimento vigilanza e controllo del Garante riveste la qualifica di ufficiale o di agente di polizia giudiziaria. Ciò comporta che, qualora nel corso dell'ispezione emergano violazioni penalmente rilevanti (artt. 167-171 del Codice), il personale addetto al Dipartimento possa procedere utilizzando i poteri investigativi che il codice di procedura penale attribuisce agli ufficiali ed agenti di polizia giudiziaria (eseguendo per esempio perquisizioni o sequestri, anche di iniziativa).

Al termine del procedimento amministrativo di controllo, del quale le attività ispettive rappresentano una fase, l'Autorità può segnalare ai titolari o responsabili del trattamento dei dati le modificazioni necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti e contestare le violazioni amministrative eventualmente rilevate; nei casi più gravi, previsti dalla legge, il Garante è tenuto ad inviare una comunicazione di notizia di reato all'autorità giudiziaria per l'accertamento delle violazioni costituenti illecito penale.

20.2. *Procedure*

Gli accertamenti di cui all'art. 157 del Codice (richiesta di informazioni ed esibizione di documenti) hanno una valenza marcatamente collaborativa. Il Garante adotta la predetta procedura nei confronti di soggetti e in relazione a materie per le quali ritiene di non dover procedere all'accesso, oppure quando sono necessarie informazioni analitiche che titolare e responsabile potrebbero avere difficoltà a fornire in modo esaustivo, nonché quando devono essere effettuati controlli incrociati rispetto a trattamenti di dati personali che interessano più titolari. Il carattere collaborativo di queste attività è evidenziato anche dalla prassi, seguita spesso dall'Autorità, di preannunciare le iniziative. I soggetti interpellati sono comunque tenuti a fornire informazioni non mendaci od omissive e ad esibire documenti genuini, al fine di non incorrere nella sanzione penale prevista dall'art. 168 del Codice (*Falsità nelle dichiarazioni al Garante*) o in quella amministrativa di cui all'art. 164 (*Omessa informazione o esibizione al Garante*).

Gli accertamenti previsti dall'art. 158 sono invece disposti quando, per acquisire gli elementi necessari alla compiuta definizione del contesto, non sia ritenuto sufficiente procedere con una mera richiesta di informazioni o di esibizione di documenti, ovvero nei casi in cui le informazioni o i documenti richiesti non siano pervenuti o siano ritenuti incompleti o non veritieri.

A differenza di quanto stabilito dall'art. 157, l'art. 158 conferisce al Garante una potestà di tipo inquisitorio ed *"i soggetti interessati agli accertamenti sono tenuti a farli eseguire"* (art. 159, comma 2, del Codice). L'accertamento è effettuato anche in caso di rifiuto e le eventuali spese sono poste a carico del titolare.

Il Codice prevede che le attività effettuate durante l'ispezione siano verbalizzate, registrando tutti gli elementi rilevanti emersi nell'operazione; agli accertamenti possono eventualmente assistere anche persone indicate dal titolare o dal responsabile (collaboratori interni, consulenti o legali) (art. 159).

20.3. *I casi più rilevanti*

Operatori sanitari

I trattamenti di dati sensibili effettuati da operatori sanitari sono stati oggetto di numerose ispezioni sia per quanto riguarda le modalità di conservazione dei dati e le connesse misure di sicurezza (anche in relazione ad episodi di gravi inadempienze che hanno avuto vasta eco attraverso gli organi di informazione), sia per quel che attiene all'osservanza dell'obbligo di notificazione.

In questo settore, i soggetti ispezionati sono stati ventidue, comprendendo Asl, ospedali e laboratori di analisi. Gli accertamenti si sono conclusi con l'invio di quattro notizie di reato per violazione dell'art. 169 (*Mancata adozione delle misure minime di sicurezza*) del Codice e con la contestazione di tredici sanzioni amministrative.

Uno dei casi più rilevanti ha riguardato un intervento effettuato presso un'azienda sanitaria a seguito della notizia apparsa su alcuni quotidiani che evidenziava la circostanza secondo la quale un'ingente quantità di documentazione sanitaria contenente dati idonei a rivelare lo stato di salute degli interessati (certificati medici, referti di analisi, registri di ricovero ecc.) era stata dispersa in un'area aperta al pubblico e abbandonata per giorni alla portata di chiunque. Durante l'accertamento è emerso che il fatto era da mettere in relazione ad un incendio, occorso circa quindici giorni prima, in un prefabbricato adibito ad archivio dove era conservata documentazione sanitaria relativa ad annualità molto risalenti nel tempo e in attesa di essere distrutta. Le operazioni di spegnimento dell'incendio avevano comportato la parziale demolizione del prefabbri-

cato e lo spostamento all'esterno di tutta la documentazione cartacea in esso contenuta.

Terminata l'emergenza, l'azienda sanitaria, pur avviando le procedure burocratiche per affidare ad una ditta specializzata la distruzione della documentazione, non aveva adottato alcun adempimento volto a ripristinare le misure di sicurezza, doverose in considerazione anche del fatto che i documenti si trovavano su un piazzale dal quale si accedeva peraltro ad una biblioteca comunale assiduamente frequentata (rendendo così accessibili a chiunque dati sensibili di migliaia di cittadini). L'Autorità, attraverso l'attività ispettiva, non solo ha provveduto ad accertare le responsabilità, ma ha anche disposto l'immediata attuazione di alcune misure di sicurezza.

In un altro caso l'Ufficio, raccogliendo la segnalazione di un programma televisivo trasmesso da una rete nazionale, si è recato in una struttura a suo tempo adibita a colonia per la cura delle malattie respiratorie infantili, attualmente dismessa, dove erano state abbandonate cartelle cliniche e altri documenti sanitari relativi ai pazienti della colonia. Anche in questo caso, gli enti che nel tempo avevano avuto in gestione l'immobile avevano dimostrato una totale inosservanza delle misure minime di sicurezza (art. 31 del Codice).

L'Ufficio si è anche occupato di un ulteriore caso di cattiva gestione della documentazione cartacea contenente dati sensibili dei cittadini, questa volta da parte di un'azienda ospedaliera della capitale. Anche in questa circostanza, una consistente quantità di documentazione sanitaria, concernente in particolare risultanze del laboratorio di analisi, era stata rinvenuta nel centro della città in prossimità di cassonetti dell'immondizia collocati su una pubblica via.

I casi sopra citati evidenziano una scarsa consapevolezza della delicatezza dell'attività di gestione della documentazione, anche di natura cartacea, contenente dati sensibili e della necessità che le misure di sicurezza previste per la conservazione di tali informazioni siano mantenute fino alla materiale distruzione della stessa. Appare irragionevole porre in essere complesse e onerose misure di conservazione e sicurezza degli archivi cartacei se poi lo smaltimento dei documenti non più necessari viene effettuato semplicemente gettandoli integri in un cassonetto dell'immondizia.

Gli episodi dimostrano inoltre, da una parte, la necessità di un "approccio sostanziale" alla legge; dall'altro, l'importanza che la documentazione contenente dati personali sia sempre conservata *"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"* (art. 11, comma 1, lettera *e*), del Codice).

Sempre in ambito sanitario, l'Ufficio ha svolto una serie di accertamenti per verificare la correttezza dei trattamenti di dati personali effettuati da un'associazione senza scopo di lucro nell'ambito di un progetto di ricerca realizzato con un'amministrazione comunale e con la collaborazione di una Asl. Il caso riguardava il rilevamento di dati personali attraverso la compilazione di minuziosi questionari, successivamente smarriti, che rivelavano anche le abitudini sessuali degli interessati. Anche in questo caso, tutte le operazioni di trattamento dei dati erano state effettuate in assenza di misure minime di sicurezza; tale circostanza è stata quindi oggetto di una comunicazione di reato alla competente autorità giudiziaria.

Anche le ispezioni effettuate nei confronti di due grosse aziende ospedaliere hanno evidenziato gravi deficienze nell'adozione delle misure di sicurezza per il trattamento dei dati sanitari mediante reti telematiche, debitamente segnalate alle competenti procure della Repubblica.

A fattor comune si evidenzia che nel caso di omessa adozione delle misure minime di sicurezza, il Garante, una volta segnalata la violazione all'Autorità giudiziaria, provvede ad impartire all'autore del reato una prescrizione fissando un termine per la regolarizzazione.

Se allo scadere del termine risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dall'Autorità a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato.

Dati genetici

Un altro dei settori oggetto di attenzione ispettiva è stato quello relativo alla raccolta e al trattamento di dati genetici.

In particolare, in relazione ad un delicato progetto di ricerca genetica, l'Ufficio ha svolto un'intensa attività ispettiva e di verifica nei confronti dei soggetti presso i quali tali dati erano stati raccolti e, pur mettendo in luce la generale correttezza sostanziale e liceità dei trattamenti effettuati, ha evidenziato ancora una volta un'inadeguatezza delle misure di sicurezza adottate che è stata segnalata all'autorità giudiziaria.

***Test* del Dna**

In un altro caso, l'ispezione è stata effettuata nei confronti di un'azienda che stava avviando la commercializzazione, via Internet, di un *test* del Dna "fai-da-te" che avrebbe consentito agli interessati di ottenere un responso mediante l'invio di campioni di materiale organico (saliva). L'intervento dell'Ufficio, avvenuto prima che la vera e propria commercializzazione del *test* avesse inizio, ha consentito di far emergere tutti i profili estremamente delicati legati alla gestione di un'attività che comporta il trattamento di dati genetici. L'Autorità ha infatti indotto l'azienda a valutare con maggiore attenzione tutte le implicazioni di carattere giuridico connesse con l'operazione prima di avviare materialmente l'iniziativa.

Informazioni sui sinistri stradali

Un'altra questione sottoposta all'attenzione del Garante (e sfociata poi in una verifica ispettiva) ha tratto origine da numerose segnalazioni di cittadini coinvolti in sinistri stradali. Gli stessi lamentavano di essere stati contattati da un'agenzia di pratiche automobilistiche che promuoveva i propri servizi volti a far ottenere il risarcimento dei danni patiti a seguito degli incidenti. Secondo i segnalanti, il contatto sarebbe avvenuto (in alcuni casi tramite lettera, in altri casi tramite visite a domicilio da parte di incaricati, in altri ancora tramite telefono), nei giorni immediatamente successivi l'incidente (in alcuni casi addirittura il giorno successivo) senza che gli interessati avessero mai comunicato i dati personali che li riguardavano all'agenzia segnalata.

Gli accertamenti hanno consentito di verificare che l'agenzia aveva organizzato un sistema informativo che le consentiva di conoscere, a distanza di poche ore dal verificarsi dei sinistri, gli elementi identificativi delle persone coinvolte, riuscendo così a proporre i propri servizi con grande anticipo rispetto alle imprese concorrenti.

Il trattamento illecito di dati personali effettuato dall'agenzia è stato segnalato alla competente autorità giudiziaria. Si è ritenuto in particolare che la causa obiettiva di punibilità prevista dall'art. 167 del Codice ("*se dal fatto deriva nocumento*") si configurasse sia per il modo in cui, immediatamente a ridosso di un evento, in taluni casi anche psicologicamente estremamente traumatico, le persone coinvolte sono state contattate, sia nella sofferenza morale che spesso deriva alle persone che si accorgono che dati personali riguardanti la salute escono dal circuito proprio nell'ambito del quale devono essere trattati.

Notificazione

Decorsi i termini utili per la presentazione della notificazione (30 aprile 2004), è stata avviata una serie di ispezioni nei confronti di trenta soggetti pubblici e privati, tra cui dodici aziende sanitarie locali e dodici società di lavoro interinale. Gli accertamenti, delegati al "Nucleo speciale funzione pubblica e *privacy*" della Guardia di finanza, hanno portato, in sedici casi, alla contestazione di violazioni per omessa o ritardata notificazione.

L'attività di vigilanza in materia di notificazione proseguirà, con modalità analo-

ghe, anche nel 2005, individuando soggetti tenuti all'adempimento anche mediante interconnessione con altre banche dati.

Videosorveglianza

Particolare attenzione è stata data ai controlli dei trattamenti effettuati mediante sistemi di videosorveglianza soprattutto nelle aree pubbliche (porti, aeroporti, metropolitane, enti pubblici). Le ispezioni effettuate hanno evidenziato, in linea di massima, un progressivo recepimento delle indicazioni del Garante (da prima con il *Provv.* 29 novembre 2000 e, da ultimo, con il *Provv.* 29 aprile 2004).

Non sono tuttavia mancati casi di inosservanza di tali indicazioni, come quello rilevato in un'ispezione presso un ente locale nel corso della quale si è rilevata l'esistenza di un complesso sistema di videosorveglianza –non adeguatamente segnalato agli interessati– collocato presso un obitorio e dotato anche di telecamere nascoste, in grado di riprendere immagini anche all'interno delle camere mortuarie. Le modalità del trattamento dei dati raccolti mediante il sofisticato sistema, la cui istallazione era stata a suo tempo motivata dal verificarsi di alcuni episodi di vilipendio nei confronti di cadaveri, sono apparse immediatamente in contrasto con i principi previsti dall'art. 11 del Codice. Su invito dell'Autorità, l'ente interessato dall'accertamento ha provveduto a sospendere il trattamento, in attesa delle determinazioni sulla complessiva liceità dello stesso.

Sempre in materia di controlli sui trattamenti effettuati mediante sistemi di videosorveglianza, sono state contestate sanzioni amministrative per la mancanza di idonee informative da parte di un'agenzia fiscale, delle società di gestione delle metropolitane di Roma e Milano e della società di gestione dell'aeroporto della Costa Smeralda.

20.4. *Alcuni riferimenti statistici*

L'attività ispettiva effettuata nel 2004 ha avuto anche quest'anno un significativo incremento rispetto a quella svolta l'anno precedente (+45%).

In generale, il volume delle attività ispettive ha continuato a crescere ogni anno a partire dal 2001, rispondendo ad una maggiore "domanda" di controllo da parte dei cittadini come dei soggetti (pubblici e privati) chiamati a dare effettiva attuazione alla disciplina di protezione dati.

Nel 2004 le attività ispettive sono state avviate sulla base di:

- accertamenti d'ufficio (43%);
- accertamenti conseguenti a segnalazioni pervenute all'Ufficio (38%);
- autonomi accertamenti a seguito di ricorsi presentati al Garante (19%).

Come si evince dal confronto con i dati dell'anno precedente, nel 2004 è stato maggiore lo spazio degli accertamenti così detti di iniziativa, avviati cioè *motu proprio* dall'Autorità, pure in assenza di atti di impulso da parte dei cittadini, a testimonianza di un atteggiamento attivo assunto dal Garante, anche attraverso lo strumento ispettivo.

Gli accertamenti eseguiti hanno riguardato in prevalenza verifiche concernenti:

- le modalità di acquisizione del consenso, in molti casi connesse ad attività effettuate sulla rete Internet mediante l'invio di sollecitazioni commerciali non richieste via *e-mail*;
- il rispetto delle disposizioni di legge in relazione al trattamento di dati mediante sistemi di videosorveglianza;
- l'accertamento dell'origine dei dati oggetto di trattamento;
- il rispetto dell'obbligo di notificazione al Garante;
- l'adozione delle misure di sicurezza.

Le ispezioni sono state effettuate:

- in novantatre casi mediante richieste di informazioni *in loco*;
- in sette casi mediante accessi a banche dati autorizzati dal Presidente del Tribunale.

Con riferimento all'ambito territoriale la ripartizione è stata omogenea:

- Nord (trentaquattro);
- Centro (trenta);
- Sud (trentasei).

L'incidenza delle violazioni penali sui procedimenti amministrativi di controllo avviati nel 2004 è pari circa al 13%. Le violazioni segnalate riguardano ipotesi di trattamento illecito di dati personali, omessa adozione di misure di sicurezza, inosservanza dei provvedimenti del Garante e false dichiarazioni al Garante.

Valutazioni di sintesi

Confermando le indicazioni emerse l'anno precedente, le ispezioni hanno in generale consentito di rilevare che nel settore privato le aziende più grandi iniziano ad adottare la legge anche attraverso la costituzione di unità organizzative con deleghe specifiche, veri e propri "uffici *privacy*", mentre le aziende medio-piccole evidenziano a volte un livello inferiore di adeguamento alla normativa e agli indirizzi del Garante. Non sempre, però, c'è perfetta corrispondenza tra osservanza formale delle disposizioni e reale e diffusa "cultura" del trattamento di dati secondo i principi stabiliti dal Codice.

Proprio nella pubblica amministrazione, come dimostrano i casi precedentemente descritti, la cultura della protezione dei dati personali stenta ad affermarsi compiutamente. Nei processi di lavoro e nella gestione delle pratiche di ufficio prevalgono ancora approcci di tipo "burocratico" e, talvolta, ad un assetto formalmente corretto non corrisponde una piena consapevolezza dei doveri e delle responsabilità connesse al trattamento dei dati personali. Sono ancora frequenti fenomeni di noncuranza e superficialità nel trattamento dei dati, soprattutto per quanto attiene la gestione degli archivi e le connesse misure di sicurezza e l'attuazione dei principi di indispensabilità, necessità, pertinenza e non eccedenza cui si è più volte fatto cenno.

20.5. *L'attività sanzionatoria del Garante*

L'attività operativa in materia di sanzioni amministrative, alla luce delle modifiche normative delle quali si è già dato conto (v. *Relazione 2003*), ha avuto ulteriore impulso a seguito delle attività di accertamento e di controllo poste in essere dal "Nucleo speciale funzione pubblica e *privacy*" della Guardia di finanza le cui unità di vigilanza, all'esito di capillari controlli svolti presso le sedi dei titolari del trattamento, hanno provveduto in decine di casi ad effettuare direttamente l'obbligatoria contestazione al momento in cui sono state rilevate le specifiche violazioni amministrative.

La linea d'azione scelta dal Garante per gli ambiti di indagine è stata quella di individuare specifici settori verso cui indirizzare le attività sopra indicate, le quali hanno coinvolto, in qualità di titolari, soggetti pubblici e privati. A ciò va aggiunta l'attività di accertamento e controllo svolta d'ufficio ovvero a seguito di segnalazioni e reclami indirizzati al Garante per lamentare un improprio utilizzo dei dati personali, che ha portato in alcuni casi alla contestazione di violazioni amministrative.

Attraverso un'analisi dettagliata dei provvedimenti sanzionatori si possono rinvenire ed individuare le operazioni di trattamento e le modalità che sono state più volte oggetto di contestazione di infrazione. Tra queste, la più significativa ha riguardato l'obbligo di notifica dei trattamenti al Garante (art. 37 del Codice), con parti-

colare riferimento agli adempimenti in materia di notificazione da parte dei titolari di trattamenti di dati sensibili (quali aziende sanitarie pubbliche e laboratori di analisi privati) e, in un caso, del trattamento di dati biometrici da parte di un istituto di credito (rilevazione di impronte digitali).

In tema di omessa o ritardata notificazione, i soggetti pubblici e privati sottoposti agli accertamenti sopra richiamati sono risultati inadempienti e pertanto oggetto di contestazione della violazione amministrativa della omessa o incompleta notificazione (art. 163 del Codice). A seguito di tali contestazioni i titolari del trattamento, in maggioranza, si sono avvalsi della facoltà di essere sentiti dal Garante (ai sensi dell'art. 18, l. n. 689/1981), in ciò confermando la previsione in materia di obbligatoria audizione formulata nella precedente *Relazione* annuale.

Nelle audizioni tenute nel 2004, è emersa in vari casi una lettura non corretta e non conforme al dettato normativo dell'art. 37, comma 1, lett. *a*) e *b*), del Codice, che ha generato nei titolari del trattamento l'erronea convinzione di non essere tenuti all'obbligo di notificazione.

In particolare, è risultata evidente una visione non sistematica delle norme sulla protezione dei dati personali, oltre che una loro non corretta interpretazione. Eppure il Garante era intervenuto sul tema nel corso del 2004 specie in due occasioni: con *Deliberazione* n. 1 del 31 marzo 2004 e con un provvedimento indirizzato ad alcune associazioni di categoria che hanno fornito le indicazioni e la corretta interpretazione del disposto dell'articolo citato. Ed è a quanto riportato in detti provvedimenti che avrebbero potuto agevolmente attenersi le organizzazioni sopra menzionate al fine del corretto adempimento dell'obbligo di notificazione al Garante.

L'attività di monitoraggio interno, prodromica ad ogni trattamento di dati personali che voglia essere conforme alle disposizioni di legge in materia, non sempre viene svolta con l'intento di verificare in modo puntuale e compiuto la natura, le modalità e le finalità del trattamento. Al contrario, si rileva spesso una tendenza a ricercare quanto necessario a far ritenere escluso un determinato adempimento. È di tutta evidenza che un tale atteggiamento comporta, per il titolare, il rischio di effettuare un trattamento non conforme alle norme di legge vigenti e di essere pertanto oggetto di provvedimento sanzionatorio da parte del Garante.

Sempre con riferimento alle risultanze di dette attività di accertamento e controllo, verranno predisposti, ai sensi dell'art. 17 della legge n. 689/1981, i rapporti necessari all'eventuale e successiva adozione dei provvedimenti di ordinanza-ingiunzione al pagamento di somme.

L'informativa all'interessato, ad esempio nelle attività effettuate per mezzo dei nuovi strumenti multimediali di comunicazione, è stata spesso omessa o è risultata incompleta al momento del raffronto con le finalità e modalità di fatto esercitate dal titolare. Significativo, in proposito, è il caso nel quale, a seguito del ricorso di un interessato, si è accertato che i dati raccolti da un'università al momento dell'iscrizione venivano utilizzati anche per attività ulteriori rispetto a quelle per le quali era stata fornita l'informativa (nel caso di specie, comunicati a terzi che li utilizzavano per inviare comunicazioni commerciali non sollecitate).

Per quanto attiene ai trattamenti di dati personali effettuati per mezzo di strumenti di videosorveglianza, sono state nuovamente accertate e sanzionate violazioni connesse ad informative assenti o incomplete riguardo agli obbligatori riferimenti alle modalità e finalità del trattamento effettuato.

Si sono verificati infine casi di mancato riscontro alle richieste di informazioni ed esibizione di documenti rivolte dal Garante ai titolari del trattamento (art. 157 del Codice) –richieste necessarie per l'assolvimento delle funzioni di controllo rimesse all'Autorità– che hanno portato alla contestazione della relativa infrazione.

21 Relazioni istituzionali

21.1. *L'Autorità e le attività di sindacato ispettivo e di indirizzo del Parlamento*

In relazione agli aspetti di specifico interesse in materia di protezione dei dati personali, l'Autorità ha seguito con attenzione l'attività di sindacato ispettivo e di indirizzo esercitata dal Parlamento, e ha fornito al Governo, ove richiesto, i chiarimenti e le indicazioni necessarie.

Sono stati inoltrati al Governo elementi in merito ad alcuni atti, fra i quali in particolare:

a) alcune interrogazioni relative all'acquisizione da parte delle autorità doganali degli Stati Uniti dei dati dei passeggeri conservati nella banche dati dell'Alitalia, presentate dall'on. Folena (3-02017), dall'on. Delmastro Delle Vedove (4-05923) e dall'on. Pagliarulo (4-04379) (*Note* 14 aprile 2004, 28 aprile 2004 e 8 ottobre 2004). In tali occasioni l'Autorità, richiamando i pareri adottati dal Gruppo dei Garanti europei, ha ricordato che la richiesta formulata dalle autorità statunitensi di accedere ai dati registrati nel *Pnr* (*Passenger name record*) deve essere valutata alla stregua delle disposizioni comunitarie in materia e in particolare dell'art. 25 della direttiva 95/46/CE (v. più diffusamente par. 22.6);
b) un'interrogazione dell'on. Delmastro Delle Vedove (3-02307) relativa al progetto USA denominato T.I.A. (*Terrorism information awareness*) (*Nota* 28 aprile 2004);
c) due mozioni della maggioranza (1-00304 Leone ed altri) e dell'opposizione parlamentare (1-00215 Folena ed altri), di contenuto analogo ed approvate all'unanimità dal Parlamento il 14 gennaio 2004, su alcune questioni in materia di protezione dei dati personali, fra le quali, in particolare, la necessità di una più efficace tutela della riservatezza in Internet;
d) un'interrogazione dell'on. Delmastro Delle Vedove (4-04007) relativa alla mancata adozione da parte dei soggetti pubblici dei regolamenti sui dati sensibili (*Nota* 3 maggio 2004).

21.2. *L'attività consultiva del Garante sugli atti del Governo*

L'art. 154, comma 4, del Codice prevede che il Presidente del Consiglio dei ministri e ciascun ministro devono consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi che incidono sulla protezione di dati personali, al fine di prevenire delicati problemi applicativi, nell'interesse pubblico e dei cittadini, in un quadro di proficua collaborazione istituzionale che diversi ministeri hanno riconosciuto più volte.

L'Autorità ha espresso diversi pareri, fra i quali quelli riguardanti:

a) il decreto del Ministro della giustizia 14 gennaio 2005 con il quale sono inseriti nell'allegato A del Codice in materia di protezione dei dati personali, il codice di deontologia e buona condotta per i trattamenti di dati

effettuati per scopi statistici e scientifici e il codice deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo e affidabilità e puntualità nei pagamenti;

b) due schemi di convenzione fra i Ministeri della giustizia e dell'interno, da un lato, e l'Isvap, dall'altro, per la consultazione della banca dati sui sinistri per finalità di lotta alle frodi assicurative (*Pareri* 11 novembre 2004);

c) lo schema di regolamento per l'organizzazione ed il funzionamento dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (*Parere* 28 settembre 2004). Il Garante ha chiesto che il Ministero delle comunicazioni e il predetto Istituto, nell'esecuzione dei compiti loro assegnati dal Codice delle comunicazioni, rispettino i principi previsti dalla disciplina anche attuativa sulla protezione dei dati, in particolare per quanto riguarda il trattamento delle informazioni contenute negli elenchi degli abbonati ai servizi telefonici;

d) lo schema di decreto del Ministro del lavoro e delle politiche sociali di concerto con il Ministro per l'innovazione e le tecnologie in materia di *"Borsa continua nazionale del lavoro"*, adottato ai sensi del d.lg. 10 settembre 2003, n. 276 di attuazione della legge 14 febbraio 2003, n. 30 (cd. legge Biagi) (*Parere* 3 settembre 2004). Il decreto è stato recentemente pubblicato in *Gazzetta Ufficiale* (decreto 13 ottobre 2004 in *G.U.* 8 ottobre 2004, n. 262) recependo, in parte, le indicazioni fornite dal Garante (come più ampiamente riferito nel par. 11.1). Non è stata recepita, invece, la richiesta dell'Autorità di espungere dai dati identificativi del lavoratore e del datore di lavoro il codice fiscale, in applicazione del principio di pertinenza e non eccedenza dei dati trattati rispetto alle finalità della Borsa;

e) lo schema di decreto ministeriale recante regole tecnico-operative per l'uso di strumenti telematici nel processo civile (cd. Processo telematico) previsto dall'art. 3, comma 3, del d.P.R. n. 123/2001 (*Parere* 23 luglio 2004, in ordine al quale, per i profili di merito, si fa rinvio al par. 2.11).

Nei primi mesi del 2004 l'Autorità ha adottato anche altri pareri, già menzionati nella *Relazione 2003*, riguardanti:

f) lo schema di decreto concernente l'individuazione dei dati da inserire nell'anagrafe nazionale degli studenti e dei laureati (*Parere* 7 aprile 2004);

g) due schemi di regolamento in attuazione della legge n. 189 del 2002 concernenti, l'uno, il riordino del regolamento di attuazione del testo unico in materia di immigrazione e condizione dello straniero (d.P.R. n. 394/1999) e, l'altro, la razionalizzazione e l'interconnessione delle comunicazioni fra amministrazioni pubbliche in materia di immigrazione, in particolare ai fini del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (*Parere* 4 marzo 2004). Quest'ultimo è stato poi adottato con il d.P.R. 27 luglio 2004, n. 242 (in *G.U.* 18 settembre 2004, n. 220) recependo, in parte, le indicazioni fornite dal Garante;

h) lo schema di decreto interministeriale (Ministri per l'innovazione e le tecnologie e dell'interno) che disciplina il permesso di soggiorno elettronico. Dopo un primo parere del 15 ottobre 2003, a seguito di incontri tecnici fra rappresentanti dell'Autorità e del Ministero dell'interno, l'Autorità ha adottato un secondo parere il 4 marzo 2004 con il quale ha indicato, fra l'altro, gli interventi necessari per garantire gli interessati in occasione della raccolta delle impronte digitali e, in particolare, nel caso di inserimento di dati biometrici nel documento elettronico. Il decreto è stato poi

adottato il 3 agosto 2004, recependo sostanzialmente le indicazioni fornite dal Garante e pubblicato nella *Gazzetta Ufficiale* del 6 ottobre 2004, n. 235. L'Autorità ha confermato la propria disponibilità a proseguire attivamente gli incontri per approfondire i problemi e i rischi derivanti dalle differenti tecniche di identificazione e di autenticazione individuate dai Garanti europei nel parere del 1° agosto 2003 sui dati biometrici. Tali approfondimenti appaiono necessari anche allo scopo di individuare idonee cautele nella fase di attivazione del documento elettronico e di consegna dei documenti o di accesso selezionato ai dati, nonché le più elevate misure di garanzie di sicurezza disponibili. L'esito di tali approfondimenti potrebbe essere poi trasfuso nelle misure e negli accorgimenti che in materia di dati biometrici devono essere prescritti dal Garante ai sensi dell'art. 55 del Codice;

i) lo schema di decreto del Presidente della Repubblica recante il regolamento di disciplina dell'accesso al servizio di informatica giuridica del Centro elettronico di documentazione (Ced) della Corte di cassazione (*Parere* 27 febbraio 2004);

l) lo schema di regolamento (Ministri per la funzione pubblica e dell'interno) di gestione dell'Indice nazionale delle anagrafi (Ina), in attuazione dell'art. 2-*quater* del decreto-legge 27 dicembre 2000, n. 392, convertito dalla legge n. 26/2001 (*Parere* 13 febbraio 2004);

m) lo schema di decreto dirigenziale del Ministero della giustizia, di attuazione in via parziale e transitoria dell'art. 39 del d.P.R. 14 novembre 2002, n. 313 (testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti), concernente la consultazione del casellario giudiziale da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi (*Parere* 29 gennaio 2004). Come già riportato nella *Relazione* 2003, in occasione degli incontri di lavoro che hanno preceduto la redazione dello schema di decreto, l'Autorità aveva constatato il carattere transitorio della soluzione elaborata, in attesa di una regolamentazione definitiva della procedura di accesso diretto ai sensi dell'art. 39 del d.P.R. n. 313/2002. Nel parere del 29 gennaio 2004 è stata sottolineata la necessità che l'accesso ai dati giudiziari registrati nel casellario giudiziale, nonché il successivo utilizzo da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi, siano consentiti nel rispetto dei limiti previsti dallo stesso d.P.R. n. 313/2002 e in misura proporzionata alle finalità da perseguire.

Nel 2004 si è tuttavia registrato un incremento dei casi di mancata consultazione dell'Autorità, persino su tematiche fondamentali nel rapporto tra Stato e cittadini che implicano il trattamento di dati sensibili o comunque particolarmente delicati, come ad esempio nel caso dei decreti attuativi del sistema di monitoraggio della spesa sanitaria e di introduzione della tessera sanitaria.

Pertanto l'Autorità ha inviato al Governo un elenco dei principali regolamenti ed atti amministrativi in relazione ai quali, negli ultimi anni, non è stato richiesto il parere al Garante ai sensi dell'art. 31, comma 2, della legge n. 675/1996 e poi dell'art. 154, comma 4, del Codice, segnalando che la mancata consultazione integra una violazione di legge e del diritto comunitario, che espone peraltro i dati personali trattati in applicazione di tali atti alla conseguenza dell'inutilizzabilità (art. 11, comma 2, del Codice).

Di seguito si riportano i casi più significativi:

a) d.P.R. 6 ottobre 2004, n. 258 "Regolamento concernente le funzioni dell'Alto Commissario per la prevenzione e il contrasto della corruzione e delle altre forme di illecito nella pubblica amministrazione" (*G.U.* 22 ottobre 2004, n. 249);
b) d.P.R. 16 settembre 2004, n. 303, recante "Regolamento relativo alle procedure per il riconoscimento dello *status* di rifugiato" (*G.U.* 22 dicembre 2004, n. 299);
c) d.P.R. 23 aprile 2004, n. 108, "Regolamento recante disciplina per l'istituzione, l'organizzazione ed il funzionamento del ruolo dei dirigenti presso le amministrazioni dello Stato, anche ad ordinamento autonomo" (*G.U.* 29 aprile 2004, n. 100);
d) decreto del Ministro dell'economia e delle finanze di concerto con il Ministro della salute 30 giugno 2004, recante "Applicazione delle disposizioni di cui al comma 6 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente l'avvio del sistema di monitoraggio della spesa nel settore sanitario" (*G.U.* 2 luglio 2004, n. 153);
e) decreto del Ministro della salute 15 luglio 2004 recante "Istituzione, presso l'Agenzia italiana del farmaco, di una banca dati centrale finalizzata a monitorare le confezioni dei medicinali all'interno del sistema distributivo" (*G.U.* 4 gennaio 2005, n. 2);
f) decreto del Ministro dell'istruzione, dell'università e della ricerca 1° luglio 2004, recante "Progetto "PC alle famiglie", di cui all'art. 4, comma 10, della legge 24 dicembre 2003, n. 350" (*G.U.* 9 agosto 2004, n. 185);
g) decreto (Ministero dell'economia e delle finanze, Ministero della salute e Presidenza del Consiglio dei ministri - Ministro per l'innovazione e le tecnologie) 11 marzo 2004, recante "Applicazione delle disposizioni di cui al comma 1 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione delle caratteristiche tecniche della Tessera sanitaria (TS)" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);
h) decreto (Ministeri dell'economia e delle finanze e della salute) 18 maggio 2004, recante "Applicazione delle disposizioni di cui al comma 2 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione dei modelli di ricettari medici standardizzati e di ricetta medica a lettura ottica" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);
i) decreto (Ministero dell'economia e delle finanze) 24 giugno 2004 recante "Applicazione delle disposizioni di cui al comma 4 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione delle modalità di trasmissione telematica al Ministero dell'economia e delle finanze dei dati riguardanti l'assegnazione dei ricettari ai medici prescrittori" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);
l) decreto (Ministero dell'economia e delle finanze) 24 giugno 2004, recante "Applicazione delle disposizioni contenute nel disciplinare tecnico di cui al comma 5 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, recante disposizioni urgenti per favorire lo sviluppo per la correzione dell'andamento dei conti pubblici, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326" (*G.U.* 13 luglio 2004, n. 162, S.O. n. 123);
m) decreto (Ministero dell'economia e delle finanze) 28 giugno 2004,

recante "Applicazione delle disposizioni di cui al comma 9 dell'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, concernente la definizione dei dati che le regioni, nonché i Ministeri e gli enti pubblici di rilevanza nazionale che li detengono, trasmettono al Ministero dell'economia e delle finanze, con modalità telematica" (*G.U.* 25 ottobre 2004, n. 251, S.O. n. 159);

n) decreto del Capo del dipartimento dell'amministrazione generale, del personale e dei servizi del tesoro del Ministero dell'economia e delle finanze 12 febbraio 2004, recante "Criteri organizzativi per l'assegnazione delle domande agli organismi di accertamento sanitario di cui all'art. 9 del d.P.R. n. 461/2001, ed approvazione dei modelli di verbale utilizzati, anche per le trasmissioni in via telematica, con le specificazioni sulle tipologie di accertamenti sanitari eseguiti e sulle modalità di svolgimento dei lavori (*G.U.* 23 febbraio 2004, n. 44);

o) provvedimento dell'Agenzia delle entrate 18 febbraio 2004 recante approvazione del nuovo modello di dichiarazione per l'integrazione degli imponibili ai sensi degli articoli 8, 9, 9-*bis* e 14 della legge 27 dicembre 2002, n. 289, termini per la trasmissione e approvazione delle specifiche tecniche per la trasmissione telematica dei dati contenuti nella dichiarazione (*G.U.* 15 marzo 2004, n. 62, S.O. n. 44);

p) provvedimento dell'Agenzia delle dogane 28 febbraio 2004, recante la realizzazione di una banca dati multimediale, ai sensi dell'art. 4, commi 54 e 55, della legge 24 dicembre 2003, n. 350 (*G.U.* 10 marzo 2004, n. 58);

q) ordinanza del Ministro della salute 25 febbraio 2004 "Misure urgenti in materia di cellule staminali da cordone ombelicale" (*G.U.* 18 marzo 2004, n. 65).

21.3. *Altra collaborazione con la Presidenza del Consiglio dei ministri*

Si è già fatto cenno all'attività di monitoraggio effettuata dall'Autorità sulle leggi regionali (cfr. par. 1.4.). Sotto diverso profilo, si intende qui rendere conto dei risultati dell'attività consultiva sollecitata dalla Presidenza del Consiglio dei ministri sul contenuto di alcune leggi regionali, per gli aspetti di competenza del Garante, al fine di segnalare questioni eventualmente rilevanti in sede di conflitto di attribuzioni tra Stato e Regioni.

Se in alcune ipotesi non si sono ravvisati profili di illegittimità costituzionale, in altre si sono rilevati aspetti problematici.

È questo il caso della legge della Regione Emilia-Romagna 25 maggio 2004, n. 11, che prevede l'utilizzo integrato delle basi di dati esistenti attraverso la collaborazione con le altre pubbliche amministrazioni e la possibilità di accesso e di cessione dei dati a privati e ad enti pubblici economici.

Come già accennato, il Garante ha preliminarmente rilevato che il diritto alla protezione dei dati personali, ascrivibile tra i diritti inviolabili riconosciuti dall'art. 2 della Costituzione, è materia di competenza esclusiva dello Stato poiché concerne l'"ordinamento civile" dello Stato e la "determinazione dei livelli essenziali delle prestazioni relative ai diritti civili e sociali" (art. 117, comma 2, lett. *l*) e *m*), della Costituzione).

In relazione ai contenuti della legge regionale, l'Autorità ha poi osservato che l'interconnessione generalizzata di archivi, gli indiscriminati flussi di dati, nonché la correlata possibilità, prevista con l'approvazione di un successivo regolamento, di

rendere disponibile anche a terzi (privati ed enti pubblici economici) il patrimonio informativo, non è coerente con la normativa vigente che stabilisce la predisposizione di garanzie poste con norme di legge statale riconoscendo ai cittadini, ad esempio, il diritto di essere previamente informati sulle ulteriori finalità perseguite nell'uso dei dati a seguito delle interconnessioni che la nuova banca dati produrrebbe (*Nota* 28 giugno 2004).

Tali rilievi sono stati fatti propri dal Consiglio dei ministri nell'impugnazione della legge davanti alla Corte Costituzionale.

In sede di esame della legge istitutiva del sistema integrato di interventi e servizi sociali, approvata dalla Regione Calabria (n. 23 del 9 dicembre 2003), l'Autorità ha evidenziato che l'istituzione di tale sistema implica necessariamente un'attività di trattamento di dati personali degli assistiti –anche di natura sensibile–, che deve essere effettuata nel pieno rispetto delle disposizioni dettate dal Codice. Tra l'altro, è stato osservato che il sistema coinvolge diversi soggetti erogatori delle prestazioni sociali, rendendo quindi necessaria l'individuazione di coloro che possono qualificarsi come titolari o contitolari del trattamento. I titolari, oltre a rispettare i principi di pertinenza e non eccedenza, devono prevedere che il sistema sia configurato in modo da ridurre al minimo l'utilizzo di dati personali e di dati identificativi, in modo da escludere 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). È stata inoltre avanzata qualche perplessità sull'istituzione di un registro degli ospiti presenti nelle strutture accreditate e di un registro degli utenti dei servizi offerti, dovendo al riguardo essere individuate con maggiore esattezza le finalità perseguite attraverso l'istituzione di detti registri e le tipologie di dati personali ivi contenute (*Nota* del 26 gennaio 2004).

In relazione alla legge della Regione Toscana 15 dicembre 2004, n. 63, recante "*Norme contro le discriminazioni determinate dall'orientamento sessuale o dall'identità di genere*" ed in particolare all'art. 7 che disciplina le modalità di prestazione del consenso informato, l'Autorità ha evidenziato che la materia è compiutamente disciplinata dal Codice, il quale, in attuazione della normativa internazionale e comunitaria, stabilisce particolari garanzie –specie ove si tratti, come nel caso in esame, di dati sensibili idonei a rivelare lo stato di salute delle persone– e disposizioni sulle modalità di acquisizione del consenso, anche nei casi di incapacità legale, naturale o temporanea (art. 20, 22, 76 e 82 ss. del Codice). Nel caso in cui la legge regionale faccia riferimento anche o solo al consenso al trattamento medico, anche se tale profilo non riguarda direttamente aspetti di competenza del Garante, sussisterebbero ugualmente profili di illegittimità costituzionale della norma, trattandosi in questo caso di diritti civili e sociali della persona. La contiguità del consenso al trattamento dei dati personali con quello relativo al trattamento sanitario è ben evidenziata, ad esempio, in un contesto normativo analogo a quello in esame, dal cd. "decreto Di Bella" che impone la contestuale acquisizione dei due consensi (art. 5-*bis*, comma 1, d.l. n. 23/1998, convertito dalla l. n. 94/1998, come modificato dall'art. 178 del Codice).

Gli stessi rilievi sono stati mossi dall'Autorità in riferimento all'articolo 8 della legge regionale, in quanto alcuni aspetti della dichiarazione di volontà che il regolamento regionale ivi previsto dovrebbe disciplinare trovano anch'essi compiuta regolamentazione nel Codice, in particolare per quanto riguarda l'individuazione di garanzie a tutela della riservatezza dei pazienti (art. 78 del Codice). La costituzione di una banca dati delle dichiarazioni di volontà viola poi il principio di proporzionalità nel trattamento dei dati personali, non apparendo giustificata la raccolta delle

informazioni in un unico archivio centrale; mancano inoltre indicazioni circa le tipologie dei dati da registrare nella banca di dati e le relative finalità della raccolta, in contrasto con i principi di necessità, indispensabilità, pertinenza e non eccedenza dei dati, in base ai quali i sistemi informativi devono essere configurati riducendo al minimo l'utilizzazione di dati personali e possono essere richiesti all'interessato i soli dati pertinenti rispetto alle finalità perseguite (artt. 3, 11 e 22 del Codice) (*Nota* 11 gennaio 2005).

L'Autorità è stata inoltre consultata dalla Regione Toscana per ciò che concerne il trattamento dei dati personali ai fini dello svolgimento delle elezioni regionali primarie del 20 febbaio 2005, inizialmente disciplinate dalla sola legge regionale 17 dicembre 2004, n. 70, recante *"Norme per la selezione dei candidati e delle candidate alle elezioni per il Consiglio regionale e alla carica di Presidente della Giunta regionale"*, che presentava profili di criticità in relazione alla protezione dei dati personali.

21.4. *Attività di cooperazione con altre istituzioni*

Anche nell'anno 2004 si è registrata un'intensa attività di cooperazione dell'Autorità con altre istituzioni su tematiche comuni.

Autorità per le garanzie nelle comunicazioni

Con l'Autorità per le garanzie nelle comunicazioni, oltre che per l'adozione del provvedimento relativo ai nuovi elenchi telefonici di cui si tratta in un apposito paragrafo, è proseguita, ai sensi dell'art. 154, comma 3, del Codice, la consueta e proficua collaborazione su vari temi come ad esempio quello relativo all'attivazione di contratti e servizi di telefonia fissa senza il preventivo consenso degli interessati.

Si è in tal modo proceduto ad esaminare in concreto il problema confrontando le segnalazioni pervenute, ciascuna per la relativa sfera di competenza. All'esito di tale scambio di informazioni il Garante ha ritenuto opportuno dar corso ad ulteriori interventi utilizzando i poteri conferiti dall'art. 157 del Codice.

Ministero delle comunicazioni

Una fattiva attività di cooperazione è stata intrapresa anche con il Ministero delle comunicazioni. In particolare, il Garante ha partecipato a numerosi incontri presso il Ministero nei quali sono stati affrontati importanti temi di interesse comune quali l'utilizzo della posta elettronica o di *Sms* telefonici per l'invio non preventivamente autorizzato di materiale pubblicitario (fenomeno comunemente noto come *spamming*) e l'illecita intestazione di utenze telefoniche mobili illecitamente operate all'insaputa degli interessati.

Per fronteggiare con uno sforzo comune il grave fenomeno della irregolare intestazione e successiva commercializzazione di carte prepagate di telefonia mobile, l'Autorità partecipa attivamente al gruppo di lavoro cui sono presenti il Ministero delle comunicazioni, l'Autorità per le garanzie nelle comunicazioni, l'Autorità garante della concorrenza e del mercato, il Ministero della giustizia e il Ministero dell'interno.

Dipartimento della protezione civile

Il Garante ha contribuito alla predisposizione di una convenzione ai sensi dell'art. 6, comma 1, della legge 24 febbraio 1992, n. 225, tra il Dipartimento della protezione civile e gli operatori di servizi di comunicazione mobile. Tale convenzione, stipulata il 28 settembre 2004, ha ad oggetto la costituzione del "Circuito nazionale dell'informazione d'emergenza" (Cnie), ossia di un sistema promosso dall'Autorità per le garanzie nelle comunicazioni, d'intesa con il Ministero delle comunicazioni e con il Dipartimento della protezione civile volto a realizzare la trasmissione di *Sms* informativi di pubblica utilità per il Dipartimento della protezione

civile, nei casi di necessità e urgenza provocati da calamità naturali e d'altra natura.

Gli operatori telefonici, in tali situazioni di emergenza, invieranno ai loro clienti messaggi *Sms* secondo le indicazioni del Dipartimento della protezione civile in relazione al contenuto del messaggio, alla tempistica, all'area geografica interessata alla diffusione. Basandosi solo su provvedimenti d'emergenza adottati ai sensi dell'art. 5, commi 1, 2 e 5, della legge n. 225/1992 (che devono indicare espressamente l'eventuale deroga a specifiche disposizioni del Codice sulla protezione dei dati personali e le relative motivazioni), l'invio può prescindere da uno specifico consenso prestato dalla clientela. Resta ferma la possibilità per gli interessati di esercitare il diritto di non ricevere messaggi.

Vi sono numerosi aspetti della convenzione che attengono, quindi, al trattamento dei dati personali. Particolare interesse riveste per l'Autorità l'individuazione dei soggetti destinatari dei messaggi *Sms*, che verrà effettuata non solo in base ai dati anagrafici degli stessi, ma anche mediante localizzazione geografica dei terminali. Il Garante, pertanto, al termine dell'attività di cooperazione svolta anche ai sensi dell'art. 154, comma 3, del Codice, ha indicato le integrazioni da inserire nella convenzione e nel relativo allegato tecnico, tenendo anche conto delle indicazioni già fornite in tema di messaggi di pubblica utilità in due diversi provvedimenti (12 marzo 2003 e 7 luglio 2004) richiamati espressamente in premessa dalla convenzione.

Nel dicembre 2004 l'Autorità è stata chiamata a prendere parte al Gruppo di lavoro interministeriale per l'istituzione del numero unico europeo per le emergenze, costituito con d.P.C.M. del 4 agosto 2003. Il Gruppo ha il compito di analizzare i problemi posti dall'attivazione sul territorio nazionale del predetto numero unico, volto a garantire agli interessati adeguata risposta alle chiamate ai servizi di emergenza. Ciò in conformità con quanto previsto in attuazione della normativa comunitaria (cfr. direttive 2002/21/CE e 2002/22/CE) e dall'art. 76 del Codice delle comunicazioni elettroniche (d.lg. n. 259/2003).

Il Garante dovrà tra l'altro valutare la conformità al Codice sulla protezione dei dati personali del sistema che consentirà di identificare la localizzazione del chiamante e di acquisirne i dati personali all'atto della ricezione della chiamata di emergenza.

21.5. *Collaborazione con la Guardia di finanza*

Nello svolgimento dell'attività ispettiva il Garante può avvalersi della collaborazione di altri organi dello Stato; già da tempo si sono avute molteplici occasioni di collaborazione con le forze di polizia ed in particolare con la Guardia di finanza, in ragione delle peculiari competenze nel campo delle attività di controllo di tipo amministrativo proprie del Corpo.

La collaborazione nel settore delle attività ispettive è stata regolata con un protocollo d'intesa che prevede che la Guardia di finanza operi attraverso:

- il reperimento di dati e informazioni sui soggetti da controllare;
- 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 delegate o sub-delegate per l'accertamento delle violazioni di natura penale e amministrativa;
- l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori.

Al fine di rafforzare ulteriormente il rapporto di collaborazione, nel mese di giugno 2004 la Guardia di finanza ha costituito, come si è già detto, il "Nucleo spe-

ciale funzione pubblica e *privacy*" il cui personale, altamente specializzato, procede direttamente all'esecuzione delle attività ispettive avvalendosi, se necessario, dei reparti territoriali del Corpo.

Una delle prime attività affidate al Nucleo è stata la verifica del rispetto dell'obbligo di notificazione al Garante, in concomitanza con la scadenza del termine previsto dal Codice (30 aprile 2004), mediante accertamenti nei confronti di un primo gruppo di trenta soggetti pubblici e privati, tra cui dodici aziende sanitarie locali e dodici società di lavoro interinale, che ha portato alla contestazione di numerose sanzioni amministrative (v. specifico approfondimento in par. 20.3).

In generale il Nucleo ha svolto per l'Autorità un ruolo di valido supporto, oltre che per l'esecuzione di attività ispettive delegate, anche per la notifica di atti urgenti e per l'acquisizione di informazioni necessarie ad individuare con certezza i titolari o i responsabili del trattamento nei cui confronti dovevano essere avviati dei procedimenti.

In alcuni casi ci si è avvalsi della componente territoriale del Corpo per verificare, anche attraverso sopralluoghi, l'ottemperanza ai provvedimenti dell'Autorità adottati a seguito di ricorsi (ad esempio, riposizionamento di impianti di videosorveglianza, apposizione di informative *ex* art. 13 del Codice, avvenuta designazione di incaricati del trattamento).

La competenza acquisita dal Nucleo in virtù del rapporto di collaborazione ha fatto assumere allo stesso un ruolo di punto di riferimento cui delegare, da parte dell'autorità giudiziaria, anche attività di indagine per le violazioni al Codice costituenti reato.

Rispetto a queste attività il Garante, su esplicita richiesta dell'Autorità giudiziaria procedente, ha fornito un supporto in termini di approfondimenti sull'applicazione della legge.

22 Relazioni internazionali

22.1. *Lo stato di recepimento delle direttive comunitarie negli Stati membri dell'Unione europea*

Il 2004 è stato l'anno dell'"allargamento" dell'Unione europea con l'ingresso di dieci nuovi Stati (Cipro, Estonia, Lettonia, Lituania, Malta, Polonia, Repubblica Ceca, Slovenia, Slovacchia, Ungheria).

Nei nuovi Stati membri, le disposizioni delle direttive europee in materia di protezione dei dati (95/46/CE) e comunicazioni elettroniche e vita privata (2002/58/CE) trovano applicazione integrale a partire dalla data di adesione all'Unione europea, ossia dal 1° maggio 2004.

Guardando più in dettaglio alla situazione esistente al 31 dicembre 2004 nei venticinque Paesi dell'Ue, il quadro relativo al recepimento nella legislazione nazionale rende opportune alcune precisazioni.

Direttiva 95/46/CE

Tutti i quindici Paesi dell'Unione europea avevano recepito la direttiva prima del 1° maggio 2004 (v. *Relazione* 2003), anche se la Francia aveva notificato la legislazione adottata nel 1978, perdurando l'*iter* parlamentare (iniziato nel 2001) per l'adozione della normativa specifica. La nuova legge francese "*Informatique et libertés*", di recepimento della direttiva 95/46/CE, è stata adottata il 6 agosto 2004 ed è entrata in vigore il giorno successivo. Rispetto alla precedente legge, il nuovo testo aumenta i poteri sanzionatori dell'autorità di protezione dati (la *Commission Nationale Informatique et Libertés*, Cnil); elimina l'obbligo di notificazione alla Cnil per i titolari che designano (su base facoltativa) un "referente per la protezione dei dati" (il cosiddetto "*correspondant à la protection des données*") incaricato di vigilare sull'applicazione della normativa da parte del titolare e di monitorare la liceità e le modalità dei trattamenti di dati personali effettuati da quest'ultimo (ai sensi dell'art. 18(2) della direttiva); infine, dispone l'obbligo di sottoporre a valutazione preliminare da parte della Cnil qualsiasi trattamento che comporti il ricorso a tecniche biometriche. La legge inasprisce anche le sanzioni previste in caso di inadempimento. Il nuovo quadro normativo sarà completato attraverso l'adozione di atti di legislazione secondaria che preciseranno le procedure di valutazione preliminare ed altri aspetti concernenti, ad esempio, i requisiti da soddisfare per svolgere la funzione di "referente per la protezione dei dati".

La valutazione della qualità del recepimento per i quindici Paesi membri è in corso da parte della Commissione, secondo il programma di lavoro fissato nel Primo rapporto sull'applicazione della direttiva.

I nuovi Stati membri sono tutti provvisti di una legge nazionale in materia di protezione dei dati, che in alcuni casi è stata adottata *ex novo*, mentre in altri ha subito vari emendamenti dopo l'adozione della direttiva 95/46/CE, in particolare al fine di istituire un'autorità per la protezione dei dati incaricata di vigilare sull'applicazione delle disposizioni in materia a livello nazionale. Va sottolineato, in proposito, che dal 2001 alcuni dei nuovi Stati membri (Estonia, Lettonia, Lituania, Polonia, Repubblica Ceca, Repubblica Slovacca e Ungheria) hanno stabilito forme più strette di collaborazione e scambio di informazioni, anche attraverso un appo-

sito sito *web* (*www.ceecprivacy.org*) e l'organizzazione di due conferenze semestrali per discutere di tematiche di interesse comune.

La Commissione sta valutando l'effettiva conformità con l'*acquis* comunitario delle disposizioni nazionali.

Direttiva 2002/58/CE

La situazione relativa al recepimento della direttiva sulla vita privata e le comunicazioni elettroniche è più articolata. Nella *Relazione* 2003 si è fatto cenno alle iniziative preliminari adottate dalla Commissione europea nei confronti di alcuni Stati, per omessa comunicazione delle misure nazionali di trasposizione, ovvero per l'incompleta trasposizione della direttiva (con particolare riguardo all'art. 13, relativo alle comunicazioni indesiderate).

Dopo il parere motivato emesso il 1° aprile 2004 nei confronti di Belgio, Finlandia, Francia, Germania, Grecia, Lussemburgo e Paesi Bassi, e dopo l'adesione dei nuovi Stati membri, alla fine del mese di giugno 2004 la Commissione ha deciso di adire la Corte di giustizia nei confronti di tre Paesi (Belgio, Grecia, Lussemburgo) come previsto dal Trattato Ue per la mancata adozione della legislazione primaria di recepimento. Gli altri Paesi (Finlandia, Francia, Germania e Paesi Bassi) hanno provveduto nel frattempo a notificare le misure nazionali adottate. Tuttavia, la Commissione ha segnalato anche ad altri Paesi l'imperfetta trasposizione delle norme della direttiva 2002/58/CE. Ciò riguarda, in particolare:

- il recepimento delle disposizioni dell'art. 13, che vieta le comunicazioni indesiderate (quindi anche lo *spam*) in assenza del consenso preventivo dell'abbonato *(opt-in)*. Repubblica Ceca, Estonia, Grecia e Lussemburgo non hanno notificato le misure nazionali adottate;
- il recepimento degli articoli 5, 6 e 9 che riguardano, rispettivamente, i dati di traffico e di ubicazione e le relative modalità di trattamento e conservazione. Belgio, Repubblica Ceca, Estonia, Grecia e Lussemburgo non hanno notificato alla Commissione le misure adottate in materia.

Anche riguardo alla direttiva 2002/58/CE, la Commissione sta valutando la piena conformità della legislazione nazionale in vigore nei Paesi dell'Unione europea.

22.2. *Le iniziative a livello europeo per una migliore applicazione delle direttive comunitarie*

Recepimento della direttiva 95/46/CE

Come segnalato nella *Relazione* 2003, sia il Primo Rapporto della Commissione europea sullo stato di attuazione della direttiva 95/46/CE (pubblicato il 15 maggio 2003), sia i risultati dell'Eurobarometro pubblicati nel febbraio 2004 hanno dipinto un quadro caratterizzato da luci e alcune ombre per quanto riguarda l'effettiva trasposizione dei principi comunitari e la percezione dell'efficacia di tali principi da parte di imprese e cittadini europei.

In particolare, nel rapporto della Commissione viene delineato un programma di lavoro in dieci punti per giungere ad una migliore applicazione della direttiva tra i Paesi dell'Unione. Su molti di essi la Commissione ha previsto e richiesto iniziative comuni da parte delle autorità di protezione dei dati, le quali hanno quindi deciso di integrare le azioni richieste anche nel loro programma di lavoro a partire dal 2004.

Del resto, le stesse autorità avevano da tempo indicato fra le priorità del proprio mandato il potenziamento dell'attuazione delle norme in materia di protezione dei dati attraverso numerose strategie. Queste ultime sono state sistematizzate in un documento che il Gruppo dei Garanti europei istituito dall'art. 29 della direttiva 95/46/CE (di seguito, semplicemente, "Gruppo art. 29") ha adottato nel set-

tembre 2004 allo scopo di indicare alcune linee comuni di attività.

Per quanto concerne, in particolare, il potenziamento dell'attuazione dei principi comunitari in materia di protezione dei dati, le autorità garanti hanno messo l'accento soprattutto:

- sulle strategie per migliorare il rispetto e l'applicazione pratica delle normative nazionali in materia, attraverso l'elaborazione di approcci comuni comprendenti anche indagini ed accertamenti ispettivi "sincronizzati" in rapporto ad alcuni settori che risultano essere particolarmente problematici nella maggioranza dei venticinque Paesi Ue (si veda, in proposito, la "*Declaration on Enforcement*" approvata dal Gruppo il 25 novembre 2004);
- sulla semplificazione degli adempimenti connessi alla notificazione dei trattamenti, attraverso una *task force* incaricata di individuare gli spazi di armonizzazione (soprattutto in tema di deroghe all'obbligo di notificazione) e di elaborare un possibile modello di notificazione "unica" per i soggetti stabiliti in più Stati membri dell'Unione europea. Sulla base delle risposte pervenute ad uno specifico questionario, la *task force* ha inoltre operato una ricognizione delle disposizioni e prassi vigenti in ciascun paese riguardo all'obbligo di notificazione dei trattamenti di dati personali; ha curato altresì la predisposizione di un *vademecum* che sarà tra breve messo a disposizione di tutti i soggetti interessati (principalmente le società private che intendono operare in più di un Paese dell'Unione) mediante la pubblicazione sul sito *web* della Commissione specificamente dedicato alla protezione dei dati ed all'attività del Gruppo art. 29 (*http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm;*
- sull'armonizzazione delle previsioni in materia di informativa, in particolare attraverso l'elaborazione di un modello redatto in termini chiaramente comprensibili ed utilizzabili da tutti i titolari di trattamento, secondo un approccio "multilivello". Il Gruppo, anche sulla scorta della risoluzione adottata in materia dalla Conferenza internazionale tenutasi a Sydney nel 2003 (v. *Relazione* 2003, p. 116) e del dibattito svolto a Wroclaw, durante la Conferenza internazionale del 2004 (v. *infra*), ha elaborato un parere, pubblicato il 25 novembre 2004, che individua le caratteristiche di tale "informativa-modello".

Le decisioni assunte dal Gruppo, volte a favorire ed incrementare le forme di cooperazione al fine di pervenire a soluzioni interpretative uniformi, sono in linea di continuità rispetto a scelte compiute da diversi anni. La collaborazione internazionale fra le autorità di protezione dei dati (compreso il Garante), prevista anche dalla Convenzione n. 108 del Consiglio d'Europa, è operativa da molto tempo ed ha sistemi di scambi di informazioni sia a livello bilaterale, sia a livello multilaterale.

Oltre agli ambiti istituzionalizzati attraverso la creazione del Gruppo art. 29 ed alle Conferenze delle autorità di protezione dei dati, si segnalano brevemente alcuni significativi esempi di tale collaborazione, rimandando ai paragrafi successivi per maggiori dettagli sull'attività svolta:

- la trattazione di segnalazioni e ricorsi che hanno carattere transnazionale e lo scambio di informazioni e buone prassi sono oggetto dei seminari organizzati fin dal 2000 con cadenza semestrale nel quadro della cosiddetta "*Complaints Handling Network*", che garantisce inoltre un supporto costante alla gestione della relativa casistica;
- le questioni attinenti al settore delle telecomunicazioni sono oggetto dell'analisi condotta dall'*International Working Group on Data Protection in Telecommunications*, che si riunisce con cadenza semestrale;

- la lotta allo *spam* è oggetto della specifica cooperazione prevista dalla rete istituita fra le autorità competenti in materia di *spam* (*Contact Network of Spam Authorities*, Cnsa), che ha iniziato la sua attività alla fine del 2003.

Direttiva 2002/58/CE

Gli aspetti della direttiva che presentano maggiori difficoltà nell'armonizzazione delle modalità applicative riguardano innanzi tutto la conservazione dei dati di traffico (art. 6) ed il principio del consenso preventivo per l'invio di comunicazioni non sollecitate (art. 13).

Sul primo aspetto, come già rammentato nella *Relazione* 2003, il Gruppo art. 29 è intervenuto per ricordare agli Stati la necessità del rispetto dei tempi e dei modi previsti dalla direttiva. Nel parere 1/2003 adottato il 29 gennaio 2003, i Garanti hanno precisato che i dati memorizzati ai fini della fatturazione e dei pagamenti di interconnessione possono essere conservati soltanto per un periodo di tempo limitato e non su base routinaria per lunghi periodi, come peraltro già indicato nella Raccomandazione n. 3/99 del Gruppo.

Il Gruppo art. 29, sulla scorta dell'applicazione del principio di proporzionalità e tenendo conto che, conformemente all'art. 6, par. 2, della direttiva 2002/58/CE, i dati relativi al traffico possono essere sottoposti a trattamento *"sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento"*, ha ritenuto che i dati dovrebbero essere conservati solo per il periodo necessario a consentire il pagamento delle fatture e la composizione delle controversie. Normalmente ciò implica un periodo di memorizzazione massimo di 3-6 mesi –e non più lungo– nei casi in cui le fatture sono state pagate e non sembrano essere state oggetto di contestazione o di richieste di delucidazioni (tenuto conto del diritto alla tutela della vita privata dei singoli abbonati).

Pertanto, considerato che i diversi sistemi giuridici degli Stati membri contemplano varie disposizioni in merito all'estensione del periodo durante il quale possono essere avviate iniziative nell'ambito del diritto contrattuale, i Garanti hanno ritenuto che tali disposizioni debbano essere applicate in conformità al principio per cui il trattamento dei dati personali deve essere limitato a quanto è strettamente necessario per conseguire i fini per i quali i dati sono stati rilevati e successivamente trattati, considerato inoltre che, di regola, il pagamento dei servizi resi è effettuato entro i termini di conservazione.

Il secondo importante aspetto, cui si è già accennato, concerne l'applicazione uniforme del principio dell'*opt-in* per le comunicazioni commerciali.

La direttiva 2002/58/CE sulla vita privata e le comunicazioni elettroniche ha in particolare disciplinato, armonizzandole, le condizioni alle quali le comunicazioni elettroniche (ad esempio la posta elettronica, gli *Sms*, il fax, il telefono) possono essere utilizzate a fini di commercializzazione diretta.

A partire dalle legislazioni introdotte in alcuni Stati (tra cui l'Italia) che prevedevano in materia la necessità di un consenso esplicito dell'interessato, l'art. 13 della direttiva ha introdotto un regime generale basato sul consenso preventivo ai fini dell'invio di questo tipo di comunicazioni.

La novità e la complessità del principio hanno indotto sia le istituzioni comunitarie, sia il Gruppo art. 29 ad intervenire per evitare divergenze applicative nei diversi Stati membri.

L'urgenza di un tale intervento risiede nell'enorme recente sviluppo dell'invio di comunicazioni indesiderate (cd. *spam*) e la necessità di presentarsi nella lotta a questo fenomeno, che si manifesta ormai in tutto il mondo, con un quadro giuridico realmente armonizzato a livello europeo. Da qui i richiami del Consiglio ad una puntuale applicazione della direttiva, le linee d'azione disegnate dalla Commissione

nella sua comunicazione del 22 gennaio 2004 e la definizione di elementi per una cooperazione tra le autorità nazionali incaricate dell'attuazione dell'art. 13 (per l'Italia, il Garante) attraverso la rete *spam* Cnsa, cui si è fatto riferimento, e l'adozione di regole comuni per la trattazione di casi di *spam* transfrontaliero.

Il Consiglio dell'Unione, proprio in considerazione del grande impegno da assumere per contrastare lo *spam,* ha adottato nel mese di novembre alcune conclusioni che impegnano gli Stati ad un recepimento puntuale della direttiva 2002/58/CE ed in particolare del suo art. 13; ha richiesto poi alla Commissione di valutare se alcune disposizioni nazionali introdotte in attuazione della direttiva possano ritenersi confliggenti con l'applicazione armonizzata del principio del consenso preliminare (*opt-in*) da parte del destinatario e pertanto incidere sull'efficacia delle misure di contrasto allo *spam* transfrontaliero.

Analoga attenzione è stata posta all'intensificazione della collaborazione internazionale –in particolare, come ricordato, in sede Ocse ed *International Communication Union* (Itu)– finalizzata alla presentazione, attraverso la Commissione europea, di una posizione unitaria dei Paesi dell'Unione. Infatti, in altri Paesi la legislazione vigente si fonda sul diverso principio del cd. *opt-out* (la possibilità, cioè, per il destinatario di chiedere di non ricevere le comunicazioni commerciali) e pertanto quello che nell'Unione europea dall'entrata in vigore della direttiva 2002/58/CE (e nei singoli Paesi dalla data di trasposizione) è assoggettato a sanzione, in altri paesi può non costituire un comportamento vietato.

In questo quadro, il contributo del Gruppo art. 29 assume una notevole rilevanza. In particolare, il parere n. 5/2004 del 27 febbraio 2004 offre indicazioni su specifici elementi che riguardano le nozioni di "posta elettronica", "previo consenso" da parte degli abbonati e "commercializzazione diretta"; si prendono altresì in considerazione l'eccezione alla norma del previo consenso e il regime per le comunicazioni indirizzate alle persone giuridiche.

22.3. *Le conferenze tra autorità di protezione dei dati a livello europeo*

La Conferenza di primavera dei Garanti europei si è svolta a Rotterdam dal 21 al 23 aprile 2004 ed è stata dedicata alle politiche finalizzate a garantire l'efficacia della protezione dei dati. I temi al centro dell'incontro hanno riguardato il ruolo e l'azione di intervento delle autorità, le comunicazioni elettroniche, il rispetto delle norme sulla protezione dei dati personali e la cooperazione giudiziaria a livello europeo.

Il segretario generale dell'Autorità ha affrontato il tema delle strategie da mettere in atto per garantire l'effettiva attuazione delle norme in materia di *privacy,* non solo attraverso verifiche e controlli, ma anche mediante una costante azione di sensibilizzazione. Per quanto riguarda in particolare l'attività di verifica, soprattutto alla luce della direttiva 95/46/CE, si è altresì evidenziata l'opportunità di potenziare la collaborazione fra le autorità nazionali della protezione dei dati, anche in considerazione del carattere transnazionale delle problematiche che investono il settore della *privacy* (esempio tipico lo *spam*).

22.4. *Conferenze delle autorità su scala internazionale*

La 26ª Conferenza internazionale dei Garanti per la protezione dei dati personali, che si è tenuta a Wroclaw dal 14 al 16 settembre, è stata dedicata al binomio società della *privacy* società e della dignità.

Il Garante ha partecipato all'incontro attraverso quattro interventi nelle differenti sessioni di lavoro:

Mauro Paissan ha svolto una relazione sul delicato rapporto tra libertà di informazione e diritti della persona, evidenziando come il diritto di sapere, la libertà di comunicare e la trasparenza non possano cancellare il bisogno di intimità e il diritto di sviluppare liberamente la personalità;

Gaetano Rasi si è soffermato sugli aspetti economici della *privacy*, sottolineando come la tutela dei dati personali sia destinata a svolgere una funzione fondamentale per disegnare i futuri assetti del rapporto tra imprese e consumatori; in particolare, il trattamento –da parte delle aziende– di informazioni relative alla clientela improntato ai criteri di correttezza e trasparenza può sensibilmente migliorare la qualità del rapporto tra azienda e cliente;

Giovanni Buttarelli è intervenuto nella sessione dedicata al *marketing* politico, evidenziando gli aspetti legati alla necessità di ottenere un consenso preventivo, da parte degli interessati, all'invio di materiale propagandistico. Ciò, soprattutto perché la "pubblicità" elettorale, fondata sul trattamento di dati che riguardano identità personale e convinzioni politiche, tocca una sfera particolarmente delicata dell'individuo. Le nuove tecnologie utilizzate anche nella propaganda politica comportano la necessità di salvaguardare ancora più attentamente il diritto alla riservatezza. Ferma restando la libera circolazione delle idee e delle proposte politiche, è opportuno promuovere –anche in questo settore– un *marketing* responsabile. La proposta del segretario generale di operare in vista di una possibile risoluzione in occasione della prossima conferenze mondiale è stata condivisa.

Al Presidente Stefano Rodotà è stato affidato il compito di chiudere i lavori della Conferenza. Nella sintesi conclusiva, il prof. Rodotà ha affermato che fra i concetti di *privacy*, libertà e dignità esiste un legame sempre più stretto, in ragione del fatto che il trattamento di dati personali può determinare discriminazioni sulla base di convinzioni politiche, credenze religiose, condizioni di salute: la *privacy*, non più riconducibile al solo diritto ad essere lasciati soli, costituisce un elemento essenziale della società dell'uguaglianza. In particolare, il Presidente ha evidenziato quattro temi che –per le loro implicazioni rispetto ai valori fondanti di una società democratica e al rispetto della persona– necessitano di una riflessione approfondita: i rischi del progressivo passaggio da forme di sorveglianza mirata verso soggetti pericolosi ad una sorveglianza "generalizzata"; le trasformazioni del corpo –utilizzato come *password* attraverso i dati biometrici– determinate dall'impiego di strumenti elettronici che rendono possibile localizzare e seguire l'individuo in modo permanente; la conservazione di dati per periodi troppo lunghi che rende ciascuno "prigioniero" del proprio passato e dei controllori delle grandi banche dati; la necessità di una protezione integrale della persona anche nella dimensione elettronica. Questi temi proiettano la tutela dei dati al di là della semplice protezione della sfera privata, per farla divenire un elemento essenziale della cittadinanza del nuovo millennio.

Al termine dei lavori sono state approvate tre risoluzioni riguardanti l'aggiornamento automatico dei *software*, l'istituzione di un *forum* comune per le questioni attinenti alla cooperazione giudiziaria e di polizia e la definizione di uno standard-quadro ISO in materia di *privacy* (v. *Documentazione* par. 75).

Nella risoluzione sull'aggiornamento automatico dei *software* i Garanti hanno preso atto con preoccupazione che le società produttrici di *software* fanno sempre più ricorso a meccanismi non trasparenti che permettono una serie di operazioni: trasferire nel *computer* degli utenti, a loro insaputa, aggiornamenti di *software* per raccogliere i dati personali memorizzati; assumere il controllo, almeno parziale, del *computer* terminale limitando la capacità dell'utente, quale titolare del trattamento, di

far fronte agli obblighi ed alle responsabilità previsti dalla legge per garantire la sicurezza dei dati trattati; modificare o provocare malfunzionamenti nel *software* installato senza la possibilità di individuarne la causa. I Garanti hanno, pertanto, invitato le aziende produttrici di *software* a prevedere che le procedure per il rilascio dei dati da parte degli utenti Internet, finalizzate anche all'aggiornamento *on-line* del *software*, siano trasparenti ed associate ad un'informativa adeguata. Tale aggiornamento dovrebbe avvenire, inoltre, solo dopo aver ottenuto il consenso dell'utente, impedendo nel contempo che possano verificarsi accessi non controllati al *computer*.

La risoluzione sulla cooperazione giudiziaria e in materia di polizia chiede l'istituzione di un *forum* comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia, nell'ambito, cioè, del cosiddetto Terzo Pilastro del Trattato di Amsterdam. Tale risoluzione poggia sulla necessità, avvertita nelle diverse sedi istituzionali europee, che gli Stati membri dell'Unione europea intensifichino ulteriormente la cooperazione giudiziaria e di polizia in ambito penale per assicurare un livello elevato di sicurezza in un'area di libertà, sicurezza e giustizia, garantendo al contempo un equo bilanciamento fra l'esigenza di sicurezza e la difesa delle libertà civili, compresi i diritti di protezione dei dati, la cui tutela è sancita dalla Carta dei diritti fondamentali dell'Unione europea. Tuttavia, le autorità per la protezione dei dati personali si trovano nella situazione di non poter esercitare la loro attività consultiva in materia a causa dell'assenza di una struttura di coordinamento. I Garanti hanno pertanto invitato il Consiglio e la Commissione, da un lato ad incorporare l'attività consultiva in materia di protezione dei dati nella struttura del Consiglio dell'Unione europea, dotandola delle necessarie risorse umane ed organizzative prima della fine del 2004 e, dall'altro, a creare i presupposti giuridici per l'armonizzazione delle attività di controllo nell'ambito del Terzo Pilastro.

Con la terza risoluzione, la Conferenza ha invece raccomandato all'Organizzazione internazionale per la standardizzazione (ISO), la definizione di uno o più *standard* globali in materia di protezione dei dati e *privacy*. I Garanti hanno chiesto, in particolare, l'individuazione di uno *standard* tecnologico fondato sulle prassi di leale informazione e sui principi di parsimonia, necessità ed anonimizzazione nell'uso dei dati, tale da supportare l'attuazione di norme di legge in materia di *privacy* e protezione dei dati, se già esistenti, e la formulazione di tali norme ove esse non siano ancora definite. Lo *standard*, si legge nella risoluzione, dovrebbe poggiare sul rispetto di tre parametri. In primo luogo, offrire criteri di valutazione e verifica che facilitino il rispetto delle normative nazionali ed internazionali da parte dei titolari. In secondo luogo, indicare se le misure volte alla tutela della *privacy* impiegate da sistemi utilizzati per la gestione di dati personali siano realmente efficaci. Infine, garantire che i dati personali siano trattati sempre nel rispetto dei parametri in base ai quali sono stati inizialmente raccolti, indipendentemente dai passaggi e dal numero di soggetti che possono intervenire nella gestione e nell'interscambio di tali dati personali. La Conferenza ha, inoltre, sottoposto all'ISO le sue preoccupazioni; le medesime sono state recepite, conducendo alla sospensione delle iniziative in corso miranti alla definizione di "*standard privacy*" per le tecnologie dell'informazione, avviate senza consultare le autorità di protezione dati.

La Conferenza internazionale che, nel 2005, tornerà a riunire le autorità garanti dei diversi Paesi, avrà ad oggetto le sfide legate alla protezione dei dati personali nel mondo globalizzato.

In particolare, la discussione si concentrerà sul carattere universale del diritto alla *privacy* pur nel necessario rispetto delle diversità. Ciò, ponendosi in una linea di continuità con le riflessioni iniziate nel corso della Conferenza internazionale *"One*

world, One privacy" (Venezia, settembre 2000) che hanno portato all'adozione della "Carta di Venezia". Già in tale occasione, infatti, le autorità –alla luce del riconoscimento della *privacy* come diritto fondamentale della persona e quale elemento costitutivo della libertà del cittadino– hanno evidenziato la necessità di perseguire regole comuni universalmente condivise per la salvaguardia di tale diritto.

22.5. *La cooperazione tra autorità garanti nell'Unione europea: il Gruppo* ex *art. 29*

Nel 2004 l'attività del Gruppo *ex* art. 29 si è incentrata, come nel passato, su tematiche attinenti agli ordinari ambiti di applicazione delle direttive 95/46/CE e 2002/58/CE soffermandosi, in particolare, su iniziative che, alla luce delle esigenze rappresentate dalle autorità giudiziaria e di polizia al fine di migliorare la raccolta e lo scambio di informazioni per la lotta al terrorismo ed alla criminalità, hanno potenzialmente un grande impatto sulla tutela della riservatezza e sul diritto alla protezione dei dati personali affermato solennemente come diritto fondamentale (già dalla Carta dei diritti fondamentali e ora) dal Trattato che adotta una Costituzione per l'Europa, firmato a Roma il 29 ottobre 2004 (articoli I-51 e II-68).

Il Gruppo, proprio per tener adeguatamente conto dei cambiamenti legati, da un lato, all'allargamento dell'Unione europea con l'adesione di dieci nuovi Stati e, dall'altro, al riconoscimento del diritto alla protezione dei dati come diritto fondamentale, ha deciso di avviare una riflessione approfondita sul proprio ruolo e sulle prospettive di lavoro futuro. Si è giunti così all'adozione di un documento di ampio respiro che disegna un programma di lavoro di medio-lungo termine e si affianca al programma di lavoro del Gruppo, che ha cadenza annuale. A giudizio delle autorità europee, i due binari da percorrere sono il miglioramento dell'attuazione dei principi comunitari in materia di protezione dei dati attraverso iniziative concrete, in parte già in corso, e la definizione ed il potenziamento della cooperazione fra il Gruppo stesso e le istituzioni comunitarie (in particolare la Commissione europea, il Parlamento europeo e il Consiglio dell'Unione), oltre che con le autorità chiamate a far rispettare le regole poste a garanzia di tale diritto (il Garante europeo per la protezione dei dati e, in particolare, le autorità comuni di controllo Europol, Schengen, Dogane ed Eurojust).

Il Gruppo ha chiesto di essere pienamente informato riguardo alle iniziative in corso di predisposizione (da parte delle istituzioni comunitarie) che possono avere un impatto sulla protezione dei dati personali, in modo da poter fornire il proprio contributo di conoscenza e competenza sin dalle fasi iniziali di formazione delle proposte di azione comunitaria. Ha in parallelo considerato opportuno sollecitare un miglioramento della cooperazione delle autorità di protezione dei dati per affrontare tematiche non più limitate agli aspetti tipici del mercato interno, ma che coinvolgano altri settori e politiche comunitarie sì da richiedere un esame ed un'azione comune da parte delle diverse autorità. Quest'ultimo punto, in particolare, riveste crescente importanza alla luce del rilievo assunto dalle questioni cosiddette di Terzo Pilastro anche in rapporto al difficile contesto internazionale. Il Gruppo è infatti intervenuto prendendo posizione con sempre maggiore frequenza anche su queste tematiche (ad esempio l'obbligo per i vettori aerei di fornire i dati *Passenger Name Record* (*Pnr*) dei passeggeri dei voli transoceanici (sul quale più compiutamente si sofferma il par. 22.6), quello di conservazione dei dati concernenti comunicazioni elettroniche, pur parzialmente sottratte all'ambito comunitario, nonché di introdurre in passaporti, visti, permessi di soggiorno elementi biometrici, foto digitalizzata ovvero scannerizzata del volto, impronte digitali).

Il programma di lavoro annuale per il 2004 ha, a sua volta, concentrato molte iniziative d'azione sui temi evidenziati dalla Commissione europea nel rapporto sull'applicazione della direttiva 95/46/CE e, segnatamente, in materia di semplificazione dei requisiti delle notificazioni, armonizzazione dei requisiti in materia di informativa, semplificazione dei trasferimenti internazionali, migliore e più coordinata attuazione di alcuni principi della direttiva.

Come illustrato in dettaglio nel par. 22.6, il Gruppo ha continuato a dedicare speciale attenzione alle richieste degli Stati Uniti di ottenere da parte delle compagnie aeree i dati personali dei passeggeri in viaggio da e verso il loro territorio. Alle richieste degli Stati Uniti si sono aggiunte quelle di alcuni altri Stati, segnatamente il Canada e l'Australia.

Sono stati al riguardo adottati, in rapida successione, cinque pareri, 3 rivolti alle richieste USA (pareri 2/2004, 6/2004 ed 8/2004) e due, rispettivamente a quelle australiane e canadesi (pareri 1/2004 e 3/2004).

In tema di trasferimento dei dati personali verso Paesi terzi, si segnala altresì la decisione adottata il 28 aprile dalla Commissione europea, sulla scorta del parere espresso in precedenza dal Gruppo, in merito all'adeguatezza della protezione dei dati personali nell'Isola di Man. Nel corso del 2004 è stata effettuata, sempre da parte della Commissione, la valutazione del funzionamento delle due decisioni di adeguatezza adottate nel 2000, relative alla Svizzera ed al cd. *Safe Harbor* (concernente il trasferimento dei dati verso gli Stati Uniti).

Entrambe le valutazioni sono state fatte precedere da uno studio affidato a consulenti esterni e le relative conclusioni sono state adottate il 20 ottobre 2004. I documenti di lavoro e gli studi su cui si fondano sono stati resi pubblici.

Per quanto riguarda il particolare il funzionamento dell'accordo sul *Safe Harbor*, il documento della Commissione conclude che, a suo avviso, pur evidenziandosi talune difficoltà applicative, non vi sono ragioni per rivedere la decisione del 2000. La Commissione ritiene apprezzabile l'aumento del numero delle società che hanno aderito al *Safe Harbor*, anche se considera necessario acquisire in futuro elementi sulla loro consistenza. Lo studio al quale la Commissione ha fatto riferimento per formulare le proprie valutazioni, svolto dal Crid (Centro di ricerca su informazione e diritto) dell'Università di Namur sotto la guida del prof. Poullet, fornisce un'approfondita ed articolata valutazione del funzionamento del sistema ed evidenzia vari aspetti problematici che vanno dal ruolo, non sempre pienamente svolto, delle autorità statunitensi preposte alla verifica del rispetto dei principi da parte delle società aderenti, alla mancanza di *privacy policy* sui siti delle stesse società, con la sensazione di una scarsa conoscenza delle implicazioni che l'adesione all'accordo determina e, quindi, di una ancora più scarsa informazione degli interessati in merito alla possibilità di far valere i loro diritti di accesso, di verifica, di rettifica e cancellazione. Altro aspetto messo in luce dallo studio consiste nella possibilità che in taluni casi la legislazione adottata negli Stati Uniti a seguito degli eventi dell'11 settembre abbia introdotto obblighi di comunicazione dei dati per le società aderenti.

Un caso segnalato specificamente dallo studio riguarda anche il possibile conflitto tra le normative statunitense ed europee con riguardo all'invio delle comunicazioni commerciali (*opt-out* vs. *opt-in*).

Alla luce di queste riflessioni, il Gruppo ha deciso nella sua ultima riunione del novembre 2004 di affidare ad un gruppo ristretto l'analisi attenta delle valutazioni offerte dallo studio del Crid.

Il Gruppo ha inoltre continuato ad approfondire il lavoro sulle cd. "soluzioni contrattuali", che consentono alle imprese di trasferire dati personali nel rispetto dei principi della direttiva anche quando il Paese di destinazione non abbia una legisla-

zione adeguata, prevedendo le idonee garanzie attraverso lo strumento contrattuale.

Da un lato, anche sulla scorta di un precedente parere del Gruppo, è stato approvato dalla Commissione europea un ulteriore modello di clausole contrattuali *standard* (in *Documentazione* par. 46). Le imprese saranno libere di scegliere se utilizzare l'uno o l'altro gruppo di regole. Il modello cd. "alternativo", cui si è fatto cenno anche nella *Relazione 2003*, è stato presentato dalla Camera di commercio internazionale e da altre organizzazioni commerciali ed è stato successivamente modificato in più parti su suggerimento del Gruppo, al fine di assicurare che le clausole contrattuali tipo proposte offrano un livello di tutela paragonabile a quelle approvate in virtù della decisione della Commissione n. 497/2001/CE.

Dall'altro lato, sono proseguiti i lavori per il riconoscimento e la possibile introduzione di un diverso sistema che consenta, in particolare, il trasferimento fra società appartenenti ad uno stesso gruppo multinazionale. Questo sistema, basato su ipotizzate "norme vincolanti d'impresa" (cd. *binding corporate rules*) era stato già analizzato dal Gruppo in un documento di lavoro (WP del 3 giugno 2003) al fine di valutare in quali termini e in base a quali condizioni questi speciali "codici di condotta" possano offrire, appunto, le "garanzie sufficienti" menzionate dall'art. 26(2) della direttiva.

Le "norme vincolanti d'impresa" sarebbero infatti veri e propri codici di condotta elaborati nell'ambito di un gruppo di imprese e validi per tutte le società che di tale gruppo fanno parte.

Basandosi sull'esperienza maturata in alcuni Stati membri e sugli approfondimenti scaturiti nel corso di un seminario internazionale svoltosi a l'Aja, il Gruppo ha recentemente adottato un documento in cui si individuano gli elementi essenziali per presentare ad una autorità di protezione dei dati la richiesta di autorizzazione (*model checklist*). Giova ricordare che, a differenza delle clausole contrattuali, sulla base delle disposizioni della direttiva la Commissione europea non è competente ad adottare una decisione vincolante in materia ed i singoli Stati (più precisamente le autorità nazionali di protezione dei dati) restano liberi di rendere o meno operanti le "norme vincolanti d'impresa" sul proprio territorio.

Dopo l'adozione di uno specifico documento di lavoro sull'uso dei sistemi biometrici (WP 80 del 1° agosto 2003), il Gruppo ha adottato l'11 agosto 2004 un parere sull'inclusione di elementi biometrici nei visti e permessi di soggiorno, che esprime dubbi sulla proporzionalità delle misure proposte rispetto alle finalità individuate dai proponenti e forti preoccupazioni in relazione al quadro più ampio in cui la proposta si colloca.

Come già evidenziato, infatti, occorre guardare in modo unitario ad una congerie di proposte formulate da Consiglio e/o Commissione, che prevedono un crescente impiego della biometria (impronte digitali e scannerizzazione del volto in particolare) rendendone obbligatorio l'inserimento nei documenti rilasciati a stranieri e cittadini (passaporti, carte d'identità, visti, permessi di soggiorno), prevedendo la creazione a livello europeo di grandi basi di dati in cui anche questi elementi vengono inseriti (Sis II, Sistema informazione visti-Vis) ed intensificando la possibilità di scambiare queste informazioni con una pluralità di Stati ed organismi esteri (in proposito si veda in allegato, anche il Regolamento (CE) n. 2252/2004 del Consiglio sulle caratteristiche di sicurezza e gli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri).

Il Gruppo, nel suo parere, ricorda che tali proposte hanno un forte impatto sui diritti umani fondamentali ed in particolare sul diritto alla protezione dei dati personali; pertanto, richiama l'attenzione sulla necessità di esserne preliminarmente informato e che le stesse proposte siano adeguatamente rese pubbliche nei confronti

dei Parlamenti e della società civile e che ai relativi lavori sia data trasparenza, anche attraverso il coinvolgimento delle autorità di protezione dei dati. Nel parere, infatti, il Gruppo ricorda l'obbligo di rispettare in particolare il principio di proporzionalità e la necessità di definire con chiarezza le finalità del trattamento dei dati biometrici. Il parere individua anche le cautele da adottare al fine di rendere "affidabile" il trattamento di tali dati e richiede precise garanzie in ordine allo stesso; chiede inoltre di ricevere informazioni approfondite sulla sicurezza del sistema scelto e sulle modalità di incorporazione dei dati nel *chip*.

Esprime infine forti preoccupazioni riguardo alla previsione della possibile creazione di un *database* centralizzato a livello europeo e ricorda che il ruolo delle autorità di supervisione deve essere mantenuto adeguato alle novità che si vogliono introdurre per evitare un abbassamento del livello di tutela.

Come già segnalato nella *Relazione* 2003, il Gruppo ha adottato il parere 4/2004 (WP 89 del 11 febbraio 2004) sul trattamento dei dati effettuato attraverso la videosorveglianza, che individua regole e garanzie precise sull'installazione di telecamere fornendo un quadro uniforme e armonizzato in materia a livello europeo. Il parere contiene un "decalogo" sulle cautele ed i principi da osservare, principi che si applicano anche ai trattamenti non soggetti espressamente alle disposizioni della direttiva europea (ad esempio, trattamenti effettuati per scopi di sicurezza pubblica o per il perseguimento di reati, oppure trattamenti effettuati da una persona fisica per scopi esclusivamente privati o familiari).

È stato altresì adottato un parere in tema di comunicazioni commerciali non richieste (parere 5/2004 WP 90 del 27 febbraio 2004), al fine di fornire una interpretazione comune dell'art. 13 della direttiva 2002/58/CE riguardo ad alcuni aspetti che potrebbero dare luogo a soluzioni divergenti in sede di recepimento o di applicazione della normativa nei diversi Stati membri.

Altro importante parere del Gruppo (parere 9/2004 del 9 novembre 2004) riguarda una proposta legislativa presentata da quattro Stati dell'Unione il 28 aprile 2004 (Doc. 8958) tendente ad imporre ai fornitori di servizi di comunicazione elettronica l'obbligo di conservazione dei dati di traffico trattati ai fini della fornitura del servizio o comunque disponibili.

La proposta, in discussione presso il Consiglio dell'Unione, nella sua forma attuale prevede la conservazione preventiva in maniera indiscriminata, per un periodo di tempo limitato solo nel minimo, di tutti i dati di traffico (telefonico, Internet, comprensivo della posta elettronica).

I Garanti hanno ritenuto tale proposta in contrasto con i principi fondamentali in materia di protezione dei dati e con la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Il Gruppo ha richiamato i precedenti pareri espressi, ha rinnovato la richiesta che sia previamente valutato, come previsto dalla stessa Convenzione, se l'ipotizzata interferenza nella vita privata abbia un'adeguata base giuridica e se risponda a criteri di necessità nel quadro di una società democratica, rammentando la necessità del rispetto dei principi in materia di protezione dei dati –in particolare dei principi di proporzionalità, pertinenza, finalità– per la conservazione dei dati di traffico anche per finalità giudiziarie e di polizia (v. art. 15 della direttiva 2002/58/CE).

Si segnala anche un primo documento di lavoro adottato dal Gruppo (WP 86 del 23 gennaio 2004) sui dispositivi proposti dal consorzio *Trusted Computing Group* per incentivare la sicurezza delle transazioni elettroniche attraverso strumenti non solo *software,* ma anche *hardware* e, soprattutto, il documento di lavoro adottato il 17 marzo 2004 (WP 91) sul trattamento dei dati genetici.

Nel documento di lavoro, come già rappresentato nella *Relazione 2003*, il

Gruppo ha preferito affrontare il progresso tecnologico nel campo della genetica e le sue ripercussioni nella sfera della riservatezza scegliendo un approccio analitico volto ad individuare i settori in cui maggiori sono le preoccupazioni in relazione al trattamento dei dati genetici.

22.6. *Il trasferimento dei dati* Pnr *dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea*

Uno dei temi più delicati e controversi a livello europeo ed internazionale resta il trasferimento dei dati *Pnr* dei passeggeri alle autorità doganali di Paesi non appartenenti all'Unione europea (v. già la *Relazione 2003*). Infatti, come sottolineato anche da un recente intervento del commissario europeo Frattini, la richiesta da parte delle autorità pubbliche di Paesi terzi di ottenere dalle compagnie aeree europee i dati dei passeggeri ai fini di prevenzione del crimine non solo deve essere valutata alla luce del rispetto del diritto fondamentale alla protezione dei dati personali, ma è collegata anche alla delicata questione della protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia nell'Unione europea (cd. Terzo Pilastro), che risulta tuttora frammentaria e non armonizzata.

Il Gruppo ha dedicato grande attenzione al tema, occupandosi non solo del sistema proposto dalle autorità statunitensi, su cui si era già espresso nel corso del 2002 e del 2003, ma anche dalle analoghe richieste provenienti dall'Australia e dal Canada, nella convinzione che i comuni obiettivi di lotta al terrorismo debbano essere perseguiti nel rispetto dei diritti fondamentali ed in particolare del diritto alla protezione dei dati personali.

Per quanto riguarda gli Stati Uniti, il Gruppo è tornato ad evidenziare, nel parere 2/2004, le lacune del sistema statunitense, proponendo una serie di miglioramenti atti a garantire che il trasferimento dei dati dei passeggeri avvenga nel rispetto dei principi stabiliti dalla normativa europea in materia di protezione dati. Fra questi, il Gruppo ha segnalato, in particolare, il principio di finalità, in base al quale i dati del *Pnr* dovrebbero essere utilizzati soltanto per contrastare il terrorismo ed altri specifici reati ad esso connessi; il principio di proporzionalità nei dati richiesti, evitando il trasferimento di dati superflui; la conservazione dei dati per un periodo limitato; il divieto di trattare dati sensibili; il diritto dei passeggeri ad essere adeguatamente informati e ad essere messi in condizione di esercitare agevolmente i propri diritti (accesso, rettifica). Inoltre, il Gruppo ha chiesto che le garanzie per i passeggeri non si basino meramente su impegni unilaterali privi di vincolatività giuridica per la controparte americana e tali da non creare diritti che i terzi (in questo caso i cittadini europei) possano far valere negli Usa in caso di controversie.

Anche il Parlamento europeo, condividendo molte delle critiche espresse dal Gruppo, nel marzo 2004 ha approvato due risoluzioni con cui, sottolineando gli insoddisfacenti risultati del negoziato tra autorità statunitensi e Commissione europea, invitava quest'ultima ad ottenere garanzie reali affinché fosse rispettato il diritto alla protezione dei dati personali dei cittadini europei, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Ue.

La Commissione ha però deciso di procedere con la propria iniziativa contenuta nel "pacchetto *Pnr*", adottando una decisione relativa all'adeguatezza della protezione accordata dagli Stati Uniti ai dati personali dei passeggeri aerei, fondata su impegni unilaterali (cd. "*undertakings*") delle autorità statunitensi. A tale iniziativa ha fatto seguito l'approvazione di un accordo internazionale da parte del Consiglio dei ministri dell'Ue,

con cui si impone alle compagnie aeree europee di consentire alle autorità doganali statunitensi l'accesso diretto ai dati contenuti nei propri sistemi di prenotazione (cfr. al riguardo i documenti riprodotti nei par. 43-45 in *Documentazione*).

Entrambi gli atti sono stati approvati a maggio 2004, nonostante le preoccupazioni espresse dal Gruppo art. 29 e la richiesta del Parlamento europeo, presentata ad aprile alla Corte di giustizia delle Comunità europee, di un parere preliminare sulla compatibilità con l'ordinamento comunitario del proposto accordo internazionale.

Ai sensi del "pacchetto *Pnr*", le autorità doganali statunitensi sono autorizzate ad accedere direttamente ad un novero molto ampio di dati (34 elementi, fra cui indirizzi, numeri di telefono, indirizzi di posta elettronica, numeri di carte di credito, informazioni contenute nei programmi "*frequent flyer*") e a conservare per almeno tre anni e mezzo le informazioni relative ai dati di tutti i passeggeri (al contrario del sistema australiano, approvato dai Garanti europei, in cui i dati vengono conservati solo in presenza di un reato o di una indagine per un presunto reato). I dati possono essere trattati per finalità che esorbitano dalla lotta al terrorismo ed essere ulteriormente trasmessi ad altre autorità, anche di Paesi terzi.

Allo stato, sono accessibili dati "neutri" e sensibili; con riguardo a questi ultimi, gli *undertakings* prevedono specifici impegni da parte delle autorità statunitensi a non farne uso. In futuro, i dati sensibili (riguardanti la salute, le convinzioni religiose o politiche, ecc.) non saranno più accessibili grazie ad un apposito sistema di filtraggio.

Infine, i diritti dei passeggeri europei ad essere informati, ad accedere ai propri dati ed eventualmente a rettificarli non sono sembrati adeguatamente garantiti: fra l'altro, sia per l'assenza di un organo di ricorso veramente indipendente, sia per la dubbia vincolatività giuridica degli impegni assunti dalle autorità statunitensi.

Pertanto, il Parlamento europeo ha deciso di presentare un ricorso alla Corte di giustizia delle Comunità europee (che si aggiunge a quello, decaduto a seguito della firma dell'accordo, presentato in sede pregiudiziale e del quale si è fatto cenno nella *Relazione 2003*) per far annullare la decisione della Commissione e l'accordo internazionale. Secondo il Parlamento europeo, non soltanto la soluzione raggiunta non tutelerebbe adeguatamente i diritti dei passeggeri, ma la stessa Commissione avrebbe oltrepassato le proprie competenze e non avrebbe assicurato la dovuta partecipazione del Parlamento al processo decisionale.

Tale ricorso è stato condiviso nel merito anche dal Garante europeo della protezione dati (la cui attività è iniziata di recente), il quale ha presentato nel novembre scorso alla Corte di giustizia una richiesta di intervento a sostegno delle posizioni del Parlamento europeo.

Nelle more della pronuncia della Corte, il Gruppo art. 29 si è adoperato per tutelare il più possibile i diritti dei passeggeri. Nel giugno 2004 è stato approvato il parere 6/2004 in cui, in relazione all'attuazione da parte delle compagnie aeree del "pacchetto *Pnr*", si è auspicato un rapido passaggio dal meccanismo che consente alle autorità statunitensi di accedere direttamente ai sistemi di prenotazione (cd. sistema *"pull"*) ad un meccanismo in cui siano le stesse compagnie aeree a filtrare i dati ed inviarli (sistema *"push"*), nonché a fornire l'informazione completa e chiara ai passeggeri.

Per approfondire tali temi, il Garante ha ospitato a Roma un incontro fra le autorità di protezione dati europee e i rappresentanti delle compagnie aeree. In seguito a questo incontro, il Gruppo art. 29 ha approvato il parere 8/2004, in cui si propongono modelli di informativa da fornirsi ai passeggeri dei voli transatlantici da parte delle compagnie aeree, degli agenti di viaggio e dei sistemi di prenotazione via *computer* facenti parte del circuito di prenotazione dei voli.

Come già detto, il sistema statunitense è solo il primo di una serie di analoghe e

sempre più numerose iniziative che hanno finora interessato Canada, Australia, Sudafrica e Corea del Sud.

Il Gruppo, pur nella convinzione che una soluzione multilaterale sia preferibile e più aderente al principio di non discriminazione, ha esaminato nel corso del 2004 le richieste dell'Australia e del Canada.

Il sistema australiano prevede il trasferimento di un numero più limitato di dati personali che sono raccolti per finalità di lotta al terrorismo e reati connessi e sono conservati solo in casi specifici. Inoltre, i diritti dei passeggeri sono garantiti a livello sia normativo, sia istituzionale. Per queste ragioni, il Gruppo ha espresso un parere sostanzialmente favorevole (parere 1/2004 del 16 gennaio 2004) ad una dichiarazione di adeguatezza da parte della Commissione dopo che saranno chiariti e risolti alcuni aspetti controversi.

Per quanto riguarda il Canada, il parere 3/2004 dell'11 febbraio 2004 ha evidenziato una serie di problemi che dovranno essere risolti prima che si possa dare avvio al trasferimento di dati.

Bisogna, infine, sottolineare come la dimensione internazionale della questione del trasferimento dei dati dei passeggeri abbia spinto diverse organizzazioni internazionali, quali l'Ocse e l'Icao, ad occuparsi del tema al fine di trovare adeguate soluzioni multilaterali (v. *infra*).

22.7. *Cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Nel 2004 si è evidenziata la tendenza ad un ulteriore incremento delle iniziative legislative adottate a livello comunitario per rafforzare la cooperazione tra le autorità nazionali di polizia e giudiziarie. Tali iniziative, come si è visto, spesso implicano lo scambio di informazioni personali e, talvolta, la creazione di nuove basi di dati europee ovvero l'ampliamento della possibilità di accesso ai dati dei sistemi di informazione esistenti a soggetti nuovi rispetto a quelli previsti nelle convenzioni istitutive.

È necessario che queste attività rispettino al contempo le esigenze richieste da un'effettiva cooperazione tra forze di polizia e autorità giudiziarie e il diritto fondamentale alla tutela dei dati personali (solennemente introdotto dalla Carta dei diritti fondamentali e dal Trattato per una Costituzione europea) e si svolgano quindi nei limiti consentiti dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Attualmente, le iniziative dell'Ue che comportano la raccolta, la conservazione o lo scambio di dati personali ai fini dell'applicazione della legge sono numerose: tra gli esempi più significativi vi sono misure per consentire lo scambio di informazioni e la cooperazione rispetto ai reati terroristici, la semplificazione dello scambio di informazioni e di "*intelligence*" tra i servizi repressivi degli Stati, l'accesso ai dati ed agli archivi da parte degli organi giudiziari e le forze di polizia, lo scambio di dati sui passeggeri di voli aerei, nonché proposte per richiedere la conservazione dei dati delle comunicazioni. Vi sono poi, come ricordato, le diverse proposte volte ad introdurre elementi biometrici nei documenti rilasciati dagli Stati Ue a cittadini e stranieri, con la previsione di larghe basi di dati a livello europeo che si aggiungerebbero a quelle già esistenti, moltiplicando i rischi e gli effetti di un erroneo inserimento di dati o di accessi non autorizzati.

Questi ed altri sviluppi, quali il suggerimento di trasformare in futuro l'Europol in un'agenzia investigativa, possono avere rilevanti implicazioni anche per i diritti degli individui.

Per il modo della loro elaborazione e per la frammentarietà delle competenze in materia in seno all'Unione, molte delle nuove iniziative dell'Unione europea che riguardano dati personali sono al momento sottratte al controllo delle autorità di protezione dei dati poiché non rientrano in modo netto in uno dei tradizionali pilastri dell'Ue. Nonostante i ripetuti inviti del Parlamento europeo, queste attività hanno continuato ad essere svolte solo in gruppi di lavoro a composizione specializzata, senza il coinvolgimento adeguato delle istituzioni e degli organismi che a livello nazionale e comunitario hanno responsabilità in materia –con la conseguenza che spesso possono sfuggire sia alla tempestiva valutazione del Gruppo articolo 29, sia all'esame delle autorità di controllo esistenti nel cd. Terzo Pilastro (Schengen, Europol, Dogane)– senza, peraltro, un'adeguata base giuridica fondata sull'elaborazione di principi di protezione dei dati validi per i trattamenti proposti.

Già da tempo le autorità di protezione dei dati avevano segnalato il progressivo venir meno di "momenti istituzionalizzati" che favorissero la necessaria valutazione dell'impatto che tali misure erano destinate a produrre sui diritti fondamentali della persona e, più specificamente, sulla tutela dei dati personali. Infatti, i gruppi di lavoro il cui mandato specifico nel Consiglio dell'Ue era la protezione dati, rispettivamente nel Primo e Terzo Pilastro, sono stati soppressi fin dal 2002 e solo nei primi mesi del 2004 il Garante europeo per la protezione dei dati ha iniziato la sua attività, peraltro limitata ai trattamenti effettuati dalle istituzioni comunitarie "nei settori di competenza del diritto comunitario".

Considerato che i pilastri dell'Ue con l'adozione del Trattato firmato a Roma il 29 ottobre 2004 sono destinati a convergere e la protezione dei dati personali ha assunto il rango di diritto fondamentale, in occasione della Conferenza delle autorità incaricate della protezione dei dati svoltasi a Rotterdam nel 2004, è stato deciso che i rappresentanti delle autorità che operano a livello comunitario si riuniscano per coordinare la loro attività e cercare di svolgere un ruolo adeguato ai bisogni rappresentati.

Alla prima riunione di questo gruppo "di pianificazione", che ha avuto luogo nel giugno 2004, hanno partecipato il Garante europeo della protezione dei dati, i presidenti delle autorità di controllo comune e la presidenza del Gruppo art. 29.

La situazione si è evoluta nel settembre 2004 in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati a Wroclaw, quando una sessione a porte chiuse delle autorità europee ha approvato una risoluzione in cui si chiede che le istituzioni dell'Ue promuovano un *forum* nel quale le autorità europee incaricate della protezione dei dati possano discutere le implicazioni a livello di protezione dei dati degli sviluppi del Terzo Pilastro. Fino alla creazione di tale *forum*, le iniziative del Terzo Pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune, saranno esaminate da un gruppo di lavoro delle autorità europee incaricate della protezione dei dati.

Le autorità di controllo hanno pertanto deciso, avvalendosi della struttura di segreteria comune prevista per assistere i lavori delle autorità Schengen, Europol e Dogane, di prevedere alcune riunioni congiunte, invitando anche il Garante europeo per la protezione dei dati e l'autorità di controllo istituita per Eurojust, ove informarsi e discutere, al momento informalmente, delle iniziative esistenti ed eventualmente definire proposte unitarie da presentare agli organismi competenti, avvalendosi anche delle aperture che sembrano presenti nel nuovo programma per il rafforzamento dell'area di libertà, sicurezza e giustizia per il periodo 2005-2009.

Un canale particolare di dialogo si è aperto con la *House of Lords*, il cui sottocomitato specializzato ha richiesto un parere sulla protezione dei dati nel Terzo Pilastro, ed è stato rafforzato il legame esistente con il Parlamento europeo, Commissione libertà e diritti dei cittadini, che ha voluto incontrare più volte i rap-

presentanti delle autorità in previsione della discussione di alcune delle iniziative menzionate. Va ricordato in proposito che a partire dal 1° gennaio 2005 il Parlamento ha acquisito il diritto alla codecisione in materie quali le politiche di visti, asilo, immigrazione e le altre politiche connesse alla realizzazione del principio della libera circolazione delle persone e sarà quindi necessario il suo accordo per la loro adozione.

Ma certamente la novità più positiva in materia è legata alla nomina del nuovo Commissario italiano come vice presidente e responsabile del settore Libertà, sicurezza e giustizia. Fin dalla presentazione del suo programma davanti al Parlamento europeo il Commissario Frattini ha infatti chiarito che intende far garantire il pieno rispetto del diritto alla protezione dei dati personali e favorire il dialogo con le autorità di protezione dei dati per le materie affidate alla sua competenza.

A rafforzamento di questo impegno il Commissario ha incontrato le autorità di controllo comuni nella loro riunione congiunta del 21 dicembre pronunciando un apprezzabile discorso disponibile in rete che contiene precise linee di azione ed impegni in materia e che dovrebbe servire da guida anche per i successivi interventi dei rappresentanti della Commissione.

22.8. *L'attività del Garante nell'Autorità di controllo comune Schengen*

Il Garante è autorità nazionale di controllo per l'Italia con il compito di esercitare un controllo indipendente dell'archivio della sezione nazionale del Sistema d'informazione Schengen (Sis) e 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 entra a comporre l'Autorità di controllo comune (Acc).

Fra le attività di maggior rilievo dell'Acc, alle cui riunioni il Garante ha partecipato attivamente 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 (e 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.

L'attività dell'Acc continua ad essere di particolare rilievo e, al riguardo, va notata la crescente attenzione prestata dal Consiglio dell'Unione europea ai pareri dalla stessa espressi, come ad esempio mostra la recente Decisione relativa alla "lotta contro la criminalità connessa con veicoli". Il testo approvato ha recepito largamente le osservazioni critiche formulate dall'Acc rispetto alla proposta iniziale e non prevede più di allargare l'accesso diretto al Sis a soggetti diversi da quelli già autorizzati, limitandosi a richiedere da parte delle autorità competenti il tempestivo inserimento nel sistema di una segnalazione ogniqualvolta vengano denunciati furti di veicoli o di carte di circolazione e l'informazione degli uffici nazionali della motorizzazione.

Nel corso del 2004 gran parte dell'attività dell'Acc ha continuato ad essere concentrata sui problemi legati allo sviluppo del Sistema informativo Schengen, il cd. Sis II.

In estrema sintesi, vi sono due aspetti che preoccupano fortemente l'Acc, il primo concernente le informazioni che il Sis deve contenere (anche a fronte delle diverse proposte per introdurre nuove categorie di informazioni e nuovi tipi di dati); l'altro,

in merito all'accesso al Sis e all'uso dei dati nel sistema. Con queste proposte, peraltro frutto e sintomo di un approccio normativo frammentario, si tende ad trasformare il Sis in un sistema di indagine e non più solo di informazione, mutandone quindi radicalmente le finalità rispetto a quelle definite dalla Convenzione del 1990.

L'Autorità ha ricordato nel parere adottato il 19 maggio che l'ampliamento delle categorie di informazioni registrabili nel sistema, il possibile inserimento di dati biometrici, la modifica di alcuni meccanismi di accesso e utilizzazione dei dati proposti a livello tecnico, possono essere praticati, ma devono essere fondati su un'appropriata base giuridica. L'Acc ha rimarcato l'assenza di tale base ed ha ricordato il necessario rispetto del testo attuale della Convenzione, la quale individua esattamente le categorie di dati inseribili e le autorità che possono accedere ai dati, fissandone i limiti. Anche i compiti delle autorità di supervisione e controllo sono disegnati in relazione alle attuali funzionalità del sistema.

Qualunque cambiamento, inclusi quelli definiti con il recente regolamento del Consiglio del 29 aprile 2004 (v. *Documentazione* par. 49), deve essere considerato ed "equilibrato" rispetto al disegno dell'intero sistema. L'Acc ha chiesto pertanto che le proposte siano previamente e adeguatamente discusse considerando anche quale sarebbe il loro impatto sui diritti fondamentali della persona e sul rispetto dei principi in materia di protezione dei dati, in particolare il principio di proporzionalità delle modifiche richieste. In questa valutazione, deve essere anche considerato il rischio che il Sis, incorporando nuove funzioni e nuove categorie di dati, possa duplicare inutilmente sistemi di informazioni già esistenti in seno all'Unione. L'Acc si è dichiarata disponibile ad assistere con la sua competenza le istituzioni comunitarie ed ha comunque richiesto una puntuale informazione sui lavori in corso, per poter essere in grado di formulare indicazioni in tempo utile rispetto all'adozione degli atti.

I timori dell'Acc si fondano sull'osservazione del modo in cui i lavori per il Sis II vengono portati avanti. Sarebbe infatti logico far precedere lo sviluppo tecnico del sistema sia da decisioni politiche che ne fissino le finalità e le relative modalità di funzionamento, sia dalla definizione di un idoneo quadro giuridico che modifichi le disposizioni attualmente vigenti specificando le finalità del sistema e stabilendo le norme necessarie per definire le modalità di accesso e gli altri elementi essenziali. Invece, in mancanza di decisioni appropriate, le proposte formulate dalla Commissione cercano di costruire un sistema basato sulla massima flessibilità tecnica, prevedendo il maggior numero di funzioni e di accessi. *"Pertanto"*, si legge nel parere dell'Acc, *"la messa a punto del sistema avviene sotto l'impulso delle mutevoli istanze provenienti dal settore giustizia e affari interni dell'Ue, anziché sulla base di obiettivi espressi e definiti all'interno di un quadro giuridico preciso"*.

Preoccupazioni analoghe sono state rappresentate anche dal Parlamento europeo che si è dimostrato molto sensibile alle sollecitazioni provenienti dalle autorità di protezione dei dati personali.

L'Acc ha inoltre proseguito l'attività di verifica sulle modalità dell'inserimento nel Sis delle segnalazioni di stranieri al fine di non ammetterli sul territorio Schengen, per valutare se vi siano discrepanze fra gli Stati Parte nell'applicazione e/o nell'interpretazione dell'art. 96 della Convenzione. Nel corso dell'anno, le autorità nazionali di controllo hanno richiesto, sulla base di un modulo appositamente predisposto, specifiche informazioni sulle procedure seguite dagli uffici che sono abilitati ad inserire i dati nel sistema (per l'Italia: oltre ad alcuni uffici centrali del Ministero dell'interno, le questure) e hanno svolto colloqui che hanno interessato anche il Sis nazionale (N-Sis) ed il Sirene.

Di queste attività, che sono state svolte in maniera coordinata in tutti gli Stati

Schengen, è stata data ampia informazione all'Acc la quale predisporrà un documento riassuntivo e, ove necessario, linee-guida. Una seconda parte dell'indagine, consistente in una ispezione agli archivi per verificare in concreto la correttezza degli inserimenti ed il rispetto delle regole in materia di trattamento e conservazione dei dati, sarà svolta, sempre con modalità coordinate, nei primi mesi del 2005.

A completamento di quanto detto, si può segnalare, anche se non direttamente legata all'attività dell'Acc, la visita di valutazione che gli esperti del Consiglio dell'Unione europea hanno svolto in Italia nel mese di settembre 2004 per gli aspetti relativi alla protezione dei dati. Di essa si è già reso conto nel par. 6.3; è opportuno evidenziare qui le preoccupazioni manifestate dagli esperti per l'alto numero di segnalazioni inserite ai sensi dell'art. 96 con il conseguente invito a verificarne la qualità.

22.9. *Europol: l'attività dell'Autorità di controllo comune e i casi di contenzioso*

L'Autorità comune di controllo ha presentato il 23 novembre scorso la seconda relazione di attività che copre il biennio da novembre 2002 ad ottobre 2004 (v. *Documentazione* par. 54).

Nella relazione, l'Acc ha ricordato come, in un periodo fortemente caratterizzato dalle misure adottate per combattere il terrorismo dopo i tragici eventi dell'11 settembre 2001 negli Stati Uniti e, recentemente, dagli attentati di Madrid nel marzo 2004, l'Autorità stessa nei suoi pareri e nelle iniziative attuate abbia dimostrato che è possibile, e per nulla incompatibile, sostenere l'obiettivo comune della lotta al terrorismo internazionale e alla criminalità organizzata, salvaguardando nel contempo i diritti dei singoli.

L'Acc ha anche evidenziato che risulta sempre più evidente che il campo della cooperazione di polizia e giudiziaria necessita di norme chiare e specifiche sulla protezione dei dati, con la formulazione di un parere indipendente e di un'attività di controllo armonica.

Relativamente all'attività svolta nel corso del 2004, si segnala in particolare la vigilanza sulle modalità di applicazione dell'accordo Europol-Stati Uniti per la trasmissione di dati personali.

Secondo i dati acquisiti dall'Acc lo scambio della maggior parte delle informazioni tra l'Ue e le autorità di polizia statunitensi sembrerebbe essere avvenuto in base ad accordi bilaterali esistenti tra gli Stati Uniti e singoli Stati membri. L'Autorità, tuttavia, ritenendo che il volume di informazioni scambiate tra Europol e Stati Uniti aumenterà, ha deliberato di concentrare le ispezioni future dell'Europol sull'esame dei dati di natura personale trasmessi nell'ambito dell'accordo, per assicurare che vi sia conformità alle disposizioni pertinenti. Inoltre, l'Acc cercherà di coordinare l'attività di vigilanza, collaborando con le autorità nazionali incaricate della protezione dei dati personali negli Stati membri e con il *Chief Privacy Officer* presso il Dipartimento della sicurezza interna negli Stati Uniti.

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.

Nel marzo 2004 è stata effettuata una nuova ispezione, incentrata sulla qualità dei dati trattati negli archivi per fini di analisi. Come risultato, il *team* d'ispezione ha riscontrato che, nel complesso, la qualità dei dati è soddisfacente, almeno per

quanto riguarda la rispondenza dei dati negli archivi con quelli forniti dagli Stati membri. Tuttavia, è stata confermata la percezione di un'incapacità generale da parte degli Stati membri di valutare correttamente i dati trasmessi ad Europol (verificando la fonte, l'affidabilità e così via). L'Acc ha sottolineato che, per risolvere questo problema, occorre migliorare la cooperazione tra Stati Membri ed Europol.

Altro tema rilevante riguarda le squadre investigative comuni: l'Acc sta attualmente valutando la portata del sostegno in materia di analisi fornito dall'Europol.

Una decisione del Consiglio ha introdotto regole comuni per queste squadre ed ha previsto la possibilità che le stesse includano "funzionari di organismi costituiti ai sensi del Trattato sull'Unione europea": una definizione che interessa dunque anche il personale dell'Europol. I particolari riguardanti la partecipazione di questo organismo a squadre investigative comuni sono stati definiti in un successivo Protocollo ai sensi del quale il suo personale parteciperebbe solamente con "funzioni di supporto". Tuttavia, sempre in base al Protocollo, gli agenti dell'Europol verrebbero comunque inseriti nella catena di comando e le informazioni detenute negli archivi sarebbero condivise con i componenti della squadra; inoltre, le informazioni da questa raccolte sarebbero a loro volta inserite nelle banche dati dell'Europol.

L'Acc ha chiesto all'Europol di essere informata in merito alle decisioni riguardanti il tipo di sostegno che sarebbe offerto alle squadre investigative comuni. Ed in particolare sul modo in cui l'organismo intende utilizzare i suoi servizi di analisi ed ha intenzione di vigilare per assicurare il rispetto della Convenzione.

L'attività del comitato ricorsi

Nel 2004 l'Europol (in base a dati dallo stesso forniti) ha ricevuto circa dieci richieste di accesso (un dato relativamente stabile negli ultimi due anni) mentre risultano in aumento i casi di contenzioso.

Nell'ultimo anno il comitato ha deciso in merito a due ricorsi e attualmente vi sono parecchi casi su cui deve ancora esprimersi.

I casi affrontati hanno portato a decisioni relative a importanti questioni di principio. In particolare, è stato affermato che l'Europol deve considerare nel merito ogni richiesta di accesso, anziché applicare un approccio generale e che deve rispondere ad ogni richiesta nella lingua in cui la stessa è formulata, purché sia una delle lingue ufficiali dell'Unione europea.

22.10. *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) per facilitare la prevenzione, ricerca e repressione delle infrazioni sia delle norme comunitarie, sia delle leggi nazionali, attraverso lo scambio di dati ed informazioni fornite dai servizi doganali di ciascuno Stato membro.

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.

Nel corso del 2004 l'Autorità si è riunita due volte ed in particolare nella seconda riunione, svoltasi nel mese di dicembre, sono stati affrontati aspetti cruciali per la sua configurazione ed attività.

In primo luogo è emerso un delicato problema di funzionalità dell'Acc: infatti, pur essendo state approvate le linee guida per svolgere la prima ispezione al Sid e costituito il *team* di esperti per effettuarla, la stessa non ha potuto svolgersi per mancanza di disponibilità finanziaria. Le attuali disposizioni di *budget* del Consiglio consentono il rimborso –tra l'altro non all'Autorità nazionale che sostiene le spese, ma al Governo– delle sole spese di viaggio di un componente in occasione delle riunioni dell'Acc e non ci sono stanziamenti per consentire le altre attività, pur previste dalla Convenzione. L'attività di ispezione dovrebbe quindi svolgersi ad intero carico delle autorità che compongono il *team* di esperti.

Ne è scaturita una riflessione tra i componenti i quali hanno lamentato che la situazione creatasi incide gravemente sulla funzionalità dell'Autorità e lede il presupposto stesso della sua esistenza, quello, cioè, di sorvegliare sul funzionamento del Sid anche attraverso l'accesso allo stesso (v. art. 18 della Convenzione). È stato chiesto al Presidente di rappresentare nei modi più appropriati tale doglianza.

Altro punto importante riguarda l'ancora scarsa utilizzazione del sistema da parte delle autorità doganali. Per approfondire gli aspetti che rendono problematico l'utilizzo del sistema, nella riunione di dicembre sono stati invitati rappresentanti dell'Olaf e del Gruppo di cooperazione doganale del Consiglio.

Ne è emerso un quadro complesso, legato anche alla presenza contestuale di numerose basi di dati nel settore: i rappresentanti delle istituzioni comunitarie hanno però confermato la volontà di far sì che il Sid sia posto al centro della cooperazione doganale e di prevederne addirittura il potenziamento, al fine di metterlo in grado di svolgere attività di analisi dei rischi. L'Autorità, su questo punto, ha ricordato la necessità del pieno rispetto della Convenzione ed ha auspicato un analogo potenziamento del suo ruolo, dichiarandosi disponibile a fornire ogni contributo ai futuri lavori.

22.11. *La partecipazione ad altri comitati e gruppi di lavoro*

IWGDPT

Il Garante ha partecipato ai due incontri dell'*International Working Group on Data Protection in Telecommunications* (IWGDPT) che si sono svolti in Argentina (Buenos Aires, 14-15 aprile 2004) e in Germania (Berlino, 18-19 novembre 2004).

Il primo incontro ha preso in esame in particolare i problemi connessi alla libertà di espressione nel mondo *on-line*, ai nuovi servizi di comunicazione (*wireless, Mms*) e agli effetti che essi producono sulla *privacy*, nonché alle problematiche concernenti le tecnologie *Rfid*. Su questi temi i delegati hanno adottato tre documenti che richiamano l'esigenza di garantire il rispetto dei principi di protezione dati, anche attraverso un'adeguata informativa del pubblico, la disponibilità di strumenti che consentano agli interessati l'esercizio dei diritti loro riconosciuti e l'adozione di idonee misure di sicurezza.

Durante il secondo incontro sono stati adottati due documenti rispettivamente dedicati agli strumenti e alle procedure per combattere le frodi informatiche nel rispetto della *privacy* e alle modalità concrete attraverso le quali i soggetti deputati alla sicurezza delle reti possano acquisire le necessarie conoscenze dal punto di vista della protezione dei dati. Sono stati inoltre affrontati i problemi legati alle tecnologie di localizzazione e di videosorveglianza (con particolare riferimento alla registrazione delle immagini, all'utilizzo di sistemi di riconoscimento dello *stress* attraverso l'analisi della voce e i pericoli connessi al *Voice over IP* nel caso in cui il terminale usato per la ricezione delle comunicazioni sia un *computer*).

La delegazione italiana ha chiesto, in conclusione, di inserire il tema dell'*e-health*, ed in particolare della cartella clinica *on-line*, nell'ordine del giorno dei prossimi incontri.

CIRCA Complaints

Gli incontri, a cadenza semestrale, dedicati alla trattazione di ricorsi e segnalazioni transnazionali ed allo scambio di buone prassi e informazioni su questioni applicative concrete, si sono svolti a Stoccolma (11-12 marzo 2004) e a Praga (4-5 novembre 2004).

Tutti i 25 Paesi dell'Unione hanno inviato propri rappresentanti. Conformemente allo spirito che da sempre ha ispirato questi incontri, molto spazio è stato dedicato all'esame di singoli casi e al confronto sugli approcci seguiti. Sono state sollevate e proposte questioni di interesse comune, quali il trattamento dei dati biometrici; le attività di sensibilizzazione svolte a livello nazionale e i possibili suggerimenti da esse ricavabili in termini di buone prassi; le attività ispettive, le tematiche inerenti al trattamento e alla conservazione dei dati di traffico da parte dei gestori di servizi di telefonia mobile, casi di bilanciamento di interessi con particolare riguardo ai rapporti di lavoro. Una particolare riflessione è stata svolta in relazione alle decisioni assunte dal Gruppo art. 29 in materia di *enforcement,* in vista del possibile sviluppo di iniziative comuni e "sincronizzate" nei settori che risultano più problematici.

In particolare, l'incontro di Praga ha offerto la possibilità di un aggiornamento sullo *status* delle autorità di protezione dati nei dieci Stati membri recentemente entrati a far parte dell'Ue e sui principali problemi che esse incontrano: da più parti è stato lamentato un *deficit* di trasparenza rispetto ai trattamenti di dati effettuati per scopi di sicurezza e giustizia da soggetti pubblici (in particolare le forze di polizia), anche se su queste tematiche le autorità mantengono grande attenzione e ricevono un forte sostegno da parte dell'opinione pubblica. Lo stesso, inoltre, ha consentito di individuare alcune priorità per le attività future con l'approvazione della proposta di una ridefinizione del mandato del *Workshop* sulla scorta di quanto indicato dalla *Spring Conference of European Data Protection Commissioners* tenutasi a Rotterdam nel mese di aprile 2004. Senza modificare l'approccio pragmatico finora seguito dai *Workshop,* è stato costituito un *drafting group* (comprendente l'Italia) per redigere una sorta di "statuto" dei *Complaints Handling Workshop* che ne fissi le caratteristiche fondamentali (trattazione di ricorsi o segnalazioni, soprattutto attraverso *case studies,* sui quali confrontare i diversi punti di vista; particolare attenzione rispetto ai casi più difficili ed alle questioni che richiedono una valutazione armonizzata a livello Ue; mantenimento della struttura flessibile del programma dei *Workshop*).

22.12. *Consiglio d'Europa*

Nel mese di maggio del 2004 sono stati definitivamente approvati dal Comitato dei Ministri del Consiglio d'Europa i principi guida elaborati dal CJ-PD rispetto al trattamento di dati personali attraverso "carte intelligenti", ossia carte contenenti un *microchip* in grado di effettuare particolari operazioni (accesso ai servizi in rete, pagamenti *on-line* ecc.) e nel quale è possibile inserire un notevole numero di informazioni personali, dai dati identificativi a quelli biometrici, come le impronte digitali (v. *Documentazione* par. 73).

I principi-guida ribadiscono che i dati personali raccolti e trattati attraverso *smart card* devono essere limitati al minimo indispensabile ed essere utilizzati solo per scopi legittimi e specifici. I dati sulla salute, in particolare, possono essere trattati solo se vi è una previsione di legge, oppure con il consenso dell'interessato, e dovranno essere adottate misure di garanzie come la cifratura. I cittadini devono essere informati sull'uso che viene fatto delle loro informazioni personali ed occorre procedere con cautela nell'utilizzazione di *smart card* come mezzo di pagamento se in esse sono registrati dati sensibili.

I principi-guida sono rivolti in via primaria ai soggetti che rilasciano le *smart card* in quanto titolari delle relative operazioni di trattamento, ma riguardano anche tutte le altri parti in causa (progettisti di sistemi, gestori, operatori, interessati); nel caso di una carta multiuso, si avrà una situazione di contitolarità da parte dei soggetti che raccolgono ed utilizzano i dati.

Il Comitato T-PD ha proseguito i lavori sulle implicazioni per la protezione dati delle applicazioni biometriche, continuando una riflessione già avviata dal CJ-PD (comitato soppresso, come ricordato nella *Relazione 2003*) e cercando di acquisire le esperienze maturate in questo settore dal Gruppo art. 29 e dall'Ocse. Nel corso della prossima riunione potrebbe essere approvato un documento che descrive lo stato dell'arte e le questioni tuttora aperte relativamente alle tecnologie biometriche, alla luce dei principi fissati nella Convenzione n. 108.

Il Comitato ha anche iniziato una attività rivolta alla valutazione dell'applicazione dei principi di protezione dati a Internet. Sulla scorta dell'analisi contenuta in un rapporto sul principio dell'autodeterminazione informativa nell'era di Internet, si stimolerà la riflessione sull'applicabilità della Convenzione n. 108 alle reti di comunicazione elettronica.

Come ben evidenziato nel rapporto, si è assistito alla crescita esponenziale dei supporti di comunicazione che ha creato la possibilità di "registrare" la vita di tutti, mentre il costo di tali operazioni è sempre più accessibile. Lo sviluppo tecnologico è, però, avvenuto su scala mondiale senza soggetti o attori in grado di stabilire i relativi limiti, e soprattutto senza che i problemi relativi alla vita privata, fortemente minacciata dalle reti, siano stati tecnicamente affrontati. Vi è oggi, quindi, la necessità di definire un modello efficace di protezione dati, attraverso l'imposizione di norme operative per i terminali, i protocolli e gli operatori di telecomunicazioni.

Per quanto concerne poi la possibilità di applicare le disposizioni della Convenzione n. 108 alle reti di telecomunicazione, è stata rilevata come preminente l'esigenza che l'utente sia adeguatamente informato sui trattamenti di dati effettuati dagli operatori e possa partecipare al "negoziato" che riguarda il trattamento dei dati personali a lui riferiti; l'obbligo di informativa dovrebbe ricadere sui produttori.

22.13. *Ocse*

Spam

Il Garante ha partecipato ai lavori del *Working Party on Information Security and Privacy* che, in relazione ai temi di protezione dati, si è occupato dell'applicazione delle linee-guida sulla sicurezza, dello *spam*, della sicurezza dei trasporti e dei modelli di informativa.

Per quanto riguarda lo *spam*, l'Ocse ha organizzato nel 2004 un seminario pubblico sullo *spam* ospitato dalla Commissione europea con l'obiettivo di studiare la dimensione internazionale del fenomeno e le possibili strategie di contrasto.

Analizzato il fenomeno dello *spam* (anche in termini di impatto economico e sociale), ha formato oggetto di discussione l'individuazione delle varie strategie di contrasto (in particolare attraverso legislazione e autoregolamentazione, in un quadro di cooperazione internazionale fra le Autorità di protezione dei dati e le altre autorità competenti, incluse le forze dell'ordine e giudiziarie).

I partecipanti comprendono rappresentanti delle istituzioni, del mondo delle imprese, della società civile e studiosi di livello universitario. Per l'Italia era presente il segretario generale dell'Autorità con una relazione sulle difficoltà e le sfide della cooperazione internazionale contro lo *spam* ed una illustrazione delle attività svolte dall'Autorità per contrastarne gli effetti. Nella analisi conclusiva delle prospettive

sulla lotta allo *spam*, tenuto conto dell'ampiezza e complessità del fenomeno, si è proposta l'adozione di strategie "multilivello".

Il nodo problematico più difficile da affrontare rimane comunque quello del *law enforcement*, anche perché le competenze in materia di *spam* sono attribuite all'interno dei singoli paesi ad istituzioni differenti e non sempre si riesce ad avere un referente unitario. Per ovviare a tale difficoltà è stata costituita una specifica *Task Force* che avrà il compito di svolgere una ricognizione delle istituzioni competenti in questa materia nei singoli paesi e dei poteri loro attribuiti. La *Task Force* si occuperà di studiare le tecniche utilizzate dagli *spammer*, di analizzare lo *spam* telefonico, di coinvolgere il settore pubblico e quello privato e di costituire una *contact list*.

Biometria

L'Ocse si è inoltre occupato del problema della sicurezza e riservatezza delle informazioni raccolte nel campo della sicurezza internazionale dei viaggiatori. È stato costituito a tal fine un gruppo di lavoro congiunto Ocse/Icao (di cui fa parte anche il Garante) che ha iniziato ad occuparsi del tema dell'inserimento dei dati biometrici nei documenti di viaggio. Sono in fase di elaborazione delle linee-guida che saranno messe a punto nei prossimi mesi. Gli aspetti più delicati sotto il profilo della protezione dati sono legati all'individuazione dei dati da inserire, all'architettura del sistema (centralizzato/decentralizzato) e alle funzionalità dello stesso (autenticazione/identificazione).

Con riferimento al tema dell'informativa, in seguito alla risoluzione approvata alla Conferenza mondiale dei Garanti della *privacy* che si è svolta a Sidney nel 2003, è stato presentato un documento volto a promuovere l'elaborazione di un modello di informativa semplice, efficace e comprensibile, nella convinzione che la trasparenza nella comunicazione delle informazioni relative ai dati personali sia il necessario presupposto di un reale sviluppo della protezione dei dati. Il valore aggiunto di un lavoro su questo tema portato avanti in sede Ocse dovrebbe essere quello di mettere insieme le esperienze maturate nel settore privato e nel settore pubblico. Uno studio condotto su modelli di informativa predisposti da numerose società multinazionali ha fatto emergere con immediatezza che i modelli predisposti sono generalmente poco leggibili e non chiari nei contenuti. Su questo tema lavorerà nei prossimi mesi un gruppo ristretto di delegati, fra i quali è presente anche il Garante.

23 Attività di ricerca, comunicazione e formazione

23.1. *La comunicazione del Garante: profili generali*

Nel 2004, l'attività di comunicazione curata dal Garante si è concentrata in maniera particolare sull'illustrazione delle maggiori novità introdotte dal Codice e sull'individuazione di criteri per bilanciare gli interessi in gioco riguardo ad alcuni temi problematici quali la sanità, la sicurezza, le grandi banche dati.

L'attività di informazione e comunicazione ha seguito, pertanto, l'impegno dell'Autorità nei confronti di particolari aspetti applicativi della normativa, incentrandosi su una serie di importanti settori, oggetto specifico di intervento da parte del Garante, che vanno dalla tutela dei dati sanitari dei lavoratori, allo *"spamming"* (telematico e telefonico), ad Internet, alle tecnologie biometriche, alle intercettazioni, alla necessaria trasparenza nelle operazioni finanziarie, al giornalismo, con speciale riguardo alla dignità della persona, alla tutela dei minori e ai rischi dell'accanimento informativo. In questi ambiti, il Garante è spesso intervenuto in favore di una nuova nozione di protezione dati come "valore aggiunto" per imprese e pubbliche amministrazioni al fine di instaurare un rapporto nuovo con utenti e consumatori nell'economia del mercato globale.

Oltre che su tali questioni, l'attività di comunicazione si è intensificata nella promozione della protezione dei dati personali come diritto fondamentale e autonomo, sancito anche dal Trattato che adotta una Costituzione per l'Europa.

L'Autorità ha mantenuto la scelta di affidare la sua informazione ad un linguaggio rigoroso, ma attento ad una funzione divulgativa, per corrispondere alle esigenze dei cittadini. Nel dar conto della propria attività e delle tematiche all'ordine del giorno, l'Autorità ha richiamato l'attenzione di istituzioni, pubbliche amministrazioni, imprese e, in generale, degli utilizzatori di dati, 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 è stata ampia, differenziata e connotata da una forte caratterizzazione, favorita peraltro dall'adozione di una *corporate identity* nella documentazione e comunicazione dell'Autorità e da una strategia integrata di comunicazione, nella quale spicca anche un aumentato utilizzo di *mass media* tradizionali, come radio e tv, nonché di media *on-line* e prodotti multimediali.

In particolare, la presenza sulle pagine dei maggiori quotidiani e periodici nazionali ed internazionali e dei media *on-line* delle tematiche riguardanti la protezione dei dati personali e l'attività del Garante si è mantenuta costantemente alta in questi anni. Nel periodo che va dal 1° gennaio 2004 al 31 dicembre 2004 le pagine dedicate alle questioni legate generalmente alla *privacy* sono risultati oltre 8400, delle quali circa 1700 dedicate specificamente all'attività del Garante. Le "prime pagine" dedicate ai temi della protezione dei dati personali sono state circa 1200 (di cui oltre 640 riguardanti la sola Autorità). Numerose sono state le interviste pubblicate sulla carta stampata (91), su tv e radio nazionali e locali (138) e diverse anche su pubblicazioni *on-line*.

23.2. *Prodotti informativi*

La *Newsletter* settimanale, che si appresta ad entrare nel suo sesto anno di pubblicazione (per un totale complessivo di 250 numeri), è diventata uno strumento di centrale riferimento dell'attività di comunicazione del Garante, fornendo una illustrazione in chiave giornalistica dei provvedimenti e dell'attività dell'Autorità, nonché un articolato panorama di temi e problematiche. Maggiore attenzione è stata sempre più dedicata a quanto avviene in campo comunitario ed internazionale, non solo riguardo ai temi della protezione dei dati, ma anche al più largo ambito della tutela dei diritti fondamentali.

La *Newsletter* può essere consultata *on-line* sul sito *web* del Garante ed è inviata in via telematica ad un numero sempre maggiore di abbonati (istituzioni, privati cittadini, imprese, liberi professionisti).

Nel 2004, è giunto alla sua XII edizione il *Cd Rom "Cittadini e Società dell'informazione"* che contiene, in forma integrale e nell'originale veste editoriale, i provvedimenti del Garante, la documentazione relativa alla normativa nazionale ed internazionale di riferimento, le pubblicazioni realizzate. L'archivio digitale ipertestuale, che consente una consultazione con funzioni di ricerca "*full-text*", rappresenta uno strumento conosciuto e costantemente richiesto da parte di amministrazioni pubbliche, imprese, liberi professionisti e cittadini. Nella recente edizione il Cd contiene anche una presentazione multimediale del Garante e dei temi di particolare interesse affrontati nel corso della sua attività.

Tra le pubblicazioni va annoverato il *Bollettino* che raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa ed altra documentazione. Per questa pubblicazione è prevista una revisione complessiva.

La necessità di promuovere una sempre maggiore conoscenza delle norme sulla protezione dei dati e dei diritti della persona oggi riconosciuti ai cittadini, ha spinto l'Autorità a sviluppare nuove modalità di informazione: oltre agli strumenti di comunicazione già utilizzati –da quelli tradizionali (comunicati stampa, *Newsletter*, conferenze stampa, *press briefing*) a quelli multimediali ed interattivi– l'Autorità ha realizzato nuovi prodotti.

L'impegno per una comunicazione agile e diretta al cittadino ha trovato attuazione nella realizzazione di *depliant* illustrativi dei diversi aspetti connessi alla protezione dei dati. I primi tre 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. Un quarto, di recente pubblicazione, riguarda le caratteristiche che avranno i nuovi elenchi telefonici.

Il progetto di comunicazione istituzionale proseguirà con la realizzazione di una ulteriore serie di *depliant* relativi a diverse tematiche (videosorveglianza, credito al consumo, rapporti di lavoro ecc.).

23.3. *Prodotti editoriali*

È giunto al suo dodicesimo numero il notiziario bimestrale, *"Garanteprivacy.it"*, una pubblicazione destinata a personalità del mondo imprenditoriale ed istituzionale, caratterizzata da una comunicazione mirata ed essenziale; la pubblicazione è volta a sottolineare l'attività dell'Autorità nei diversi settori di intervento, con particolare attenzione anche al panorama internazionale.

Prosegue la pubblicazione di volumi nell'ambito della collana *"Contributi"*, che ospita testi attinenti specifiche problematiche sulla protezione dei dati personali e la

tutela della dignità della persona. Ai primi due volumi della collana, il *"Massimario 1997-2001"*, a cura di Luigi Pecora e Giuseppe Staglianò, e *"Privacy e giornalismo"*, a cura di Mauro Paissan, si è aggiunto *"Da costo a risorsa. La tutela dei dati personali nelle attività produttive"*, curato da Gaetano Rasi.

Nel primo libro, l'attività di massimazione dei provvedimenti assunti nel corso degli anni è stata preordinata alla formazione di una rassegna di giurisprudenza che, attraverso un'articolazione in voci e sottovoci, permetta la rapida e corretta individuazione degli argomenti trattati e delle decisioni assunte. L'opera –a breve disponibile anche in formato elettronico– si indirizza in particolar modo a giuristi, operatori del diritto, ordini professionali, imprese, istituzioni pubbliche e private.

Il secondo volume, preceduto da un saggio introduttivo del curatore, raccoglie, invece, diverse decisioni adottate dall'Autorità in materia di tutela della persona e libertà di manifestazione del pensiero. Come in una sorta di manuale pratico per i giornalisti, ma anche per i cittadini, si possono agilmente rintracciare le decisioni riguardanti la tutela dei minori, i rapporti tra cronaca e giustizia, l'uso dei dati di personaggi pubblici, la trasparenza delle fonti pubbliche, i divieti e i rischi derivanti dalla diffusione dei dati sulla salute e sulla vita sessuale, l'uso di fotografie e foto segnaletiche.

L'ultima opera, invece, affronta i temi della funzione della protezione dei dati in un mercato globale e della necessità che essa debba essere ormai considerata come valore aggiunto e *asset* competitivo per le imprese, fornendo peraltro anche un contributo utile per ridisegnare le relazioni tra aziende e consumatori. Il volume raccoglie i contributi di autorevoli studiosi ed esperti italiani e stranieri che hanno partecipato ad una conferenza internazionale organizzata dal Garante e tenuta a Roma, presso la sede dell'Autorità, nel dicembre 2002. Riproducendo le quattro sessioni della conferenza, il libro si pone l'obiettivo di aprire un ampio confronto tra coloro che operano nelle attività imprenditoriali, professionali e della cultura economica e giuridica.

A queste prime pubblicazioni se ne aggiungerà presto un'altra dedicata ai rapporti tra tutela dei dati personali e nuove tecnologie.

23.4. *Il rapporto con il pubblico*

Il rapporto diretto con la società riveste un'importanza fondamentale per l'Autorità che, fin dall'inizio della sua attività, ha inteso presentarsi come un'istituzione vicina ai cittadini, presidio dei nuovi diritti della persona. L'informazione e "formazione" del pubblico è svolta anche mettendo a disposizione sul sito una quantità significativa di documenti, con continui aggiornamenti e *dossier* tematici. In questo senso, la piena attività dell'Ufficio relazioni con il pubblico (Urp) ha consentito, in collegamento con un *call center*, di offrire non solo un contributo di chiarificazione e supporto, ma anche di favorire modalità di interazione ancora più funzionali e dirette con tutti i cittadini che hanno bisogno di informazioni, strumenti illustrativi e divulgativi, sviluppando così un flusso costante di informazioni verso l'esterno e consentendo, nello stesso tempo, di conoscere le esigenze provenienti dalla società civile, dal mondo delle imprese, dal settore della ricerca e dalle pubbliche amministrazioni.

Il grande interesse suscitato dalla *privacy* è quotidianamente dimostrato dal numero consistente di contatti diretti del cittadino con l'Urp, in costante aumento. Tali significativi incrementi registrati nel corso dell'anno rispetto al 2003 hanno stimolato la ricerca di nuove e più mirate risposte per favorire il dialogo con i cittadini, che avviene attraverso una attività di *back office* –con la ricezione di quesiti e

richieste di documentazione per *e-mail* (13.000)– nonché in maniera diretta mediante un'impegnativa, quanto essenziale, attività di *front office*, attraverso il *call-center* (10.000 telefonate pervenute) e il ricevimento diretto del pubblico presso l'Ufficio (2.400 visitatori).

Le tematiche che nel periodo in esame hanno formato maggiormente oggetto di quesiti rivolti all'Ufficio o per le quali è stato più frequentemente richiesto materiale informativo, sono state: il trattamento dei dati da parte di sistemi di informazione creditizia; la videosorveglianza con gli approfondimenti dettati dalle nuove regole in materia; l'esercizio dei diritti previsti dall'art. 7 del Codice; lo *spamming;* l'applicazione delle misure minime di sicurezza ed il trattamento dei dati nell'ambito del rapporto di lavoro.

23.5. *Le attività di formazione*

Al fine di promuovere la cultura della protezione dei dati personali, nella convinzione che la conoscenza e la comprensione dei principi e delle norme del Codice siano il presupposto per una corretta attuazione degli adempimenti nell'attività quotidiana, nel primo semestre del 2004 sono state realizzate presso la sala conferenze del Garante tre giornate di formazione, denominate *"Incontri con il Garante"*: due dirette alle imprese, uno alle pubbliche amministrazioni (con particolare riferimento alle problematiche degli enti locali). La conduzione di questi corsi è stata affidata ai responsabili dei dipartimenti giuridici interni dell'Autorità, coordinati dal segretario generale.

L'iniziativa, nuova per l'Autorità, ha suscitato vivo interesse, rivelando una domanda di formazione/informazione qualificata molto forte (in particolare, nell'ambito della consulenza professionale).

In parallelo a queste iniziative sono stati elaborati due CD-Rom multimediali, rivolti rispettivamente al mondo imprenditoriale e professionale e a quello delle pubbliche amministrazioni, che hanno come punto di riferimento l'esperienza maturata nell'ambito dei predetti incontri; è prevista a breve la distribuzione di tali prodotti, al fine di renderne possibile un'agevole fruizione ad un numero molto elevato di utenti interessati ad approfondire norme ed adempimenti previsti dal Codice.

Altre iniziative, di natura analoga, verranno intraprese nel corso del 2005. In particolare, il Garante ha organizzato un incontro di approfondimento sull'applicazione del Codice presso organismi sanitari pubblici e privati (2 febbraio 2005).

Principale obiettivo dell'iniziativa, destinata prevalentemente agli operatori degli organismi sanitari, è quello di illustrare le concrete modalità di realizzazione delle misure adottate per garantire nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati. Sulla base delle più significative esperienze maturate da taluni organismi sanitari, avvalendosi anche di un confronto dialettico con il Garante, sarà possibile offrire una gamma di modelli operativi, utili alle varie realtà sanitarie chiamate ad applicare le disposizioni del Codice.

23.6. *Manifestazioni e conferenze*

Anche nel corso del 2004 si è confermato un grande interesse da parte del pubblico per l'attività dell'Autorità in occasione di seminari, convegni ed altre iniziative. 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.

Nell'ambito del *Forum P.A.* edizione 2004, svoltosi a Roma dal 10 al 14 maggio, il Garante è stato invitato ad illustrare i temi dei rapporti tra comunicazione al cittadino e *privacy*, del rispetto delle norme sulla riservatezza da parte delle pubbliche amministrazioni, delle misure organizzative e tecnologiche da adottare per garantire la sicurezza dei dati personali.

Il presidente Stefano Rodotà è intervenuto al convegno dal titolo: *"Tra norme e prassi: per una organizzazione della funzione di comunicazione nelle pubbliche amministrazioni"* con un intervento dedicato al tema: *"La funzione di comunicazione nell'interpretazione delle Autorità garanti"*. Il vice presidente Giuseppe Santaniello ha invece partecipato al convegno *"Semplificazione e qualità delle regole"*. Gaetano Rasi, componente dell'Autorità, ha partecipato al convegno dal titolo: *"La sicurezza partecipata: coordinamento e cooperazione interistituzionale"*. Il segretario generale Giovanni Buttarelli, oltre che nel convegno *"L'identità digitale e gli strumenti di autenticazione in rete tra necessità di semplicità e tutela della* privacy*"*, è intervenuto anche a quello sul tema: *"Funzionamento e organizzazione delle* authorities*: esperienze a confronto"*. Lo stesso segretario generale è stato poi relatore al Master P.a. sul tema: *"Il Codice per la protezione dei dati personali: le novità riguardanti la Pubblica Amministrazione"*.

L'Autorità Garante è stata presente anche al Com-P.a. 2004, Salone della comunicazione pubblica, dedicato quest'anno al tema *"La comunicazione pubblica guarda all'Europa"*, svoltosi a Bologna dal 3 al 5 novembre. In particolare, il Com-P.a. ha offerto l'occasione per affrontare i temi legati alla protezione dei dati nelle telecomunicazioni, nell'*e-government* e per approfondire le novità più significative introdotte dal Codice.

Il vice presidente dell'Autorità ha partecipato al convegno dedicato a *"Democrazia e partecipazione, accesso e comunicazione"*. Nell'ambito di una tavola rotonda, organizzata dalle Asl della regione Emilia-Romagna, dedicata al diritto di cronaca e alla *privacy* nella sanità è stato presentato un video con un contributo di Mauro Paissan, componente dell'Autorità. Rappresentanti dell'Ufficio del Garante hanno partecipato a diversi convegni e incontri dedicati rispettivamente a: *"Comunicazione pubblica, tutela dei dati e sicurezza"*; *"La nuova frontiera della comunicazione nelle autorità di garanzia e promozione"*; *"Sicurezza dei dati nelle scuole"*.

L'Autorità è stata presente alle due manifestazioni con un proprio *stand* presso il quale è stato programmato un video esplicativo sull'attività del Garante e sulle tematiche della *privacy* e sono state distribuite le pubblicazioni curate dall'Ufficio, i *depliant* divulgativi e la nuova edizione del CD-Rom *"Cittadini e Società dell'informazione"*, aggiornata con il Codice in materia di protezione dei dati personali.

Incontri internazionali

L'Autorità ha ricevuto il 26 maggio 2004 Peter Schaar, Incaricato federale tedesco per la protezione dei dati ed attuale presidente del Gruppo che riunisce le Autorità di protezione dei dati europee. L'incontro è stato l'occasione per uno scambio di opinioni sulla situazione della tutela della protezione dei dati nei rispettivi Paesi, sulle iniziative del Gruppo dei Garanti europei e sulle questioni strategiche oggi al centro dell'attenzione, quali ad esempio, i dati genetici, Internet e l'uso delle nuove tecnologie, in particolare delle *Rfid*, le cosiddette *"etichette intelligenti"*. Riguardo a questo aspetto in particolare, Schaar ha annunciato la costituzione di un sottogruppo *ad hoc* nell'ambito dell'attività del Gruppo dei Garanti Ue.

Sul problema del trasferimento dei dati da parte delle compagnie aeree alle auto-

rità americane, le due Autorità hanno convenuto di intraprendere un'azione comune al fine di sensibilizzare ulteriormente il Parlamento Europeo e di individuare modalità rispettose della *privacy* dei cittadini europei, dichiarandosi pronte ad una collaborazione bilaterale sui temi affrontati nell'incontro.

Nel maggio del 2004 il segretario generale dell'Autorità, Giovanni Buttarelli, ha partecipato alla Conferenza organizzata a Washington dall'*Electronic Privacy Information Center (Epic)* per celebrare il decennale della propria attività. Epic è una delle principali organizzazioni *no-profit* attive negli Usa nel settore dei diritti civili e della tutela della riservatezza. La conferenza, cui hanno preso parte i proff. Santaniello e Rasi, ha dato l'opportunità a molti dei più autorevoli studiosi in materia di fare il punto della situazione rispetto ai rischi per libertà e diritti civili negli USA ed in altri Paesi.

Nel settembre 2004 presso l'Istituto italiano di cultura di Lisbona si è svolta una Conferenza su *"Il sistema delle garanzie della privacy nell'ordinamento italiano, alla luce del nuovo Codice per la protezione dei dati personali"*. La conferenza ha offerto l'occasione per trattare i temi legati alle novità introdotte dal Codice, che segna il passaggio dalla concezione della *privacy* come inviolabilità della sfera privata alla proiezione della persona nella società, e per sottolineare l'importanza che la tutela dei dati personali dei consumatori riveste in quanto requisito essenziale per la competitività delle imprese.

23.7. *L'attività di ricerca e documentazione*

Il carattere trasversale della normativa sulla protezione dei dati personali rende necessario procedere ad un costante aggiornamento sulle novità normative e giurisprudenziali di interesse dell'Autorità, nonché rivolgere una particolare attenzione alle innovazioni che, specie nel settore delle nuove tecnologie, possono avere ripercussioni sull'applicazione delle norme del Codice.

L'attività di ricerca dell'Ufficio è proseguita nella consapevolezza che essa ha un ruolo determinante al fine dell'acquisizione di un adeguato bagaglio conoscitivo indispensabile all'Autorità per rispondere alle costanti sollecitazioni provenienti dall'esterno. Ciò, tanto nell'ipotesi in cui il Garante sia chiamato ad intervenire in base a ricorsi, reclami o segnalazioni provenienti dai cittadini, quanto nei casi in cui l'Autorità ritenga opportuno agire di proprio impulso anche in vista dei molteplici eventi che a livello normativo, scientifico e tecnologico, si ripercuotono sulla materia della protezione dei dati.

È in questa prospettiva che sono state affrontate, ad esempio, le problematiche emerse nel cd. *Digital Rights Management*, o, ancora, le tematiche legate al controllo del lavoratore attraverso strumenti elettronici. Sempre in tale ottica, è inoltre proseguita l'attività di approfondimento su televisione interattiva, sistemi di geolocalizzazione e *Rfid*, attraverso la quale si è cercato di fornire un quadro di insieme sulle tecnologie in questione, nonché di prospettare soluzioni e proposte sui profili applicativi del Codice anche in vista dell'elaborazione di provvedimenti da parte dell'Autorità.

Per ciò che concerne l'attività di aggiornamento e documentazione, essa si è concretata nella predisposizione di notiziari periodici nei quali si sono raccolte le novità normative e giurisprudenziali di rilevanza per il lavoro dell'Ufficio, nonché le elaborazioni della dottrina in merito alle tematiche legate alla protezione dei dati e, più in generale, dei diritti della persona.

La documentazione e l'aggiornamento del personale sono stati svolti attraverso

la diffusione di un Notiziario, la predisposizione di un apposito sito Intranet e l'invio di una *Newsletter* interna nella quale sono raccolti, proposti e commentati articoli apparsi su riviste e siti di informazione giuridica. In tal quadro, hanno formato oggetto di studio, ad esempio, le problematiche legate all'*e-government* e alla documentazione informatica nella pubblica amministrazione; la firma elettronica; la carta sanitaria elettronica; i codici deontologici nel settore delle telecomunicazioni; il diritto alla conoscenza delle proprie origini biologiche; il diritto alla riservatezza nelle tecniche di riproduzione assistita.

Sempre attraverso la *Newsletter*, sono stati diffusi diversi approfondimenti tematici, talvolta resi in occasione della pubblicazione di sentenze provenienti anche da giurisdizioni straniere e da istituzioni europee e comunitarie.

Particolare attenzione è stata data, ad esempio, alla recente decisione della Corte di giustizia delle Comunità europee in materia di fatturazione dettagliata (14 settembre 2004, Causa C-411/02), agli ultimi orientamenti della Corte europea dei diritti dell'uomo sulla pubblicazione di foto di personaggi noti (59320/00, 24 giugno 2004, v. par. 6.4) e di persone coinvolte in procedimenti penali (50774/99, 11 gennaio 2005, v. par. 6.4), alla giurisprudenza statunitense in merito alle liste negative per il *direct marketing* e ai messaggi di posta elettronica, nonché al recente orientamento della Corte di cassazione sul reato di illecito trattamento di dati personali (Cass. n. 30134/2004; Cass. n. 28680/2004).

III - L'Ufficio del Garante

24 La gestione amministrativa dell'Ufficio

24.1. *Il bilancio e gli impegni di spesa*

Il bilancio di previsione del 2004, riferito all'ottavo anno di attività del Garante, è stato elaborato secondo le direttive del regolamento del Garante n. 3/2000.

Le risorse finanziarie sono state indirizzate prevalentemente verso i settori individuati nel documento programmatico di accompagnamento al bilancio di previsione che ha fissato gli obiettivi dell'Ufficio per l'esercizio 2004.

Nell'anno di riferimento sono stati raggiunti numerosi obiettivi: il più significativo, dal punto di vista contabile, è stato quello concernente la notificazione per via telematica (*on-line*). Con l'entrata in vigore del Codice, avvalendosi dei poteri accordati dall'art. 156, comma 3, lett. *e*), l'Autorità ha aggiornato per il 2004 i diritti di segreteria per le notificazioni fissati ad euro 150,00. Il conseguente incremento delle entrate legate a questa voce ha rappresentato circa il 14 per cento del totale delle entrate dell'anno 2004.

Le risorse a disposizione del Garante per il 2004, previste nell'esercizio in euro 12.356.000,00, al 31 dicembre 2004 sono state riscosse per euro 12.186.638,40 di cui euro 9.618.000,00 provenienti dal contributo dello Stato. Le restanti risorse finanziarie sulle quali ha potuto contare l'Autorità per entrate proprie si riferiscono invece ai circoscritti diritti di segreteria per le notificazioni, per i ricorsi e le autorizzazioni, ai rimborsi spese provenienti dal Consiglio d'Europa e dalle istituzioni comunitarie per la partecipazione di rappresentanti del Garante a riunioni a Bruxelles e nelle altre sedi comunitarie, agli interessi maturati sui fondi relativi agli avanzi pregressi, alle entrate derivanti dalla sublocazione dei locali del IV piano della scala A dell'edificio di piazza di Monte Citorio 115, ad entrate accertate per sanzioni pecuniarie, ai rimborsi spese per la concessione in uso della sala delle conferenze.

Il contributo dello Stato per il 2004 è stato ridotto rispetto all'anno precedente di euro 634.000,00; si tratta di una sensibile riduzione di risorse ormai costante, con continui decrementi a partire dal 2001.

L'anno appena concluso finanziariamente è stato comunque solo in parte condizionato dalla forte riduzione del contributo dello Stato, poiché le minori entrate sono state compensate da alcuni maggiori introiti provenienti dai diritti dovuti per le notificazioni: si tratta, tuttavia, di entrate (sostanzialmente *una tantum*) che non si ripeteranno in analoga misura nei successivi esercizi finanziari.

Mentre la forte riduzione del contributo dello Stato all'Autorità ha condizionato solo in parte l'anno finanziario relativo al 2004, i primi inconvenienti legati alla progressiva riduzione delle risorse prevista dalla tabella C della legge finanziaria (euro 9.177.000,00 per il 2005; euro 8.906.000,00 per il 2006) inizieranno a farsi avvertire a partire dal 2005. Ciò, per due motivi:

- le spese rispetto al 2004 aumenteranno sia perché nell'anno trascorso si sono compressi tutti gli oneri, sia perché con la deliberazione n. 10 del 10 dicembre 2004 si è proceduto a ratificare gli accordi negoziali per i dovuti incrementi retributivi al personale che erano fermi al 1° gennaio 2002;
- le entrate del Garante diminuiranno drasticamente: quelle provenienti dallo Stato si ridurranno di euro 634.000,00; quelle proprie si prevede che subiscano una riduzione di circa euro 1.000.000,00.

D'altro canto, le entrate per notificazioni si stabilizzeranno approssimativamente su euro 10.000,00-12.000,00 mensili, cosicché si dovrà far ricorso massicciamente all'avanzo di amministrazione pregresso per coprire anche le spese correnti. Sarebbe stata intenzione del Garante, invece, ricorrere all'utilizzo dell'avanzo soltanto per le spese d'investimento, soprattutto per quelle tecnologiche e informatiche.

La tabella allegata riassume sinteticamente per gli anni di attività del Garante, dal 1997 al 2004, 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. Da essa si rileva che il Garante ha condotto un'accorta amministrazione delle sue risorse e che soltanto l'esercizio 2003 si è necessariamente chiuso con un piccolo disavanzo coperto dall'avanzo di amministrazione.

Anno di riferimento	Traferimenti 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		12.680.672,89
*2005		9.177.000,00		10.955.000,00		16.376.846,00

Obiettivo dell'esercizio 2004 è stato il massimo contenimento delle spese dirette di gestione e delle spese per gli investimenti. Ciò ha comportato, come si rileva dai dati riportati in tabella, che anche nell'anno chiuso al 31 dicembre 2004 –e nel quale, come detto, vi è stata la forte riduzione delle risorse finanziarie trasferite dallo Stato– l'esercizio si chiuderà con un leggero prevalere delle entrate sulle uscite.

24.2. *L'attività contrattuale*

Tra le novità normative si segnala sul piano comunitario la direttiva 2004/18/CE del Parlamento europeo e del Consiglio del 31 marzo 2004 relativa al coordinamento delle procedure di aggiudicazione degli appalti pubblici di lavori, di forniture e di servizi, che unifica e razionalizza la disciplina in materia e dovrà essere attuata entro il 31 gennaio 2006.

Nell'ordinamento interno appare di particolare rilievo la legge 30 luglio 2004, n. 191, di conversione, con modificazioni, del decreto-legge 12 luglio 2004, n. 168, recante interventi urgenti per il contenimento della spesa pubblica, il cui art. 1, in particolare –per quanto riguarda le convenzioni stipulate dalla Consip per l'acquisizione di beni e servizi per le pubbliche amministrazioni– consente di utilizzare i rela-

(*) dati previsionali del 2005 per le somme da riscuotere le somme da pagare

tivi parametri di prezzo-qualità come limiti massimi, prevedendo la responsabilità amministrativa per la stipulazione di un contratto in violazione della disposizione.

I contratti stipulati non rendono compiutamente conto dell'attività svolta, da un lato, nel determinare in maniera apprezzabile le prestazioni necessarie, per eventualmente verificare previamente la disponibilità di risorse proprie, ovvero per individuare le procedure più adeguate di acquisizione, ed accorpare per quanto possibile richieste diverse in modo da ottenere condizioni complessivamente più vantaggiose, nonché, dall'altro lato, nei rapporti con i fornitori, anche nella fase esecutiva dei contratti. Si è in particolare registrata l'esigenza di verificare attentamente la regolarità delle fatture trasmesse che, in più di un caso, non tengono conto delle riduzioni del prezzo convenute ai sensi dell'art. 54 del regolamento per l'amministrazione del patrimonio e per la contabilità generale dello Stato (r.d. n. 827/1924).

L'attività si è svolta principalmente sulla base di trattative private con ricerche di mercato, in considerazione della norma regolamentare che prevede tale modalità (art. 25 del regolamento di contabilità del 2000), del limitato importo delle acquisizioni, relative ad una struttura ormai per vari aspetti consolidata ed a prestazioni al momento non oggetto di convenzioni Consip, mentre sulla base di convenzione con la Consip è stato stipulato il contratto per l'allestimento della sala conferenze dell'Autorità.

Nel rispetto dell'art. 26 del citato regolamento di contabilità del 2000 si è proceduto con comparazione di offerte per gli acquisti oltre i cinque milioni di vecchie lire: data la relativa macchinosità per acquisizioni di importo contenuto, sono allo studio ipotesi di modifica del regolamento che consentano un ulteriore snellimento delle procedure riservate agli acquisti di modesto valore.

Tra i contratti conclusi si segnala quello sulla connettività IP, affidato al precedente fornitore congiuntamente al servizio di *housing* per i relativi apparati, dopo averne sia pur sinteticamente verificato la convenienza rispetto ad ipotesi alternative.

Tra le forniture *in itinere* va segnalata quella per la telefonia mobile, per la quale, essendo in fase di studio la relativa convenzione Consip, si è prevista in termini relativamente ampi la possibilità di recedere (anche da parte dell'impresa), nonché l'obbligo per l'impresa selezionata, nel caso in cui risulti aggiudicataria anche la convenzione Consip, di informarne il Garante per consentirgli l'adesione alla convenzione medesima con adeguato preavviso.

Degna di menzione, per quanto riguarda la difficoltà di accrescere il grado di concorrenza tra i fornitori senza incidere sul livello di affidabilità, la vicenda della predisposizione dei supporti tecnologici nell'ambito dei concorsi pubblici per la selezione di personale; in questo caso, tramite una ricerca di mercato sull'allestimento tecnologico si è riusciti ad ottenere un apprezzabile risparmio rispetto all'esborso che si sarebbe sostenuto rivolgendosi anche per questo alla struttura ospitante il concorso.

24.3. *Le novità legislative e regolamentari e l'organizzazione dell'Ufficio*

Il 2004 ha segnato un'altra importante tappa nel processo di consolidamento e potenziamento dell'Ufficio del Garante.

In attuazione dell'art. 182 del Codice sono state completate le procedure propedeutiche all'inquadramento nel ruolo organico del personale in posizione di fuori ruolo o equiparato presso l'Ufficio del Garante in servizio alla data di pubblicazione del Codice nella *Gazzetta Ufficiale*, sulla base dei presupposti individuati dall'Autorità.

Nel dicembre 2004, a conclusione di una lunga trattativa, sono stati sottoscritti quattro accordi negoziali con organizzazioni sindacali del personale.

Gli accordi sono finalizzati ad attuare alcuni istituti retributivi già previsti e rimasti in parte inattuati, ad un riequilibrio del trattamento economico di segmenti di personale di cui si compone l'Ufficio, nonché all'adeguamento di taluni profili della disciplina dei contratti a tempo determinato e dell'orario di lavoro alle novità legislative di recente intervenute.

Ciò ha comportato circoscritte modifiche al regolamento del Garante n. 2/2000, concernente il trattamento giuridico ed economico del personale, pubblicate sulla *Gazzetta Ufficiale* 23 dicembre 2004, n. 300.

In particolare, con tali modifiche sono state ridefinite nuove modalità applicative dell'istituto della progressione economica (già previsto dalle disposizioni regolamentari) e sono stati introdotti criteri per valutare e valorizzare l'esperienza e la professionalità del personale di nuova immissione.

Con deliberazione del Garante sono stati rimodellati alcuni profili della disciplina dei contratti a tempo determinato adeguandoli 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 (rinnovabili 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.

24.4. *Il personale e i collaboratori esterni*

Il processo di consolidamento dell'Autorità è proseguito nel periodo considerato con l'immissione in servizio, il 21 gennaio 2005, dei vincitori di due concorsi pubblici banditi nel febbraio del 2004 (*G.U.* 9 febbraio 2004, n. 3, quarta serie speciale); tali concorsi prevedevano una riserva del trenta per cento dei posti per il personale non di ruolo, in conformità all'art. 182 del Codice.

Le commissioni esaminatrici, composte da tre docenti universitari e dal segretario generale e presiedute da due magistrati amministrativi nominati, su richiesta del Garante, dal Consiglio di presidenza della giustizia amministrativa, hanno concluso i lavori nel mese di ottobre. Dei tredici posti complessivamente banditi (di cui nove per la qualifica di funzionario e quattro per quella impiegato operativo), ne sono stati coperti solo dieci (n. 7 posti di funzionario e n. 3 di impiegato operativo); la riserva di posti, altresì, è rimasta inutilizzata in quanto i candidati riservatari risultati idonei si sono classificati in posizione utile nella graduatoria di merito di ciascun concorso.

Con il completamento di tali procedure l'organico dell'Autorità risulta attualmente coperto all'ottantacinque per cento. E ciò malgrado le crescenti difficoltà finanziarie, segnalate in altra parte della presente *Relazione*, le quali hanno imposto valutazioni e scelte di ordine organizzativo e di politica del personale volte prevalentemente al rafforzamento delle qualificazioni medio-alte da destinare all'area giuridica, in considerazione dei nuovi compiti che il Codice assegna al Garante.

La definizione delle procedure per l'inquadramento nel ruolo organico del personale in posizione di fuori ruolo o equiparato, ai sensi dell'art. 182, comma 1, lett. *a*), del Codice, e la contestuale immissione in servizio dei vincitori dei predetti concorsi pubblici, contribuiscono a rendere più stabile l'organico dell'Ufficio, sinora caratterizzato da una relativa precarietà dovuta alla notevole incidenza sul totale di personale in prestito da altre amministrazioni o a contratto.

L'inversione di tale tendenza è sottolineata da una contrazione, sia pur limitata, del contingente di contratti a tempo determinato, che per espressa previsione normativa non può essere superiore a venti unità.

La selezione per il reclutamento di (sino a) 3 giovani laureati con contratto di specializzazione a tempo determinato, bandita nel febbraio del 2004 ed in via di imminente ultimazione, è destinata ad incrementare tale contingente.

Nel periodo considerato si sono svolti alcuni *stage* (vedi *Relazione 2003*), taluni dei quali in collaborazione con università (nell'ambito di *master*) e con la Scuola superiore della pubblica amministrazione nell'ambito di corsi di formazione dirigenziale. Attualmente è in corso un solo *stage*.

Allo stato l'Ufficio può contare su 94 unità (di ruolo, in posizione di fuori ruolo o a contratto), di cui 87 effettivamente in servizio (cfr. prospetto in par. 25.1).

L'Autorità al momento non si avvale della collaborazione di consulenti. Nel periodo considerato si è reso necessario ricorrere solo a esigui incarichi professionali occasionali per acquisire competenze qualificate in materia informatica per le problematiche concernenti il sistema informativo interno e il sito *web* del Garante, per la sistemazione della biblioteca e dell'ampio materiale documentale acquisito e prodotto dall'Autorità nel corso della sua attività, nonché per la verifica, la manutenzione e il necessario aggiornamento del registro informatico dei trattamenti.

Avvalendosi delle convenzioni Consip, sono state conferite in *outsourcing* e *insourcing* alcune attività di natura esecutiva che non richiedono un apporto lavorativo di elevato contenuto professionale (ad esempio, con riguardo al *call center*).

Il Garante si avvale, altresì, di un servizio di controllo interno presieduto da un dirigente della Ragioneria generale dello Stato e composto, altresì, da un magistrato della Corte dei Conti e da un dirigente generale in quiescenza della medesima Ragioneria generale.

24.5. *Lo sviluppo del sistema informativo e l'attività in ambito tecnologico*

L'attività del Dipartimento risorse tecnologiche nel 2004 è stata volta principalmente a consolidare il sistema informativo, arricchendolo di nuove funzionalità e perfezionando quelle esistenti, e ad incrementare l'efficienza della sua gestione, per pervenire ad un'efficacia ancora maggiore delle risorse tecnologiche offerte come strumento di produttività individuale e collettiva o come soluzioni sistemiche nell'ambito dell'Ufficio del Garante.

Perdurando una situazione di carenza di risorse umane specialistiche, massima priorità hanno assunto le attività di manutenzione e di assistenza agli utenti interni, con relativa riduzione dell'attività di sviluppo e progettazione di nuovi interventi. È utile porre in evidenza che, a prescindere dalle sue formali attribuzioni, il Dipartimento ha svolto un'intensa attività di consulenza e supporto nei confronti dei dipartimenti giuridici e dell'Unità ricorsi, contribuendo ad esempio a definire le procedure di trattamento tecnico dei ricorsi in materia di *spam* e di abusi relativi alla rete Internet; ha collaborato con il collegio e con il segretario generale nella trattazione di casi che hanno richiesto una competenza tecnica informatica.

Nel gennaio 2004 è stato attivato un nuovo sistema di gestione del protocollo basato su una moderna tecnologia *web oriented*, che ha reso interscambiabili le postazioni di lavoro ed ha consentito l'accesso diversificato al registro e ai documenti in esso memorizzati tramite la rete interna. Con il nuovo sistema ciascun assegnatario di documenti protocollati riceve una notifica di assegnazione a mezzo *e-mail* e può accedere, tramite interfaccia *web*, ai documenti per i quali ha ricevuto apposita

autorizzazione. Il sistema si presta all'implementazione di un vero e proprio sistema di *workflow* documentale, e in tal senso se ne prevede l'espansione già nel corso del 2005, unitamente alla realizzazione di meccanismi di accesso selettivo tramite cui implementare procedure per l'accesso ai documenti amministrativi improntate alla massima trasparenza ma con garanzie di sicurezza.

Contestualmente al sistema di protocollo è stato attivato un nuovo sistema di posta elettronica, totalmente basato su *software open source*, progettato, organizzato e gestito dal personale tecnico dell'Ufficio. Questo sistema ha consentito di interrompere il ricorso a fornitori esterni di servizi *e-mail* e, nello stesso tempo, di raggiungere un elevato livello di prestazioni grazie alla rete locale ad alta velocità su cui si basano tutti i servizi informatici interni e alla disponibilità di adeguate risorse di memoria secondaria. Tra i servizi offerti nell'ambito del sistema vi è l'accesso tramite interfaccia *webmail* dalle reti esterne, con il ricorso a protocolli sicuri (Ssl), la certificazione digitale dell'identità dei *server* utilizzati, l'accettazione da parte degli stessi *server* di flussi di trasporto crittografati, l'autenticazione del mittente per l'accettazione della posta da instradare e non destinata alla consegna locale, che consente anche al personale in missione e collegato a reti esterne di usufruire dei servizi *Smtp* dell'Ufficio.

La disponibilità del nuovo protocollo informatico, che consente anche la protocollazione automatica di documenti e posta elettronica, con la verifica delle firme digitali, ha reso possibile l'avvio della procedura *web* per la notificazione telematica, che ha permesso a più di diecimila titolari di trattamento di dati personali di adempiere agli obblighi di legge tramite la rete Internet, realizzando così il primo esperimento di interazione in rete di una pubblica amministrazione con i cittadini, con una procedura avente un rilevante significato giuridico, andando quindi oltre il livello meramente informativo che ha finora caratterizzato la presenza in rete delle pubbliche amministrazioni. Si è trattato inoltre del primo utilizzo su larga scala in ambito pubblico della firma digitale, da cui sono state ricavate interessanti indicazioni in favore di una maggiore apertura delle procedure amministrative nei confronti dell'interazione in rete.

La procedura *web* è stata realizzata interamente all'interno dell'Ufficio, integrandosi con il protocollo informatico e la posta elettronica e con un sistema di *database* sviluppato con la collaborazione di una ditta specializzata.

Il sistema amministrativo contabile è stato perfezionato e arricchito di nuove funzionalità ed ha permesso, per la prima volta, di gestire un intero esercizio in modo totalmente automatizzato. L'esperienza di questo primo anno ha consentito di ricavare indicazioni e parametri su cui basare l'affinamento del sistema per andare incontro ancora di più alle esigenze dell'Ufficio.

La disponibilità di dati di bilancio e amministrativi da una parte, insieme ai dati relativi alle pratiche inserite nel protocollo informatico, a quelli relativi al lavoro nei vari servizi e dipartimenti desunti dal sistema automatizzato di rilevamento delle presenze, ha consentito di avviare alcune procedure di analisi statistica dei carichi di lavoro, nell'ottica della graduale implementazione di un sistema informativo direzionale per il controllo di gestione.

Sono state sviluppate e programmate estese funzionalità di *reporting*, corrispondendo adeguatamente alle esigenze informative dei vertici amministrativi e istituzionali dell'Autorità. Terminata una dettagliata fase di analisi, le funzioni di *reporting* confluiranno nel futuro sistema informativo direzionale.

Per consentire una migliore efficienza nell'attività di assistenza è stato realizzato il portale *web* dei servizi informatici dell'Ufficio, tramite cui l'utenza interna può contattare il personale tecnico per ogni esigenza e, in particolare, per le richieste di

assistenza. Queste ultime vengono gestite tramite un sistema di *helpdesk* integrato, sviluppato con *software opensource*, che consente di tracciare le richieste, gestire il processo di assegnazione e di monitoraggio della prestazione richiesta, elaborare statistiche.

Accanto alle attività prettamente strumentali alle necessità funzionali dell'Ufficio, è stato dato un contributo cospicuo allo svolgimento di altre attività di rilevante interesse istituzionale: in particolare, con riguardo allo svolgimento delle attività ispettive e dell'attività formativa e divulgativa (con un contributo in materia di sicurezza informatica nel corso dei segnalati *"Incontri con il Garante"*); inoltre, organizzando presso la sede dell'Autorità una giornata di studio sugli *standard* di sicurezza informatica, in collaborazione con esperti dell'Università di Pisa e, in collaborazione con *"Società Internet"* (sezione italiana di *Internet Society*), un seminario sullo *spam* che ha visto la presenza dei maggiori specialisti italiani del settore (i cui lavori sono stati successivamente pubblicati da Società Internet nella collana *"Quaderni"*).

Avvalendosi del contributo specifico del Dipartimento risorse tecnologiche, l'Ufficio ha preso parte a convegni e seminari sulla sicurezza informatica organizzati dall'Università di Udine (nel marzo 2004), dalla società Inet di Milano (*Internet Security Day*, nell'aprile 2004), dall'Università di Genova (nel maggio 2004) e dall'Ordine dei dottori commercialisti di Palermo (nel giugno 2004).

Per quanto riguarda la collaborazione istituzionale, l'Ufficio ha preso parte ai lavori del Comitato per la biometria nella p.a. istituito presso il Cnipa (Centro nazionale per l'informatica nella pubblica amministrazione), che ha prodotto le linee-guida per l'utilizzo delle tecnologie biometriche in un quadro di piena compatibilità con il dettato normativo. In ambito internazionale, ha partecipato ai lavori della *Internet Task Force* che svolge attività di supporto nei confronti del *Working Party Art. 29* in sede europea, contribuendo all'elaborazione dei *dossier* sugli importanti casi affrontati in quella sede, tra cui si segnalano i sistemi di autenticazione in rete (*Passport, Liberty Alliance*), i nuovi servizi di posta elettronica (tra questi, il discusso servizio *Gmail* di *Google*) e le tecnologie *Rfid*.

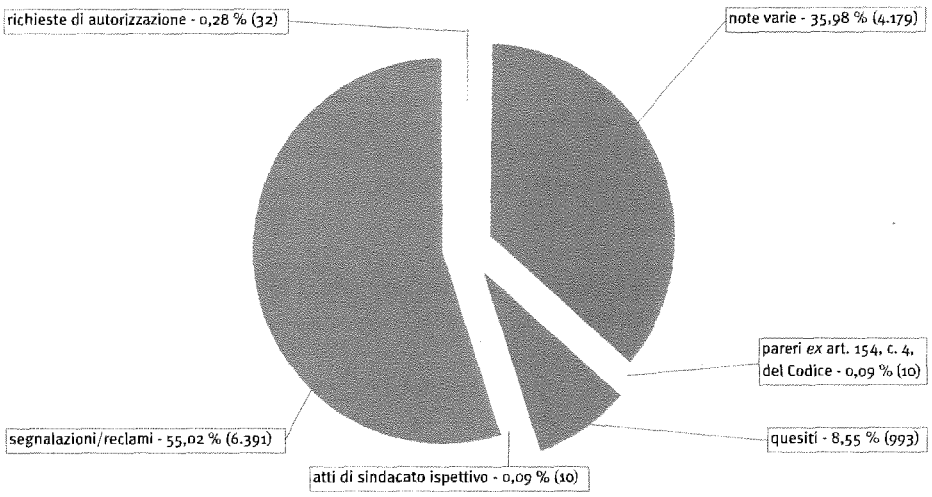
In particolare nel corso del 2004, l'Autorità ha proseguito il monitoraggio del rispetto da parte di Microsoft degli impegni assunti sulla base delle Raccomandazioni del Gruppo art. 29, attraverso la *road map* concordata con la Commissione europea nel 2003. Va segnalato, inoltre, che a fine 2004 Microsoft ha annunciato la cessazione del progetto "*Passport*" come sistema di autenticazione unica su Internet, limitandone l'uso futuro ai soli servizi offerti da Microsoft.

Il Garante ha, inoltre, preso parte al coordinamento tra i servizi di supporto e consulenza informatica delle autorità di garanzia europee sulla *privacy*, avviato per impulso dell'autorità francese Cnil con il convegno di Parigi del giugno 2004.

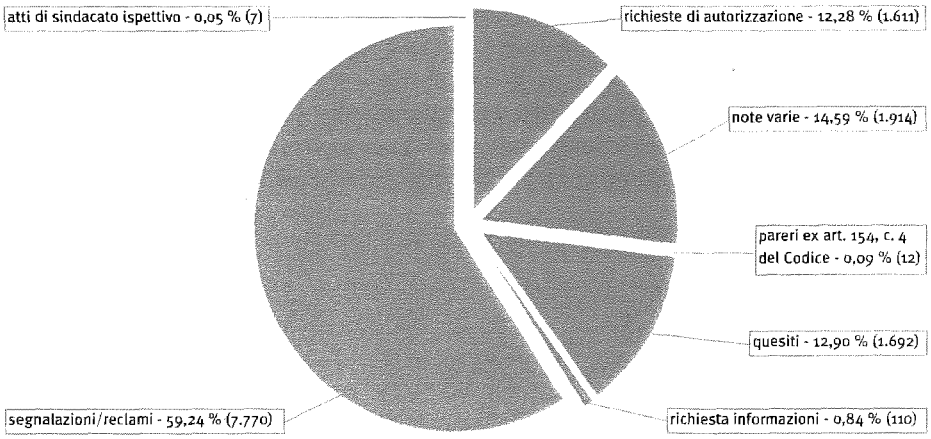
25 Dati statistici

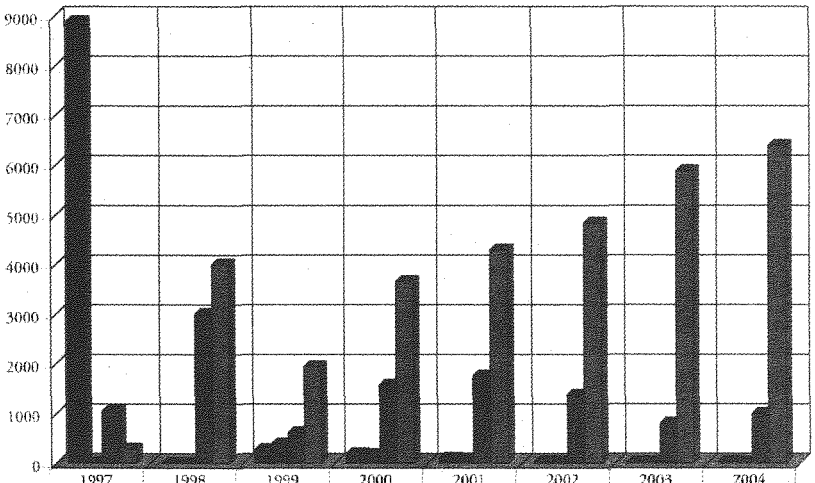
25.1. *Grafici e tabelle*

1. Principali tipologie di richieste pervenute nel 2004



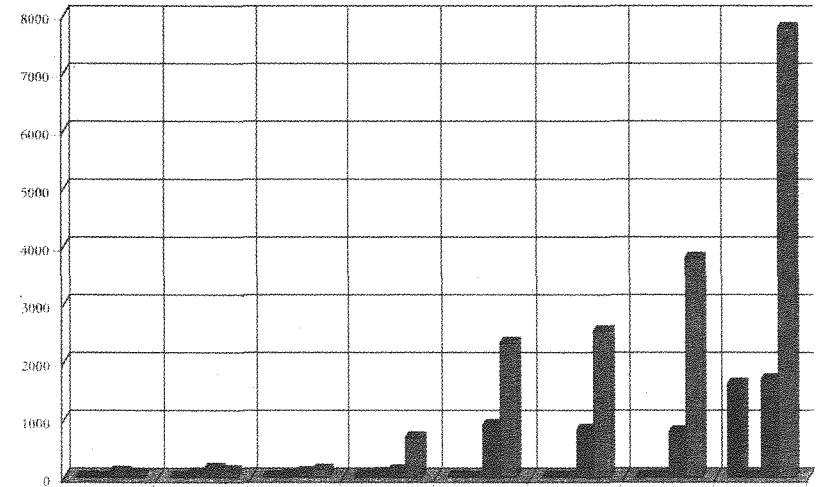
2. Principali tipologie di risposte rese nel 2004





	1997	1998	1999	2000	2001	2002	2003	2004
Autorizzazioni	8889	0	272	191	98	28	17	32
Pareri	0	0	386	170	81	22	16	10
Quesiti	1050	3000	615	1569	1755	1371	799	993
Segnalazioni/Reclami	285	4000	1946	3661	4295	4836	5880	6391

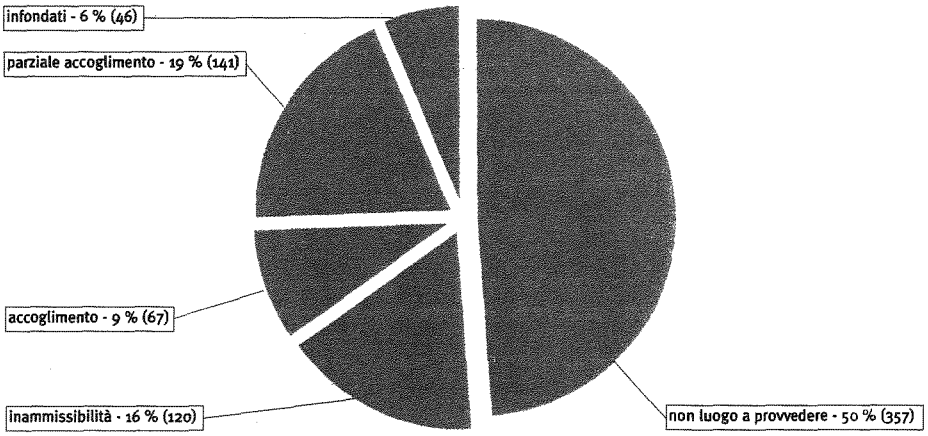
3. Principali tipologie di richieste pervenute negli anni 1997 - 2004



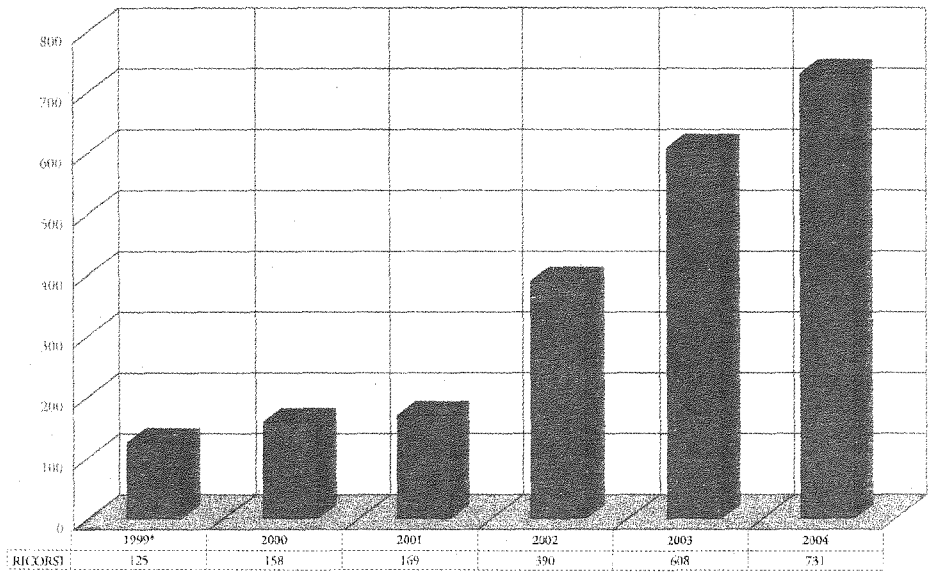
	1997	1998	1999	2000	2001	2002	2003	2004
Autorizzazioni	6	6	11	20	19	7	7	1611
Pareri	0	70	27	70	3	7	14	12
Quesiti	95	150	89	118	898	824	786	1692
Segnalazioni/Reclami	31	112	130	687	2327	2532	3796	7770

4. Principali tipologie di risposte rese negli anni 1997 - 2004

5. Tipologie delle decisioni adottate su ricorso nel 2004



6. Ricorsi decisi negli anni 1997 - 2004



(*) A partire
dal 16 febbraio 1999

7. Richieste di autorizzazione

Richieste di autorizzazione	
pubbliche amministrazioni	2
assicurazioni	1
associazioni di volontariato	1
aziende di ricerca medica ed epidemiologica	3
aziende editoriali	1
aziende private in generale	10
comuni	2
liberi professionisti	7
regioni	1
strutture del servizio sanitario nazionale	1
strutture sanitarie private	2
altri settori	1
Totale richieste presentate nel 2004	**32**
Totale risposte inviate nel 2004	**22**
Totale risposte relative a richieste presentate negli anni precedenti	**1.589**

8. Segnalazioni/Reclami

Segnalazioni/Reclami	
agenzie fiscali	22
pubbliche amministrazioni	79
altri enti locali diversi da regioni provincie e comuni	4
assicurazioni	134
associazioni	38
associazioni di volontariato	7
aziende di consulenza e revisione contabile	2
aziende di fornitura acqua gas elettricità	22
aziende di investigazione privata	9
aziende di *marketing*	11
aziende di ricerca e selezione del personale	4
aziende di ricerca medica ed epidemiologica	2
aziende di ricerca sociologica e di opinione	4
aziende di sorveglianza privata	4
aziende di trasporto	23
aziende editoriali	157
aziende per il lavoro interinale	1
aziende postali e di recapito	47
aziende private in generale	628
aziende radiofoniche e televisive	145
aziende telefoniche	580
Banca d'Italia	18
banche e finanziarie	2.515
biblioteche	3
camere di commercio	55
centrali rischi private	778
centri di assistenza fiscale	1
comuni	218

(segue)

Avvertenza:
le tabelle illustrano l'attività del Garante per tipologia di intervento e, limitatamente al 2004, per settore di riferimento.
I dati sono riferiti al 2004. Viene altresì rappresentato il dato aggregato delle risposte fornite dall'Autorità nel 2004, in relazione a richieste pervenute al Garante negli anni precedenti.

(segue)

concessionari per la riscossione dei tributi	23
condomini e multiproprietà	32
enti pubblici non economici nazionali	3
forze armate	7
forze di polizia	45
informazioni commerciali	2
Internet service provider	49
Istat	1
istituti pubblici di previdenza e assistenza	46
istituti scolastici	34
liberi professionisti	72
ministeri	46
ordini professionali	13
partiti e movimenti politici	52
prefetture uffici territoriali del governo	3
privati	48
province	15
questure	1
regioni	13
sindacati	22
strutture del servizio sanitario nazionale	161
strutture sanitarie private	28
uffici di collocamento	4
uffici giudiziari	41
Ufficio italiano dei cambi	1
università pubbliche	8
altri settori	110
Totale richieste presentate 2004	**6.391**
Totale risposte inviate 2004	**3.595**
Totale risposte relative a richieste presentate negli anni precedenti	**4.175**

9. Pareri *ex* art. 154, comma 4, del Codice

Pareri *ex* art. 154, comma 4, del Codice	
Totale richieste 2004	**10**
Totale risposte 2004	**10**
Totale risposte anni 1997-2003	**2**

10. Atti di sindacato ispettivo e di controllo

Atti di sindacato ispettivo e di controllo	
pubbliche amministrazioni	2
trattamento dati passeggeri vs. USA	3
Internet	2
altri settori	3
Totale richieste 2004	**10**
Totale risposte 2004	**7**
Totale risposte relative a richieste degli anni precedenti	**–**

11. Note varie

Note varie	
agenzie fiscali	8
pubbliche amministrazioni	34
assicurazioni	2
associazioni	54
associazioni di volontariato	3
aziende di consulenza e revisione contabile	1
aziende di investigazione privata	1
aziende di *marketing*	1
aziende di ricerca e selezione del personale	2
aziende di ricerca medica ed epidemiologica	3
aziende di ttasporto	4
aziende editoriali	5
aziende private in generale	226
aziende radiofoniche e televisive	4
aziende telefoniche	23
Banca d'Italia	1
banche e finanziarie	55
camere di commercio	2
centrali rischi private	27
chiese e organizzazioni religiose	1
comuni	185
condomini e multiproprietà	2
enti pubblici non economici nazionali	2
forze armate	1
forze di polizia	8
Internet service provider	3
Istat	6
istituti pubblici di previdenza e assistenza	16
istituti scolastici	11
liberi professionisti	45
ministeri	42
ordini professionali	8
organismi di sicurezza	1
privati	37
province	10
regioni	21
sindacati	11
strutture del servizio sanitario nazionale	92
strutture sanitarie private	60
uffici giudiziari	4
università private	1
università pubbliche	11
altri settori	3.145
Totale richieste 2004	**4.179**
Totale risposte 2004	**1.098**
Totale risposte relative a richieste degli anni precedenti	**816**

12. Richieste di informazioni da parte del Garante

Richieste di informazioni da parte del Garante (*)	
altre pubbliche amministrazioni	1
associazioni	4
aziende di ricerca medica ed epidemiologica	2
aziende di trasporto	1
aziende editoriali	3
aziende postali e di recapito	3
aziende private in generale	21
aziende radiofoniche e televisive	1
aziende telefoniche	6
banche e finanziarie	21
camere di commercio	5
centrali rischi private	14
comuni	9
Internet service provider	1
istituti pubblici di previdenza e assistenza	2
istituti scolastici	3
liberi professionisti	1
ministeri	1
partiti e movimenti politici	1
privati	2
regioni	1
strutture del servizio sanitario nazionale	5
strutture sanitarie private	1
università pubbliche	1
Totale anno 2004	**110**

13. Quesiti

Quesiti (*)	
agenzie fiscali	8
altre pubbliche amministrazioni	23
altri enti locali diversi da regioni province e comuni	5
assicurazioni	9
associazioni	32
associazioni di volontariato	1
aziende di consulenza e revisione contabile	5
aziende di fornitura acqua gas elettricità	10
aziende di investigazione privata	9
aziende di *marketing*	3
aziende di previdenza e assistenza	2
aziende di ricerca e selezione del personale	1
aziende di ricerca medica ed epidemiologica	3
aziende di ricerca storica	1
aziende di sorveglianza privata	1
aziende di trasporto	6
aziende editoriali	4
aziende postali e di recapito	3
aziende private in generale	122
aziende radiofoniche e televisive	2
aziende telefoniche	9

(*) Avvertenza:
oltre alle risposte singole, ai numerosi quesiti aventi caratteristiche analoghe, l'Autorità fornisce riscontro con atti di carattere generale

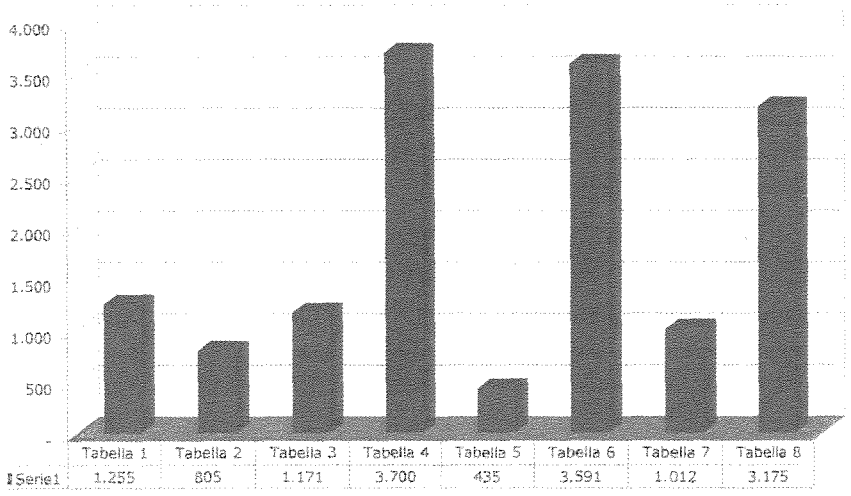
(segue)

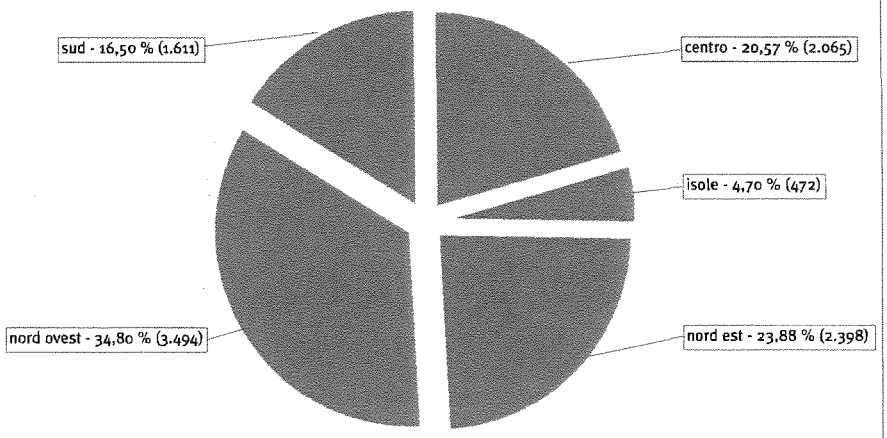
segue

Banca d'Italia	1
banche e finanziarie	37
biblioteche	1
camere di commercio	8
centrali rischi private	10
comuni	272
concessionari per la riscossione dei tributi	1
condomini e multiproprietà	8
enti pubblici non economici di regioni ed enti locali	2
enti pubblici non economici nazionali	1
forze armate	2
forze di polizia	5
informazioni commerciali	1
Internet service provider	1
Istat	3
istituti pubblici di previdenza e assistenza	9
istituti scolastici	21
liberi professionisti	51
ministeri	17
ordini professionali	15
partiti e movimenti politici	6
prefetture uffici territoriali del governo	5
privati	30
province	24
questure	1
regioni	22
sindacati	10
strutture del servizio sanitario nazionale	85
strutture sanitarie private	40
uffici giudiziari	12
università private	1
università pubbliche	10
altri settori	22
Totale richieste 2004	993
Totale risposte 2004	319
Totale risposte relative a richieste degli anni precedenti	1.373

14. Tabella e grafico riferiti alla tipologia dei trattamenti notificati

Tabella 1 - Trattamento di dati genetici	1.255
Tabella 2 - Trattamento di dati biometrici	805
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	1.171
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	3.700
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	435
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	3.591
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	1.012
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	3.175

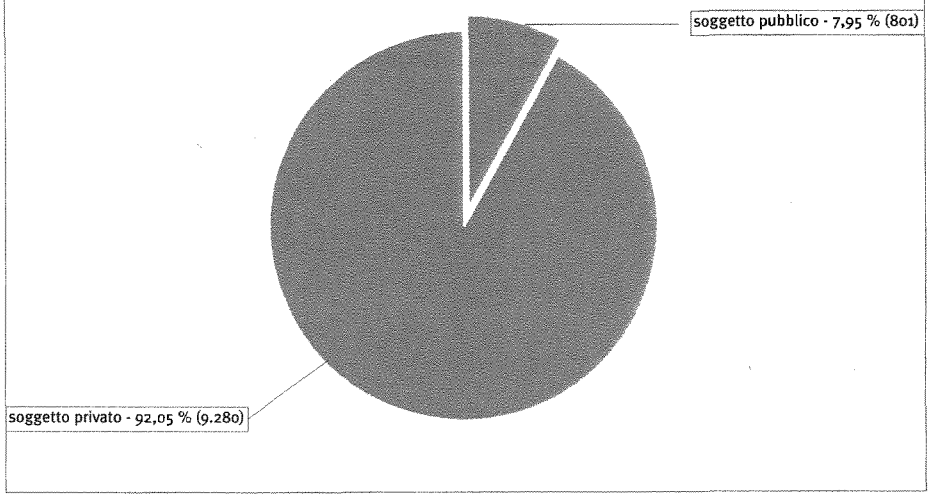




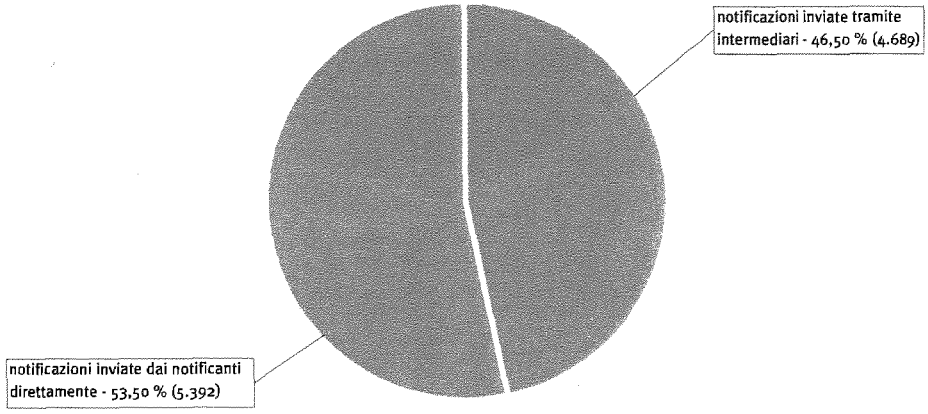
15. Distibuzione notificazioni per aree (esclusi paesi esteri)

Tipologia	Numero pervenute	di cui soggetto pubblico	di cui soggetto privato
Cessazione	36	0	36
Modifica	168	11	157
Prima notificazione	9.877	790	9.087
Totale	**10.081**	**801**	**9.280**

16. Tabella e grafico riferiti ai soggetti notificanti, pubblici e privati



17. Modalità di invio della notificazione



18. Attività Urp dal 1° gennaio 2004 al 31 dicembre 2004

e-mail in entrata *urp@garanteprivacy.it*	13.000
e-mail in entrata *garante@garanteprivacy.it*	9.900
Telefonate	10.000
Visitatori	2.400

19. Personale in servizio

Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	Personale a contratto	TOTALE
Dirigenti	26	15	5		20
Funzionari	45	35	5		40
Operativi	26	17	5		22
Esecutivi	3				0
Personale a contratto	20			12	12
TOTALE	120	67	15	12	94

Documentazione

PAGINA BIANCA

Provvedimenti normativi

26 Decreto legislativo 22 gennaio 2004, n. 42 Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137 (*)

IL PRESIDENTE DELLA REPUBBLICA

[*omissis*]

Emana

il seguente decreto legislativo:

[*omissis*]

Art. 184. Norme abrogate

1. Sono abrogate le seguenti disposizioni:

[*omissis*]

- decreto legislativo 30 giugno 2003, n. 196, limitatamente all'articolo 179, comma 4;

[*omissis*]

(*) *G.U.* 24 febbraio 2004, n. 45.

27 Legge 26 febbraio 2004, n. 45 Conversione in legge, con modificazioni, del d.l. 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia (*)

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1

1. Il decreto-legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

ALLEGATO

Modificazioni apportate in sede di conversione al d.l. 24 dicembre 2003, n. 354

[*omissis*]

All'articolo 3:

- al comma 1, capoverso "Art. 132", comma 1, le parole "i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi" sono sostituite dalle seguenti "i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi";

- al comma 1, capoverso "Art. 132", comma 2, dopo le parole "i dati" sono inserite le seguenti: "relativi al traffico telefonico" e le parole: "trenta mesi per esclusive finalità di accertamento e repressione dei delitti" sono sostituite dalle seguenti: "ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti";

- al comma 1, capoverso "Art. 132", comma 3, le parole: "dell'autorità giudiziaria, d'ufficio o su istanza" sono sostituite dalle seguenti: "del giudice su istanza del pubblico ministero o" e sono aggiunte, in fine, le parole: "ferme restando le condizioni di cui all'articolo 8, comma 2, lettera *f*) , per il traffico entrante";

- al comma 1, capoverso "Art. 132", il comma 4 è sostituito dal seguente:

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, nonchè dei delitti in danno di sistemi informatici o telematici";

- al comma 1, capoverso "Art. 132", comma 5, l'alinea è sostituito dal seguente: "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:";

- al comma 1, capoverso "Art. 132", comma 5, alla lettera *c*) le parole: "di accesso ai" sono sostituite dalle seguenti: "di trattamento dei" e le parole: "l'accesso sia consentito" sono sostituite dalle seguenti: "l'utilizzazione dei dati sia consentita";

- al comma 1, capoverso "Art. 132", il comma 6 è soppresso.

(*) *G.U.* 27 febbraio 2004, n. 48.

All'articolo 4:

- al comma 1, le parole: "Fino alla data del 31 dicembre 2005 per la conservazione del traffico si osserva il termine della prescrizione di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171" sono sostituite dalle seguenti: "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".

[*omissis*]

28 Legge 26 maggio 2004, n. 138 Conversione in legge, con modificazioni, del decreto-legge 29 marzo 2004, n. 81, recante interventi urgenti per fronteggiare situazioni di pericolo per la salute pubblica (*)

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1.

1. Il decreto-legge 29 marzo 2004, n. 81, recante interventi urgenti per fronteggiare situazioni di pericolo per la salute pubblica, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Roma, 26 maggio 2004

ALLEGATO

Modificazioni apportate in sede di conversione al decreto-legge 29 marzo 2004, n. 81

[*omissis*]

Art. 2-*quinquies*.

1. Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 37, dopo il comma 1, è inserito il seguente:

"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";

b) all'articolo 83, dopo il comma 2, è aggiunto il seguente:

"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";

c) all'articolo 89, dopo il comma 2, è aggiunto il seguente:

"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";

d) all'articolo 181, la lettera *e*) del comma 1 è abrogata.

(*) *G.U.* 29 maggio 2004, n 125.

29 Legge 27 luglio 2004, n. 188 Conversione in legge, con modificazioni, del decreto-legge 24 giugno 2004, n. 158, concernente permanenza in carica degli attuali consigli degli ordini professionali e proroga di termini in materia di difesa d'ufficio e procedimenti civili davanti al tribunale per i minorenni, nonché di protezione dei dati personali (*)

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1.

1. Il decreto-legge 24 giugno 2004, n. 158, concernente permanenza in carica degli attuali consigli degli ordini professionali e proroga di termini in materia di difesa d'ufficio e procedimenti civili davanti al tribunale per i minorenni, nonché di protezione dei dati personali, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

Roma, 27 luglio 2004

ALLEGATO

Modificazioni apportate in sede di conversione al decreto-legge 24 giugno 2004, n. 158

[omissis]

All'articolo 1, dopo il comma 1, è aggiunto il seguente:

"1-*bis*. Il regolamento previsto dall'articolo 4, comma 3, del regolamento di cui al decreto del Presidente della Repubblica 5 giugno 2001, n. 328, è emanato entro il 31 dicembre 2004. Entro la medesima data devono essere indette, ove il mandato non abbia più lunga durata, le elezioni per il rinnovo dei consigli degli ordini e collegi interessati".

(*) *G.U.* 30 luglio 2004, n. 177.

30 Legge 27 dicembre 2004, n. 306 Conversione in legge, con modificazioni, del decreto-legge 9 novembre 2004, n. 266, recante proroga o differimento di termini previsti da disposizioni legislative. Disposizioni di proroga di termini per l'esercizio di deleghe legislative (*)

IL PRESIDENTE DELLA REPUBBLICA

Promulga la seguente legge:

Art. 1.

1. Il decreto-legge 9 novembre 2004, n. 266, recante proroga o differimento di termini previsti da disposizioni legislative, è convertito in legge con le modificazioni riportate in allegato alla presente legge.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

[omissis]

Roma, 27 dicembre 2004

DECRETO-LEGGE 9 NOVEMBRE 2004, N. 266

[omissis]

Art. 6. Trattamento di dati personali

1. All'articolo 180 del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modifiche:

a) al comma 1, le parole: "31 dicembre 2004" sono sostituite dalle seguenti: "30 giugno 2005";

b) al comma 3, le parole: "31 marzo 2005" sono sostituite dalle seguenti: "30 settembre 2005".

(*) *G.U.* 27 dicembre 2004, n. 302.

Provvedimenti del Garante

31 Autorizzazione n. 1/2004 al trattamento dei dati sensibili nei rapporti di lavoro (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, 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 dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 111 del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi volti a ridurre al

(*) *G.U.* 14 agosto 2004, n. 190.

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. Stefano Rodotà;

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, lett. 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), lett. h).

2) INTERESSATI AI QUALI I DATI SI RIFERISCONO

Il trattamento può riguardare i dati sensibili attinenti:

a) a lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione e lavoro, 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 o ad altri lavoratori autonomi in rapporto di collaborazione 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 pub-

bliche iniziative, 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, lett. 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, qua-

lora 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 d.lg. 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° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 1/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

32 Autorizzazione n. 2/2004 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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 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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, 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 dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi 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, princìpi 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.* 14 agosto 2004, n. 190.

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. Stefano Rodotà;

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 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, lett. 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. 3/2004;

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. 1/2004 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, lett. 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° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 2/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

33 Autorizzazione n. 3/2004 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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 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";

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;

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);

(*) *G.U.* 14 agosto 2004, n. 190.

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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, 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 dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice;

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 i movimenti politici, alle associazioni e alle organizzazioni sindacali, ai patronati e alle associazioni di categoria, alle casse di previdenza, alle organizzazioni assistenziali o di volontariato,

nonché le 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.

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 inoltre 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;
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. 2/2004.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 4, comma 1, lettera 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 perseguite 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, 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 indispensabile, 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.

10) EFFICACIA TEMPORALE E DISCIPLINA TRANSITORIA

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia

già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 3/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

34 Autorizzazione n. 4/2004 al trattamento dei dati sensibili da parte dei liberi professionisti (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, 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 dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 135 del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi 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;

(*) *G.U.* 14 agosto 2004, n. 190.

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;

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. Giuseppe Santaniello;

Autorizza:

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 4, comma 1, lettera 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. 2/2004;
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. 1/2004;
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. 2/2004.

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), lett. 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 modificato 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° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 4/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

35 Autorizzazione n. 5/2004 al trattamento dei dati sensibili da parte di diverse categorie di titolari (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata tenuto conto dei codici di deontologia e di buona condotta di cui agli articoli 106 e 140 del Codice;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione dei codici di deontologia e di buona condotta riguardanti alcuni specifici settori presi in considerazione dal presente provvedimento (articoli 111 e 140 del Codice);

Considerata la necessità di garantire il rispetto di alcuni princìpi 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;

(*) *G.U.* 14 agosto 2004, n. 190.

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. Gaetano Rasi;

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

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.

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, lett. 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, sempreché 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. 1/2004, rilasciata il 30 giugno 2004, 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. 4/2004, rilasciata il 30 giugno 2004, 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 imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di attività svolta anche di propria iniziativa nell'interesse di terzi, ai soli fini della ricerca o della selezione del personale.

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, lett. 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. 2/2004, rilasciata il 30 giugno 2004.

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 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;

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° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 5/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

36 Autorizzazione n. 6/2004 al trattamento dei dati sensibili da parte degli investigatori privati (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, 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 dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 135 del Codice;

Considerata la necessità di garantire il rispetto di alcuni princìpi 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;

(*) *G.U.* 14 agosto 2004, n. 190.

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. 2/2004, rilasciata il 30 giugno 2004), anche in riferimento alle predette finalità di ordine giudiziario;

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. 2/2004 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 prof. Gaetano Rasi;

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. 1/2004, rilasciata il 30 giugno 2004);
b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2004, rilasciata il 30 giugno 2004);
c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione n. 3/2004, rilasciata il 30 giugno 2004);
d) da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione n. 4/2004, rilasciata il 30 giugno 2004);
e) relativamente ai dati di carattere giudiziario (autorizzazione n. 7/2004, rilasciata il 30 giugno 2004).

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'investigatore 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. 2/2004 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 d.lg. 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 processuali o 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° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 6/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

37 Autorizzazione n. 7/2004 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, con la partecipazione 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;

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, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

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;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice;

(*) *G.U.* 14 agosto 2004, n. 190.

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 prof. Giuseppe Santaniello;

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 dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione lavoro, 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° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 7/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 30 giugno 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

38 Disposizioni in materia di comunicazione e di propaganda politica (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza 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;

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;

RELATORI il prof. Giuseppe Santaniello e il dott. Mauro Paissan;

Premesso:

1. FINALITÀ DEL PROVVEDIMENTO

Le iniziative di propaganda elettorale intraprese da partiti, organismi politici, comitati promotori, sostenitori e singoli candidati costituiscono un momento particolarmente significativo della partecipazione alla vita democratica (art. 49 Cost.) che deve però rispettare i diritti e le libertà fondamentali delle persone cui si riferiscono le informazioni utilizzate.

Con l'approssimarsi di una tornata di consultazioni elettorali, l'Autorità ritiene necessario richiamare l'attenzione sulle garanzie vigenti dopo l'entrata in vigore del Codice in materia di protezione dei dati personali che ha sostituito la legge n. 675/1996 (d.lg. 30 giugno 2003, n. 196), e fornire in particolare indicazioni sull'informativa alle persone interessate.

A tal fine, verranno segnalati in questo provvedimento i casi in cui si possono utilizzare dati personali a fini di propaganda informando gli interessati, ma senza richiedere il loro consenso, e i casi in cui al contrario il consenso è necessario. Saranno poi evidenziati i diritti degli interessati di conoscere le modalità di utilizzazione dei dati che li riguardano e di far interrompere l'attività di propaganda nei propri confronti.

2. DATI TRATTI DA REGISTRI O ELENCHI PUBBLICI

a) Quando si può prescindere dal consenso

È possibile utilizzare dati personali senza il consenso degli interessati per la propaganda elettorale solo se i dati sono estratti da fonti "pubbliche" nel senso proprio del termine, ovvero conoscibili da chiunque senza limitazioni.

Questa ipotesi ricorre quando si utilizzano registri, elenchi, atti o documenti che sono detenuti da un soggetto pubblico, e al tempo stesso sono liberamente accessibili –senza discriminazioni– in base ad un'espressa disposizione di legge o di regolamento.

Se non ricorre questa condizione, l'amministrazione o l'ente pubblico che detiene i dati non può permetterne l'utilizzo a partiti, forze politiche o candidati, dovendo utilizzarli solo per svolgere funzioni istituzionali e osservando i presupposti e i limiti stabiliti, caso per caso, da norme generali o speciali contenute anche nel Codice (art. 18, commi 2 e 3, d.lg. cit.), che a volte rendono i dati "pubblici" solo per permetterne l'uso per alcune finalità.

Possono essere ad esempio utilizzate per la propaganda elettorale:

a) le c.d. liste elettorali (ovvero, le liste degli aventi diritto al voto detenute presso i

(*) Provvedimento 12 febbraio 2004, in *G.U.* 24 febbraio 2004, n. 45.

comuni), le quali "possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo ... o per il perseguimento di un interesse collettivo o diffuso" (art. 51 d.P.R. 20 marzo 1967 n. 223, come modificato dall'art. 177, comma 5, del d.lg. n. 196/2003);

b) gli elenchi di iscritti ad albi e collegi professionali (art. 61, comma 2, d.lg. n. 196/2003), e i dati contenuti in taluni registri detenuti dalle camere di commercio;

c) altri elenchi e registri in materia di elettorato attivo e passivo. Sebbene sia opportuno al riguardo un chiarimento normativo, risultano utilizzabili a fini di propaganda le seguenti fonti:
   - l'elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo (formato sulla base dei dati contenuti nelle liste elettorali e trasmesso agli uffici consolari: art. 4, commi 1 e 5, d.l. 24 giugno 1994, n. 408, convertito con l. 3 agosto 1994, n. 483);
   - le c.d. liste aggiunte dei cittadini elettori di uno Stato membro dell'Unione europea (istituite a livello comunale anche in riferimento ai dieci Paesi che vi faranno parte dal 1° maggio 2004), residenti in Italia e che intendano ivi esercitare il diritto di voto alle elezioni del Parlamento europeo (d.lg. n. 197/1996; circolare Min. interno 30 dicembre 2003, n. 134, in Gazzetta Ufficiale 8 gennaio 2004, n. 5; v. anche Com. della Commissione europea COM (2003) 174 def. dell'8 aprile 2003);
   - l'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle liste elettorali, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (AIRE) e degli schedari consolari (art. 5 l. 27 dicembre 2001, n. 459);
   - l'elenco dei cittadini italiani residenti all'estero aventi diritto al voto per l'elezione del Comitato degli italiani all'estero (Comites), reso pubblico con modalità definite con un regolamento (artt. 13 e 26 l. 23 ottobre 2003, n. 286; art. 5, comma 1, l. 27 dicembre 2001, n. 459; art. 5, comma 1, d.P.R. 2 aprile 2003, n. 104).

Va comunque segnalato a chi utilizza fonti "pubbliche" la necessità di porre attenzione:
- alle modalità prescritte in alcuni casi per accedere ai dati (ad esempio, per identificare il soggetto che ne ottiene copia);
- alla circostanza che i dati siano accessibili al pubblico solo per finalità specifiche. Non possono ad esempio ritenersi utilizzabili a fini di propaganda le informazioni sugli studenti ricavabili dalla pubblicazione degli esiti di attività scolastiche, oppure gli elenchi di immigrati o affetti da determinate malattie o di beneficiari di provvidenze economiche concesse da amministrazioni comunali a portatori di handicap, invalidi e indigenti, le graduatorie per il ricovero in istituti di sostegno o in case di cura, le liste di assegnazione degli alloggi di edilizia residenziale pubblica, gli elenchi dei beneficiari di parcheggi riservati a persone con ridotta capacità motoria;
- alle condizioni e ai limiti eventualmente posti per stabilire come utilizzare i dati dopo averne ottenuta copia. Tale utilizzazione deve poi avvenire sempre in termini compatibili con gli scopi per i quali i dati sono stati raccolti e registrati (art. 11, comma 1, lett. b), d.lg. n. 196/2003), e che in alcuni casi è possibile solo se si indica la data della loro estrazione e l'origine.

Non sono invece utilizzabili per la propaganda elettorale altre fonti della pubblica amministrazione, quali, ad esempio:

1) atti anagrafici e dello stato civile

I dati degli iscritti nelle anagrafi comunali della popolazione non possono essere forniti in alcun modo a privati per scopi di propaganda elettorale (tantomeno in forma elaborata di elenchi di intestatari di nuclei familiari), anche se il richiedente è un amministratore locale o il titolare di una carica elettiva.

Possono rivolgere una motivata richiesta di rilascio di elenchi solo le amministrazioni pubbliche per esclusivo uso di pubblica utilità (art. 34 d.P.R. n. 223/1989). Questa garan-

zia opera anche nei confronti del comune, il quale può utilizzare anch'esso i dati anagrafici che detiene solo per usi di pubblica utilità, anche in caso di comunicazione istituzionale (art. 177 d.lg. n. 196/2003), sicché tali dati non possono essere utilizzati per la propaganda elettorale o per pubbliche relazioni di carattere personale.

Anche gli atti dello stato civile sono soggetti ad un regime ben diverso da quello delle liste elettorali (art. 450 cod. civ.; d.P.R. n. 396/2000) e non possono quindi ritenersi "pubblici" nel senso proprio del termine sopra indicato;

2) dati tratti dalle liste elettorali di sezione già utilizzate nei seggi

Le liste elettorali di sezione già utilizzate nei singoli seggi e sulle quali sono stati annotati dati relativi alle persone che hanno votato non possono essere utilizzate a fini di propaganda. Tali liste contengono dati particolari a volte sensibili (idonei a rivelare l'effettiva partecipazione dei cittadini alle votazioni o, in tutto o in parte, a particolari consultazioni), e sono verificabili da ogni cittadino entro quindici giorni dal deposito in cancelleria, solo per il controllo sulla regolarità delle operazioni elettorali (art. 62 d.P.R. 16 maggio 1960 n. 570, recante il t.u. delle leggi per la composizione e l'elezione degli organi delle amministrazioni comunali, applicabile anche alle elezioni regionali ex art. 1, comma 6, l. 17 febbraio 1968, n. 108). A tali liste non è applicabile né la disciplina di cui al citato art. 51 del d.P.R. n. 223/1967, né il diritto di accesso riconosciuto ai titolari di cariche elettive ai fini dell'espletamento del relativo mandato;

3) dati annotati da scrutatori e rappresentanti di lista

Scrutatori e rappresentanti di lista, nell'esercitare funzioni affidate o consentite dalla legge e connesse al regolare svolgimento delle operazioni di voto, possono venire a conoscenza di dati anche sensibili (quali quelli relativi a coloro che hanno votato o meno presso una determinata sezione), da trattare con ogni opportuna cautela anche a garanzia della libertà e segretezza del voto, soprattutto nei casi in cui (come i referendum abrogativi o le votazioni di ballottaggio) la partecipazione al voto o l'astensione può evidenziare di per sé una particolare opzione politica. In particolare, tali soggetti non possono compilare elenchi di persone astenutesi dal voto, specie al fine di invitarle a votare in successivi appuntamenti elettorali;

4) schedari istituiti presso gli uffici consolari

Ai dati anagrafici dei cittadini iscritti negli schedari istituiti presso gli uffici consolari ai sensi dell'art. 67 del d.P.R. n. 200/1967, possono ritenersi applicabili le disposizioni sul rilascio degli atti anagrafici, che prevedono la possibilità di rilasciare elenchi degli iscritti nell'anagrafe della popolazione residente unicamente alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità.

3. CASI EQUIPARATI AI REGISTRI PUBBLICI: ELENCHI TELEFONICI

La disciplina degli elenchi telefonici, cartacei ed elettronici, è stata oggetto di recenti modifiche che hanno mutato in radice la loro natura in attuazione di norme comunitarie.

Il nuovo regime sarà attuato prevedibilmente nella seconda metà del 2004 e la propaganda sarà possibile in futuro solo nei confronti di chi vi acconsenta.

Nel frattempo, gli elenchi della telefonia fissa (e non anche quelli della telefonia mobile) restano utilizzabili per la propaganda elettorale solo mediante invio di posta ordinaria o chiamate telefoniche effettuate da un operatore, a meno che gli interessati si siano opposti (cfr. art. 55 e 75 d.lg. 1 agosto 2003, n. 259).

4. PROPAGANDA LECITA CON IL CONSENSO

Fuori dei predetti casi, benché la propaganda elettorale abbia una sua specificità rispetto alla comunicazione commerciale e di *marketing*, non è possibile effettuarla senza un consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente l'utilizzo dei dati a tale fine (e sia espresso in forma scritta se, come si vedrà, i dati hanno natura sensibile), in particolare quando si ricorre ai seguenti mezzi:

a) invio di fax;

b) invio di messaggi *Sms* e *Mms*;
c) chiamate telefoniche senza l'intervento di un operatore.
Ci si riferisce all'utilizzo di sistemi automatizzati che effettuano chiamate vocali preregistrate senza l'intervento, caso per caso, di un operatore;
d) chiamate di ogni tipo a terminali di telefonia mobile.

Il regime transitorio menzionato per la telefonia fissa non riguarda la telefonia mobile.

Senza il consenso preventivo e informato dell'abbonato, o del reale ed unico utilizzatore della scheda di traffico prepagato, non è lecito effettuare chiamate vocali di propaganda a terminali mobili, automatizzate e non, o inviare -anche in questo caso- messaggi *Sms* o *Mms* anche tramite siti *web*.

La volontà dell'interessato deve essere manifestata prima della chiamata o del messaggio e non può essere elusa inviando senza consenso un primo messaggio con il quale si chieda di aderire all'invio di ulteriori messaggi di propaganda.

Il consenso deve essere espresso in forma chiara (specificando la finalità di propaganda specie quando è richiesto con una formula ampia, riferita anche a scopi commerciali e di *marketing*) e "positiva" (anziché con una modalità di silenzio-assenso);

e) indirizzi di posta elettronica.

Gli indirizzi di posta elettronica recano dati personali che non rientrano tra le fonti "pubbliche" liberamente accessibili da chiunque e sono utilizzabili solo sulla base di un libero consenso (artt. 24 e 130 d.lg. n. 196/2003; v. Provv. del Garante 29 maggio 2003 sul c.d. *spamming*, in *www.garanteprivacy.it*).

Il consenso è necessario anche quando gli indirizzi o altri dati personali:
- sono ricavati da pagine *web*;
- sono formati ed utilizzati automaticamente con un *sofiware* senza l'intervento di un operatore, oppure in mancanza di una verifica della loro attuale attivazione o dell'identità del destinatario;
- quando gli indirizzi non sono registrati dopo l'invio dei messaggi.

La circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi di qualunque genere.

Il principio del consenso si applica anche per:
- i dati di utenti che prendono parte a forum o *newsgroup*, resi conoscibili in Internet per partecipare ad una determinata discussione e che non sono utilizzabili per fini diversi senza un consenso specifico (art. 11, comma 1, lettere a) e b), d.lg. n. 196/2003);
- gli indirizzi compresi nella lista "anagrafica" di abbonati ad un Internet provider, o pubblicati su siti *web* per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale od associativa;
- comunicazioni inviate a gestori anche privati di siti web utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio;

f) iscritti ad associazioni politiche o a partiti.

L'utilizzazione da parte di partiti o associazioni politiche di dati relativi a loro iscritti, a simpatizzanti o a partecipanti ad iniziative politiche in occasione delle quali si raccolgano informazioni sul loro conto (come pure di dati acquisiti sottoscrivendo petizioni, proposte di legge, richieste di referendum o raccolte di firme), comporta un trattamento di dati personali "sensibili".

In questi casi il consenso specifico deve essere manifestato per iscritto.

Quando il consenso è raccolto all'atto di adesione all'organizzazione, occorre un'idonea informativa collegata ad un chiaro contesto interno risultante dallo statuto o da altri atti dell'organizzazione noti agli interessati (v. comunicato stampa del Garante del 16 ottobre 1997, in *Bollettino* n. 2, p. 82). Particolare attenzione va prestata poi alla chiarezza dell'informativa e alla formula di consenso presenti su siti *web* che raccolgano dati sensibili di aderenti o simpatizzanti anche ai fini dell'invio di *newsletter* a contenuto politico.

Se i dati sono acquisiti nell'ambito di altri eventi politici, l'informativa deve evidenziare parimenti con chiarezza l'utilizzazione dei dati che si prevede in aggiunta alle finalità perseguite in via principale (ad esempio, nel caso in cui si intenda comunicare i dati a singoli candidati o a comitati elettorali delle medesime formazioni politiche).

Ogni eventuale comunicazione ad altri soggetti (organizzazioni di simpatizzanti, enti, associazioni, società e persone fisiche non direttamente connesse all'attività del titolare del trattamento), indipendente ed ulteriore rispetto alle finalità della raccolta dei dati, deve essere basata su un consenso distinto da quello previsto per il predetto trattamento "principale";

g) utenti o aderenti a organizzazioni non politiche.

Quando si presta un'attività (ad esempio, assicurativa) o un servizio (ad esempio, presso una casa di cura) o si svolge un'attività associativa no-profit a scopo diverso da quello politico, non è lecito utilizzare indirizzari o altri dati personali per propagandare candidati interni alla società, all'ente o all'associazione o da questi sostenuti (v. Provv. Garante del 5 ottobre 1999 e del 9 ottobre 2000, in Bollettino n. 14/15, p. 17 s.).

L'utilizzazione a fini di propaganda dei dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politica, è possibile solo quando ricorrono le seguenti condizioni:

- venga disposta legittimamente in base all'ordinamento interno;
- le modalità di utilizzo dei dati a fini di propaganda siano compatibili con gli scopi principali perseguiti dall'associazione o altro organismo;
- sia prevista specificamente nell'informativa resa agli iscritti al momento dell'adesione o del suo rinnovo.

5. DATI ACQUISITI NELL'ESERCIZIO DI UN MANDATO

I titolari di alcune cariche elettive, nel corso del mandato e sulla base di specifiche disposizioni volte a favorire il suo pieno esercizio, possono venire lecitamente a conoscenza di dati personali (cfr., ad esempio, art. 37 d.lg. 18 agosto 2000, n. 267; cfr. anche parere del 20 maggio 1998, in Bollettino n. 4, pag. 7 s. e del 7 marzo 2001, in Bollettino n. 18, p. 24) da utilizzare, anche a fini di trasparenza e buon andamento, per scopi pertinenti all'esercizio del mandato che possono rendere legittimo anche un eventuale contatto con gli interessati.

È in questo quadro illegittima l'eventuale richiesta di ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intete basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per la propaganda anche dopo la scadenza dal mandato.

Possono al contrario essere utilizzati i dati personali raccolti direttamente dal titolare della carica elettiva, nel quadro delle relazioni interpersonali con cittadini ed elettori.

6. USO DI DATI RACCOLTI DA TERZI

Diversi interessati divengono consapevoli solo a seguito di una loro contestazione che il consenso espresso in precedenza in modo generico è stato utilizzato anche per attività di propaganda elettorale.

Il candidato o l'organismo politico, quando acquisisce i dati da un privato che li ha raccolti in base a formule di consenso vaghe, riferite a scopi di vario tipo non meglio precisati (spesso, prevalentemente di tipo commerciale), ha l'onere di verificare in modo adeguato –anche con modalità a campione e avvalendosi della figura del mandatario elettorale: cfr. art. 7 l. 10 dicem-

bre 1993, n. 515– che gli interessati siano stati informati in modo specifico e abbiano prestato un consenso idoneo, che è validamente espresso solo se è manifestato "specificamente in riferimento ad un trattamento chiaramente individuato ... e se sono state rese all'interessato le informazioni di cui all'articolo 13" del Codice (art. 23, comma 3, d.lg. n. 196/2003).

Tale consenso deve essere manifestato liberamente, in forma differenziata rispetto alla prestazione di beni e servizi, in modo esplicito e documentato per iscritto: altrimenti, il trattamento è illecito e i dati sono inutilizzabili (art. 11, comma 2, d.lg. n. 196/2003).

Sull'organismo politico o candidato grava altresì l'onere di verificare –anche avvalendosi del predetto mandatario– che l'informativa sia fornita in caso di servizi di propaganda curati da terzi che inviino lettere o messaggi di propaganda utilizzando fonti conoscitive accessibili a chiunque.

7. INFORMATIVA AGLI INTERESSATI

Chi effettua attività di propaganda elettorale, anche se utilizza dati "pubblici" nel senso proprio del termine, deve fornire agli interessati la prevista informativa (art. 13 d.lg. n. 196/2003).

Si può adempiere a tale obbligo anche attraverso un'informazione sintetica, ma efficace, ed utilizzando, a titolo esemplificativo, una formula di tenore analogo al seguente:

"I dati che ci ha fornito liberamente (oppure: che sono stati estratti da ...) sono utilizzati da ... solo a fini di propaganda elettorale, anche con strumenti informatici, e non saranno comunicati a terzi (eventuale: salvo che all'organizzazione che cura le spedizioni). Può in ogni momento accedere ai dati, opporsi al loro trattamento o chiedere di integrarli, rettificarli o cancellarli, rivolgendosi a ... (indicare almeno un responsabile del trattamento, se è stato designato)".

Questa informativa deve essere inserita nel materiale di propaganda caratterizzato da lettere o da messaggi di posta elettronica.

Analoghe formule sintetiche possono essere utilizzate in caso di chiamate a numeri estratti da elenchi telefonici, fornendo all'inizio della conversazione un'informativa che indichi subito chi effettua la propaganda, la finalità della chiamata e i diritti del ricevente.

Chi effettua propaganda, qualora non ritenga di inviare il predetto materiale potrebbe:
- estrarre i dati da pubblici registri, elenchi, atti o altri documenti conoscibili da chiunque senza contattare tutti gli interessati;
- oppure, potrebbe inviare materiale propagandistico di dimensioni ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non permetta di inserire efficacemente un'idonea informativa anche di tenore sintetico.

Limitatamente a questi ultimi due casi, il Garante ritiene proporzionato rispetto ai diritti degli interessati sollevare il soggetto che utilizza i dati per esclusivi fini di propaganda elettorale dall'obbligo di fornire l'informativa. Ciò solo per le consultazioni della primavera del 2004 conformemente a quanto già provveduto con il provvedimento del 7 febbraio 2001 (in Gazzetta Ufficiale n. 36 del 13 febbraio 2001, p. 65).

Questa misura evita anche 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 nella campagna elettorale e che utilizzano le medesime fonti conoscitive, in particolare le liste elettorali comunali.

La disciplina applicabile (art. 13, commi 4 e 5, lett. c), d.lg. n. 196/2003) affida al Garante il compito di verificare se l'informativa comporti un impiego di mezzi sproporzionato rispetto al diritto tutelato, considerata la possibilità di prescrivere altre misure appropriate. La manifesta sproporzione può ravvisarsi caso per caso o in relazione a settori generali o tipi di trattamento.

Nel caso dell'attività di propaganda elettorale oggetto del presente provvedimento, l'integrale adempimento agli obblighi di informativa agli interessati può essere considerato sproporzionato rispetto al diritto tutelato, quando la persona cui si riferiscono i dati estratti da fonti pubbliche accessibili a chiunque non è contattata da chi utilizza i dati, oppure riceve materiale di propaganda che non permette un agevole inserimento dell'informativa.

Nel caso in cui, invece, l'interessato è contattato mediante l'invio di lettere, oppure di messaggi per posta elettronica, l'informativa – secondo la predetta formula – può essere inserita nella lettera o nel messaggio, anziché essere inviata all'atto della registrazione "interna" dei dati.

Resta fermo l'obbligo di informativa nel caso in cui i dati siano acquisiti direttamente presso l'interessato, anziché da fonti pubbliche conoscibili da chiunque.

8. MISURE DI SICUREZZA ED ALTRI ADEMPIMENTI

Ciascun partito, movimento o comitato elettorale, nonostante non debba notificare al Garante il trattamento dei dati (cfr. artt. 37 e 38 d.lg. n. 196/2003), è tenuto, oltre che agli adempimenti di cui agli artt. 29 e 30 del Codice in ordine all'individuazione e alla designazione degli incaricati del trattamento e degli eventuali responsabili, ad adottare idonee misure di sicurezza per i trattamenti di dati cartacei e automatizzati e, comunque, quelle "minime" (artt. 31, 33, 34, 35 e allegato B) d.lg. n. 196/2003).

Restano ferme le specifiche prescrizioni che limitano la propaganda elettorale per talune consultazioni dopo la chiusura della campagna elettorale (v., ad esempio, art. 2 l. n. 515/1993).

9. GARANZIE PER GLI INTERESSATI

La possibilità che l'interessato non debba acconsentire all'uso dei dati per finalità di propaganda elettorale, o possa non ricevere alle condizioni sopra indicate un'apposita informativa, non lo priva delle garanzie previste dal Codice come quella di chiedere al titolare del trattamento se vi sono dati che lo riguardano, di conoscerne il contenuto in modo intelligibile, l'origine, ecc.

L'interessato può opporsi in ogni momento al trattamento dei dati e, in particolare, alla propaganda, anche quando abbia manifestato un consenso.

Tali richieste obbligano i titolari del trattamento a darvi riscontro e, in caso di opposizione, a non recapitare più all'opponente ulteriori messaggi anche in occasione di successive campagne.

Qualora il titolare di trattamento non fornisca un riscontro idoneo ad una richiesta di esercizio dei diritti di cui al predetto art. 7, l'interessato può rivolgersi all'autorità giudiziaria o presentare un reclamo o un ricorso al Garante con le modalità previste dagli artt. 142 s. del d.lg. n. 196/2003.

10. USO DEI DATI DECORSO IL PERIODO DI ESONERO

Decorsa la data del 30 giugno 2004, partiti, movimenti politici, comitati promotori, sostenitori e candidati potranno continuare a trattare (anche mediante mera conservazione) i dati estratti da fonti pubbliche accessibili a chiunque per finalità di propaganda elettorale o di connessa comunicazione politica, solo se informeranno gli interessati entro il 30 settembre 2004 nei modi previsti dall'art. 13 del Codice. Diversamente, i dati dovranno essere cancellati o distrutti non oltre la medesima data. Tali considerazioni non riguardano dati per i quali gli interessati siano stati invece informati nei termini sopra indicati.

TUTTO CIÒ PREMESSO IL GARANTE:

a) segnalaai titolari di trattamento interessati, ai sensi dell'art. 154, comma 1, lett. c), del d.lg. n. 196/2003, la necessità di conformare il trattamento ai principi richiamati nel presente provvedimento;
b) ai sensi dell'art. 13, comma 5, del d.lg. n. 196/2003, 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 del primo semestre del 2004, possano astenersi dall'informare gli interessati alle condizioni indicate in motivazione;
c) dispone che il presente provvedimento sia pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 12 febbraio 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello
Paissan

IL SEGRETARIO GENERALE
Buttarelli

39 Casi da sottrarre all'obbligo di notificazione al Garante (*)

Registro delle Deliberazioni
n. 1 del 31 marzo 2004

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza 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. 37, commi 1 e 2, del d.lg. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

RILEVATO che tale Codice indica i trattamenti di dati da notificare al Garante e demanda a questa Autorità il compito di individuare, tra essi, quelli sottratti all'obbligo di notificazione purché non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle modalità di trattamento o della natura dei dati (art. 37, comma 1);

RILEVATO che il medesimo Codice demanda altresì al Garante il compito di individuare ulteriori trattamenti in aggiunta a quelli elencati nella predetta disposizione;

VISTA la documentazione in atti;

RILEVATO in sede di prima applicazione del Codice che taluni trattamenti sono effettuati con modalità che permettono, allo stato, di sottrarli all'obbligo di notificazione, ferma restando l'osservanza degli ulteriori principi ed obblighi previsti dal Codice in materia di protezione dei dati personali;

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

RELATORE il prof. Stefano Rodotà;

DELIBERA:

A) di sottrarre all'obbligo di notificazione al Garante, tra i casi previsti dall'art. 37, comma 1, del d.lg. 30 giugno 2003, n. 196:

1) con riferimento ai casi di cui al comma 1, lett. a) di tale disposizione:

a) i trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica. Ciò limitatamente ai dati e alle operazioni, compresa la comunicazione, indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;

b) i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla legge n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria. Ciò sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

c) i trattamenti di dati che indicano la posizione geografica di mezzi di tra-

(*) *G.U.* 6 aprile 2004, n. 81.

sporto aereo, navale e terrestre, effettuati esclusivamente a fini di sicurezza del trasporto;

2) con riferimento ai casi di cui al comma 1, lett. b) della medesima disposizione, i trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti:
   a) a fini di procreazione assistita, di trapianto di organi e tessuti, indagine epidemiologica, rilevazione di malattie mentali, infettive, diffusive o di sieropositività. Ciò sempre che i trattamenti siano effettuati non sistematicamente, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica e limitatamente ai dati e alle operazioni indispensabili per la tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;
   b) ad esclusivi fini di monitoraggio della spesa sanitaria o di adempimento di obblighi normativi in materia di igiene e sicurezza del lavoro e della popolazione;
3) con riferimento ai casi di cui al comma 1, lett. c), i trattamenti di dati idonei a rivelare la sfera psichica di lavoratori:
   a) effettuati da associazioni, enti od organismi a carattere sindacale per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di rapporto di lavoro o di previdenza, anche in tema di diritto al lavoro dei disabili;
   b) effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico o religioso riguardo a dati di propri dipendenti o collaboratori, per adempiere esclusivamente a specifici obblighi previsti dalla normativa in materia di rapporto di lavoro o di previdenza;
4) con riferimento ai casi di cui al comma 1, lett. d), i trattamenti di dati personali:
   a) che non siano fondati unicamente su un trattamento automatizzato volto a definire profili professionali, effettuati per esclusive finalità di occupazione o di gestione del rapporto di lavoro, fuori dei casi di cui alla lettera e) del medesimo art. 37, comma 1;
   b) che non siano fondati unicamente su un trattamento automatizzato volto a definire il profilo di un investitore, effettuati esclusivamente per adempiere a specifici obblighi previsti dalla normativa in materia di intermediazione finanziaria;
   c) relativi all'utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet;
5) con riferimento ai casi di cui al comma 1, lett. e), i trattamenti di dati sensibili effettuati:
   a) al solo fine di selezione di personale per conto esclusivamente di soggetti appartenenti al medesimo gruppo bancario o societario;
   b) da soggetti pubblici per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di occupazione e mercato del lavoro;
   c) da associazioni o organizzazioni di categoria al solo fine di svolgere ricerche campionarie relativamente a dati riguardanti l'adesione alla medesima associazione o organizzazione;
6) con riferimento ai casi di cui al comma 1, lett. f), i trattamenti di dati personali:
   a) effettuati da soggetti pubblici per la tenuta di pubblici registri o elenchi conoscibili da chiunque;
   b) registrati in banche di dati utilizzate in rapporti con l'interessato di fornitura di beni, prestazioni o servizi, o per adempimenti contabili o fiscali, anche in caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato;
   c) registrati in banche di dati utilizzate da soggetti pubblici o privati per adempiere esclusivamente ad obblighi normativi in materia di rapporto di

lavoro, previdenza o assistenza;

d) registrati in banche di dati utilizzate da soggetti pubblici al solo fine della tenuta ed esecuzione di atti, provvedimenti e documenti, in tema di riscossione di tributi, applicazione di sanzioni amministrative, o rilascio di licenze, concessioni o autorizzazioni;

e) relativi a immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio;

f) trattati, in base alla legge, dai soggetti autorizzati in relazione alle operazioni e ai dati necessari all'esclusivo fine di prestare l'attività di garanzia collettiva dei fidi e i servizi a essa connessi o strumentali ("confidi");

B) di inviare copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 31 marzo 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

40 Sistemi di informazioni creditizie e bilanciamento di interessi (*)

Registro delle Deliberazioni
n. 9 del 16 novembre 2004

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza 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 il provvedimento adottato in data odierna da questa Autorità con il quale il Garante ha verificato la conformità alle leggi e ai regolamenti ed ha disposto la pubblicazione sulla Gazzetta ufficiale del codice di deontologia e di buona condotta sottoscritto in tema di sistemi informativi di cui sono titolari soggetti privati, utilizzati per la concessione di credito al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti (art. 20, comma 2, lett. e), d.lg. n. 467/2001; art. 117 del Codice in materia di protezione dei dati personali);

VISTI i precedenti provvedimenti adottati al riguardo dal Garante il 10 aprile 2002 (in Gazzetta ufficiale 8 maggio 2002, n. 106) e il 31 luglio 2002 (in Bollettino del Garante n. 30/2002, p. 47) e ritenuta la necessità che questa Autorità, anche in relazione agli elementi acquisiti durante i lavori propedeutici alla sottoscrizione del predetto codice di deontologia e di buona condotta, indichi in materia modalità di attuazione idonee ed efficaci delle disposizioni del Codice sui presupposti di liceità del trattamento;

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

Relatore il prof. Gaetano Rasi;

PREMESSO:

1. SISTEMI DI INFORMAZIONI CREDITIZIE

I sistemi informativi gestiti da soggetti privati ai fini della concessione di crediti al consumo o della valutazione dell'affidabilità dei richiedenti e della puntualità nei pagamenti non sono attualmente oggetto di specifica normativa, a differenza di quanto avviene per:

- servizi o sistemi centralizzati di rilevazione dei rischi creditizi, prevalentemente di rilevante importo, istituiti in base al testo unico delle leggi in materia bancaria e creditizia con deliberazioni del Cicr, regolati da istruzioni della Banca d'Italia e sottoposti alla relativa vigilanza;
- altri registri, banche di dati e archivi pubblici conoscibili da chiunque, utilizzati anche ai fini della concessione di crediti e disciplinati con specifiche normative (es.: registro informatico dei protesti, conservatorie dei registri immobiliari, ecc.).

In Italia, i sistemi informativi gestiti da privati si sono sviluppati prima dell'introduzione della normativa sulla protezione dei dati personali, in assenza di regole e di criteri comuni ed in forme diverse. Ciò, è avvenuto nell'ambito di associazioni o consorzi di operatori finanziari o di attività o servizi a pagamento svolti su iniziativa di società specializzate, in genere sulla base di accordi o contratti tra i gestori dei sistemi e i privati che vi partecipano.

Tali sistemi sono utilizzati da operatori del settore creditizio e finanziario -banche ed

(*) *G.U.* 23 dicembre 2004, n. 300.

intermediari finanziari come, ad esempio, le società finanziarie e di *leasing* finanziario- per condividere e scambiare informazioni su finanziamenti anche di contenuto importo e su pagamenti ratei. I fini perseguiti sono quelli di tutela del credito e di contenimento dei relativi rischi, in relazione anche alla necessità di accrescere la stabilità del sistema bancario e finanziario e all'esigenza rappresentata nel settore volta a sviluppare le attività produttive attraverso il sostegno della domanda di beni di consumo e di servizi (con particolare riferimento a contesti come quello del credito al consumo, presi in considerazione solo indirettamente o parzialmente nell'ambito delle "centrali rischi" di natura pubblica disciplinate, come detto, a livello normativo).

I sistemi privati in esame, già correntemente denominati come "centrali rischi" private, sono stati ora disciplinati dal previsto codice di deontologia e di buona condotta che li ha anche definiti come "sistemi di informazioni creditizie".

2. CONSENSO ED ALTRI PRESUPPOSTI DI LICEITÀ DEL TRATTAMENTO

Con riferimento al trattamento dei dati personali, inclusi quelli relativi allo svolgimento "positivo" dei rapporti di credito, i soggetti privati che gestiscono i predetti sistemi informativi devono acquisire, per l'eventuale tramite degli organismi partecipanti, il consenso libero ed informato degli interessati, espresso specificamente in rapporto ai vari trattamenti, in conformità a quanto stabilito dal Codice (art. 23) e dal predetto codice di deontologia e buona condotta.

Nel quadro di un elevato livello di garanzie per gli interessati (art. 2 del Codice), va garantito agli stessi il diritto di decidere consapevolmente se i propri dati possano essere registrati nei predetti sistemi informativi (allo scopo, ad esempio, di rendere più agevole il rilascio di futuri finanziamenti), senza condizionamenti anche di fatto o timori che tale determinazione si ripercuota negativamente sui propri rapporti, attuali o futuri, con gli operatori finanziari.

In alternativa al consenso, il titolare del trattamento di dati effettuato ai fini della concessione di credito al consumo, della valutazione dell'affidabilità dei richiedenti e della puntualità nei pagamenti, può già ora avvalersi, in alcuni casi, di altri presupposti di liceità previsti dal Codice. Ciò, quando il medesimo trattamento:

a) è necessario per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato (ad esempio, per istruire una richiesta di finanziamento rivolta alla banca o alla società finanziaria: art. 24, comma 1, lett. b), del Codice);
b) riguarda dati relativi allo svolgimento di attività economiche da parte di società, imprenditori individuali e liberi professionisti, rispettando i limiti richiamati dal Codice (art. 24, comma 1, lett. d);
c) è necessario per finalità di difesa giudiziaria e per il tempo a ciò strettamente necessario, nonché in relazione a richieste degli interessati o di competenti autorità pubbliche, nei casi previsti dalla legge (art. 24, comma 1, lettere a) e f);
d) riguarda dati anonimi trattati per finalità statistiche, per i quali il Codice non è applicabile.

Tali presupposti sono utilizzabili dagli operatori entro i predetti ambiti limitati. Risulta quindi necessario verificare se, in vista della prossima applicazione del codice di deontologia e di buona condotta, il trattamento di determinati dati personali relativi a ritardati o mancati pagamenti effettuati nell'ambito dei predetti sistemi informativi privati possa essere basato su un ulteriore presupposto di liceità, utilizzabile anch'esso dagli operatori in alternativa al consenso libero, espresso e documentato degli interessati (art. 23 del Codice).

Un'idonea alternativa al consenso va ravvisata nell'istituto del bilanciamento di interessi, che il Codice ha confermato nel nostro ordinamento apportandovi un'opportuna integrazione sulla base dell'esperienza (art. 24, comma 1, lett. *g*).

Il presente provvedimento intende dare attuazione a tale istituto, individuando, sulla base dei principi stabiliti dall'art. 11 del Codice, i casi in cui il trattamento di alcuni dati personali relativi ai predetti rapporti di credito potrà avvenire, nell'ambito dei già menzio-

nati sistemi informativi, anche senza il consenso degli interessati, al solo fine di perseguire i legittimi interessi del titolare o dei terzi destinatari dei dati e con le modalità stabilite dal presente provvedimento e dal predetto codice di deontologia e di buona condotta.

3. DIRITTI DELLE PERSONE E LEGITTIMI INTERESSI DEL SETTORE CREDITIZIO E FINANZIARIO

Nel procedere a tale attuazione, va rilevato che i complessi trattamenti di dati personali effettuati negli ambiti sopra descritti presentano alcuni rischi per i diritti e le libertà fondamentali degli interessati, potendo spiegare effetti negativi per la vita privata, per il legittimo accesso all'acquisto di beni e alla fruizione di servizi, nonché, più in generale, per la dignità e la reputazione, per le loro relazioni sociali o professionali e per l'iniziativa privata.

Considerato il rilevante impatto che i sistemi privati di informazioni creditizie spiega nei rapporti produttivi e commerciali attraverso le valutazioni effettuate per la concessione di crediti al consumo o nella valutazione dell'affidabilità dei richiedenti e della puntualità nei pagamenti, occorre evitare duplicazioni e sovrapposizioni di basi informative e la proliferazione di banche di dati plurisettoriali, centralizzate o interconnesse, con un eccesso di informazioni rivolte a vari scopi, che riguardano un numero elevato di persone e che possono risultare particolarmente invasive a causa dei diversi incroci di dati possibili.

Per altro verso, va constatato che l'acquisizione e lo scambio di informazioni significative relative a ritardati o mancati pagamenti di crediti al consumo, anche attraverso sistemi informativi gestiti da privati, possono risultare rilevanti per la corretta valutazione del merito creditizio e della situazione finanziaria dei richiedenti da parte di banche, società finanziarie e altri intermediari (tenuti ad assicurare una sana e prudente gestione dei finanziamenti) o per contenere eccessivi indebitamenti degli interessati e sovraesposizioni rispetto ai redditi dei debitori, nonché per prevenire artifizi e raggiri.

4. BILANCIAMENTO DEGLI INTERESSI IN CASO DI TRATTAMENTO DI DATI RELATIVI AD INFORMAZIONI DI TIPO NEGATIVO

Una conoscenza più agevole delle informazioni appena indicate può risultare quindi particolarmente utile per le valutazioni che gli operatori del settore effettuano per concedere crediti o finanziamenti. Resta ferma la necessità che i dati siano trattati nei predetti sistemi solo per i periodi specificati nel citato codice di deontologia e di buona condotta, tenendo conto di vari fattori (evoluzione del settore; funzioni dei menzionati sistemi informativi; corrispondenti tempi di conservazione previsti per altre rilevazioni di rischi creditizi disciplinate e sottoposte alla vigilanza della Banca d'Italia; termini attualmente previsti per conservare i dati riferiti a comportamenti debitori, registrati presso diversi archivi pubblici per finalità diverse da quelle proprie del rischio creditizio, termini di cui è prevista a breve l'armonizzazione in attuazione dell'art. 119 del Codice).

In base ai richiamati principi di pertinenza, completezza e non eccedenza dei dati, e tenuto conto del nuovo quadro di regole e garanzie introdotto dal codice di deontologia e buona condotta, il Garante ritiene di poter individuare come necessari per perseguire i legittimi interessi dei titolari del trattamento effettuato nell'ambito dei menzionati sistemi informativi, i trattamenti di dati personali relativi a:

a) ritardi nel pagamento di un credito, dati che possono essere conservati nei predetti sistemi, in caso di ritardi pari a due rate o mesi, per dodici mesi dalla data di registrazione dei dati relativi alla loro regolarizzazione e, in caso di ritardi di entità superiore, per ventiquattro mesi dalla data medesima;
b) rapporti di credito per i quali si sono verificati ritardi o inadempimenti non successivamente regolarizzati, dati che possono essere conservati nei predetti sistemi per 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. In quest'ultimo caso, tenendo conto del requisito della completezza dei dati in rapporto alle finalità perseguite (art. 11, comma 1, lett. d), del Codice), possono essere conservati ulteriormente anche i dati personali relativi ad informazioni creditizie di tipo positivo eventualmente presenti nel

sistema informativo, anche se riferiti ad altri rapporti di credito riguardanti il medesimo interessato.

Nei casi individuati nel presente punto 4, il trattamento dei dati personali appena indicati è pertanto lecito per le finalità menzionate anche in assenza del consenso degli interessati, ai sensi dell'art. 24, comma 1, lett. g), del Codice, con effetto dal 1° gennaio 2005, data in cui il predetto codice di deontologia e buona condotta entrerà in vigore.

La presente decisione riguarda solo i soggetti definiti come "gestore" o "partecipante" nell'art. 1 del predetto codice di deontologia e buona condotta.

PER QUESTI MOTIVI, IL GARANTE:

1) individua nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. g), del Codice, i casi nei quali il trattamento dei dati personali nell'ambito dei sistemi informativi oggetto del codice di deontologia e di buona condotta di cui in motivazione, può essere effettuato dai gestori e dai partecipanti a tali sistemi nei limiti e alle condizioni sopra indicate, al solo fine di perseguire i predetti legittimi interessi e senza richiedere il consenso degli interessati;
2) dispone infine che il presente provvedimento sia pubblicato sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 16 novembre 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

41 Contributo spese in caso di esercizio dei diritti dell'interessato

Registro delle Deliberazioni
n. 14 del 23 dicembre 2004

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza 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. 12, lett. *a*), della direttiva europea n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui l'esercizio del diritto di accesso dell'interessato ai dati personali che lo riguardano e a talune informazioni sul loro trattamento deve essere garantito liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi;

VISTO l'art. 8 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;

VISTI gli articoli da 7 a 10 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) in tema di esercizio dei diritti dell'interessato e, in particolare, di esercizio del diritto di accesso;

RILEVATO che il principio introdotto dalla previgente disciplina (art. 13, comma 2, legge n. 675/1996; art. 17, commi 7 e 8, d.P.R. 31 marzo 1998, n. 501) e confermato dal Codice è quello della tendenziale gratuità dell'esercizio del diritto di accesso, trattandosi appunto di un diritto e non di richiesta di prestazione dietro corrispettivo;

VISTO l'art. 10, commi 7 e 8, del Codice in riferimento all'articolo 7, commi 1 e 2, lettere *a*), *b*) e *c*), secondo cui si può eventualmente chiedere all'interessato un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata in ciascun caso specifico, anziché la copertura di tutti gli eventuali costi derivanti dall'esercizio del diritto, solo a seguito di alcune richieste (richiesta di conferma dell'esistenza o meno di dati personali che riguardano l'interessato, oppure dell'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento o della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici);

CONSIDERATO che il predetto contributo spese può essere chiesto quando non risulta confermata l'esistenza di dati che riguardano l'interessato e che il medesimo contributo, oltre a non poter eccedere i costi effettivamente sopportati per la ricerca effettuata nel caso specifico, non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale; rilevato che il Garante può individuare l'importo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente;

RILEVATO che l'esistenza di dati che riguardano l'interessato deve intendersi confermata, agli effetti dell'applicazione del presente provvedimento, anche quando i dati cancellati o non più reperibili risultino, comunque, essere stati trattati in precedenza;

CONSIDERATO che, se risulta confermata l'esistenza di dati, può essere chiesto un contributo spese quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione;

RITENUTA la necessità di determinare in termini generali la predetta misura del contributo spese relativamente ai menzionati casi di esercizio del diritto di accesso ai dati personali o a talune informazioni;

CONSIDERATO ALTRESÌ:

1. Casi considerati di esercizio dei diritti

Il presente provvedimento riguarda le seguenti istanze rivolte a qualunque titolare del trattamento pubblico o privato, in conformità al Codice (artt. 7, commi 1 e 2, lettere *a*), *b*) e *c*), 8 e 9):

- richiesta di ottenere conferma dell'esistenza di dati personali;
- richiesta di ottenere la comunicazione dei dati in forma intelligibile;
- richiesta di ottenere l'indicazione dell'origine dei dati;
- richiesta di conoscere le finalità del trattamento;
- richiesta di conoscere le modalità del trattamento;
- richiesta di conoscere la logica applicata al trattamento effettuato con l'ausilio di strumenti elettronici.

Il contributo spese in esame non si riferisce, quindi, all'esercizio di diritti dell'interessato diversi da quelli sopra specificamente indicati (ad esempio, non è ipotizzabile un contributo in caso di richiesta di rettificazione o di opposizione al trattamento).

Gli importi massimi del contributo spese qui previsti in base al Codice sono determinati tenendo conto della normativa comunitaria e internazionale, della corrispondente misura prevista anteriormente al Codice e della necessità di non rendere oneroso l'esercizio dei diritti dell'interessato.

Il principio generale resta, infatti, quello secondo cui l'esercizio del diritto di accesso ai dati che riguardano l'interessato è gratuito.

2. Casi in cui non risulta confermata l'esistenza di dati

In riferimento ai casi in cui non può ritenersi confermata l'esistenza dei dati, va nuovamente rilevato che il contributo spese non è integralmente compensativo di tutti gli eventuali costi di un riscontro.

Tale contributo, per disposizione di legge, non può in ogni caso eccedere i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

Ciò premesso, l'importo massimo che può essere richiesto è determinato dal Garante nella misura di euro dieci, in termini sostanzialmente corrispondenti all'importo già previsto direttamente dalla normativa previgente (L. 20.000; art. 17, comma 7, d.P.R. n. 501/1998).

Con riferimento al medesimo caso in cui non risulti confermata l'esistenza dei dati, lo stesso contributo è individuato forfettariamente in misura pari a euro 2,50, in relazione al caso in cui i dati siano trattati con strumenti elettronici e la risposta (negativa) sia fornita oralmente.

Il contributo spese di cui al presente punto 2 non può essere chiesto quando i dati, cancellati o comunque non reperibili, risultano essere stati comunque trattati in precedenza.

3. Casi in cui risulta confermata l'esistenza di dati

Negli altri casi in cui, a seguito di una richiesta dell'interessato, risulta invece confermata

l'esistenza di dati che lo riguardano, l'esercizio del diritto è gratuito, ma può essere chiesto un contributo spese in presenza di una richiesta di riprodurre uno speciale supporto su cui i dati personali figurano.

L'interessato può infatti richiedere specificamente la riproduzione di uno speciale supporto sul quale sono presenti già i dati personali (art. 10, comma 8).

Tale caso riguarda solo le richieste di comunicare i dati in forma intelligibile e non attiene, inoltre, alle richieste di trasporre i dati su supporti di uso più comune, come ordinari *floppy disk* o *cd-rom*, concernendo solo richieste attinenti a determinati supporti di maggior costo quali audiovisivi, lastre, nastri o altri specifici supporti magnetici.

In riferimento a questi casi, si deve ritenere legittima la richiesta, rivolta all'interessato, di contribuire alla particolare spesa necessaria per comunicare i dati, sempre che l'interessato medesimo abbia chiesto specificamente di ottenere in tale forma la comunicazione dei dati che lo riguardano.

Sulla base di una valutazione ponderata delle principali situazioni verificabili, e della circostanza che si tratta anche in questo caso di un contributo, va ritenuto congruo l'importo di euro 20,00.

Si tratta di un importo massimo in quanto, anche in questo caso, il contributo non può comunque eccedere i costi effettivamente sostenuti e documentabili nel caso specifico;

VISTI gli altri atti d'ufficio;

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:

determina gli importi relativi al contributo spese in caso di esercizio dei diritti dell'interessato nei termini di cui in motivazione e prescrive ai titolari del trattamento, ai sensi dell'art. 154, comma 1, lett. *c*), del Codice in materia di protezione dei dati personali di adottare le misure necessarie indicate nel presente provvedimento per rendere il trattamento conforme alle disposizioni vigenti.

Roma, 23 dicembre 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

Unione europea

42 Decisione della Commissione del 28 aprile 2004 sulla adeguata protezione dei dati personali nell'Isola di Man (*)

DECISIONE DELLA COMMISSIONE

del 28 aprile 2004

sulla adeguata protezione dei dati personali nell'Isola di Man

[*notificata con il numero C(2004) 1556*]

(Testo rilevante ai fini del SEE)

(2004/411/CE)

(*) G.U.C.E. 30 aprile 2004, L 151/50.

43 Decisione della Commissione del 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti *United States Bureau of Customs and Border Protection* (*)

Notificata con il numero C(2004) 1914
Testo rilevante ai fini del SEE
2004/535/CE

LA COMMISSIONE DELLE COMUNITÀ EUROPEE

visto il trattato che istituisce la Comunità europea,

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[1], in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) In virtù della direttiva 95/46/CE gli Stati membri dispongono che la trasmissione di dati personali ad un paese terzo possa aver luogo soltanto se il paese terzo di cui si tratta garantisce un livello di protezione adeguato e se le leggi nazionali di attuazione delle altre disposizioni della direttiva sono rispettate prima della trasmissione.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Sulla base di tale constatazione, dati personali possono essere trasmessi dagli Stati membri senza che sia necessaria alcuna garanzia supplementare.

(3) In virtù della direttiva 95/46/CE il livello di protezione dei dati è valutato con riguardo a tutte le circostanze relative ad una trasmissione o a una categoria di trasmissioni di dati e tenendo conto, in particolare, delle condizioni elencate all'articolo 25, paragrafo 2.

(4) Nell'ambito dei trasporti aerei, la scheda nominativa del passeggero (*Passenger Name Record*, nel prosieguo «PNR») è una scheda comprendente le informazioni relative al viaggio di ciascun passeggero. Essa contiene tutte le informazioni necessarie per consentire il trattamento e il controllo delle prenotazioni da parte delle compagnie aeree della prenotazione e delle compagnie aeree partecipanti. Ai fini della presente decisione i termini «passeggero» e «passeggeri» comprendono i membri dell'equipaggio. Per «compagnia aerea della prenotazione» s'intende la compagnia aerea presso la quale il passeggero ha fatto la sua prenotazione originale, o presso la quale delle prenotazioni addizionali sono state fatte dopo l'inizio del viaggio. Per «compagnie aeree partecipanti» s'intende qualsiasi compagnia aerea alla quale la compagnia aerea della prenotazione ha chiesto un posto per un passeggero su uno o vari voli.

(5) L'ufficio statunitense delle dogane e della protezione delle frontiere (United States

(*) *G.U.C.E.* 6 luglio 2004, L 235/11.
(1) *G.U.C.E.* 23 novembre 1995, L 281/ 31. Direttiva modificata da ultimo dal regolamento (CE) n. 1882/2003 (*G.U.C.E.* 31 ottobre 2003, L 284, p.1).

Bureau of Customs and Border Protection, nel prosieguo «CBP») del ministero della Sicurezza interna (Department of Homeland Security) richiede a ciascuna compagnia aerea che garantisce un servizio internazionale di trasporto di passeggeri con destinazione o in partenza dagli Stati Uniti di fornirgli un accesso elettronico ai dati PNR, nella misura in cui tali dati siano stati raccolti e memorizzati nei sistemi informatici di prenotazione della compagnia aerea.

(6) L'obbligo di trasmissione dei dati personali contenuti nei PNR dei passeggeri aerei al CBP si basa su una legge adottata dagli Stati Uniti nel novembre 2001[1], e su regolamenti di attuazione adottati dal CBP in base a tale legge[2].

(7) La legislazione statunitense in questione riguarda il rafforzamento della sicurezza, nonché le condizioni di ingresso negli Stati Uniti e di uscita dal paese. Si tratta di questioni su cui gli Stati Uniti hanno un potere di decisione nell'ambito della propria sovranità. Del resto tali esigenze non sono incompatibili con gli impegni internazionali che il paese ha contratto. Gli Stati Uniti sono un paese democratico, governato dal principio dello stato di diritto e dotato di una solida tradizione in materia di libertà civili. La legittimità del suo procedimento legislativo e la forza e l'indipendenza del suo apparato giudiziario non sono in discussione. La libertà di stampa costituisce un'ulteriore solida garanzia contro le violazioni delle libertà civili.

(8) La Comunità sostiene pienamente gli Stati Uniti nella loro lotta contro il terrorismo nei limiti imposti dal diritto comunitario. La legislazione comunitaria provvede a trovare l'equilibrio necessario tra le esigenze della sicurezza e il rispetto della vita privata. Ad esempio, l'articolo 13 della direttiva 95/46/CE consente agli Stati membri di adottare le misure legislative intese a limitare la portata degli obblighi e dei diritti previsti da tale direttiva, qualora tale restrizione sia giustificata dalla necessità di salvaguardare la sicurezza dello Stato, la difesa, la pubblica sicurezza, nonché la prevenzione, le indagini, l'accertamento e la punizione di reati.

(9) Le trasmissioni di dati riguardano dei responsabili specifici del trattamento, vale a dire le compagnie aeree che garantiscono i collegamenti tra la Comunità e gli Stati Uniti, e un solo destinatario negli Stati Uniti, vale a dire il CBP.

(10) Qualunque accordo volto a stabilire una disciplina normativa per le trasmissioni di PNR agli Stati Uniti, in particolare attraverso la presente decisione, deve essere limitato nel tempo. È stato concordato un periodo di tre anni e mezzo. Nel corso di tale lasso di tempo, il contesto può cambiare in modo radicale e la Comunità e gli Stati Uniti convengono che è necessaria una futura revisione degli accordi.

(11) Il trattamento da parte del CBP dei dati personali contenuti nei PNR dei passeggeri aerei che gli sono inviati è disciplinato dalle disposizioni che figurano nella «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» (nel prosieguo «la dichiarazione d'impegno») e dalla legislazione americana, alle condizioni previste dalla dichiarazione d'impegno.

(12) Per quanto riguarda la legislazione americana, la legge sulla libertà d'informazione (Freedom of Information Act) è rilevante nel contesto attuale nella misura in cui disciplina le condizioni alle quali il CBP può opporsi alle domande di trasmissioni di dati e trattare in tale modo i dati dei PNR in modo confidenziale. Detta legge disciplina inoltre la trasmissione dei PNR alle persone interessate, elemento che è strettamente collegato al diritto di accesso di cui esse dispongono. La legge sulla libertà d'informazione si applica senza distinzione ai cittadini americani e stranieri.

(13) Per quanto riguarda la dichiarazione d'impegno, e conformemente a quanto previsto al paragrafo 44, le disposizioni della dichiarazione sono state o saranno recepite da leggi, direttive o altri atti normativi negli Stati Uniti e hanno, pertanto, diversi gradi di efficacia giuridica. La dichiarazione d'impegno è pubblicata integralmente nel registro federale sotto la responsabilità del ministero della Sicurezza interna. Essa rappresenta indubbiamente un

(1) Titolo 49, United States Code, sezione 44909, lettera c), paragrafo 3.
(2) Titolo 19, Code of Federal Regulations, sezione 122.49, lettera b).

impegno politico serio e maturo da parte del ministero della Sicurezza interna e il suo rispetto è controllato congiuntamente dagli Stati Uniti e dalla Comunità. L'inadempimento può essere eventualmente fatto valere attraverso mezzi giuridici, amministrativi e politici e, se persistente, comporta la sospensione degli effetti della presente decisione.

(14) I criteri in virtù dei quali il CBP tratta i dati PNR dei passeggeri sulla base della legislazione americana e della dichiarazione d'impegno comprendono i principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche.

(15) Per quanto riguarda la limitazione delle trasmissioni di dati ad una finalità specifica, i dati personali dei passeggeri aerei contenuti nei PNR che sono trasmessi al CBP sono trattati per uno scopo specifico e sono utilizzati o comunicati ulteriormente soltanto nella misura in cui ciò non sia incompatibile con la finalità della trasmissione. In particolare, i dati dei PNR devono essere utilizzati al solo scopo di prevenire e di combattere il terrorismo e i reati collegati al terrorismo, altri reati gravi, compresa la criminalità organizzata transnazionale, la fuga in caso di mandato d'arresto emesso o di pena detentiva comminata per quei reati.

(16) Per quanto riguarda la qualità dei dati e il principio di proporzionalità, che devono essere considerati in rapporto agli importanti motivi d'interesse pubblico che giustificano la trasmissione dei dati dei PNR, i dati dei PNR non devono essere ulteriormente modificati dal CBP. Un massimo di trentaquattro categorie di dati PNR sono trasmesse e le autorità americane sono tenute a consultare la Commissione prima di aggiungere nuovi elementi. Ulteriori informazioni personali ricercate sulla base di quanto è stato direttamente ricavato dai dati PNR sono ottenute da fonti diverse da quelle governative soltanto mediante ricorso a mezzi legittimi. In linea generale, i PNR sono cancellati dopo un periodo massimo di tre anni e sei mesi, ad eccezione dei dati consultati nell'ambito di inchieste specifiche ovvero manualmente.

(17) Per quanto riguarda il principio di trasparenza, il CBP fornisce informazioni ai viaggiatori in merito alla finalità della trasmissione e del trattamento, nonché all'identità del responsabile del trattamento nel paese terzo, ed altre informazioni.

(18) Per quanto riguarda il principio di sicurezza, il CBP adotta le misure di sicurezza tecniche e organizzative adeguate al rischio presentato dal trattamento.

(19) Il diritto di accesso e di rettifica sono riconosciuti, in quanto le persone interessate possono chiedere una copia dei loro dati PNR, nonché una rettifica dei dati inesatti. Le eccezioni previste sono in linea di massima paragonabili alle restrizioni che possono essere imposte da uno Stato membro in forza dell'articolo 13 della direttiva 95/46/CE.

(20) Le trasmissioni successive di dati vengono effettuate, caso per caso, ad altre autorità governative, anche di altri paesi, incaricate della lotta contro il terrorismo o dell'applicazione della legge, per finalità corrispondenti a quelle stabilite nella dichiarazione di limitazione ad una finalità specifica. Le trasmissioni possono anche essere effettuate ai fini della protezione degli interessi vitali della persona interessata o di altre persone, in particolare nei casi di importanti rischi sanitari o nell'ambito di un procedimento penale o negli altri casi previsti dalla legge. Le autorità che ricevono i dati devono, in virtù delle condizioni esplicite di diffusione, impiegare i dati unicamente ai fini previsti e non possono procedere ad una trasmissione successiva senza l'accordo delle CBP. Nessun'altra autorità straniera, federale, statale o locale dispone di un accesso elettronico diretto ai dati del PNR attraverso le basi di dati del CBP. Il CBP si oppone alla divulgazione pubblica dei PNR sulla base delle deroghe previste dalle relative disposizioni della legge sulla libertà di informazione.

(21) Il CBP non utilizza i dati sensibili di cui all'articolo 8 della direttiva 95/46/CE e, in attesa della creazione di un sistema di selezione che consenta di escludere tali dati dai PNR trasferiti, si impegna ad introdurre gli strumenti per la loro cancellazione e nel frattempo a non utilizzarli.

(22) Per quanto riguarda i meccanismi di attuazione volti a garantire il rispetto di questi principi da parte del CBP, è previsto un sistema di formazione e d'informazione del per-

sonale del CBP, nonché di sanzioni per i membri del personale. Il rispetto da parte del CBP della vita privata in generale sarà controllato dal responsabile della Protezione della vita privata (Chief Privacy Officer) presso il ministero della Sicurezza interna, il quale, pur essendo un funzionario di tale ministero, dispone di un'ampia autonomia organizzativa e deve rendere conto ogni anno al Congresso. Le persone i cui dati PNR sono stati trasmessi possono inviare i loro reclami al CBP o, in caso di mancata risoluzione, al responsabile della Protezione della vita privata, direttamente o tramite le autorità incaricate della protezione dei dati negli Stati membri. L'ufficio responsabile della Protezione della vita privata del ministero della Sicurezza interna esamina con procedura d'urgenza i reclami che gli sono trasmessi dalle autorità incaricate della protezione dei dati negli Stati membri a nome dei residenti della Comunità, se questi ultimi ritengono che i loro reclami non siano stati trattati in modo soddisfacente dal CBP o dall'ufficio responsabile della protezione della vita privata del ministero della Sicurezza interna. Il rispetto della dichiarazione d'impegno è oggetto di un esame annuale congiunto, effettuato dal CBP in collaborazione con il ministero della Sicurezza interna e da un gruppo diretto dalla Commissione.

(23) Al fine di contribuire alla trasparenza e di assicurare la capacità delle autorità competenti negli Stati membri di garantire la protezione degli individui per quanto riguarda il trattamento dei loro dati personali, è opportuno precisare le circostanze eccezionali nelle quali la sospensione di specifici flussi di dati possa essere giustificata, indipendentemente dalla constatazione del livello di protezione adeguato.

(24) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, ha espresso numerosi pareri sul livello di protezione garantito dalle autorità americane per quanto riguarda i dati PNR, i quali hanno guidato la Commissione nel corso del negoziato con il ministero della Sicurezza interna. La Commissione ha preso atto di questi pareri nell'elaborazione di questa decisione[1].

(25) Le misure di cui alla presente decisone sono conformi al parere del comitato istituito dall'articolo 31, paragrafo 1, della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, l'Ufficio statunitense delle dogane e della protezione delle frontiere (CBP) è considerato in grado di garantire un livello di protezione adeguato dei dati delle schede nominative dei passeggeri (PNR) trasmessi dalla Comunità per quanto riguarda i voli con destinazione o partenza dagli Stati Uniti, conformemente alla dichiarazione d'impegno che figura nell'allegato.

Articolo 2

La presente decisione riguarda il livello di protezione adeguato garantito dal CBP al fine di rispondere ai requisiti posti dall'articolo 25, paragrafo 1, della direttiva 95/46/CE e non incide sulle condizioni o restrizioni imposte in attuazione di altre disposizioni della direttiva e che si applicano al trattamento di dati personali negli Stati membri.

Articolo 3

1. Fatti salvi i poteri che consentono loro di adottare misure volte a garantire il rispetto delle disposizioni nazionali adottate conformemente alle disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono esercitare i poteri di cui dispongono attualmente per sospendere la trasmissione di dati al CBP al fine di proteggere le persone fisiche per quanto riguarda il trattamento dei loro dati personali in uno dei casi seguenti:

a) quando un'autorità degli Stati Uniti competente ha accertato che il CBP non rispetta le norme in materia di protezione;

b) quando è probabile che le norme di protezione stabilite nell'allegato I non siano rispettate; quando vi sono motivi ragionevoli di credere che il CBP non adotta o non adotterà, in tempi opportuni, le misure che s'impongono per regolare il caso in questione; quando il proseguimento della trasmissione di dati comporterebbe un rischio

(1) Parere 6/2002 sulla trasmissione da parte delle compagnie aeree d'informazioni relative ai passeggeri e ai membri dell'equipaggio e di altri dati agli Stati Uniti, adottato dal gruppo di lavoro il 24 ottobre 2002, disponibile su: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf

Parere 4/2003 sul livello di protezione garantito negli Stati Uniti per la trasmissione di dati relativi ai passeggeri, adottato dal gruppo di lavoro il 13 giugno 2003, disponibile su: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf

Parere 2/2004 su «Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)», adottato dal gruppo di lavoro il 29 gennaio 2004, disponibile su: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

imminente di grave pregiudizio per le persone interessate e le autorità competenti dello Stato membro si sono ragionevolmente sforzate, in tali circostanze, di avvertire il CBP e di dargli la possibilità di rispondere.

2. La sospensione della trasmissione cessa dal momento in cui è garantita l'applicazione delle norme di protezione e l'autorità competente interessata negli Stati membri ne è avvertita.

Articolo 4

1. Gli Stati membri informano immediatamente la Commissione in merito alle misure adottate in forza dell'articolo 3.

2. Gli Stati membri e la Commissione si informano reciprocamente in merito a qualsiasi modificazione delle norme di protezione e ai casi nei quali le misure adottate dalle autorità incaricate di assicurare il rispetto da parte del CBP delle norme di protezione stabilite nell'allegato I non siano sufficienti a garantire tale rispetto.

3. Se le informazioni raccolte in virtù dell'articolo 3 e dei paragrafi 1 e 2 del presente articolo dimostrano che principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche non sono più rispettati, o che un qualunque organismo incaricato di assicurare il rispetto da parte del CBP delle norme di protezione stabilite nell'allegato non svolge efficacemente la sua missione, il CBP ne sarà informato e, se necessario, si applica la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di revocare o sospendere la presente decisione.

Articolo 5

L'applicazione della presente decisione è oggetto di un controllo sistematico e le constatazioni relative sono comunicate al comitato istituito dall'articolo 31 della direttiva 95/46/CE, con particolare riguardo ad elementi che possano incidere sulla valutazione di cui all'articolo 1 della presente decisione relativa all'adeguatezza del livello di protezione dei dati personali contenuti nei PNR dei passeggeri aerei trasmessi al CBP in forza dell'articolo 25 della direttiva 95/46/CE.

Articolo 6

Gli Stati membri adottano tutte le misure necessarie per conformarsi alla presente decisione entro quattro mesi a decorrere dalla notificazione della medesima.

Articolo 7

La presente decisione scade tre anni e sei mesi dopo la data della sua notificazione, a meno che la sua vigenza non sia prorogata secondo la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE.

Articolo 8

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 14 maggio 2004.

Per la Commissione
Frederik BOLKESTEIN
Membro della Commissione

ALLEGATO

DICHIARAZIONE D'IMPEGNO DELL'UFFICIO DELLE DOGANE E DELLA PROTEZIONE DELLE FRONTIERE DEL MINISTERO DELLA SICUREZZA INTERNA

A sostegno del progetto della Commissione europea per l'esercizio dei poteri che le sono conferiti dall'articolo 25, paragrafo 6, della direttiva 95/46/CE (in prosieguo la «direttiva») e l'adozione di una decisione che riconosca che l'Ufficio delle dogane e della protezione delle frontiere (Bureau of Customs and Border Protection, CBP) del ministero della Sicurezza interna (Department of Homeland Security) fornisce una protezione adeguata ai fini delle trasmissioni da parte dei vettori aerei dei dati delle schede nominative dei passeggeri (Passenger Name Record, PNR)[1], che possono rientrare nell'ambito d'applicazione della direttiva, il CBP assume i seguenti impegni:

Fondamento giuridico del diritto di ottenere il PNR

1. In virtù della legge [titolo 49, sezione 44909(c)(3), dell'USC - United States Code - Codice degli Stati Uniti] e dei regolamenti di attuazione (provvisori) (titolo 19, sezione 122.49b, del codice dei regolamenti federali), ciascun vettore aereo che assicura il trasporto aereo internazionale di passeggeri da e per gli Stati Uniti deve fornire al CBP un accesso elettronico ai dati del PNR nella misura in cui essi sono raccolti e conservati nei sistemi automatici di prenotazione/controllo delle partenze (nel prosieguo i «sistemi di prenotazione») dei vettori aerei.

Uso dei dati del PNR da parte del CBP

2. Il CBP può ottenere la maggior parte dei dati contenuti nel PNR tramite l'esame del biglietto aereo e di altri documenti di viaggio di un dato passeggero applicando i normali poteri di controllo alle frontiere. La possibilità di ottenere tali dati per via elettronica aumenterà significativamente la capacità del CBP di facilitare i viaggi bona fide e di svolgere con efficacia una valutazione anticipata dei rischi presentati dai passeggeri.

3. I dati del PNR sono utilizzati dal CBP al solo fine di prevenire e combattere: 1) il terrorismo e i crimini connessi; 2) altri reati gravi, compresa la criminalità organizzata transnazionale; e 3) la fuga dall'arresto o da pena detentiva per i suddetti crimini. L'uso dei dati del PNR a tali scopi consente al CBP di concentrare le proprie risorse su casi di elevato rischio, facilitando e salvaguardando i viaggi bona fide.

Requisiti relativi ai dati

4. I dati richiesti dal CBP sono elencati nell'allegato A. (I dati così identificati sono in appresso denominati «PNR» ai fini della presente dichiarazione d'impegno.) Il CBP, pur richiedendo l'accesso a ciascuno dei trentaquattro tipi di dati elencati nell'allegato «A», ritiene che raramente un singolo PNR conterrà l'intera serie dei dati identificati. Nei casi in cui il PNR non contenga l'intera serie dei dati, il CBP non cercherà di accedere direttamente ad altri dati del PNR non elencati nell'allegato «A» mediante il sistema di prenotazione dei vettori aerei.

5. Per quanto riguarda i dati classificati come «OSI» e «SSI/SSR», normalmente qualificati come note generali e campi aperti, il sistema automatizzato del CBP cercherà tali campi per ciascuno degli altri dati di cui all'allegato «A». Il personale del CBP non è autorizzato ad esaminare manualmente la totalità dei campi OSI e SSI/SSR, a meno che la persona oggetto di un PNR sia stata classificata dal CBP come persona ad alto rischio in relazione ad uno o più degli obiettivi di cui al punto 3.

6. Ulteriori informazioni personali ricercate direttamente dai dati del PNR possono essere ottenute da fonti estranee al governo soltanto mediante mezzi legali, compresi, se del caso, quelli di cooperazione giudiziaria, e soltanto ai fini di cui al punto 3. Ad esempio, se in un PNR figura un numero di carta di credito, le informazioni sulle transazioni legate a quel conto possono essere ricercate mediante mezzi legali quali un ordine di comparizione emesso da un gran giurì o da un giudice, o come altrimenti previsto dalla legge. Inoltre, l'accesso ai dati relativi agli indirizzi di posta elettronica ottenuti da un PNR deve rispettare le leggi degli

(1) Ai fini della presente dichiarazione d'impegno i termini "passeggero" e "passeggeri" comprendono i membri dell'equipaggio.

Stati Uniti sugli ordini di comparizione, i provvedimenti dei giudici, i mandati d'arresto e gli altri procedimenti autorizzati dalla legge, a seconda del tipo delle informazioni ricercate.

7. Il CBP consulta la Commissione in merito alla revisione dei dati del PNR richiesti, di cui all'allegato A, prima di effettuare tale revisione, se si rende conto di ulteriori campi del PNR che le compagnie aeree possano aggiungere ai propri sistemi e che potrebbero aumentare significativamente la capacità del CBP di valutare i rischi presentati dai passeggeri, o se le circostanze indicano che un campo del PNR precedentemente non richiesto sia necessario ai fini di cui al punto 3.

8. Il CBP può trasmettere i PNR in blocco all'Amministrazione per la sicurezza dei trasporti (Transportation Security Administration) affinché quest'ultima controlli il proprio sistema informatizzato di analisi preventiva dei passeggeri CAPPS II (Computer Assisted Passenger Prescreening System II). Tali trasmissioni non saranno effettuate fino a che non sarà stata autorizzato il controllo dei dati del PNR per i voli interni negli Stati Uniti. I dati del PNR trasmessi in virtù della presente disposizione non saranno conservati dall'Amministrazione per la sicurezza dei trasporti né da altre parti direttamente coinvolte nei controlli oltre il periodo necessario per i controlli stessi, e non saranno trasmessi a terzi [1]. L'obiettivo di tale trasmissione è strettamente limitato al controllo del sistema CAPPS II e relative interfaccia e, tranne in situazioni d'emergenza relative all'identificazione di un noto terrorista o individuo legato al terrorismo, non potrà avere conseguenze operative. In virtù del punto 10, che prevede un sistema automatizzato di selezione, il CBP selezionerà e cancellerà i dati «sensibili» prima di trasmettere qualunque PNR in blocco all'Amministrazione per la sicurezza dei trasporti a norma del presente punto.

Trattamento dei dati «sensibili»

9. Il CBP non userà i dati «sensibili» del PNR, vale a dire i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche e le convinzioni religiose o filosofiche, l'appartenenza a sindacati o i dati riguardanti la salute e la vita sessuale delle persone.

10. Il CBP attuerà al più presto un sistema automatizzato che selezioni e cancelli determinati codici e termini PNR «sensibili» individuati dal CBP stesso previa consultazione con la Commissione europea.

11. Fintantoché un sistema automatizzato di selezione non sarà realizzato, il CBP s'impegna a non utilizzare dati del PNR «sensibili» e a cancellare i dati «sensibili» da ogni divulgazione discrezionale di dati PNR a norma dei punti da 28 a 34[2].

Metodo di accesso ai dati del PNR

12. Per quanto riguarda i dati del PNR cui il CBP accede o che riceve direttamente dai sistemi di prenotazione dei vettori aerei per identificare le persone suscettibili di essere sottoposte ad un controllo alla frontiera, il personale del CBP potrà avere accesso o ricevere e usare unicamente i dati del PNR relativi alle persone il cui viaggio comprende un volo diretto o proveniente[3] dagli Stati Uniti.

13. Il CBP estrarrà informazioni sui passeggeri dai sistemi di prenotazione dei vettori aerei fino a quando questi ultimi saranno in grado di attuare un sistema per trasmettere i dati al CBP.

14. Il CBP estrarrà i dati del PNR associati a un volo particolare non prima di 72 ore precedenti la partenza di tale volo, e ricontrollerà i sistemi non più di tre volte tra l'estrazione iniziale, la partenza del volo dall'estero e l'arrivo del volo negli Stati Uniti, oppure tra l'estrazione iniziale e la partenza del volo dagli Stati Uniti, se del caso, per individuare eventuali cambiamenti delle informazioni. Qualora i vettori aerei siano in grado di trasmettere i dati del PNR, il CBP dovrà ricevere i dati 72 ore prima della partenza del volo, purché tutti i cambiamenti dei dati del PNR effettuati tra quel momento e l'ora d'arrivo del volo negli Stati Uniti o la partenza dagli stessi siano a loro volta trasmessi al CBP[4]. Nel raro caso in cui il CBP ottenga in anticipo informazioni, in base alle quali una o più persone particolarmente sospette potrebbero viaggiare in un volo diretto, proveniente o facente scalo negli Stati Uniti, il CBP può ottenere o richiedere di ottenere i dati del PNR prima delle 72 ore

(1) Ai fini di questa disposizione, il CBP non è considerato una parte direttamente coinvolta nei controlli di CAPPS II o una «parte terza».

(2) Fintantochè non sono attuati i sistemi automatizzati di selezione di cui al punto 10, il CBP adotterà, nel rispetto della legislazione degli Stati Uniti, ogni misura necessaria ad evitare la divulgazione di dati «sensibili» del PNR, qualora tali dati figurino in un PNR oggetto di una comunicazione non discrezionale da parte del CBP conformemente al punto 35.

(3) Comprese le persone che transitano attraverso gli Stati Uniti.

(4) Qualora i vettori aerei siano d'accordo a trasmettere i dati del PNR al CBP, quest'ultimo esaminerà coi vettori la possibilità di trasmettere i dati del PNR a intervalli regolari entro 72 ore prima della partenza dall'estero e l'arrivo del volo negli Stati Uniti, o entro 72 ore prima della partenza del volo dagli Stati Uniti, come del caso. Il CBP vuole utilizzare un metodo di trasmissione dei dati necessari del PNR che soddisfi le esigenze di un'efficace valutazione dei rischi, riducendo nel contempo il relativo impatto economico sui vettori aerei.

precedenti la partenza del volo, al fine di garantire un'azione adeguata essenziale per prevenire o combattere uno dei reati di cui al punto 3. Per quanto possibile nei casi in cui debba accedere ai dati del PNR prima delle 72 ore che precedono la partenza del volo, il CBP farà uso dei mezzi ordinari di applicazione delle leggi.

Conservazione dei dati del PNR

15. Previa approvazione dell'Amministrazione degli archivi nazionali (National Archives and Records Administration) (44 U.S.C. 2101, et seq.), il CBP limiterà l'accesso in linea ai dati del PNR agli utenti CBP autorizzati[1] per un periodo di sette giorni, dopodiché il numero dei funzionari autorizzati ad accedere ai dati del PNR sarà ancor più limitato per un periodo di tre anni e sei mesi a decorrere dalla data in cui si verifica l'accesso alle o il ricevimento delle informazioni del sistema di prenotazione del vettore aereo. Dopo tre anni e sei mesi, i dati del PNR cui non si sia avuto un accesso manuale nel periodo previsto saranno distrutti. I dati del PNR per i quali vi è stato un accesso manuale durante il periodo iniziale di tre anni e sei mesi saranno trasferiti dal CBP verso un file di dati cancellati[2], in cui rimarranno per un periodo di otto anni prima di essere distrutti. Tale calendario peraltro non si applicherebbe ai dati del PNR collegati ad un documento specifico contenente misure di applicazione. Tali dati resterebbero accessibili fino all'archiviazione del documento contenente misure di applicazione. Per quanto riguarda i PNR cui il CBP accede o che riceve direttamente dai sistemi di prenotazione dei vettori aerei durante il periodo di validità della presente dichiarazione d'impegno, il CBP rispetterà le regole di conservazione di cui al presente punto, indipendentemente dalla possibile scadenza del periodo di validità della presente dichiarazione a norma del punto 46.

Sicurezza del sistema informatico del CBP

16. Al personale autorizzato del CBP è consentito l'accesso al PNR attraverso il sistema chiuso di intranet del CBP completamente crittato e il cui collegamento è controllato dal Centro dati delle dogane (Customs Data Center). I dati del PNR immagazzinati nella banca dati CBP sono accessibili come file di «sola lettura» da parte del personale autorizzato, il che significa che i dati possono essere sistematicamente riformattati, ma che il loro contenuto non può essere in alcun modo modificato una volta ottenuti dal sistema di prenotazione del vettore aereo.

17. Nessun altro ente straniero, federale, statale o locale dispone di un accesso elettronico diretto ai dati del PNR tramite le banche dati del CBP, compreso il sistema integrato d'informazione doganale (Interagency Border Inspection System - IBIS).

18. I dati relativi all'accesso alle informazioni contenute nelle banche dati del CBP [come, per esempio: chi, dove, quando (data e ora) e ogni revisione dei dati] sono automaticamente registrati e verificati periodicamente dall'Ufficio per gli affari interni (Office of Internal Affairs) per evitare un uso non autorizzato del sistema.

19. Soltanto taluni dirigenti, dipendenti o subappaltatori per le tecnologie dell'informazione[3], sotto il controllo del CBP, che abbiano superato un'indagine relativa al loro passato, abbiano un titolo operativo di accesso protetto da password al sistema informatico del CBP, e siano formalmente incaricati della revisione dei dati del PNR, possono accedere a tali dati.

20. Ai dirigenti, dipendenti e subappaltatori del CBP si richiede di seguire un corso di formazione in materia di sicurezza e riservatezza dei dati, compreso il superamento di un esame ogni due anni. Per controllare e assicurare l'ottemperanza a tutte le norme relative alla protezione della vita privata e della sicurezza dei dati si usa il sistema di audit del CBP.

21. L'accesso senza autorizzazione del personale del CBP ai sistemi di prenotazione dei vettori aerei o al sistema informatico del CBP che raccoglie il PNR è punito con severe sanzioni disciplinari, che possono giungere fino al licenziamento e con la comminazione di pene, quali multe, detenzione fino ad un anno, o entrambe (cfr. titolo 18, sezione 1030, dell'USC).

22. Le direttive ed i regolamenti del CBP prevedono inoltre una severa azione disciplinare, in esito alla quale è previsto anche il licenziamento, nei confronti dei dipendenti del

(1) Tra gli utenti autorizzati del CBP rientrano i dipendenti addetti ai servizi di analisi degli uffici competenti, nonché i dipendenti addetti al National Targeting Center. Come precedentemente esposto le persone incaricate della conservazione, sviluppo e controllo delle banche dati del CBP potranno accedere a tali dati per le finalità indicate.

(2) Benché il documento del PNR non sia tecnicamente cancellato una volta trasferito nel file dei documenti cancellati, esso è archiviato come dato grezzo (non si tratta di una cartella immediatamente consultabile e, perciò, è inutile ai fini delle indagini «tradizionali») ed è a disposizione, per quanto necessario all'espletamento del compito, del solo personale autorizzato dell'Ufficio degli affari interni del CBP (e in alcuni casi dell'Ufficio dell'ispettore generale per le finalità di audit) e del personale incaricato della conservazione della banca dati dell'ufficio per l'informazione tecnologica del CBP.

(3) L'accesso da parte dei «subappaltatori» ai dati del PNR contenuti nel sistema informatizzato del CBP è limitato alle persone che hanno stipulato un contratto di appalto con il CBP per assisterlo nella gestione o nello sviluppo del suo sistema informatizzato.

CBP che rivelino dati contenuti nel sistema informatico del CBP senza autorizzazione (cfr. titolo 19, sezione 103.34, del codice dei regolamenti federali).

23. Le sanzioni penali, comprese le multe, la detenzione fino ad un anno o entrambe, possono essere comminate a tutti i dirigenti e dipendenti negli Stati Uniti per aver rivelato dati del PNR di cui siano giunti a conoscenza per motivi di lavoro, qualora non siano autorizzati a rivelarli dalla legge (cfr. titolo 18, sezioni 641, 1030, 1905, dell'USC).

Trattamento e tutela dei dati del PNR da parte del CBP

24. Il CBP tratta le informazioni del PNR, qualunque sia la nazionalità o il paese di residenza delle persone interessate, come dati sensibili in relazione all'applicazione della legge, come informazioni personali riservate relative al soggetto interessato, e come informazioni commerciali riservate del vettore aereo. Pertanto, esso non può rivelare tali dati al pubblico, salvo quando disposto dalla presente dichiarazione d'impegno o altrimenti previsto dalla legge.

25. La pubblicazione di dati del PNR è in generale disciplinata dalla legge sulla libertà di informazione (Freedom of Information Act) (titolo 5, sezione 552 dell'USC) che consente l'accesso di ogni persona, indipendentemente dalla nazionalità o dal paese di residenza, agli archivi di un ente federale statunitense, tranne quando tali archivi o una parte di essi siano sottratti alla divulgazione in forza di una deroga prevista da tale legge. Rientra tra tali deroghe anche quella che consente ad un ente di non divulgare un'informazione archiviata o una parte di essa quando si tratti di un'informazione commerciale riservata, quando la sua rivelazione rappresenterebbe una violazione chiaramente ingiustificata della vita privata dell'individuo, oppure quando l'informazione sia raccolta ai fini dell'applicazione della legge, nella misura in cui si può ragionevolmente ritenere che tale rivelazione rappresenti una violazione ingiustificata della vita privata dell'individuo [titolo 5, sezioni 552(b)(4), (6), (7)(C) dell'USC].

26. Le norme del CBP (titolo 19, sezione 103.12, del codice dei regolamenti federali), che regolano il trattamento delle richieste di informazioni, come quelle di dati del PNR, in attuazione della legge sulla libertà di informazione, dispongono che, salvo limitate eccezioni nel caso in cui la richiesta provenga dalla persona interessata, le regole in materia di divulgazione previste dalla legge sulla libertà di informazione non siano applicabili agli archivi del CBP per quanto riguarda le informazioni commerciali riservate, le informazioni che riguardano la vita privata dell'individuo quando la divulgazione costituirebbe una violazione manifestamente ingiustificata della vita privata dell'individuo e le informazioni raccolte in vista dell'applicazione della legge, qualora si possa ragionevolmente ritenere che la divulgazione costituisca una violazione ingiustificata della vita privata dell'individuo[1].

27. Nell'ambito di ogni ricorso amministrativo o giudiziario cui dia adito una richiesta, presentata in forza della legge sulla libertà di informazione, di dati del PNR raccolti dai vettori aerei, il CBP sosterrà che tali archivi non sono soggetti alla divulgazione prevista dalla legge sulla libertà di informazione.

Trasmissione dei dati del PNR ad altre amministrazioni pubbliche

28. Ad eccezione delle trasmissioni tra il CBP e l'Amministrazione per la sicurezza dei trasporti, a norma del punto 8, i servizi del ministero della Sicurezza interna saranno trattati come «enti terzi» soggetti alle stesse norme e condizioni di trasmissione dei dati del PNR valide per le altre autorità governative esterne a tale ministero.

29. Il CBP, nell'esercizio del suo potere discrezionale, trasmetterà i dati del PNR ad altre autorità governative, comprese le autorità degli altri paesi incaricate di far rispettare la legge o della lotta contro il terrorismo, previo esame del caso singolo, a fini di prevenzione e lotta contro i reati di cui al punto 3. Le autorità cui il CBP può trasmettere tali informazioni saranno in prosieguo denominate «autorità designate».

30. Il CBP esercita con prudenza il proprio potere discrezionale di trasmettere dati del PNR ai fini di cui al punto 3. Innanzitutto, esso determinerà se il motivo per la divulgazione dei dati a un'altra autorità designata sia conforme alle finalità indicate (cfr. punto 29). In caso affermativo, il CBP determinerà se tale autorità designata abbia il compito di prevenire la violazione di leggi o regolamenti connessi con tali finalità, di condurre indagini o esperire azioni

(1) Il CBP dovrebbe applicare tali deroghe in modo uniforme, indipendentemente dalla nazionalità o dal paese di residenza della persona oggetto dei dati.

giudiziarie a tal riguardo, o di attuare o far rispettare dette leggi o regolamenti, laddove il CBP venga a conoscenza di una violazione, concreta o potenziale, della legge. La fondatezza della divulgazione dovrà essere esaminata alla luce di tutte le circostanze presentate.

31. Per regolare la divulgazione dei dati PNR che possono essere trasmesse ad altre autorità designate, il CBP è considerato il «proprietario» dei dati, e le autorità designate sono soggette, in forza delle specifiche condizioni di trasmissione: 1) all'obbligo di usare i dati PNR soltanto ai fini di cui ai punti 29 o 34; 2) di garantire la cancellazione sistematica delle informazioni del PNR ricevute, in conformità con le procedure di conservazione dei dati applicate dall'autorità designata e 3) di richiedere l'autorizzazione esplicita del CBP per ogni trasmissione successiva dei dati. Il mancato rispetto delle condizioni per la trasmissione può dar luogo ad un'ispezione e ad una relazione del responsabile della Protezione della vita privata (Chief Privacy Officer) presso il ministero della Sicurezza interna a seguito della quale l'autorità designata può essere privata del diritto ad altre trasmissioni di dati del PNR da parte del CBP.

32. La divulgazione di dati del PNR da parte del CBP è soggetta alla condizione che l'ente destinatario tratti i dati in questione come informazioni riservate di carattere commerciale, come dati sensibili in relazione all'applicazione della legge o come dati riservati di carattere personale dei soggetti interessati, a norma dei punti 25 e 26, e come tali da ritenersi sottratti alla divulgazione in virtù della legge sulla libertà di informazione (titolo 5, sezione 552, dell'USC). Inoltre, l'ente destinatario è informato del fatto che ogni divulgazione successiva delle informazioni di cui trattasi è vietata senza previa autorizzazione espressa del CBP. Il CBP non autorizzerà alcuna trasmissione successiva di dati del PNR per finalità diverse da quelle indicate ai punti 29, 34 o 35.

33. I membri del personale di tali autorità designate che, senza autorizzazione, rivelano i dati del PNR sono passibili di sanzioni penali (titolo 18, sezioni 641, 1030, 1905, dell'USC).

34. Nessuna disposizione della presente dichiarazione d'impegno potrà impedire l'uso o la divulgazione dei dati del PNR alle autorità governative competenti qualora tale divulgazione sia essenziale per la tutela degli interessi vitali della persona interessata o di altre persone, in particolare in caso di gravi rischi per la salute. Le divulgazioni effettuate a tal fine sono soggette alle stesse condizioni applicabili alle trasmissioni descritte ai punti 31 e 32.

35. Nessuna disposizione della presente dichiarazione d'impegno può impedire l'uso o la divulgazione di dati del PNR nell'ambito di un procedimento penale o negli altri casi previsti dalla legge. Il CBP informerà la Commissione in ordine all'adozione, da parte delle autorità americane, delle leggi che incidono sulle dichiarazioni contenute nella presente dichiarazione d'impegno.

Informazione, accesso ai dati e mezzi di ricorso per le persone interessate dal PNR

36. Il CBP informerà i passeggeri dei requisiti del PNR e di tutti gli aspetti connessi al suo funzionamento, per esempio tramite la pubblicazione sul sito Internet del CBP, o negli opuscoli e altro materiale destinato ai passeggeri di informazioni di carattere generale relative all'autorità responsabile per la raccolta dei dati, alla finalità di tale raccolta, alla protezione dei dati, alla trasmissione degli stessi, all'identità del funzionario responsabile, ai mezzi di ricorso e agli sportelli cui rivolgersi per eventuali domande o problemi.

37. Le richieste delle persone interessate (note anche come «richiedenti principali»), volte a ottenere copia delle informazioni del PNR che li riguardano contenute nelle banche dati del CBP, sono trattate a norma della legge sulla libertà di informazione. Dette richieste possono essere inviate al seguente indirizzo: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, per posta. La richiesta può anche essere consegnata al Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C. Ulteriori informazioni riguardanti le procedure per presentare richieste a norma della legge sulla libertà di informazione si trovano alla sezione 103.5 del titolo 19 del codice dei regolamenti federali degli Stati Uniti. Al richiedente principale che presenti una tale domanda non potrà essere opposto, come motivo previsto dalla legge sulla libertà di informazione per non comunicare i dati del

PNR, il fatto che il CBP consideri di norma tali dati come informazioni riservate di carattere personale o informazioni commerciali segrete del vettore aereo.

38. In talune circostanze eccezionali il CBP può valersi della facoltà attribuitagli dalla legge sulla libertà di informazione di rifiutare o di rinviare la divulgazione di tutto o più probabilmente parte del fascicolo del PNR a un richiedente principale, a norma del titolo 5, sezione 552(b), dell'USC (ad esempio se si possa ragionevolmente ritenere che la divulgazione in virtù della legge sulla libertà di informazione sia tale da interferire con procedimenti penali o qualora essa sveli le tecniche e le procedure relative ad indagini, con il conseguente pericolo di elusione della legge). In virtù della legge sulla libertà di informazione ogni richiedente ha la possibilità di impugnare, per via amministrativa o giudiziaria, la decisione di rifiuto del CBP di comunicare le informazioni richieste [cfr. il titolo 5, sezione 552, lettera a), punto 4B, dell'USC, nonché il titolo 19, sezioni 103.7-103.9, del codice dei regolamenti federali - CFR].

39. Il CBP si impegna a rettificare[1] i dati su richiesta dei passeggeri o dei membri dell'equipaggio, dei vettori aerei o delle autorità incaricate della protezione dei dati negli Stati membri dell'Unione europea, nei limiti del mandato conferito dalla persona interessata, qualora il CBP accerti che tali dati figurano nella sua banca dati e ritenga che la rettifica sia giustificata e debitamente motivata. Il CBP informerà tutte le autorità designate che hanno ricevuto tali dati del PNR di tutte le rettifiche degli stessi.

40. Le richieste di rettifica dei dati del PNR contenute nella banca dati del CBP e i reclami dei singoli sul trattamento dei loro dati PNR da parte del CBP possono essere presentati, direttamente o tramite l'autorità incaricata della protezione dei dati competente, nei limiti del mandato conferito dalla persona interessata, all'indirizzo seguente: Assistano Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

41. Qualora l'oggetto di un reclamo non possa essere risolto dal CBP, esso può essere presentato per iscritto al Responsabile della protezione della vita privata, Chief Privacy Officer, Department of Homeland Security, Washington, D.C. 20528, che esaminerà il caso e cercherà di risolvere la controversia[2].

42. Inoltre, l'Ufficio responsabile per la protezione della vita privata del ministero della Sicurezza interna tratterà con procedura accelerata i reclami sottopostigli dalle autorità incaricate della protezione dei dati degli Stati membri dell'Unione europea per conto di un residente dell'Unione europea, qualora quest'ultimo abbia autorizzato l'autorità incaricata della protezione dei dati ad agire per suo conto e ritenga che il suo reclamo sulla protezione dei dati riguardante il PNR non sia stato trattato in modo soddisfacente dal CBP, conformemente ai punti da 37 a 41, o dall'Ufficio responsabile della protezione della vita privata del ministero della Sicurezza interna. L'Ufficio per la privacy comunicherà le proprie conclusioni e fornirà un parere alla o alle autorità incaricate della protezione dei dati riguardo alle eventuali azioni intraprese. Nella sua relazione al Congresso, il responsabile della Protezione della vita privata del ministero della Sicurezza interna farà riferimento al numero, al merito e alla soluzione data alle controversie relative al trattamento dei dati personali, quali i dati del PNR[3].

Rispetto delle regole

43. Il CBP, in collaborazione col ministero della Sicurezza interna, s'impegna a svolgere, una volta all'anno o più spesso se così deciso dalle parti, un'analisi congiunta con la Commissione, assistita se del caso da rappresentanti delle autorità europee preposte all'esercizio dell'azione penale e/o delle autorità degli Stati membri dell'Unione europea[4], sull'attuazione della presente dichiarazione d'impegno, al fine di contribuire all'effettivo funzionamento dei procedimenti descritti nella dichiarazione stessa.

44. Il CBP adotta regolamenti, direttive o altri documenti contenenti le presenti disposizioni per assicurare il rispetto della presente dichiarazione d'impegno da parte dei dirigenti, dei dipendenti e dei subappaltatori del CBP. Come indicato, i dirigenti, i dipendenti e i subappaltatori del CBP che non ottemperino alle direttive dell'ente contenute in tali documenti sono passibili di gravi sanzioni disciplinari ed eventualmente penali.

(1) Per quanto riguarda tale possibilità di «rettifica», il CBP vuole precisare di non avere la possibilità di modificare i dati contenuti nei documenti del PNR che raccoglie dai vettori aerei. Si creerà, invece, un fascicolo distinto collegato al documento PNR per indicare i dati errati e le relative correzioni. Più precisamente, il CBP apporterà nel documento di esame secondario (secondary examination record) del passeggero un'annotazione per segnalare che taluni dati del PNR sono (forse) errati.

(2) Il responsabile della Protezione della vita privata del ministero della Sicurezza interna è indipendente da qualunque direzione del ministero, e ha l'obbligo di garantire che le informazioni personali siano utilizzate in modo conforme alla legge (cfr. nota 13). Le decisioni del responsabile della Protezione della vita privata sono vincolanti per il ministero e non possono essere annullate per motivi politici.

(3) Ai sensi della sezione 222 della legge sulla sicurezza interna (Homeland Security Act) del 2002 (Public Law 107-296, del 25 novembre 2002), il responsabile della Protezione della vita privata del ministero della Sicurezza interna ha il compito di procedere a un esame dell'impatto sulla protezione della vita privata delle misure proposte dal ministero per quanto riguarda la riservatezza delle informazioni di carattere personale, compreso il tipo di informazioni raccolte e il numero di persone interessate. Inoltre, egli deve presentare annualmente al Congresso una relazione sulle attività del ministero che incidono sulla protezione della vita privata.

segue nota 3 e 4

Reciprocità

45. Qualora nell'Unione europea sia istituito un sistema di identificazione dei passeggeri aerei in forza del quale i vettori aerei siano tenuti a fornire alle autorità l'accesso ai dati del PNR delle persone, il cui itinerario di viaggio preveda un volo diretto verso o proveniente dall'Unione europea, il CBP solleciterà, in base al principio di reciprocità, la collaborazione delle compagnie aeree con sede negli Stati Uniti.

Revisione e durata di validità della dichiarazione d'impegno

46. La presente dichiarazione d'impegno si applica per un periodo di tre anni e sei mesi a decorrere dalla data di entrata in vigore di un accordo tra gli Stati Uniti e la Comunità europea che autorizzi il trattamento dei dati del PNR da parte dei vettori aerei ai fini del trasferimento di tali dati al CBP, in conformità con la direttiva. Scaduto il termine di due anni e sei mesi dall'entrata in vigore della presente dichiarazione d'impegno, il CBP, in collaborazione col ministero della Sicurezza interna, avvierà una trattativa con la Commissione al fine di estendere la dichiarazione stessa e gli eventuali accordi ad essa connessi a condizioni accettabili da entrambe le parti. Se un accordo accettabile da entrambe le parti non è raggiunto prima della data di scadenza della presente dichiarazione d'impegno, quest'ultima cessa di essere valida.

Non sono creati diritti privati o precedenti

47. La presente dichiarazione d'impegno non crea o conferisce alcun diritto o beneficio a persone fisiche o giuridiche, private o pubbliche.

48. Le disposizioni contenute nella presente dichiarazione d'impegno non costituiscono un precedente per le future trattative con la Commissione, l'Unione europea, gli enti collegati o uno Stato terzo per quanto riguarda il trasferimento di qualunque tipo di dati.

11 maggio 2004

ALLEGATO «A»

Dati del PNR richiesti dal CBP ai vettori aerei

1. Codice del documento PNR
2. Data di prenotazione
3. Data/e prevista/e di viaggio
4. Nome
5. Altri nomi che compaiono nel PNR
6. Indirizzo
7. Informazioni su tutte le modalità di pagamento
8. Indirizzo di fatturazione
9. Recapiti telefonici
10. Itinerario completo per lo specifico PNR
11. Informazioni sui viaggiatori abituali «Frequent flyer» (solo per le miglia percorse e indirizzo/i)
12. Agenzia viaggi
13. Agente di viaggio
14. Informazioni del PNR sul code share (scambio dei codici)
15. Fase di viaggio del passeggero
16. PNR scissi/divisi
17. Indirizzi di posta elettronica
18. Dati sull'emissione del biglietto
19. Osservazioni generali
20. Numero del biglietto
21. Numero del posto
22. Data di emissione del biglietto
23. Precedenti assenze all'imbarco
24. Numero di etichetta dei bagagli
25. Passeggero senza prenotazione

segue nota 3 e 4

La sezione 222, paragrafo 5, della legge inoltre prevede espressamente che il responsabile della Protezione della vita privata del ministero della Sicurezza interna riceva e riferisca al Congresso tutte le «denunce di violazioni della vita privata».

(4) La composizione dei gruppi delle due parti sarà comunicata in anticipo e può comprendere le autorità competenti per la protezione della vita privata/la protezione dei dati, per i controlli doganali e l'applicazione delle norme, per la sicurezza dei confini e/o dell'aviazione. Le autorità partecipanti dovranno ottenere tutte le autorizzazioni di sicurezza necessarie e rispettare la riservatezza delle discussioni e della documentazione cui potranno avere accesso. La riservatezza però non sarà un ostacolo a che entrambe le parti presentino una relazione sui risultati dell'analisi congiunta alle rispettive autorità competenti, compresi il Congresso degli Stati Uniti e il Parlamento europeo. Tuttavia, in nessun caso le autorità partecipanti potranno rivelare i dati personali di una persona, né qualunque informazione non pubblica derivante da documenti cui viene loro consentito di accedere, o informazioni operative o interne agli enti interessati che ottengono durante l'analisi congiunta. Le due parti determinano le modalità dettagliate per l'analisi congiunta.

26. Informazioni OSI
27. Informazioni SSI/SSR
28. Informazioni sulla fonte
29. Cronistoria dei cambiamenti fatti al PNR
30. Numero di viaggiatori nel PNR
31. Informazioni relative al posto
32. Biglietti di sola andata
33. Informazioni APIS eventualmente assunta
34. Campi ATFQ

44 Decisione del Consiglio del 17 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 Dipartimento per la sicurezza interna degli Stati Uniti (*)

(2004/496/CE)

IL CONSIGLIO DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 95 in combinato disposto con l'articolo 300, paragrafo 2, primo comma, prima frase, vista la proposta della Commissione, considerando quanto segue:

(1) Il 23 febbraio 2004 il Consiglio ha autorizzato la Commissione a negoziare, in nome della Comunità, un accordo con 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 dipartimento per la sicurezza interna degli Stati Uniti.

(2) Il Parlamento europeo non ha espresso il suo parere nel termine fissato dal Consiglio, ai sensi dell'articolo 300, paragrafo 3, primo comma del trattato, dato l'urgente bisogno di porre rimedio alla situazione di incertezza in cui si trovano le compagnie aeree ed i passeggeri, nonché di proteggere gli interessi finanziari degli interessati.

(3) È opportuno approvare il presente accordo,

DECIDE:

Articolo 1

L'accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti è approvato in nome della Comunità.

Il testo dell'accordo è accluso alla presente decisione.

(*) *G.U.C.E.* 20 maggio 2004, L 183/83.

Articolo 2

Il Presidente del Consiglio è autorizzato a designare la (le) persona (persone) abilitata (abilitate) a firmare l'accordo in nome della Comunità europea.

Bruxelles, 17 maggio 2004

Per il Consiglio
Il Presidente
B. COWEN

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 dipartimento per la sicurezza interna degli Stati Uniti

LA COMUNITÀ EUROPEA E GLI STATI UNITI D'AMERICA

RICONOSCENDO l'importanza di rispettare i diritti e le libertà fondamentali, in particolare il diritto alla vita privata, e l'importanza di rispettare tali valori nella prevenzione e nella lotta contro il terrorismo e i reati ad esso connessi, nonché altri reati gravi di natura transnazionale, tra cui la criminalità organizzata;

VISTI le leggi e i regolamenti statunitensi che impongono a ciascun vettore aereo che assicura il trasporto di passeggeri da e per gli Stati Uniti nello spazio aereo estero di fornire all'ufficio doganale e di protezione dei confini (Bureau of Customs and Border Protection, in seguito denominato «CBP») del dipartimento per la sicurezza interna (Department of Homeland Security, in seguito denominato «DHS»), un accesso elettronico ai dati di identificazione delle pratiche (Passenger Name Record, in seguito denominato «PNR») nella misura in cui questi sono raccolti e conservati nei sistemi automatici di prenotazione/controllo dei vettori aerei;

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, in particolare l'articolo 7, lettera c);

VISTE le dichiarazioni di impegno del CBP dell'11 maggio 2004, che saranno pubblicate nel registro federale (in seguito denominate «le dichiarazioni di impegno»);

VISTA la decisione C(2004) 1799 della Commissione adottata il 17 maggio 2004, ai sensi dell'articolo 25, paragrafo 6 della direttiva 95/46/CE, con cui si ritiene che il CBP, conformemente alle dichiarazioni di impegno allegate, assicuri un livello di protezione adeguato dei dati PNR trasferiti dalla Comunità europea (in seguito denominata «Comunità») in relazione ai voli da o per gli Stati Uniti (in seguito denominata «la decisione»);

CONSTATANDO che i vettori aerei dotati di sistemi di prenotazione/controllo situati nel territorio degli Stati membri della Comunità europea dovrebbero provvedere a trasmettere i dati PNR al CBP non appena ciò sia tecnicamente possibile, ma che, fino a quel momento, dovrebbe essere consentito alle autorità statunitensi di accedere direttamente a tali dati, ai sensi delle disposizioni del presente accordo;

AFFERMANDO che il presente accordo non costituisce un precedente per eventuali futuri discussioni o negoziati tra gli Stati Uniti e la Comunità europea, o tra una delle due parti e uno Stato terzo, in merito al trasferimento di una qualsiasi altra forma di dati;

VISTO l'impegno di entrambe le parti a collaborare per trovare senza indugio una solu-

zione appropriata e soddisfacente per entrambe in merito al trattamento dei dati relativi alle informazioni preventive sui passeggeri (Advance Passenger Information, API) trasferiti dalla Comunità agli Stati Uniti,

HANNO CONVENUTO QUANTO SEGUE:

1) 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 assoluta conformità della decisione, per tutto il periodo in cui la decisione è applicabile e solo finché non sia in vigore un sistema soddisfacente che permetta la trasmissione di tali dati da parte dei vettori aerei.

2) 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 assoluta conformità della decisione e per tutto il periodo in cui la decisione è applicabile.

3) Il CBP prende nota della decisione e attesta che sta attuando le dichiarazioni di impegno allegate a detta decisione.

4) Il CBP tratta i dati PNR ricevuti e i titolari dei dati interessati da tale trattamento in conformità delle leggi e degli obblighi costituzionali statunitensi applicabili, senza discriminazioni illegittime, in particolare in base alla nazionalità e al paese di residenza.

5) Il CBP e la Commissione europea rivedono congiuntamente e su base periodica l'attuazione del presente accordo.

6) Qualora nell'Unione europea sia istituito un sistema di identificazione dei passeggeri aerei in forza del quale i vettori aerei siano tenuti a fornire alle autorità l'accesso ai dati PNR delle persone il cui itinerario di viaggio preveda un volo da o per l'Unione europea, il DHS, per quanto fattibile e unicamente su una base di reciprocità, promuove attivamente la cooperazione dei vettori aerei rientranti nella sua giurisdizione.

7) Il presente accordo entra in vigore all'atto della sua firma. Ciascuna parte può denunciare il presente accordo in qualsiasi momento, mediante notifica per via diplomatica. In tal caso, l'accordo cessa di essere in vigore novanta (90) giorni dopo la data di tale notifica. Il presente accordo può essere modificato in ogni momento mediante consenso scritto di entrambe le parti.

8) Il presente accordo non intende derogare o apportare modifiche alla normativa delle parti; esso non crea né conferisce alcun diritto o beneficio ad altre persone o enti, pubblici o privati.

Firmato, il 17 maggio 2004

Il presente accordo è redatto in duplice originale in lingua ceca, danese, estone, finlandese, francese, greca, inglese, italiana, lettone, lituana, maltese, olandese, polacca, portoghese, slovacca, slovena, spagnola, svedese, tedesca e ungherese, ciascun testo facente ugualmente fede. In caso di divergenze di interpretazione si considera determinante il testo inglese.

Per la Comunità europea

Per gli Stati Uniti d'America
Tom RIDGE
Segretario del Dipartimento
per la sicurezza interna degli Stati Uniti

45 Accordo fra la Comunità europea e gli Stati Uniti d'America sul trattamento ed il trasferimento di dati PNR da parte di vettori aerei al *Department of Homeland Security, Bureau of Customs and Border Protection* degli Stati Uniti (*)

AGREEMENT
BETWEEN THE EUROPEAN COMMUNITY AND
THE UNITED STATES OF AMERICA
ON THE PROCESSING AND TRASFER OF PRN DATA BY AIR CARRIES
TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY,
BEREAU OF CUSTOMS AND BORDER PROTECTION

(*) Firmato a Washington il 28 maggio 2004.

CE/USA/EN1

46 Decisione della Commissione del 27 dicembre 2004 che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a Paesi Terzi

DECISIONE DELLA COMMISSIONE

del 27 dicembre 2004

che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a Paesi Terzi

[*notificata con il numero C(2004) 5271*]

(Testo rilevante ai fini del SEE)

(2004/915/CE)

(*) *G.U.C.E.* 29 dicembre 2004, L 385/74.

47 Documento di lavoro della Commissione – L'attuazione della Decisione della Commissione 520/2000/CE sulla protezione adeguata dei dati personali offerta dai principi di *Safe Harbour* in materia di *privacy* e dalle relative Domande più frequenti, pubblicati dal *Department of Commerce* degli USA (*)



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20.10.2004
SEC (2004) 1323

COMMISSION STAFF WORKING DOCUMENT

The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce

(*) http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2004-1323_en.pdf

48 Studio sull'attuazione della decisione relativa al *Safe Harbour*, redatto su richiesta della Commissione Europea, DG Mercato Interno (*)



Safe Harbour Decision Implementation Study

prepared by

Jan Dhont, María Verónica Pérez Asinari, and Prof. Dr. Yves Poullet
(Centre de Recherche Informatique et Droit,
University of Namur, Belgium)

with the assistance of

Prof. Dr. Joel R. Reidenberg
(Fordham University School of Law, New York, USA)

and Dr. Lee A. Bygrave
(Norwegian Research Centre for Computers and Law,
University of Oslo, Norway)

at the request of the
European Commission, Internal Market DG
Contract PRS/2003/A0-7002/E/27

Namur, 19 April 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/studies/safe-harbour-2004_en.pdf

49 Regolamento (CE) n. 871/2004 del Consiglio del 29 aprile 2004 relativo all'introduzione di alcune nuove funzioni del sistema d'informazione Schengen, compresa la lotta contro il terrorismo (*)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 66,

vista l'iniziativa del Regno di Spagna[1],

visto il parere del Parlamento europeo[2],

considerando quanto segue:

(1) Il sistema d'informazione Schengen, in seguito denominato "SIS", istituito a norma del titolo IV della convenzione del 1990 di applicazione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni[3], in seguito denominata "convenzione di Schengen del 1990", rappresenta uno strumento fondamentale per l'applicazione delle disposizioni dell'acquis di Schengen integrate nell'ambito dell'Unione europea.

(2) È stata riconosciuta la necessità di elaborare un nuovo SIS di seconda generazione, in seguito denominato "SIS II", in vista dell'allargamento dell'Unione europea e che consenta l'introduzione di nuove funzioni e si giovi nello stesso tempo degli ultimi sviluppi nel settore delle tecnologie dell'informazione. Sono stati compiuti i primi passi per lo sviluppo di questo nuovo sistema.

(3) Alcuni adattamenti di disposizioni vigenti e l'introduzione di talune nuove funzioni possono già essere realizzati rispetto alla versione attuale del SIS, in particolare per quanto riguarda la concessione dell'accesso ad alcuni tipi di dati inseriti nel SIS alle autorità che sarebbero agevolate nel corretto espletamento dei loro compiti dalla possibilità di consultare tali dati, compresi l'Europol e i membri nazionali dell'Eurojust, l'estensione delle categorie di oggetti smarriti per i quali possono essere inserite segnalazioni e la registrazione delle trasmissioni di dati a carattere personale. È dapprima necessario istituire in ciascuno Stato membro i dispositivi tecnici necessari a tal fine.

(4) Le conclusioni del Consiglio europeo di Laeken del 14 e 15 dicembre 2001 e, in particolare, il punto 17 (cooperazione tra i servizi speciali nella lotta contro il terrorismo) e 43 (Eurojust e cooperazione di polizia per quanto riguarda l'Europol) e il piano d'azione del 21 settembre 2001 contro il terrorismo si riferiscono alla necessità di rafforzare il SIS e migliorarne le capacità.

(5) È inoltre utile adottare disposizioni per quanto riguarda lo scambio di tutte le informazioni supplementari tramite le autorità all'uopo designate in tutti gli Stati membri (Informazioni supplementari richieste all'atto dell'ingresso nel territorio nazionale - SIRENE), fornendo a tali autorità una base giuridica comune nel quadro delle disposizioni della convenzione di Schengen del 1990 e stabilendo norme relative alla cancellazione dei dati da esse detenuti.

(6) Le modifiche da apportare a tal fine alle disposizioni dell'acquis di Schengen concer-

(*) *G.U.C.E.* 30 aprile 2004, L 162/29.
(1) *G.U.C.E.* 4 luglio 2002, C 160/ 5.
(2) G.U.C.E. 5 febbraio 2004, C 31/122.
(3) *G.U.C.E. 22 luglio 2000,* L 239/19.

nenti il SIS constano di due parti: il presente regolamento e una decisione del Consiglio basata sull'articolo 30, paragrafo 1, lettere a) e b), sull'articolo 31, lettere a) e b) e sull'articolo 34, paragrafo 2, lettera c) del trattato sull'Unione europea. Questo perché, come indicato nell'articolo 93 della convenzione di Schengen del 1990, scopo del SIS è quello di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza nazionale, nel territorio degli Stati membri e di applicare le disposizioni della summenzionata convenzione sulla circolazione delle persone in detti territori avvalendosi delle informazioni trasmesse tramite il SIS ai sensi delle disposizioni di detta convenzione. Poiché alcune delle disposizioni della convenzione di Schengen del 1990 devono essere applicate per entrambi gli scopi nello stesso tempo, è opportuno che esse siano modificate negli stessi termini tramite atti paralleli basati su ciascuno dei trattati.

(7) Il presente regolamento lascia impregiudicata la futura adozione della necessaria normativa che descriva nei dettagli l'impalcatura giuridica, gli obiettivi, il funzionamento e l'uso del SIS II, quali, ma non solo, le norme che definiscano ulteriormente le categorie di dati da inserire nel sistema, gli scopi per cui sono inserite e i criteri per l'inserimento, le norme riguardanti il contenuto delle registrazioni SIS, l'interconnessione delle segnalazioni, la compatibilità tra le stesse e ulteriori norme sull'accesso ai dati SIS e sulla protezione di dati a carattere personale e relativo controllo.

(8) Per quanto riguarda l'Islanda e la Norvegia, il presente regolamento costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen che rientrano nel settore di cui all'articolo 1, punto G, della decisione 1999/437/CE[1], relativa a talune modalità di applicazione di detto accordo.

(9) A norma degli articoli 1 e 2 del protocollo sulla posizione della Danimarca allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, la Danimarca non partecipa all'adozione del presente regolamento, non è da esso vincolata e non è soggetta alla sua applicazione. Dato che il presente regolamento si basa sull'acquis di Schengen in applicazione delle disposizioni della parte terza, titolo IV, del trattato che istituisce la Comunità europea, la Danimarca decide, a norma dell'articolo 5 del succitato protocollo, entro un periodo di sei mesi dall'adozione del presente regolamento da parte del Consiglio, se intende recepirlo nel proprio diritto interno.

(10) Il presente regolamento rappresenta uno sviluppo del SIS ai fini della sua applicazione in relazione alle disposizioni dell'acquis di Schengen sulla circolazione delle persone. Il Regno Unito non ha chiesto di partecipare al SIS e non vi partecipa per questi fini, ai sensi della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[2]. Il Regno Unito non partecipa pertanto all'adozione del presente regolamento, non è da esso vincolato e non è soggetto alla sua applicazione.

(11) Il presente regolamento rappresenta uno sviluppo del SIS ai fini della sua applicazione in relazione alle disposizioni dell'acquis di Schengen sulla circolazione delle persone. L'Irlanda non ha chiesto di partecipare al SIS e non vi partecipa per questi fini, ai sensi della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen[3]. L'Irlanda non partecipa pertanto all'adozione del presente regolamento, non è da esso vincolata e non è soggetta alla sua applicazione.

(12) Il presente regolamento costituisce un atto basato sull'acquis di Schengen o ad esso altrimenti connesso ai sensi dell'articolo 3, paragrafo 2, dell'atto di adesione,

(1) *G.U.C.E.* 10 luglio 1999, L 176/31.
(2) *G.U.C.E.* 1° giugno 2000, L 131/43.
(3) *G.U.C.E.* 7 marzo 2002, L 64/20.

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Le disposizioni della convenzione di Schengen del 1990 sono modificate come segue:

1) all'articolo 92 è aggiunto il paragrafo seguente:

"4. Gli Stati membri si scambiano, conformemente alla legislazione nazionale, tramite le autorità all'uopo designate (SIRENE) tutte le informazioni supplementari necessarie in relazione all'inserimento di segnalazioni e ai fini dell'adeguata azione da intraprendere nei casi in cui persone e oggetti, i cui dati sono stati inseriti nel sistema d'informazione Schengen, siano reperiti grazie alla consultazione di tale sistema. Tali informazioni possono essere usate solo per lo scopo per il quale sono state trasmesse."

2) all'articolo 94, paragrafo 3, primo comma, le lettere da a) a i) sono sostituite dalle seguenti:

"a) cognome e nomi, 'alias' eventualmente registrati separatamente;
b) segni fisici particolari, oggettivi ed inalterabili;
c) (...)
d) data e luogo di nascita;
e) sesso;
f) cittadinanza;
g) indicazione che le persone in questione sono armate, violente o sono evase;
h) motivo della segnalazione;
i) linea di condotta da seguire"

3) alla fine dell'articolo 101, paragrafo 1, è aggiunta la seguente frase:

"Tuttavia, l'accesso ai dati inseriti nel sistema d'informazione Schengen e il diritto di consultarli direttamente possono essere esercitati anche dalle autorità giudiziarie nazionali, tra cui quelle responsabili dell'avvio di investigazioni del pubblico ministero nelle azioni penali e indagini giudiziarie prima dell'atto di accusa, nell'assolvimento dei propri compiti, conformemente alla legislazione nazionale."

4) l'articolo 101, paragrafo 2, è sostituito dal seguente:

"2. Inoltre, l'accesso ai dati inseriti a norma dell'articolo 96 e i dati riguardanti documenti relativi a persone inseriti a norma dell'articolo 100, paragrafo 3, lettere d) e e), ed il diritto di consultarli direttamente possono essere esercitati dalle autorità competenti per il rilascio dei visti, dalle autorità centrali competenti per l'esame delle domande di visti e dalle autorità competenti per il rilascio dei documenti di soggiorno e per l'amministrazione degli stranieri nel quadro dell'applicazione delle disposizioni in materia di circolazione delle persone previste dalla presente convenzione. L'accesso ai dati da parte di tali autorità è disciplinato dal diritto nazionale di ciascuno Stato membro."

5) la seconda frase dell'articolo 102, paragrafo 4, è sostituita dalla seguente:

"In deroga a quanto precede, i dati inseriti a norma dell'articolo 96 e i dati relativi a documenti riguardanti persone inseriti a norma dell'articolo 100, paragrafo 3, lettere d) e e) possono essere utilizzati solo per gli scopi di cui all'articolo 101, paragrafo 2, conformemente alla legislazione nazionale di ciascuno Stato membro."

6) l'articolo 103 è sostituito dal seguente:

"Articolo 103

Ciascuno Stato membro provvede affinché ciascuna trasmissione di dati personali sia registrata nella sezione nazionale del sistema d'informazione Schengen dall'organo di gestione degli archivi di dati, ai fini del controllo dell'ammissibilità della ricerca. La registrazione può essere utilizzata soltanto a questo scopo e deve essere cancellata al più presto dopo un periodo di un anno e al più tardi un periodo di tre anni."

7) è inserito l'articolo seguente:

"Articolo 112 bis

1. I dati di carattere personale archiviati dalle autorità di cui all'articolo 92, paragrafo 4, in seguito allo scambio di informazioni a norma di detto paragrafo sono conservati soltanto per il tempo necessario a conseguire gli scopi per i quali sono stati forniti. Essi sono in ogni caso cancellati al più tardi un anno dopo che sono state cancellate dal sistema d'informazione Schengen le segnalazioni riguardanti la persona interessata o l'oggetto in questione.
2. Il paragrafo 1 non pregiudica il diritto di uno Stato membro di conservare negli archivi nazionali i dati relativi ad una determinata segnalazione effettuata da detto Stato membro o ad una segnalazione in collegamento con la quale è stata svolta un'azione nel suo territorio. Il periodo di tempo per cui tali dati possono essere conservati in tali archivi è regolato dalla legislazione nazionale."

8) è inserito l'articolo seguente:

"Articolo 113 bis

1. I dati diversi dai dati di carattere personale archiviati dalle autorità di cui all'articolo 92, paragrafo 4, in seguito allo scambio di informazioni a norma di detto paragrafo sono conservati soltanto per il tempo necessario a conseguire gli scopi per i quali sono stati forniti. Essi sono in ogni caso cancellati al più tardi un anno dopo che sono state cancellate dal sistema d'informazione Schengen le segnalazioni riguardanti la persona interessata o l'oggetto in questione.
2. Il paragrafo 1 non pregiudica il diritto di uno Stato membro di conservare negli archivi nazionali i dati relativi ad una determinata segnalazione effettuata da detto Stato membro o ad una segnalazione in collegamento con la quale è stata svolta un'azione nel suo territorio. Il periodo di tempo per cui tali dati possono essere conservati in tali archivi è regolato dalla legislazione nazionale."

Articolo 2

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale* dell'Unione europea.

2. Esso si applica a decorrere da una data che sarà fissata dal Consiglio che delibera all'unanimità, non appena adempiute le condizioni preliminari necessarie. Il Consiglio può decidere di fissare date differenti per l'applicazione di disposizioni differenti.

3. La decisione del Consiglio a norma del paragrafo 2 è pubblicata nella Gazzetta ufficiale dell'Unione europea.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Lussemburgo, 29 aprile 2004

Per il Consiglio
Il Presidente
M. McDowell

50 Decisione del Consiglio n. 2004/512/CE dell' 8 giugno 2004 che istituisce il sistema di informazione visti (VIS) (*)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 66,

vista la proposta della Commissione,

visto il parere del Parlamento europeo,

considerando quanto segue:

(1) Il Consiglio europeo di Siviglia del 21 e 22 giugno 2002 ha giudicato una priorità assoluta l'istituzione di un sistema comune d'identificazione dei dati dei visti e ne ha chiesto l'introduzione, al più presto, sulla scorta di uno studio di fattibilità e sulla base degli orientamenti adottati dal Consiglio il 13 giugno 2002 .

(2) Il 5 - 6 giugno 2003 il Consiglio ha accolto favorevolmente lo studio di fattibilità presentato dalla Commissione nel maggio 2003, ha confermato gli obiettivi stabiliti nei suoi orientamenti per il VIS ed ha invitato la Commissione a proseguire, di concerto con gli Stati membri, i lavori preparatori sullo sviluppo del VIS sulla base di un'architettura centralizzata, tenendo conto della possibilità di una piattaforma tecnica comune con il sistema d'informazione Schengen di seconda generazione (SIS II).

(3) Il Consiglio europeo riunitosi a Salonicco il 19 e 20 giugno 2003 ha ritenuto necessario che, a seguito dello studio di fattibilità, fossero elaborati quanto prima possibile orientamenti riguardanti la pianificazione dello sviluppo del VIS, la base giuridica appropriata che consentirà la sua istituzione e l'impegno delle risorse finanziarie necessarie.

(4) La presente decisione costituisce il fondamento giuridico necessario per l'iscrizione nel bilancio generale dell'Unione europea degli stanziamenti necessari allo sviluppo del VIS e l'esecuzione di tale parte del bilancio, comprese le misure preparatorie necessarie per gli elementi biometrici che devono essere inseriti in una fase successiva ai sensi delle conclusioni del Consiglio del 19 febbraio 2004 .

(5) Le misure per l'attuazione della presente decisione sono adottate secondo la decisione 1999/468/CE del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione[1]. Il comitato che assiste la Commissione dovrebbe, ove necessario, tenere riunioni in due diverse composizioni a seconda dell'ordine del giorno.

(6) Poiché lo scopo della presente decisione, vale a dire lo sviluppo di un VIS comune, non può essere realizzato in misura sufficiente dagli Stati membri e può dunque, a causa delle dimensioni e degli effetti dell'azione in questione, essere realizzato meglio a livello comunitario, la Comunità può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato. La presente decisione si limita a quanto è necessario per conseguire tale scopo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(7) La presente decisione rispetta i diritti fondamentali e osserva i principi riconosciuti, in particolare nella Carta dei diritti fondamentali dell'Unione europea.

(*) *G.U.C.E.* 15 giugno 2004, L 213/5.
(1) *G.U.C.E. 17 luglio 1999,* L 184/23.

(8) A norma degli articoli 1 e 2 del protocollo sulla posizione della Danimarca allegato al trattato sull'Unione europea e al trattato che istituisce la Comunità europea, la Danimarca non partecipa all'adozione della presente decisione, non è da essa vincolata e non è soggetta alla sua applicazione. Dato che la presente decisione si basa sull'acquis di Schengen in applicazione delle disposizioni della parte terza, titolo IV, del trattato che istituisce la Comunità europea, la Danimarca decide, a norma dell'articolo 5 del succitato protocollo, entro un periodo di sei mesi dall'adozione della presente decisione da parte del Consiglio, se intende recepirla nel proprio diritto interno.

(9) Per quanto riguarda l'Islanda e la Norvegia, la presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen[1], che rientrano nel settore di cui all'articolo 1, lettera B, della decisione 1999/437/CE del Consiglio[2], relativa a talune modalità di applicazione di detto accordo.

(10) È necessario concludere un accordo per permettere a rappresentanti dell'Islanda e della Norvegia di essere associati ai lavori dei comitati che assistono la Commissione nell'esercizio delle sue competenze d'esecuzione. Tale accordo è stato previsto nello scambio di lettere che ha avuto luogo tra la Comunità e l'Islanda e la Norvegia[3] e che è allegato all'accordo in questione.

(11) La presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen al quale il Regno Unito non partecipa, ai sensi della decisione 2000/365/CE del Consiglio, del 29 maggio 2000, riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen[4]. Il Regno Unito non partecipa pertanto alla sua adozione, non è da essa vincolato e non è soggetto alla sua applicazione.

(12) La presente decisione costituisce uno sviluppo delle disposizioni dell'acquis di Schengen al quale l'Irlanda non partecipa ai sensi della decisione 2002/192/CE del Consiglio, del 28 febbraio 2002, riguardante la richiesta dell'Irlanda di partecipare ad alcune disposizioni dell'acquis di Schengen[5]. L'Irlanda non partecipa pertanto alla sua adozione, non è da essa vincolata e non è soggetta alla sua applicazione,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1.È istituito un sistema di scambio tra gli Stati membri di dati relativi ai visti, in seguito denominato «sistema d'informazione visti» (VIS), che permette alle autorità nazionali autorizzate di inserire e aggiornare dati relativi ai visti, nonché di consultare tali dati per via elettronica.

2.Il sistema d'informazione visti è basato su un'architettura centralizzata ed è costituito da un sistema d'informazione centrale, in seguito denominato «sistema centrale d'informazione visti» o «CS-VIS», con un'interfaccia in ciascuno Stato membro, in seguito denominata «interfaccia nazionale» o «NI-VIS», che assicura il collegamento con la competente autorità centrale nazionale del rispettivo Stato membro, e dall'infrastruttura di comunicazione tra il sistema centrale d'informazione visti e le interfacce nazionali.

Articolo 2

1.Il sistema centrale d'informazione visti, l'interfaccia nazionale in ciascuno Stato membro e l'infrastruttura di comunicazione tra il sistema centrale di informazione visti e le interfacce nazionali sono sviluppati dalla Commissione.

2.Le infrastrutture nazionali sono adeguate e/o sviluppate dagli Stati membri.

Articolo 3

Le misure necessarie allo sviluppo del sistema centrale d'informazione visti, dell'interfaccia nazionale in ciascuno Stato membro e dell'infrastruttura di comunicazione tra il

(1) *G.U.C.E.* 10 luglio 1999, L 176/36.
(2) *G.U.C.E.* 10 luglio 1999, L 176/31.
(3) *G.U.C.E.* 10 luglio 1999, L 176/53.
(4) *G.U.C.E.* 1 giugno 2000, L 131/43.
(5) *G.U.C.E.* 7 marzo 2002, L 64/20.

sistema centrale d'informazione visti e le interfacce nazionali sono adottate secondo la procedura di cui all'articolo 5, paragrafo 2, quando riguardano questioni diverse da quelle elencate nell'articolo 4.

Articolo 4

Le misure necessarie allo sviluppo del sistema centrale d'informazione visti, dell'interfaccia nazionale in ciascuno Stato membro e dell'infrastruttura di comunicazione tra il sistema centrale d'informazione visti e le interfacce nazionali sono adottate secondo la procedura di cui all'articolo 5, paragrafo 3, per quanto riguarda i seguenti aspetti:

a) la progettazione dell'architettura fisica del sistema, compresa la relativa rete di comunicazione;
b) gli aspetti tecnici che influiscono sulla protezione dei dati di carattere personale;
c) gli aspetti tecnici con importanti implicazioni finanziarie per i bilanci degli Stati membri o con implicazioni tecniche di rilievo per i sistemi nazionali degli Stati membri;
d) lo sviluppo dei requisiti di sicurezza, compresi gli aspetti biometrici.

Articolo 5

1.La Commissione è assistita dal comitato istituito dall'articolo 5, paragrafo 1, del regolamento (CE) n. 2424/2001 del Consiglio, del 6 dicembre 2001, sullo sviluppo del sistema d'informazione Schengen di seconda generazione (SIS II)[1].

2.Nei casi in cui è fatto riferimento al presente paragrafo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE.

Il periodo di cui all'articolo 4, paragrafo 3, della decisione 1999/468/CE è fissato a due mesi.

3.Nei casi in cui è fatto riferimento al presente paragrafo, si applicano gli articoli 5 e 7 della decisione 1999/468/CE.

Il periodo di cui all'articolo 5, paragrafo 6, della decisione 1999/468/CE è fissato a due mesi.

4.Il comitato adotta il proprio regolamento interno.

Articolo 6

La Commissione presenta una relazione annuale al Parlamento europeo e al Consiglio sulla situazione dello sviluppo del sistema centrale d'informazione visti, dell'interfaccia nazionale in ciascuno Stato membro e dell'infrastruttura di comunicazione tra il sistema centrale di informazione visti e le interfacce nazionali e la prima di tali relazioni è presentata entro la fine dell'anno in cui è firmato il contratto per lo sviluppo del VIS.

Articolo 7

La presente decisione si applica a decorrere dal ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea .

Articolo 8

Gli Stati membri sono destinatari della presente decisione conformemente al trattato che istituisce la Comunità europea.

Lussemburgo, 8 giugno 2004

Per il Consiglio
Il presidente
M. McDowell

(1) *G.U.C.E.* 13 dicembre 2001, L 328/4.

51 Lettera inviata il 30 novembre 2004 dal Gruppo *ex* art. 29 al Presidente del Consiglio dell'UE, Jan Peter Balkenende, al Presidente del Parlamento europeo, Josep Borrell Fontelles, ed al Presidente della Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo, Jean-Louis Bourlanges, in merito alla Proposta di Regolamento del Consiglio sullo standard applicabile agli elementi di sicurezza e biometrici nei passaporti dei cittadini dell'Unione europea (*)

ARTICLE 29 - DATA PROTECTION WORKING PARTY

Brussels, 30 November 2004

Mr. Joseph BORREL FONTELLES
President of the European Parliament
European Parliament
Rue Wiertz
B - 1047 BRUSSELS

Subject: Proposal for a Council Regulation on standards for security features and biometrics in EU citizens's passports

(*) www.europa.eu.int/comm/internal_market/privacy/docs/news/art29-eupassports_en.pdf

52 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 (*)

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

(*) *G.U.C.E.* 29 dicembre 2004, L 385/1.

53 Rete Ue di esperti indipendenti in materia di diritti fondamentali (CFR-CDF) – Rapporto sulla situazione dei diritti fondamentali nell'Unione europea nel 2003 (*)

FUNDAMENTAL RIGHTS SERIES

E.U. NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS
(CFR-CDF)
RÉSEAU U.E. D'EXPERTS INDÉPENDANTS EN MATIÈRE DE DROITS FONDAMENTAUX

REPORT ON THE SITUATION OF FUNDAMENTAL RIGHTS IN THE EUROPEAN UNION IN 2003

January 2004

Reference : CFR-CDF.repEU.2003



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.

(*) http://europa.eu.int/comm/justice_home/cfr_cdf/doc/report_eu_2003_en.pdf

Autorità di controllo comune dell'Europol

54 La seconda relazione di attività dell'Autorità di controllo comune dell'Europol

Novembre 2002 - Ottobre 2004

L'Europol e l'autorità di controllo comune

L'Europol è l'organizzazione creata per assistere gli Stati membri dell'UE nella prevenzione e nella lotta di forme gravi di criminalità organizzata internazionale, soltanto ove ciò implichi una struttura criminale organizzata e riguardi almeno due Stati membri. A livello pratico, l'Europol si occupa principalmente di agevolare lo scambio d'informazioni tra gli Stati membri e fornire competenze in materia di analisi criminologiche.

Poiché l'Europol gestisce un'ingente quantità di dati sensibili a carattere personale, la convenzione Europol contiene una serie di disposizioni che impongono all'Europol di tenere conto dei diritti delle persone nell'utilizzare tali informazioni. La convenzione prevede inoltre l'istituzione dell'autorità di controllo comune (ACC), un organismo indipendente incaricato di assicurare l'ottemperanza dell'Europol ai principi relativi alla protezione dei dati personali.

Al fine di promuovere la trasparenza, la convenzione dell'Europol richiede all'autorità di controllo comune di pubblicare, a intervalli regolari, una relazione sulle attività svolte: il presente documento è la seconda di dette relazioni.

Premessa

Sono onorato di presentare la seconda relazione di attività dell'autorità di controllo comune dell'Europol (ACC). Il documento riguarda il periodo compreso tra novembre 2002 e ottobre 2004 e riflette i risultati conseguiti dall'ACC sotto la presidenza di Klaus Kalk. A nome dei miei colleghi dell'ACC, desidero rendere omaggio alla dedizione di Klaus Kalk al nostro lavoro, nonché alla sua ferma posizione a favore della dignità umana e del diritto fondamentale della protezione dei dati. Sono inoltre consapevole che i risultati ottenuti da questo organismo sono stati possibili soltanto grazie all'impegno e all'entusiasmo di Varges Gomes e Giuseppe Busia, i due presidenti del comitato per i ricorsi in carica nel periodo in questione, unitamente agli sforzi congiunti di tutti i membri dell'ACC e del suo segretariato.

La presente relazione fornisce una rassegna dettagliata dei temi principali di cui si è occupata l'ACC in un periodo fortemente caratterizzato dalle misure adottate per combattere il terrorismo dopo i tragici eventi dell'11 settembre 2001 negli Stati Uniti e, recentemente, dagli attentati di Madrid nel marzo 2004. Nei suoi pareri e nelle iniziative attuate, l'ACC ha dimostrato che è sicuramente possibile, e per nulla incompatibile, sostenere l'obiettivo comune della lotta al terrorismo internazionale e alla criminalità organizzata, salvaguardando nel contempo i diritti dei singoli.

Infine, considerato che i pilastri dell'UE continuano a convergere e la protezione dei dati di natura personale è stata inclusa come diritto fondamentale nella Carta dei diritti fondamentali dell'Unione europea e nel progetto del Trattato costituzionale, risulta sempre più

evidente che il campo della cooperazione di polizia e giudiziaria necessita di norme chiare e specifiche sulla protezione dei dati, con la formulazione di un parere indipendente e di un'attività di controllo armonica. Svariate iniziative riguardanti questo aspetto saranno valutate nei prossimi mesi ed è intenzione dell'ACC seguire con attenzione gli sviluppi, offrendo assistenza e consulenza, con l'intento di assicurare che ogni cambiamento proposto si traduca in un progetto pratico, sempre nel pieno rispetto dei diritti e dei valori della protezione dei dati.

Emilio Aced Félez
Presidente

CAPITOLO I - INTRODUZIONE

Dal momento che, sottoscrivendo il Trattato di Amsterdam, gli Stati membri hanno assunto l'impegno di creare "uno spazio di libertà, sicurezza e giustizia", uno degli obiettivi principali dell'Unione europea è stato quello di intensificare la cooperazione tra le autorità incaricate dell'applicazione della legge. La maggior parte delle volte, tale cooperazione comporta lo scambio di dati personali.

L'atrocità dei recenti attacchi terroristici ha dato nuovo slancio a questa tendenza, promuovendo una più stretta collaborazione; inoltre, la convinzione degli Stati membri della necessità di collaborare per far fronte al terrorismo ha determinato una riconsiderazione delle misure in atto nell'UE a salvaguardia della sicurezza.

Questo primo capitolo presenta un resoconto delle reazioni dell'ACC di fronte ad alcuni dei cambiamenti che si sono verificati in quest'area, concentrandosi in particolare su due situazioni che si sono venute a creare: una determinata dalla decisione presa dal direttore dell'Europol e l'altra conseguente all'iniziativa di aggiornare le disposizioni della convenzione Europol.

L'Europol e gli Stati Uniti

Poco dopo gli attacchi terroristici contro gli Stati Uniti avvenuti nel settembre 2001, il direttore dell'Europol decise di autorizzare la trasmissione di dati personali da parte dell'Europol agli Stati Uniti.

Le norme che disciplinano la trasmissione di dati personali detenuti dall'Europol a Stati terzi solitamente prevedono un accordo ufficiale tra l'Europol e lo Stato in questione, in cui sono indicate le disposizioni riguardanti le categorie di dati da trasmettere e le finalità per cui tali informazioni possano essere impiegate. Un accordo di questo genere non può essere concluso senza aver prima ottenuto il parere dell'autorità di controllo comune (ACC).

In casi eccezionali, tuttavia, il direttore dell'Europol può evitare questa procedura e decidere di trasmettere dei dati personali senza la stipulazione di un accordo, se ritiene che ciò sia assolutamente necessario per tutelare gli interessi fondamentali degli Stati membri oppure per impedire un pericolo imminente.

In risposta alla decisione del direttore, l'ACC ha formulato un parere in cui sottolineava che soltanto un accordo ufficiale avrebbe potuto costituire un fondamento giuridico soddisfacente per una cooperazione a lungo termine tra l'Europol e gli Stati Uniti, e che pertanto in alcun modo la decisione avrebbe potuto essere equivalente a un'autorizzazione illimitata alla trasmissione di dati agli Stati Uniti.

Nel corso delle negoziazioni per la stesura di un accordo tra Europol e gli Stati Uniti, entrambe le parti hanno cercato di risolvere numerose questioni nodali, tra cui le finalità per cui i dati avrebbero potuto essere utilizzati e il problema della supervisione dell'attuazione dell'accordo.

Nel suo parere sul progetto di accordo, l'ACC riconosceva l' "imperativo" di migliorare la cooperazione tra Stati Uniti ed Europol nella lotta contro la criminalità organizzata e, rimar-

cando i notevoli progressi compiuti durante i negoziati, l'ACC concludeva che il Consiglio poteva autorizzare la sottoscrizione dell'accordo da parte del direttore dell'Europol.

L'ACC, tuttavia, sottolineava che considerata la legislazione statunitense in materia di protezione di dati di natura personale, avrebbe dovuto essere esercitato un efficace controllo per garantire l'osservanza delle disposizioni dell'accordo da parte dei suoi sottoscrittori.

In che modo l'ACC controlla l'accordo tra Europol e gli Stati Uniti?

Dalla firma dell'accordo l'ACC ha operato come segue:

ha istituito dei collegamenti con il Chief Privacy Officer (responsabile per la protezione della vita privata) del Dipartimento statunitense della sicurezza interna. Il Chief Privacy Officer ha il compito di assicurare che il Dipartimento della sicurezza interna ottemperi alle disposizioni dell'accordo e ad altre importanti misure relative alla tutele della privacy. Nel marzo 2004, il sostituto del Chief Privacy Officer ha partecipato a una riunione dell'ACC per fornire informazioni sulla legislazione statunitense sulla privacy attualmente in vigore. I membri dell'ACC hanno colto l'occasione per rivolgere delle domande sul preciso ruolo del Chief Privacy Officer. L'ACC è desiderosa di sviluppare ulteriormente questo rapporto in futuro, in quanto costituirà un'opportunità non solo per accertare che cosa avviene dei dati inviati negli Stati Uniti nell'ambito dell'accordo, ma anche per permettere all'ACC di conoscere quali misure siano adottate negli Stati Uniti per verificare la correttezza dei dati inviati all'Europol.

Inoltre, l'ACC ha vigilato sugli sviluppi. L'ACC ha notato che in seguito a cambiamenti della legislazione statunitense, l'FBI non era più tenuto a garantire la correttezza dei dati conservati nel National Crime Information Center, la più grande banca dati penale-giudiziaria del Paese. Questa cambiamento suscita preoccupazione, in quanto l'FBI è una delle autorità federali che, ai sensi dell'accordo, è autorizzata allo scambio di dati personali con l'Europol. L'ACC ha richiesto ulteriori informazioni all'Europol per stabilire se questo cambiamento influirà sui dati personali trasmessi ai sensi del presente accordo. L'ACC si rammarica di non aver ricevuto fino ad oggi una risposta.

L'ACC mantiene fede all'impegno di vigilare sull'ottemperanza all'accordo. Dalla sua sottoscrizione, lo scambio della maggior parte delle informazioni tra l'UE e le autorità di polizia statunitensi sembrerebbe essere avvenuto ai sensi di accordi bilaterali esistenti tra gli Stati Uniti e singoli Stati membri. Tuttavia, dato che il volume di informazioni scambiate tra Europol e Stati Uniti aumenterà, le ispezioni future dell'Europol si concentreranno sull'esame dei dati di natura personale scambiati nell'ambito dell'accordo, per assicurare che vi sia conformità alle disposizioni pertinenti. Inoltre, l'ACC cercherà di coordinare l'attività di vigilanza, collaborando con le autorità nazionali incaricate della protezione dei dati personali negli Stati membri e con il Chief Privacy Officer presso il Dipartimento della sicurezza interna negli Stati Uniti.

L'emendamento della convenzione Europol: tempi di conservazione dei dati

Nel 2002, la Presidenza danese ha varato un'iniziativa per modificare la convenzione dell'Europol. L'autorità di controllo comune ha espresso un parere, in cui commentava le proposte legate al trattamento dei dati di natura personale. La Presidenza danese ha tenuto conto delle perplessità dell'ACC e molte proposte sono state emendate conseguentemente.

Al momento della sua pubblicazione nel dicembre 2002, un progetto di protocollo per emendare la convenzione Europol includeva una proposta di estensione del periodo di conservazione dei dati di natura personale negli archivi di lavoro per fini di analisi. L'Articolo 21 della convenzione Europol stabilisce che le informazioni su una persona conservate in archivi di lavoro per fini di analisi all'Europol devono essere cancellate al più tardi dopo tre anni dalla loro introduzione, se in tale periodo non sono state aggiunte ulteriori informazioni sulla persona in questione. Il progetto di protocollo si prefiggeva di estendere il periodo di conservazione a cinque anni.

Inizialmente l'ACC non riteneva giustificato il prolungamento del periodo di conservazione, nonostante l'Europol sostenesse che, nel caso di alcune forme di criminalità, ed in particolare del terrorismo, fossero necessari periodi di conservazione più lunghi per svolgere analisi efficaci.

Nel febbraio 2003, il gruppo d'ispezione dell'ACC esaminò approfonditamente gli archivi di lavoro per fini di analisi e concluse che periodi di conservazione più lunghi erano indubbiamente necessari in alcuni casi, ma che, per stabilire se dei dati di natura personale dovessero essere conservati o meno, sarebbe stato più utile ricorrere ad una verifica della necessità dell'archivio, anziché ad un limite temporale fisso.

Convinta di ciò, l'ACC ha quindi proposto di emendare la convenzione Europol in modo che il periodo di conservazione fosse collegato all'archivio anziché ai dati di natura personale in esso contenuti. L'Europol dovrebbe cancellare gli archivi di lavoro dopo un periodo di tre anni, salvo nel caso in cui, alla scadenza di tale periodo, l'Europol non ritenga assolutamente necessaria la prosecuzione di un particolare archivio. In tal caso, l'archivio potrebbe restare aperto per altri tre anni.

Sebbene in tal caso l'Europol avrebbe la possibilità di verificare la necessità dell'archivio alla fine di ogni triennio, una volta presa la decisione di tenere attivo un archivio, l'Europol dovrebbe ripetere la procedura per la costituzione di un archivio di lavoro per fini di analisi di cui all'articolo 10 della convenzione Europol. In tal modo, l'ACC e il consiglio di amministrazione dell'Europol avrebbero la possibilità di esaminare le ragioni per mantenere attivo un determinato archivio e il processo sarebbe tenuto sotto controllo, eliminando l'eventualità che un archivio resti aperto illimitatamente.

Per impedire che i dati personali siano conservati anche quando non è più necessario, è stato proposto che la convenzione continui a prevedere l'obbligo per l'Europol di valutare annualmente la necessità di conservare dati personali presenti negli archivi di lavoro. Inoltre, l'ACC potrà chiedere specificatamente al gruppo d'ispezione di esaminare qualsiasi archivio ancora attivo, nel corso di un'ispezione.

L'emendamento proposto dall'ACC è stato approvato e incluso nella versione finale del protocollo per la modificare la convenzione Europol[1].

Collaborare per promuovere la protezione dei dati

Attualmente le iniziative dell'UE che comportano la raccolta, la conservazione o lo scambio di dati personali ai fini dell'applicazione della legge, sono numerose; tra gli esempi più significativi vi sono misure per consentire lo scambio di dati sui passeggeri di voli aerei nonché proposte per richiedere la conservazione dei dati delle comunicazioni. Questi ed altri sviluppi, quali il suggerimento di trasformare un giorno l'Europol in un'agenzia investigativa, potrebbero avere rilevanti implicazioni per i diritti degli individui. Pertanto, l'ACC ha ricercato la collaborazione di altre autorità che si occupano della protezione dei dati per garantire che i responsabili delle decisioni politiche tengano conto dei problemi legati a questo aspetto.

Per un certo periodo di tempo l'ACC è stata schierata con istituzioni omologhe quali l'autorità di controllo comune di Schengen e l'autorità di controllo comune delle dogane, che hanno il compito di vigilare rispettivamente sul sistema d'informazione di Schengen e sul sistema d'informazione doganale. Tutte e tre le autorità di vigilanza si avvalgono dello stesso segretariato con sede a Bruxelles e, tra le iniziative volte a coordinare le loro attività, è rientrata la creazione di un gruppo di lavoro composto da esperti tecnici delle istituzioni nazionali incaricate della protezione dei dati. Questo gruppo, che è stato istituito per fornire sostegno tecnico alle autorità di controllo comune, sta attualmente sviluppando uno strumento standard per l'ispezione dei sistemi d'informazione del terzo pilastro.

Inoltre, in vista di un invito a presentare resoconto dinanzi a un comitato ristretto della "Camera dei Lord" (House of Lords), le tre autorità di controllo comune hanno di recente tenuto una riunione congiunta insieme ai rappresentanti dell'autorità di controllo comune di Eurjoust, da cui è scaturito un parere comune sulla protezione dei dati nell'ambito del terzo pilastro. Sono previsti ulteriori incontri di questo tipo, per consentire alle autorità di controllo comune di esaminare le questioni di mutuo interesse.

È chiaro, tuttavia, che molte delle nuove iniziative dell'Unione europea che riguardano dati personali non fanno parte di mandati specifici delle autorità di controllo comune e,

(1) Atto del Consiglio del 27 novembre 2003 che stabilisce un protocollo recante modifica alla convenzione Europol.

sicuramente, non tutte rientrano in modo netto in uno dei tradizionali pilastri dell'UE.

Per questo motivo, in occasione della conferenza delle autorità incaricate della protezione dei dati svoltasi a Rotterdam nel 2004, è stato deciso che i rappresentanti di quelle autorità che operano a livello comunitario, si riuniscano per coordinare la loro attività. Alla prima riunione di questo gruppo "di pianificazione", che ha avuto luogo nel giugno 2004, hanno partecipato il garante europeo della protezione dei dati, i presidenti delle autorità di controllo comune, la presidenza del gruppo di lavoro dell'articolo 29, che ha il compito di fornire consulenza alla Commissione su questioni inerenti alla protezione dei dati nell'ambito del primo pilastro.

La situazione si è ulteriormente evoluta nel settembre 2004 in occasione della conferenza delle autorità internazionali incaricate della protezione dei dati a Wroclaw, quando una sessione a porte chiuse delle autorità europee ha approvato una risoluzione in cui si chiede che le istituzioni dell'UE promuovano un forum in cui le autorità europee incaricate della protezione dei dati possano discutere le implicazioni a livello di protezione dei dati degli sviluppi del terzo pilastro. Fino alla creazione di tale forum, le iniziative del terzo pilastro che non rientrano nell'ambito di responsabilità delle autorità di controllo comune, saranno esaminate da un gruppo di lavoro delle autorità europee incaricate della protezione dei dati.

CAPITOLO II
PARTE A - ATTIVITÀ DI VIGILANZA

1. Ispezione dell'Europol

La conduzione d'ispezioni in loco delle attività dell'Europol è uno dei modi adottati dall'autorità di controllo comune per ottemperare al suo mandato generale.

Ispezione - Febbraio 2003

Nel dicembre 2003, l'ACC ha dato incarico al suo gruppo d'ispezione di esaminare gli archivi di lavoro per fini di analisi e i sistemi d'informazione dell'Europol, nonché il grado di conformità agli accordi ufficiali tra Europol e Stati terzi.

Nel febbraio 2003, detto gruppo ha condotto un'ispezione di tre giorni presso l'Europol. Nella relazione finale, approvata nel luglio 2003, si dichiarava che il livello di protezione dei dati all'Europol era migliorato dalla prima ispezione effettuata nel 2000, pur notando che l'Europol aveva incontrato problemi per quanto riguarda la salvaguardia della qualità dei dati. Questo era da imputarsi soprattutto al fatto che l'Europol deve affidarsi alla qualità dei dati ricevuti dagli Stati terzi. L'ACC, pertanto, ha proposto alle autorità nazionali incaricate della protezione dei dati di cercare di risolvere questo problema a livello nazionale.

Nel complesso, il gruppo di ispezione ha concluso che, sulla base dei controlli effettuati durante l'ispezione, il trattamento dei dati di natura personale da parte dell'Europol avveniva nel pieno rispetto delle relative disposizioni in materia, osservando che in alcuni campi particolari, quali la verifica e la registrazione dei dati, l'Europol aveva applicato sistemi conformi ad elevati standard di protezione dei dati.

Sono state quindi formulate delle raccomandazioni con l'intento di migliorare ulteriormente la conformità dell'Europol; un'ispezione di verifica ha avuto luogo nel novembre 2003.

Ispezioni - Obiettivi strategici

È chiaro che il ruolo dell'Europol si sta sviluppando rapidamente, con un numero sempre maggiore di dati trattati. Poiché è ferma convinzione dell'ACC che le ispezioni dell'Europol debbano tenere il passo con tali evoluzioni, nel 2003 l'autorità di controllo comune ha fissato una serie di obiettivi volti a guidare le ispezioni future. In sintesi, gli obiettivi sono i seguenti:

- le ispezioni dell'Europol devono avvenire con scadenza annuale;
- occorre ispezionare con particolare attenzione la qualità dei dati personali conservati da Europol;
- infine, il gruppo di ispezione deve godere di una maggior discrezionalità relativamente

alla portata dell'ispezione, disponendo della duttilità necessaria per esaminare particolari aree di interesse nel momento in cui queste si presentino.

Ispezione - marzo 2004

Tenendo conto di questi obiettivi, l'ACC ha approvato una nuova ispezione dell'Europol, sottolineando che avrebbe dovuto incentrarsi sulla qualità dei dati trattati negli archivi per fini di analisi.

L'ispezione, durata tre giorni, è iniziata il 30 marzo 2004. Prima dell'ispezione, il gruppo aveva scelto un certo numero di archivi di lavoro da esaminare. Per ognuno di essi il gruppo valutava la conformità alla decisione costitutiva dell'archivio per stabilire se le categorie di dati personali conservati e gli Stati membri partecipanti all'attività dell'archivio corrispondessero a quelli elencati nella decisione. Da ogni archivio venivano poi estrapolati dei campioni di dati e la loro qualità era confrontata con quella del documento originale.

Nonostante siano state individuate alcune imprecisioni, nel complesso la qualità dei dati è stata ritenuta soddisfacente, almeno per quanto riguarda la rispondenza dei dati negli archivi con quelli forniti dagli Stati membri. Tuttavia, è stata riscontrata un'incapacità generale da parte degli Stati membri di valutare correttamente i dati (verificando la fonte, l'affidabilità e così via). Ancora una volta, l'ACC ha sottolineato che, per risolvere questo problema, occorre migliorare la cooperazione tra Stati Membri ed Europol.

Inoltre, il gruppo ha rilevato che, in alcuni casi, si presentava una palese divergenza tra quanto indicato nella decisione costitutiva di un particolare file e quanto avveniva in realtà. Per esempio, le decisioni costitutive non sempre comprendevano un elenco recente delle parti che contribuivano all'archivio e, in alcuni casi, soltanto alcune delle categorie di dati riportate nella decisione costitutiva venivano realmente trattate nell'archivio. Il gruppo, pertanto, ha raccomandato all'Europol di procedere ad un esame dell'archivio dopo un certo periodo di tempo dalla sua costituzione (per esempio un anno), per chiarire la natura dei contributi degli Stati partecipanti. La decisione costitutiva dovrebbe poi essere aggiornata per rispecchiare la reale portata della partecipazione.

Il sistema d'informazione dell'Europol

All'epoca dell'istituzione dell'Europol, una delle sue priorità era quella di sviluppare un sistema d'informazione a livello europeo, che avrebbe raccolto informazioni su persone sospettate di essere coinvolte in reati che rientrassero nell'area di competenza dell'Europol. Uno dei compiti principali dell'ACC è quello di controllare detto sistema (il sistema d'informazione dell'Europol) e verificare la sua ottemperanza alle disposizioni sulla protezione dei dati.

È opportuno fornire un breve resoconto dello sviluppo del sistema, che è stato irto di difficoltà.

Il processo di pianificazione e sviluppo del sistema ebbe inizio nel 1996. Questioni di carattere contrattuale emersero sin dall'inizio, aggravati da richieste di aggiunte al sistema (per esempio fu deciso di ampliare il sistema per includere funzionalità relative alla falsificazione dell'euro). Pertanto, ci sono state numerose versioni del sistema nel corso del suo sviluppo. Una versione limitata del sistema che consente all'Europol di scaricare la proprie responsabilità relativamente all'euro, è entrata in funzione nel 2001.

Nella relazione annuale 2003 dell'Europol sono stati illustrati i recenti problemi incontrati con la versione finale del sistema.

"Delivery of the Europol Information System (EIS) ... was planned for February 2003. However, it was not delivered due to the underestimation of the number of problems that would arise... The expected revised delivery date of June was met but when delivered, the product was not up to standard." [La consegna del sistema di informazione dell'Europol (Europol Information System - EIS)... era prevista per febbraio 2003. Tuttavia, la consegna non ha potuto aver luogo perché sono stati sottovalutati gli eventuali problemi... . La prevista data di consegna rivista di giugno è stata rispettata ma, il prodotto si è rivelato al di sotto dello standard richiesto.]

Quando la versione finale del sistema sarà operativa negli Stati membri (è stato anticipato che ciò potrebbe avvenire prima della fine del 2004), l'ACC ha intenzione di collaborare con le autorità nazionali incaricate della protezione dei dati per vigilare attentamente sul sistema, tenendo sotto costante sorveglianza il modo in cui viene utilizzato. Inoltre, una buona parte delle ispezioni future saranno dedicate a esaminare il sistema per garantire che ci si attenga alle disposizioni pertinenti sulla protezione dei dati.

2. Europol - Un ruolo di sostegno

Si continua a discutere in merito alla forma che con precisione deve assumere il sostegno in materia di analisi dell'Europol agli Stati membri. Il problema è sorto inizialmente alla luce di una scoperta fatta dal gruppo di ispezione dell'ACC.

Progetti operativi degli Stati membri con il supporto dell'Europol (MSOPES)

Nel corso della prima ispezione dell'Europol avvenuta nel novembre 2000 il gruppo di ispezione scoprì che l'Europol forniva sostegno in materia di analisi a indagini condotte dagli Stati membri. Questi progetti (noti come *Member States' Operational Projects with Europol Support – MSOPES*, ovvero Progetti operativi degli Stati membri con il supporto dell'Europol) prevedevano la creazione di archivi di lavoro per fini di analisi presso l'Europol, la cui responsabilità, tuttavia, era degli Stati membri anziché dell'Europol.

Nonostante l'Europol abbia il compito generico di contribuire alle indagini negli Stati membri, l'articolo 10 della convenzione Europol stabilisce una procedura da seguire quando si costituiscono archivi per fini di analisi all'Europol. Oltre a stabilire le categorie di dati di carattere personale che possono essere conservate in questi archivi, l'articolo prevede che il direttore dell'Europol dia all'ACC la possibilità di esprimersi sulla decisione costitutiva di un archivio. Gli archivi dei MSOPES, tuttavia, non erano costituiti conformemente a questa procedura. L'ACC puntualizzò che la creazione e l'uso di archivi per fini di analisi all'Europol, doveva essere limitato a quanto previsto dall'articolo 10 della convenzione Europol e che, pertanto, la costituzione degli archivi dei MSOPES era illegittima. In considerazione delle preoccupazioni dell'ACC, il Consiglio ha deciso di non creare un fondamento giuridico per i MSOPES, con la conseguente cessazione del funzionamento degli archivi associati.

Squadre investigative comuni

L'ACC sta attualmente valutando la portata del sostegno in materia di analisi fornito dall'Europol nell'ambito di un'altra struttura. Il Trattato di Amsterdam contemplava l'impegno a creare delle "squadre investigative comuni", con l'auspicio che questi gruppi contribuissero a indagini comuni condotte da due o più Stati.

Una decisione quadro del Consiglio[1] ha introdotto delle regole comuni per queste squadre e ha specificato che potevano includere "funzionari di organismi costituiti ai sensi del Trattato sull'Unione europea", una definizione che interessa anche il personale dell'Europol. I particolari specifici riguardanti la partecipazione di Europol a squadre investigative comuni sono quindi stati definiti in un Protocollo adottato dal Consiglio[2]. Anche se le disposizioni del protocollo stabilivano che il personale dell'Europol doveva partecipare con "funzioni di supporto", gli agenti dell'Europol che seguivano una squadra investigativa comune sarebbero stati inseriti nella catena di comando della squadra e le informazioni dell'Europol sarebbero state condivise direttamente attraverso il componenti della squadra dell'Europol; inoltre le informazioni raccolte dalla squadra sarebbero state inserite nelle banche dati dell'Europol.

L'ACC riconosce che dopo la ratifica da parte degli Stati membri del protocollo recante modifica della convenzione, l'Europol potrà partecipare a squadre investigative comuni e scambiare informazioni con gli altri componenti di una squadra in particolare. Ciò tuttavia non comporta un'aggiunta nell'elenco delle autorità con cui l'Europol è attualmente autorizzato a scambiare informazioni. Tuttavia, se la partecipazione ad una squadra investigativa comune dovesse comportare la creazione di archivi per fini di analisi presso l'Europol, si potrebbe stabilire un parallelo con la situazione verificatasi nel caso dei MSOPES, soprattutto dal momento che nel protocollo non si rinviene alcun fondamento giuridico per la costituzione di archivi per fini di analisi al di fuori di quanto previsto dall'articolo 10.

(1) Decisione quadro del Consiglio del 13 giugno 2002 relativa alle squadre investigative comuni.
(2) Atto del Consiglio del 28 novembre 2002 che stabilisce un protocollo recante modifica della convenzione.

L'ACC ha chiesto informazioni in merito all'esistenza di una eventuale politica formulata dall'Europol riguardante il tipo di sostegno che sarebbe offerto alle squadre investigative comuni. In particolare l'ACC si è informata sul modo in cui l'Europol intende utilizzare i suoi servizi di analisi.

Apparentemente il processo decisionale relativamente al tipo di sostegno da fornire alle squadre investigative comuni quando il protocollo sarà stato ratificato da tutti gli Stati membri, è attualmente in corso. Fino alla ratifica del protocollo, l'Europol potrà assistere le squadre investigative comuni conformemente a quanto previsto dalla convenzione Europol. L'Europol ha comunicato all'ACC che il sostegno fornito alle squadre investigative comuni nel frattempo si limiterà all'analisi di informazioni e di dati in linea con le disposizioni della convenzione, all'individuazione di divari nelle informazioni, alla divulgazione di relazioni analitiche che forniscono valutazioni di informazioni assemblate e all'identificazione di nuovi progetti in seguito all'analisi.

L'ACC ha intenzione di vigilare sulla situazione per assicurare il rispetto della convenzione Europol. Sarà particolarmente interessante vedere come l'Europol interpreterà il suo ruolo nelle squadre investigative comuni dopo la modifica della convenzione.

3. Decisione costitutiva di archivi per fini di analisi

Ogni qual volta l'Europol intenda costituire un nuovo archivio di lavoro per fini di analisi ai sensi dell'articolo 10 della convenzione Europol, è necessario adottare una decisione costitutiva. Tale decisione deve stabilire, tra i vari aspetti, le finalità dell'archivio e le categorie di dati di natura personale che possono essere conservati. Le decisioni devono essere approvate dal consiglio di amministrazione dell'Europol, che è obbligato a sottoporle al parere dell'autorità di controllo comune. È politica dell'ACC esprimere il proprio parere su ogni decisione costitutiva.

Nel periodo trattato dalla presente relazione, l'ACC ha formulato osservazioni relativamente a nove decisioni costitutive di archivi per fini di analisi. Nella maggior parte dei casi non ha espresso alcun commento, anche se in un'occasione l'ACC ha chiesto chiarimenti su un certo numero di punti e ha posto domande in merito all'inclusione di alcune categorie di dati nella decisione costitutiva. Europol ha risposto eliminando queste categorie di dati dalla decisione.

Al momento della stesura della presente relazione, Europol stava trattando dati personali in diciannove diversi archivi per fini di analisi.

4. Accordi con Stati/organismi terzi

Se l'Europol intende trasmettere dati personali al di fuori dell'UE, tale trasmissione deve essere preceduta dalla firma di un accordo ufficiale tra l'Europol e lo Stato in questione. Prima della stipulazione di un accordo di questo genere l'Europol deve ricevere il parere dell'ACC.

Negli ultimi due anni l'Europol ha siglato accordi con i seguenti Stati terzi: Repubblica slovacca, Cipro, Lettonia, Lituania e Malta (tutti questi paesi sono nel frattempo entrati a far parte dell'UE, cessando di essere Stati terzi) nonché Bulgaria e Romania. In tutte le occasioni, ha formulato numerose osservazioni a carattere generale, concludendo, tuttavia, che, sotto l'aspetto della protezione dei dati, non sussistevano impedimenti alla sottoscrizione dell'accordo da parte dell'Europol.

Eurojust

L'Europol ha altresì firmato un accordo ufficiale con Eurojust, l'autorità incaricata di migliorare la cooperazione giudiziaria nell'Unione europea. Nel suo primo parere formulato sull'accordo di massima tra Europol e Eurojust, l'ACC ha rilevato che la decisione del Consiglio che istituiva Eurojust prevedeva che il Consiglio consultasse l'autorità di controllo comune dell'Eurojust prima di approvare l'accordo stesso. Poiché in questo caso la procedura coinvolgeva due organismi di controllo comune, l'ACC dell'Europol ha chiarito che, prima di adottare la posizione definitiva, avrebbe voluto conoscere il parere dell'ACC dell'Eurojust. Visto che l'ACC dell'Eurojust non era ancora operativa all'epoca della formu-

lazione del primo parere dell'ACC dell'Europol (maggio 2003), tale primo parere doveva essere considerato un parere provvisorio sull'accordo di massima.

Nel suo parere provvisorio l'ACC sottolineava che, anche dopo la sottoscrizione dell'accordo, i membri nazionali del collegio di Eurojust avrebbero avuto diritto di ricevere dati personali dall'Europol soltanto nell'ambito dell'articolo 6 della decisione del Consiglio relativa alla costituzione di Eurojust e per nessun'altra finalità. Nel parere si suggeriva anche di modificare l'accordo in modo che Europol ed Eurojust fossero obbligati a rispettare eventuali condizioni relativamente all'uso dei dati trasmessi nell'ambito dell'accordo.

Una volta costituita l'ACC dell'Eurojust, il suo presidente e il sig. Kalk (all'epoca presidente dell'ACC dell'Europol) si sono incontrati per discutere l'accordo. Nel dicembre 2003, l'ACC dell'Europol ha espresso un secondo parere in cui si affermava che non sussistevano più impedimenti al perfezionamento dell'accordo, a condizione che lo scambio di dati iniziasse soltanto dopo l'applicazione da parte di Eurojust di misure supplementari per salvaguardare la sicurezza dei dati.

È possibile prendere visione dei pareri dell'ACC sui vari accordi nel sito web dell'ACC all'indirizzo: http://europoljsb.ue.eu.int.

5. Diritti

La convenzione Europol conferisce ai singoli individui numerosi diritti. Ai sensi dell'articolo 19 della convenzione, chiunque ha diritto di accesso a qualsiasi informazione detenuta da Europol che lo riguarda. Se l'informazione relativa al richiedente risulta errata, la persona interessata può domandare all'Europol di sopprimere o correggere l'informazione in questione.

Dai dati forniti dall'Europol emerge che sono state presentate dieci richieste di accesso nel 2002; nel 2003 sono state inoltrate soltanto sei domande e nel 2004 l'Europol ha fino ad ora ricevuto dieci richieste di accesso (a tutto settembre).

Gli interessati possono chiedere all'ACC di garantire la legittimità e la correttezza delle modalità di raccolta, memorizzazione, trattamento e impiego dei dati personali che li riguardano. Sinora, l'ACC ha ricevuto due richieste di questo tipo e, dopo aver effettuato l verifiche necessarie, è risultato che in entrambi i casi l'Europol aveva agito conformemente alla convenzione Europol.

PARTE B - GESTIONE DELL'AUTORITÀ DI CONTROLLO COMUNE

L'autorità di controllo comune si è riunita nove volte dal novembre 2002 all'ottobre 2004. L'ACC è costituita da rappresentanti delle autorità nazionali incaricate della protezione dei dati degli Stati membri. Un elenco dei membri è riportato nel sito web dell'ACC.

I preparativi all'allargamento hanno costituito una delle sfide che l'ACC ha dovuto affrontare; contestualmente, l'autorità di controllo comune ha riflettuto su come garantire maggiore trasparenza e accessibilità più agevole ai suoi utenti. Una breve sintesi di entrambi gli aspetti è illustrata qui di seguito.

1. Preparativi all'allargamento

In occasione della riunione del giugno 2003, l'ACC ha dato il benvenuto a colleghi degli Stati in fase di adesione. Anche se i dieci Paesi avrebbero aderito all'Unione soltanto nel 2004, i rappresentanti degli Stati in fase di adesione sono stati invitati a partecipare a questa riunione e a quelle future in qualità di osservatori, con la speranza che in tal modo acquisiscano familiarità con i lavori dell'ACC. Prima della riunione, è stato distribuito un questionario con l'intento di raccogliere informazioni sia sulla legislazione in materia di protezione dei dati di natura personale in detti Stati, sia sulla misura in cui tale legislazione si applica alle forze di polizia.

Particolarmente incoraggiante è stato apprendere che le autorità incaricate della prote-

zione dei dati negli Stati in fase di adesione si sono impegnate a fondo per creare rapporti di lavoro con le autorità di polizia. Dai risultati del questionario è emerso che, tra le varie iniziative, le autorità incaricate della protezione dei dati hanno condotto ispezioni sulle procedure adottate dalla polizia, hanno svolto verifiche delle condizioni di sicurezza, hanno tenuto riunioni per discutere la politica da adottare e hanno tenuto formazioni per la polizia su questioni relative alla protezione dei dati personali.

L'ACC ha organizzato una visita dell'Europol per gli osservatori per dare loro un'idea di come l'Europol svolge i suoi vari compiti. Nell'ottobre 2003, le delegazioni di cinque Stati in fase di adesione hanno trascorso due giorni al quartiere generale dell'Europol a L'Aia. Erano presenti anche i rappresentanti delle autorità incaricate della protezione dei dati di Islanda e Norvegia, Stati terzi che beneficiano del diritto di partecipare allo scambio di dati personali.

Nonostante gli Stati in fase di adesione siano entrati a far parte dell'UE nel maggio 2004, le loro delegazioni sono diventate membri a pieno titolo dell'ACC soltanto dopo che i rispettivi Paesi hanno aderito alla convenzione Europol, soddisfacendo tutte le condizioni dell'articolo 46. Dal 1° ottobre 2004, le delegazioni che rappresentano le autorità incaricate della protezione dei dati di Cipro, Repubblica ceca, Ungheria, Lettonia, Lituania e Slovacchia sono diventate membri a tutti gli effetti.

In qualità di membri dell'ACC, questi nuovi colleghi ricopriranno un ruolo cruciale nella protezione dei diritti fondamentali in tutta l'Unione europea allargata.

2. Trasparenza

L'ACC svolge le sue funzioni per conto del pubblico e quindi è importante che l'Accstessa e i suoi processi decisionali siano trasparenti.

Il regolamento interno dell'ACC stabilisce che i documenti prodotti dall'autorità di controllo comune sono riservati, tranne nel caso in cui essa non decida altrimenti. È attualmente in corso una modifica del regolamento che prevede l'inversione di questo principio, per cui tutti i documenti saranno accessibili al pubblico a meno non si ritenga che esiste un interesse pubblico prevalente contro la pubblicazione, per esempio nel caso in cui rendere noto un particolare documento possa compromettere seriamente l'attività dell'Europol.

I documenti saranno messi a disposizione del pubblico o direttamente in forma elettronica (nel sito *web* dell'Acc), oppure in seguito ad una richiesta scritta. Ogni domanda di accesso ad un documento comporterà una valutazione dell'eventuale esistenza di motivi per cui il documento non possa essere messo a disposizione. Nei casi in cui soltanto una parte del documento sia esente dalla proibizione di pubblicazione, il documento sarà nuovamente redatto e sarà fornita la versione parziale.

L'ACC si propone di pubblicare tutti i nuovi pareri unitamente alle decisioni del comitato per i ricorsi nel suo sito web all'indirizzo: *http://europoljsb.ue.eu.int*

CAPITOLO III - IL COMITATO PER I RICORSI

Chiunque ha accesso alle informazioni che lo riguardano in possesso dell'Europol ed ha il diritto di richiedere che tali informazioni siano verificate, corrette o soppresse. Chiunque volesse esercitare uno di questi diritti e non fosse soddisfatto della risposta dell'Europol, può appellarsi al comitato per i ricorsi dell'ACC. Nonostante i suoi componenti facciano parte dell'ACC, il comitato per i ricorsi è un organismo autonomo ed imparziale, e non è condizionato da istruzioni dell'ACC. Le decisioni del comitato per i ricorsi sono definitive per tutte le parti interessate.

Sebbene il comitato per i ricorsi abbia deciso in merito a due casi soltanto nel corso degli ultimi due anni, il numero dei ricorsi è aumentato e attualmente vi sono parecchi casi su cui il comitato deve esprimersi. È ragionevole supporre che il numero di ricorsi continuerà ad aumentare a mano a mano che i cittadini impareranno a conoscere l'Europol e saranno mag-

giormente consapevoli dei propri diritti; il comitato per i ricorsi si è pertanto preoccupato di snellire le sue procedure per assicurare che i ricorsi futuri siano trattati celermente.

I due casi illustrati dettagliatamente qui di seguito hanno portato a decisioni relative a importanti questioni di principio.

Nel primo caso, il comitato per i ricorsi ha deciso che l'Europol deve considerare nel merito ogni richiesta di accesso, anziché applicare un approccio generale.

Nel secondo caso, il comitato per i ricorsi ha deciso che l'Europol deve rispondere ad una richiesta di accesso nella lingua in cui tale richiesta è stata formulata, purché essa sia una delle lingue ufficiali dell'Unione europea.

1. Sintesi del ricorso presentato dal signor Y

Il signor Y si è rivolto all'autorità olandese incaricata delle protezione dei dati per chiedere di accedere ad eventuali dati che lo riguardano in possesso dell'Europol. La richiesta è stata inoltrata all'Europol.

Nella sua risposta, l'Europol ha concluso affermando che:

"Ai sensi dell'articolo 19 della convenzione Europol e della legislazione dei Paesi Bassi, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della convenzione Europol".

In risposta a quest'argomentazione, il sig. Y ha presentato un ricorso al comitato per i ricorsi, lamentandosi del "velo di segretezza" che circondava la decisione dell'Europol.

Il diritto di accesso è sancito dall'articolo 19, paragrafo 1, della convenzione Europol e, nonostante l'estensione di tale diritto non sia specificatamente definita alla luce dell'articolo 14, paragrafo 1 delle convenzione Europol, deve essere considerata alla stregua del diritto definito dall'articolo 8 della convenzione d'Europa del 28 gennaio 1981. Tale diritto consente a chiunque di accertare se sono archiviati dati di carattere personale che lo riguardano e, in caso affermativo, gli conferisce il diritto di prenderne conoscenza. Il ricorso del sig. Y riguardava entrambi gli aspetti del diritto di accesso.

Ai sensi dell'articolo 19, paragrafo 3, il diritto di accesso deve essere esercitato conformemente alla legislazione dello Stato membro presso il quale la persona interessata l'ha fatto valere, in questo caso i Paesi Bassi. L'articolo 19, paragrafo 3, stabilisce altresì che, qualora la legislazione dello Stato membro interpellato preveda la "comunicazione relativa ai dati" (con cui si intende sia la comunicazione di un'eventuale trattamento dei dati, sia la comunicazione dei dati che sono trattati), quest'ultima è rifiutata dall'Europol se ciò è necessario per: il corretto svolgimento delle funzioni dell'Europol; per la protezione della sicurezza e dell'ordine pubblico; per la lotta contro i crimini; oppure per la protezione dei diritti di terzi.

Le eccezioni previste al diritto di accesso agli archivi di polizia ai sensi della legislazione olandese sono molto simili a quelli elencati nella convenzione Europol e il comitato per i ricorsi ha stabilito che le disposizioni sia della convenzione Europol, sia della legislazione olandese impongono che, per ogni richiesta di accesso, si proceda a una verifica della necessità di applicare un'eccezione al pieno esercizio del diritto di accesso. Le eccezioni sono ammesse soltanto se gli interessi della polizia o di terzi contano di più dell'interesse della persona interessata nell'esercizio del proprio diritto di accesso.

L'argomentazione dell'Europol per non confermare, né negare l'esistenza di informazioni in suo possesso riguardanti il sig. Y si basa sull'articolo 19, paragrafo 4 della convenzione Europol. In base a questo articolo, se uno Stato membro obietta alla comunicazione dei dati, l'Europol notifica al richiedente che le verifiche sono state effettuate *senza fornire informazioni che possano rivelargli se abbia o meno informazioni sul suo conto.* L'Europol sosteneva che, per poter adempiere a questo obbligo, non avrebbe mai potuto informare apertamente una persona interessata l'effettiva inesistenza presso l'Europol di dati sul suo conto, poiché, facendolo, si consentirebbe ad altri di dedurre che l'Europol detiene informazioni su di loro,

confrontando le varie risposte ricevute dall'Europol. Pertanto, dire al sig. Y che l'Europol non è in possesso di informazioni che lo riguardano, costituirebbe, stando all'argomentazione, un indiretto inadempimento dell'obbligo di cui all'articolo 19, paragrafo 4.

Il comitato per i ricorsi ha rilevato che anche se l'articolo 19, paragrafo 4, impone all'Europol di tenere conto dei desideri delle parti interessate nel trattamento dei dati di natura personale in questione, le disposizioni non stabiliscono la procedura nei casi in cui non sono conservati dati. Il comitato per i ricorsi ha pertanto decretato che la procedura di cui all'articolo 19, paragrafo 4, non doveva essere considerata come un obbligo per l'Europol alla stessa stregua dell'articolo 19, paragrafo 3. Una richiesta di accesso, quando non ci sono dati trattati, deve sempre essere valutata caso per caso e l'Europol non è libero di decidere in merito alla richiesta basandosi soltanto su di un obbligo che esiste in situazioni in cui è in possesso dati personali trattati.

Dopo aver considerato la risposta dell'Europol alla richiesta di accesso del sig. Y, il comitato per i ricorsi ha concluso che la decisione dell'Europol non si basava su di una valutazione del singolo caso e pertanto non era conforme all'articolo 19, paragrafo 3 della convenzione Europol. L'Europol avrebbe almeno dovuto verificare se le eccezioni menzionate nell'articolo 19, paragrafo 3 della convenzione Europol erano applicabili a questo caso in particolare. In assenza di tale evidenza, o anche di elementi che la suggeriscano, l'Europol non avrebbe dovuto rifiutare una comunicazione.

La decisione dell'Europol è stata ritenuta contravvenire alla legislazione olandese applicabile e all'articolo 19, paragrafo 3, della convenzione Europol. Dopo un'attenta valutazione delle informazioni disponibili, il comitato per i ricorsi ha concluso che in questo caso l'articolo 19, paragrafo 3 della convenzione Europol non poteva giustificare un'eccezione al diritto di accesso e ai sensi dell'articolo 19, paragrafo 7 di tale convenzione e ha decretato che l'Europol avrebbe dovuto chiarire al sig. Y che nessun dato che lo riguardava era stato trattato.

2. Sintesi del ricorso presentato dal sig. Z

Dopo aver inoltrato una richiesta di accesso (attraverso l'autorità incaricata della protezione dei dati), il sig. Z ha ricevuto una risposta dall'Europol, in cui si dichiarava quanto segue:

"In conformità con la procedura stabilita dalla convenzione Europol e della legislazione del Belgio, desidero comunicarLe che, facendo seguito alla sua richiesta sono state compiute le verifiche negli archivi dell'Europol. Ai sensi dell'articolo 19 della convenzione Europol e della legislazione del Belgio, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della convenzione Europol".

Il sig. Z ha presentato ricorso al comitato per i ricorsi, comunicandogli successivamente che poiché aveva "scelto l'olandese come lingua ufficiale" voleva una traduzione della decisione dell'Europol, che era stata fornita soltanto in inglese. Il ricorso del sig. Z è stato riconosciuto ammissibile per quanto attiene al suo reclamo di non aver ricevuto una risposta nella propria lingua.

Il comitato per i ricorsi ha chiesto all'Europol perché avesse risposto in inglese, dato che tutta la corrispondenza con il sig. Z era stata in olandese.

L'Europol, a sua volta, ha informato il comitato che rispondere alle domande relative all'articolo 19 in inglese costituiva la procedura standard, tranne nel caso in cui il richiedente chiedesse esplicitamente di volere ricevere una risposta nella propria lingua, nel qual caso l'Europol cercava di soddisfare la richiesta purché ciò non richiedesse eccessivo sforzo. L'Europol non era stato informato, se non dal comitato per i ricorsi, del desiderio del sig. Z di ricevere la traduzione in olandese della risposta alla sua domanda di accesso.

La convenzione Europol non prevede un regime linguistico specifico per l'Europol. Tuttavia, ai sensi dell'articolo 14 della convenzione, il diritto di accesso alle informazioni in possesso dell'Europol deve essere considerato alla stessa stregua di quello contemplato dall'articolo 8 della convenzione del 1981 del Consiglio d'Europa relativo alla protezione dei

dati. L'articolo 8 della convenzione del Consiglio d'Europa dispone che ogni persona deve ottenere la conferma dell'esistenza o meno nel casellario automatizzato dei dati di carattere personale a essa relativi, come pure la trasmissione di tali dati "in forma intelleggibile". Il comitato per i ricorsi ha ritenuto che la lingua in cui le informazioni sono state fornite era rilevante per stabilire se una risposta poteva essere considerata intelleggibile.

Considerando l'Europol un organismo dell'Unione europea che prevede l'attiva partecipazione delle autorità incaricate del rispetto della legge nei singoli Stati membri, il comitato per i ricorsi ha suggerito che, nei casi di domande di accesso ai sensi dell'articolo 19 della convenzione Europol, esso applichi un regola simile a quella contemplata dall'articolo 21 del Trattato che istituisce la Comunità europea, il quale prevede che chiunque scriva a uno qualsiasi degli organismi dell'UE in una lingua ufficiale dell'Unione, riceva una risposta in quella stessa lingua.

Il comitato per i ricorsi ha pertanto deciso che l'Europol non aveva ottemperato ai principi dell'articolo 8 della convenzione del 1981 del Consiglio d'Europa nel rispondere alla richiesta di accesso del sig. Z: l'Europol avrebbe dovuto comunicare la sua decisione nella lingua impiegata dal sig. Z, anche se egli non l'aveva richiesto esplicitamente. Poiché il diritto di accesso ha lo scopo di consentire alle persone interessate di accertarsi che le informazioni che le riguardano siano archiviate conformemente alla legge, l'Europol deve rispondere ai richiedenti nella loro lingua, se questa è una lingua ufficiale dell'UE.

In conclusione il comitato ha osservato che, poiché l'Europol aveva poi fornito al sig. Z una traduzione in olandese della decisione originale, il caso era chiuso. Il comitato per i ricorsi ritiene che l'Europol da allora abbia aggiornato le sue procedure e che adesso risponda alle richieste di accesso nella lingua utilizzata dal richiedente.

È possibile prendere visione di tutte le decisioni del comitato per i ricorsi, unitamente ad altre informazioni sui diritti sanciti dalla convenzione Europol, nel sito web dell'ACC all'indirizzo: http://europoljsb.ue.eu.int

CAPITOLO IV - GLI ULTIMI DUE ANNI

Il primo capitolo della presente relazione fornisce un resoconto del modo in cui l'ACC ha affrontato due situazioni diverse che si sono verificate proprio nel momento in cui l'UE è stata costretta a riflettere sulla sua sicurezza.

Nel trattare questi due casi, l'ACC ha adottato un approccio pragmatico. Il parere dell'ACC sull'accordo dell'Europol con gli Stati Uniti, con il suo riconoscimento della necessità di migliorare la cooperazione, è stato oggetto di critiche da parte di certi ambienti. Ciononostante, l'ACC continua a tener fede al suo impegno di vigilare sull'attuazione dell'accordo per assicurare che questa sia conforme con le disposizioni dell'accordo stesso.

L'ACC ha adottato un atteggiamento proattivo nel proporre la modifica della convenzione Europol e la proposta in sé rispecchia la convinzione dell'ACC che le disposizioni relative alla protezione dei dati contenute nella convenzione Europol non vogliono essere un ostacolo al lavoro dell'Europol, bensì esistono per garantire il rispetto dei diritti dei singoli da parte dell'Europol nello svolgimento dei suoi compiti legittimi.

Anche se l'aggiunta di nuovi colleghi provenienti da dieci nuovi Stati membri ha ovviamente fatto una notevole differenza per l'ACC come organismo, l'allargamento è risultato un fatto positivo e l'ACC sta oggi beneficiando del patrimonio di esperienze dei suoi nuovi membri.

L'ACC ha continuato a svolgere la sua funzione di vigilanza, esaminando tutti gli accordi che l'Europol ha formulato con Stati ed organismi terzi e verificando le decisioni di costituzione di archivi. L'ACC attribuisce una notevole importanza alle ispezioni dell'Europol, in quanto forniscono ai gruppi d'ispezione un'esperienza diretta del lavoro dell'Europol e danno un'idea di come le procedure scritte volte alla salvaguandia dei diritti funzionano realmente nella pratica. L'ACC ha riscontrato che durante queste ispezioni il personale

dell'Europol è estremamente collaborativo e dalle ispezioni di controllo è emerso che l'Europol considera prioritaria l'attuazione delle raccomandazioni dell'ACC.

Nel corso degli ultimi due anni, l'ACC ha cercato di adottare un approccio costruttivo, garantendo nel contempo l'adozione di misure di tutela per salvaguardare i diritti fondamentali.

Il futuro

Ci sono stati molti sviluppi che hanno coinvolto l'Europol negli ultimi due anni e ci sono indicazioni che il ruolo dell'Europol continuerà ad evolversi. La creazione di squadre investigative comuni, per esempio, lascia supporre che le attività dell'Europol siano destinate a diventare di natura sempre più operativa.

Contemporaneamente, degli sviluppi altrove (in particolare i progetti di un sistema d'informazione di Schengen di seconda generazione) hanno suggerito l'idea di rendere interoperativi i sistemi d'informazione dell'Unione con finalità collegate. Tutti questi cambiamenti devono essere affrontati con cautela, specialmente in considerazione dei problemi che sono stati incontrati nello sviluppare il sistema d'informazione dell'Europol. Inoltre qualsiasi intervento in questa direzione dovrebbe essere preceduto da una valutazione del suo impatto sulla privacy, per stabilire le potenziali implicazioni per i diritti delle persone.

Le misure per salvaguardare la protezione dei dati devono andare di pari passo con gli sviluppi, e sarà particolarmente importante assicurare una reale vigilanza dell'Europol, oltreché degli altri sistemi d'informazione a livello europeo. Da parte sua l'ACC ha intrapreso azioni per migliorare la cooperazione con altre autorità incaricate della protezione dei dati nel tentativo di superare le intese alquanto rigide per vigilare sulla protezione dei dati a livello UE. L'ACC si aspetta di contribuire a qualsiasi dibattito relativo a modi per migliorare queste soluzioni.

C'è anche la questione di più vasta portata del controllo parlamentare dell'Europol. Nel 2002 la Commissione ha concluso che le misure di controllo esistenti, adottate per vigilare sull'operato dell'Europol (esercitate dai parlamenti nazionali, dal Parlamento europeo, dalle autorità incaricate della protezione dei dati, dall'ACC e dal consiglio di amministrazione dell'Europol), non erano da considerarsi "giuridicamente insufficienti". Si osservava, tuttavia, che "era necessario qualcosa di più chiaro e trasparente".(1)

Questioni di questo genere non rientrano nell'ambito di responsabilità dell'ACC, ma è chiaro che nel momento in cui i compiti dell'Europol diventeranno sempre più operativi, l'attività di controllo e vigilanza dell'operato dell'Europol dovrà adeguarsi per tenere conto di questo cambiamento.

Obiettivi per i prossimi due anni

Nei prossimi due anni l'ACC si adopererà per:

- svolgere le ispezioni annuali dell'Europol, riservando una particolare attenzione all'attuazione del sistema d'informazione dell'Europol;
- elevare il suo profilo all'interno delle istituzioni dell'UE per assicurare che i problemi relativi alla protezione dei dati siano presi in considerazione al momento della formulazione di nuove iniziative che coinvolgono l'Europol. In particolare, l'ACC ha intenzione di proporre l'instaurazione di regolari contatti con il comitato del Parlamento europeo sulle libertà civili, giustizia e affari interni;
- collaborare con i colleghi dei nuovi Stati membri, aiutandoli a fornire informazioni alle autorità di polizia sulle disposizioni in materia di protezione dei dati della convenzione Europol;
- collaborare con le autorità omologhe e la più vasta comunità che si occupa della protezione dei dati per formulare una risposta coerente e costruttiva alle nuove iniziative che coinvolgono l'impiego di dati personali per finalità legate all'applicazione della legge;
- accrescere la consapevolezza dei diritti conferiti alle persone dalla convenzione Europol;
- continuare a esaminare le decisioni costitutive di archivi e gli accordi per lo scambio di dati di carattere personale con Stati e organismi terzi.

(1) Comunicazione della Commissione al Parlamento europeo e al Consiglio - Controllo democratico dell'Europol 26 febbraio 2002 COM (2002) 95 finale.

Autorità di controllo comune Schengen

55 Il parere 2004 SIS II

1. Introduzione

Nell'intento di garantire che il sistema informativo Schengen di seconda generazione – SIS II – rispettasse gli standard più elevati di protezione dei dati, l'Autorità Comune di Controllo (ACC) si è adoperata per incidere sullo sviluppo del sistema fin dall'inizio.

Nonostante che il Consiglio, nelle conclusioni raggiunte in data 5 e 6 giugno 2003, avesse previsto alcuni requisiti generali per il nuovo sistema, non si è pervenuti ad una decisione definitiva rispetto agli specifici contenuti ed alle funzionalità da includere nel sistema stesso né, elemento questo di essenziale importanza, in merito alle specifiche finalità di questo sistema di seconda generazione[1].

Il presente parere prende in esame l'evoluzione subita dalle finalità per le quali il SIS è stato inizialmente costituito, e passa in rassegna le varie proposte concernenti il SIS II analizzando quali possibili modifiche esse comportino rispetto alla natura del sistema. Infine, sono esposte le motivazioni per le quali l'ACC ritiene che sia necessario giungere quanto prima ad una decisione sui compiti che si intende attribuire al nuovo sistema.

L'ACC continuerà a seguire gli sviluppi del SIS II e fornirà indicazioni più puntuali non appena siano confermate proposte specifiche in merito al sistema.

2. Il Sistema Informativo Schengen

2.1. Il contesto di riferimento

Il SIS è stato costituito inizialmente quale una delle misure compensative previste al fine di consentire la libera circolazione delle persone. Il sistema in quanto tale offriva lo strumento per effettuare controlli alle frontiere ed altri controlli di polizia e doganali.

Poiché le competenti autorità dovevano avere la possibilità di effettuare rapidamente tali controlli, il sistema fu sviluppato secondo una configurazione hit/no-hit. In pratica, ciò significava che la ricerca effettuata nel SIS rispetto ad una determinata persona avrebbe indicato se tale persona era oggetto di una segnalazione e, in caso affermativo, le misure da adottare immediatamente. Si prevedeva che il SIS avrebbe trattato esclusivamente i dati necessari a tal fine, e che ogni ulteriore informazione dovesse essere ottenuta attraverso gli uffici SIRENE.

La Convenzione Schengen ha stabilito chi fosse responsabile del trattamento dei dati contenuti nel SIS, ed ha previsto una serie di garanzie per i diritti degli interessati. Secondo i dati più recenti, nel SIS sono contenute attualmente informazioni relative a circa un milione di individui.

2.2. Il contesto si modifica

Nel 2003, si leggeva quanto segue nelle conclusioni del Consiglio:

"Il SIS è un sistema a configurazione hit/no-hit che consente lo scambio di informazioni

(1) Nel presente documento ogni riferimento alle conclusioni del Consiglio deve intendersi come relativo alle conclusioni dell'incontro del Consiglio europeo nel settore giustizia ed affari interni tenutosi a Lussemburgo il 5 e 6 giugno 2003.

al fine di regolamentare la libera circolazione delle persone e mantenere la pubblica sicurezza, ed in particolare assistere autorità nazionali nella lotta contro la criminalità transnazionale, nel quadro dell'obiettivo fissato dall'UE di mantenere e sviluppare l'Unione come un'area di libertà, sicurezza e giustizia".

Si tratta di una definizione più ampia di quella prevista dall'Articolo 93 della Convenzione di Schengen, e ben segnala il contesto in cui il SIS è venuto a collocarsi dopo l'incorporazione dell'acquis di Schengen nella struttura giuridica e istituzionale dell'Unione europea.

Il potenziamento della cooperazione fra le autorità di polizia nazionali e la creazione di nuovi organismi, come Europol, hanno dato luogo ad una situazione in cui le informazioni detenute nel SIS sono considerate una preziosa risorsa nella lotta alla criminalità ed al terrorismo.

È stato proposto un nuovo Sistema informativo Schengen per fare fronte all'allargamento dell'UE, nella convinzione che tale nuovo sistema avrebbe potuto beneficiare delle nuove tecnologie tenendo conto, al contempo, di altri sviluppi nel settore della giustizia e degli affari interni. È in questo contesto, ed alla luce di questi obiettivi generali, che sono state messe a punto le proposte concernenti il SIS II.

3. SIS II

3.1. Lo sviluppo di un nuovo sistema

Si potrebbe affermare che lo sviluppo di un nuovo sistema del tipo descritto si svolge su tre fronti: il processo decisionale di natura politica, che dovrebbe definire quali siano le finalità previste per il sistema e le relative modalità di funzionamento; il quadro giuridico, che dovrebbe fornire la base giuridica specificando le finalità del sistema e stabilendo le norme relative all'accesso e ad altri elementi; lo sviluppo tecnico del sistema in quanto tale.

La previsione iniziale era che dal Consiglio del giugno 2003 sarebbero dovute emergere proposte ben definite sulle finalità e le funzionalità del SIS II; tuttavia, come sottolineato dal Parlamento europeo nella raccomandazione adottata sul punto, "il Consiglio non ha ancora adottato decisioni in merito a questioni concrete come le nuove categorie di oggetti o persone da inserire".(1)

Questa mancanza di indicazioni univoche ha generato una situazione tale da obbligare la Commissione a formulare una proposta in cui si chiede di garantire la massima flessibilità possibile al nuovo sistema. Pertanto, la messa a punto del sistema avviene sotto l'impulso delle mutevoli istanze provenienti dal settore giustizia e affari interni dell'UE, anziché sulla base di obiettivi espressi e definiti all'interno di un quadro giuridico preciso. Se questo stato di cose dovesse permanere, la natura del sistema potrebbe modificarsi in misura radicale trasformando il SIS II in uno strumento investigativo ed amministrativo multiscopo. Sarebbe un fatto preoccupante che lo sviluppo del SIS II proseguisse in questo modo frammentario, poiché la mancanza di trasparenza connaturata a tale approccio complica la valutazione delle modifiche che tutto ciò comporta rispetto alla natura del sistema stesso.

3.2. SIS II – Uno strumento flessibile

"Fin dalle prime riflessioni sul SIS II è stato chiaro che il sistema dovrebbe essere uno strumento flessibile, ... in grado di adattarsi al mutare delle circostanze e di rispondere, in tempi ragionevoli e senza eccessivi costi e sforzi aggiuntivi, alle richieste formulate dagli utenti durante il suo periodo di operatività".

Il brano sopra riportato è tratto dalle conclusioni del Consiglio del giugno 2003 ed evidenzia un elemento basilare nello sviluppo del SIS II. In effetti, nella sua più recente Comunicazione in merito, la Commissione ha indicato la "flessibilità" fra i requisiti essenziali del nuovo sistema, affermando che "Il SIS II dovrebbe avere le potenzialità per trattare un numero di dati molto più grande e per essere inoltre in grado, una volta che il sistema sarà operativo, di gestire nuovi tipi di informazioni, nuovi oggetti e nuove funzioni, di cui si sta discutendo all'interno del Consiglio".(2)

(1) Raccomandazione del Parlamento europeo al Consiglio sul Sistema informativo Schengen di seconda generazione (SIS II), del 20 novembre 2003.

(2) Comunicazione della Commissione al Consiglio ed al Parlamento europeo: Sviluppo del Sistema di informazione Schengen II e possibili sinergie con un futuro Sistema di informazione visti, dell'11 dicembre 2003.

Il requisito di configurare un sistema flessibile di natura indefinita comporta vari problemi.

In primo luogo, esiste la preoccupazione che un sistema flessibile si presti più facilmente ad una "deriva funzionale", nel senso che le richieste provenienti da un'ampia gamma di organismi ed enti potrebbero dare luogo ad una situazione per cui le informazioni detenute nel sistema verrebbero utilizzate per scopi diversi da quelli inizialmente previsti.

In secondo luogo, è difficile comprendere come sia possibile valutare adeguatamente le implicazioni potenziali del SIS II se il suo sviluppo deve essere flessibile al punto da non fare luce sulla configurazione finale del sistema. La creazione di un sistema caratterizzato da un tale margine di flessibilità in assenza di limitazioni di alcun genere non può che rendere più difficile per chi sta lavorando alla sua messa a punto tenere conto del principio di proporzionalità, che dovrebbe essere uno dei cardini nella definizione di qualsiasi progetto di tale natura.

Man mano che procede lo sviluppo del sistema, ed aumentano gli utenti e le categorie di dati, anche la cornice giuridica dovrà subire un'evoluzione conseguente – non da ultimo perché le garanzie attualmente in vigore per tutelare i diritti degli interessati sono state progettate soltanto in rapporto al SIS nella sua configurazione originale. A parere dell'ACC, il primo passo da compiere al riguardo dovrebbe consistere in una valutazione dell'impatto-privacy per stabilire in quali termini il SIS II e le sue nuove e molteplici funzionalità potrebbero incidere sui diritti degli interessati. Le risultanze di tale valutazione potrebbero successivamente fungere da base per la definizione di una nuova cornice giuridica.

4. SIS II – Le proposte di modifica del sistema

4.1. Accesso al sistema

Le istanze avanzate nei confronti del SIS durante gli ultimi anni riflettono gli sviluppi intervenuti nell'UE per quanto riguarda la lotta alla criminalità ed al terrorismo. Vi è stata, ad esempio, un'iniziativa del Regno di Spagna finalizzata a consentire ad Europol ed Eurojust di accedere al SIS.[1] Permettere a tali soggetti di accedere al sistema comporterà alcune conseguenze sulla natura del SIS II, essendo maggiormente probabile che i dati ricavati dal sistema siano utilizzati operativamente dai due soggetti in questione, ad esempio per quanto riguarda le Squadre Investigative Comuni in ambito Europol. L'ACC resta dell'opinione che le attività in rapporto alle quali si consente l'accesso debbano essere conformi agli articoli della Convenzione Schengen che regolamentano l'accesso a e l'utilizzazione delle informazioni contenute nel sistema.

Consentire che soggetti esterni accedano al SIS può persino modificare radicalmente le finalità per le quali si utilizzano le informazioni presenti nel sistema. In un recente parere su una proposta della Commissione che mirava a concedere l'accesso al SIS alle autorità responsabili dell'immatricolazione dei veicoli, l'ACC ha rilevato che una scelta del genere avrebbe costituito una deviazione rispetto alle finalità originali del sistema in quanto, dando corso alla proposta, il SIS sarebbe stato utilizzato a sostegno della politica comune dell'UE in materia di trasporti.

Ciononostante, la tendenza a consentire ad un numero crescente di soggetti di accedere al SIS sembra destinata a continuare. Il Consiglio ha concluso che altre autorità devono avere la possibilità di accedere al SIS, anche se ciò dovesse comportare la possibilità di "un accesso parziale o per scopi diversi da quelli inizialmente previsti dalla segnalazione".

L'ACC è consapevole dell'essenzialità di un potenziamento della cooperazione fra autorità giudiziarie e di polizia per migliorare la sicurezza in Europa e, in tal senso, potrebbe risultare opportuno consentire ad altri soggetti, in determinati casi, di accedere ai dati presenti nel SIS. Tuttavia, si dovrebbe permettere l'accesso al sistema soltanto se ciò risulti necessario e proporzionato, e non semplicemente perché ne è data la possibilità. È per tale motivo che l'ACC ritiene necessario che si chiariscano le specifiche finalità per le quali Europol ed Eurojust – e qualsiasi altro ente – chiedono di accedere al SIS II. L'adeguamento normativo che dovrebbe accompagnare la messa a punto del nuovo sistema sembra offrire

(1) L'iniziativa è culminata, da ultimo, nell'adozione del Regolamento del Consiglio (CE) n. 871/2004 del 29 aprile 2004.

l'occasione ideale per garantire che le finalità ed i rapporti in questione siano fissati nell'ambito di una chiara cornice giuridica.

Tale cornice giuridica dovrebbe prevedere una serie di limiti all'utilizzabilità dei dati ricavati dal sistema, ed è importante garantire che i soggetti abilitati ad accedere al SIS siano tenuti a rispettare gli stessi standard di protezione dei dati previsti nella Convenzione Schengen ed in altri atti normativi pertinenti, come la Convenzione del Consiglio d'Europa del 1981 sulla protezione dei dati.

L'approccio frammentario seguito nello stabilire quali autorità debbano accedere al SIS continua ad essere fonte di preoccupazione per l'ACC. Nonostante le conclusioni del Consiglio del giugno 2003, e l'intenzione manifestata dalla Commissione di configurare il nuovo sistema con la massima flessibilità possibile, l'ACC ritiene di fare propria la raccomandazione formulata dal Parlamento europeo secondo cui "l'uso dei dati [deve avvenire] per motivi espressamente dichiarati in anticipo". Nella raccomandazione, il Parlamento si opponeva a qualsiasi deroga rispetto a tale principio, "come quella di cui alle conclusioni del Consiglio del 5 e 6 giugno 2003 che chiede lo studio ulteriore della "possibilità per talune autorità di utilizzare i dati SIS a scopi diversi da quelli per i quali essi sono stati inizialmente inseriti nel SIS".

Se si vuole assicurare la possibilità che altri soggetti siano abilitati ad accedere al SIS II una volta che quest'ultimo sia operativo, devono essere stabiliti chiaramente i parametri sui quali basare ogni decisione in materia. Tali parametri dovrebbero essere fissati attraverso norme di rango legislativo che prendano in considerazione, ad esempio, la possibilità di consentire l'accesso sia ai soggetti privati sia a quelli pubblici.

4.2. Le informazioni presenti nel sistema

4.2.1. Ulteriori categorie di dati

Appare verisimile un aumento delle pressioni finalizzate all'ampliamento delle categorie di dati presenti nel sistema, soprattutto perché la proposta di configurare il SIS II come sistema flessibile faciliterà l'aggiunta in futuro di nuove categorie. Vi sono già stati alcuni sviluppi in questo campo. La decisione-quadro del Consiglio che stabilisce un mandato di arresto europeo prevede che le informazioni contenute nel nuovo mandato di arresto siano trattate in ambito SIS. L'aggiunta di nuove categorie di dati potrebbe trasformare il SIS II in un doppione di altri sistemi informativi UE quali il sistema di informazione Europol o il sistema informativo doganale, ed uno sviluppo del genere potrebbe avere riflessi sul livello di protezione dei dati.

L'ACC ritiene che siano necessari parametri univoci onde stabilire quali informazioni possano essere contenute nel SIS II e, ancora una volta, il punto di partenza per giungere ad una decisione in materia non può che essere la valutazione delle finalità del sistema.

4.2.2. Nuove tipologie di dati: identificatori biometrici

Vi sono progetti che prevedono l'introduzione di nuove tipologie di dati, e particolare interesse hanno suscitato i dati biometrici.

Si afferma che è necessario che il SIS II contenga identificatori univoci allo scopo di consentire alle competenti autorità nazionali di risolvere eventuali problemi legati all'identità di singoli individui, e nelle conclusioni del Consiglio si legge che il SIS II dovrebbe permettere "la conservazione, il trasferimento e l'eventuale ricerca di dati biometrici, in particolare fotografie ed impronte digitali".

La Comunicazione della Commissione (dicembre 2003) fornisce alcuni esempi di situazioni nelle quali sarebbe utile disporre di identificatori biometrici. Una di esse riguarda il caso in cui le autorità arrestino una persona in possesso di documenti falsi. Attualmente non sarebbe possibile stabilire, sulla base delle informazioni presenti nel SIS, se sia stata inserita una segnalazione concernente la stessa persona ma sotto altro nome. Tuttavia, se nel sistema fossero conservati anche identificatori biometrici, come le impronte digitali, si potrebbe riuscire a confrontare i rilievi dattiloscopici della persona in oggetto con tutti quelli conservati

nel sistema. In tal modo gli utenti potrebbero stabilire se sia stata inserita o no una segnalazione concernente la stessa persona sotto un altro nome.

In un altro esempio citato per dimostrare l'utilità di accedere a identificatori biometrici, la Commissione menzionava il caso in cui il sistema rilevi uno hit ma la persona in oggetto affermi che la segnalazione riguarda un'altra persona (risulta che i "falsi positivi" siano molto frequenti quando si ha a che fare con nomi di larga diffusione). Si affermava che casi del genere troverebbero rapida soluzione se le autorità potessero confrontare l'identificatore biometrico della persona in oggetto con quello conservato unitamente alla segnalazione presente nel sistema. In tal modo, le autorità sarebbero in grado di stabilire se la persona in oggetto sia realmente quella nei cui confronti era stata inserita una precedente segnalazione.

Questi esempi illustrano i due possibili campi di applicazione delle tecnologie biometriche incorporate in un sistema di informazione. La prima opzione, in cui l'utente effettua una ricerca su tutti gli identificatori biometrici nel sistema fino a trovare una corrispondenza (one-to-many), è nota come sistema di "identificazione"; la seconda opzione, in cui l'identificatore biometrico di uno specifico individuo viene confrontato con una specifica segnalazione presente nel sistema per stabilire se si tratti della stessa persona (one-to-one), è nota come sistema di "verifica".

L'affidabilità dei due sistemi è diversa, come diversi sono gli scopi per i quali i due sistemi possono essere utilizzati; tuttavia, quale che sia il sistema prescelto, siamo di fronte ad un altro esempio di decisione da assumere partendo dalla valutazione delle finalità del sistema ed applicando un test di proporzionalità.

4.2.3. Nuove tipologie di dati: alcune garanzie fondamentali

L'inserimento di dati biometrici comporta tutta una serie di problemi di natura pratica che attendono ancora soluzione (ad esempio, le modalità di raccolta degli identificatori biometrici), e fin quando non saranno disponibili progetti più dettagliati sarà difficile individuare le garanzie ulteriori da prevedere; tuttavia, l'inserimento di dati biometrici richiederebbe quantomeno la definizione di un chiaro quadro giuridico, in cui si stabilisca con precisione in quali circostanze e per quali scopi sia consentito effettuare interrogazioni su dati biometrici. Si tratta di un elemento di particolare importanza, poiché l'inserimento di dati biometrici aumenta la probabilità di una deriva funzionale: vari soggetti, ed in particolare le autorità giudiziarie e di polizia, potrebbero sfruttare la prevista flessibilità del SIS II per chiedere l'accesso a dati biometrici in rapporto ad una molteplicità di scopi.

I rischi sarebbero ancora più consistenti se i dati biometrici fossero conservati nelle sezioni nazionali oltre che nella sezione centrale del SIS II, in quanto le autorità giudiziarie e di polizia dei singoli Stati avrebbero maggiori occasioni di utilizzare tali dati per finalità che esulano da quelle previste nella Convenzione di Schengen.

Per garantirsi contro una simile eventualità, si dovrebbe prevedere la registrazione degli accessi a queste nuove categorie di dati e l'effettuazione di verifiche periodiche del sistema onde assicurare che ai dati si acceda soltanto per scopi legittimi e da parte di soggetti autorizzati. Inoltre, nelle norme concernenti la conservazione di nuove tipologie di dati deve essere specificato con chiarezza che tali dati possono essere conservati esclusivamente per il periodo necessario a raggiungere uno scopo determinato.

4.3. Nuove funzionalità tecniche

Uno dei motivi alla base dello sviluppo del SIS II era la volontà di beneficiare delle nuove tecnologie introducendo nuove funzionalità. Si propone che il SIS II consenta la "interconnessione" delle segnalazioni presenti nel sistema al fine di migliorarne l'efficienza. L'ACC ha indicato che, prima di procedere in tal senso, è necessario prevedere il quadro giuridico di riferimento e, in un precedente parere, ha segnalato che l'interconnessione delle segnalazioni potrebbe permettere agli utenti di accedere ad informazioni per le quali non sono abilitati. Pertanto, l'ACC accoglie con favore l'affermazione contenuta nelle conclusioni del Consiglio, secondo cui è necessario prevedere garanzie atte ad assicurare che l'interconnessione di segnalazioni "non modifichi i diritti di accesso in essere rispetto alle singole categorie di segnalazioni".

Ciononostante, l'interconnessione di segnalazioni rappresenta un esempio di funzionalità in grado di modificare la natura del sistema, che da sistema di informazione diventerebbe un sistema di investigazione.

5. Controllo del SIS II

L'architettura proposta per il nuovo sistema solleva alcuni interrogativi in materia di controllo e monitoraggio. Se il sistema aumenta il proprio grado di centralizzazione, quale dovrà essere l'evoluzione dei meccanismi di controllo? Può darsi che l'ACC abbia bisogno di maggiori poteri per far fronte ad eventuali modifiche nell'architettura del sistema.

Nella Comunicazione della Commissione si afferma che le Parti contraenti sono libere di scegliere se mantenere un database nazionale, oppure prevedere soltanto un'interfaccia nazionale ed interrogare direttamente il sistema centrale. Quali potrebbero essere le implicazioni di una modifica del genere?

Attualmente, la Convenzione di Schengen conferisce alle autorità nazionali di protezione dei dati il potere di controllo sulla rispettiva sezione nazionale del sistema. Se le sezioni nazionali fossero sostituite da un'interfaccia, ciò avrebbe ripercussioni sul controllo nazionale e potrebbe rendersi necessario modificare in conseguenza i poteri conferiti alle autorità nazionali. Sorgerebbe, inoltre, l'esigenza di garantire che tutte le pertinenti autorità nazionali dispongano di risorse sufficienti per svolgere in modo efficace la propria funzione di controllo del sistema. In ogni caso, nel dibattito a venire sul controllo ed il monitoraggio del SIS II dovrebbero essere coinvolte le autorità nazionali di protezione dei dati nonché l'ACC ed il Garante europeo della protezione dei dati, da poco nominato.

6. Conclusioni

Anche ammettendo che non vi sia l'intento di modificare la natura del SIS, che è un sistema di controllo del tipo hit/no-hit, l'ACC ritiene che l'aggiunta di nuove funzionalità (come l'interconnessione di segnalazioni), l'inserimento di nuove categorie di dati, e la tendenza ad ampliare il novero dei soggetti autorizzati ad accedere al sistema possano dar luogo, congiuntamente alla prevista flessibilità del nuovo sistema, ad una modifica de facto della natura del sistema stesso, trasformando il SIS II in uno strumento di indagine.

Non si tratta di una novità assoluta, visto che nel 2001 la stessa Commissione ha affermato quanto segue:

"La Commissione desidera sottolineare l'importanza di progredire nella definizione delle funzionalità del SIS. In particolare, alcune delle proposte attualmente in discussione comporterebbero modifiche sostanziali delle finalità del SIS, trasformandolo da sistema di informazione in sistema di informazione e di indagine."[1]

Ci sono validi motivi per nutrire preoccupazioni rispetto a questo tipo di sviluppi. In primo luogo, esiste la possibilità che il SIS II, man mano che incorporerà nuove categorie di dati, duplichi sistemi di informazione già esistenti in ambito UE. In secondo luogo, è necessario aggiornare le norme sulla protezione dei dati per garantire che il nuovo sistema, con le sue mutate potenzialità, non incida sui diritti degli interessati – e queste norme saranno sempre un passo indietro se non si fisseranno limiti alle modalità di sviluppo del sistema. Inoltre, è essenziale che il SIS II si sviluppi in conformità con il principio di proporzionalità, ossia che le funzionalità e le categorie di dati presenti nel SIS II non eccedano quanto è necessario per raggiungere gli scopi del sistema. Tuttavia, prima occorre stabilire quali siano queste finalità, e successivamente si potrà procedere a tale verifica.

L'ACC ribadisce che non è possibile risolvere le questioni tecniche e giuridiche senza che vi sia prima una decisione politica sulle finalità prefigurate per il SIS II, e che sarebbe opportuno stabilire in modo particolareggiato quali siano le funzionalità e le categorie di dati delle quali il sistema dovrebbe disporre per raggiungere tale obiettivo.

Inoltre, non sembra che, al momento, vi siano iniziative in seno al Consiglio finalizzate

(1) Comunicazione della Commissione al Consiglio ed al Parlamento europeo: Sviluppo del Sistema di informazione Schengen II, 18 dicembre 2001.

alla definizione di un nuovo quadro giuridico per il SIS II e, per le motivazioni esposte in questo parere, l'ACC sollecita a dare corso quanto prima a queste iniziative. Le risultanze di una valutazione dell'impatto-privacy potrebbero rivelarsi utili nella formulazione di tale cornice giuridica e, attraverso una valutazione di questo tipo, si potrebbero prendere in considerazione le tematiche attinenti al controllo del sistema ed alla necessità di garanzie ulteriori, oltre ad esaminare eventuali proposte connesse quali la ventilata sinergia fra SIS II ed un nuovo Sistema di informazione visti.

Per parte sua, l'ACC è pronta a collaborare in ogni modo possibile. Inoltre, alla luce delle significative implicazioni per il SIS II legate alle proposte in oggetto, l'ACC ritiene auspicabile che ogni ulteriore sviluppo le sia comunicato con tempestività in modo da disporre del tempo necessario per formulare indicazioni che possano successivamente essere tenute presenti dagli attori del processo decisionale.

Bruxelles, 19 maggio 2004

56 Attività dell'Autorità di controllo comune - Sesto Rapporto gennaio 2002 - dicembre 2003 (*)

JSA ACC SCHENGEN

Sixth report

january 2002 / december 2003



Activities of the Joint Supervisory Authority

SCHENGEN

www.schengen-jsa.dataprotection.org

(*) www.schengen-jsa.dataprotection.org/garante/document?ID=571347

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

(art. 29 direttiva 95/46/CE)

57

Parere 1/2004 sul livello di protezione garantito in Australia per la trasmissione dei dati delle registrazioni dei nomi dei passeggeri da parte delle compagnie aeree (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10031/03/IT
WP 85

PARERE 1/2004 SUL LIVELLO DI PROTEZIONE GARANTITO IN AUSTRALIA PER LA TRASMISSIONE DEI DATI DELLE REGISTRAZIONI DEI NOMI DEI PASSEGGERI DA PARTE DELLE COMPAGNIE AEREE

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp85_it.pdf

Adottato il 16 gennaio 2004

58 Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da *Trusted Computing Group* (Gruppo TCG) (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali



11816/03/FR
WP 86

DOCUMENTO DI LAVORO SULLE PIATTAFORME INFORMATICHE FIDATE, IN PARTICOLARE PER QUANTO RIGUARDA IL LAVORO EFFETTUATO DA TRUSTED COMPUTING GROUP (GRUPPO TCG)

Adottato il 23 gennaio 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp86_it.pdf

59

Parere 2/2004 sul livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche Passeggeri (PNR - *Passenger Name Records*) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (*Bureau of Customs and Border Protection* - US CBP) (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali



10019/04/IT
WP 87

PARERE 2/2004 SUL LIVELLO DI PROTEZIONE ADEGUATO DEI DATI A CARATTERE PERSONALE CONTENUTI NELLE PRATICHE PASSEGGERI (PNR - PASSENGER NAME RECORDS) TRASFERITE ALL'UFFICIO DELLE DOGANE E DELLA PROTEZIONE DI FRONTIERA DEGLI STATI UNITI (BUREAU OF CUSTOMS AND BORDER PROTECTION - US CBP)

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_it.pdf

Adottato il 29 gennaio 2004

60 Parere 3/2004 sul livello di protezione assicurato in Canada ai fini della trasmissione da parte di vettori aerei dei *Passenger Name Records* e di informazioni avanzate sui passeggeri (*)

ARTICLE 29 Data Protection Working Party

10037/04/EN
WP 88

OPINION 3/2004 ON THE LEVEL OF PROTECTION ENSURED IN CANADA FOR THE TRANSMISSION OF PASSENGER NAME RECORDS AND ADVANCED PASSENGER INFORMATION FROM AIRLINES

Adopted on 11th February 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp88_en.pdf

61 Parere 4/2004 relativo al trattamento dei dati personali mediante videosorveglianza

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali



11750/02/IT
WP 89

PARERE 4/2004 RELATIVO AL TRATTAMENTO DEI DATI PERSONALI MEDIANTE VIDEOSORVEGLIANZA.

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp89_it.pdf

Adottato l'11 febbraio 2004

62 Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'articolo 13 della direttiva 2002/58/CE

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali



11601/IT
WP 90

PARERE 5/2004 RELATIVO ALLE COMUNICAZIONI INDESIDERATE A FINI DI COMMERCIALIZZAZIONE DIRETTA AI SENSI DELL'ARTICOLO 13 DELLA DIRETTIVA 2002/58/CE.

Adottato il 27 febbraio 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp90_it.pdf

63 Documento di lavoro sui dati genetici (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali



12178/03/IT
WP 91

DOCUMENTO DI LAVORO SUI DATI GENETICI

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp91_it.pdf

Adottato il 17 marzo 2004

64 Dichiarazione comune in risposta agli attentati terroristici di Madrid (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10649/04/IT
WP 93

DICHIARAZIONE COMUNE IN RISPOSTA AGLI ATTENTATI TERRORISTICI DI MADRID

Adottata il 17 marzo 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp93_it.pdf

65

Parere 6/2004 sull'attuazione della Decisione della Commissione del 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti (*United States Bureau of Customs and Border Protection*), e dell'Accordo fra la Comunità europea e gli Stati Uniti d'America sul trattamento ed il trasferimento di dati PNR da parte di vettori aerei al *Department of Homeland Security, Bureau of Customs and Border Protection* degli Stati Uniti (*)

ARTICLE 29 Data Protection Working Party



11221/04/EN
WP 95

OPINION 6/2004 ON THE IMPLEMENTATION OF THE COMMISSION DECISION OF 14-V-2004 ON THE ADEQUATE PROTECTION OF PERSONAL DATA CONTAINED IN THE PASSENGER NAME RECORDS OF AIR PASSENGERS TRANSFERRED TO THE UNITED STATES' BUREAU OF CUSTOMS AND BORDER PROTECTION, AND OF THE AGREEMENT BETWEEN THE EUROPEAN COMMUNITY AND THE UNITED STATES OF AMERICA ON THE PROCESSING AND TRANSFER OF PNR DATA BY AIR CARRIERS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY, BUREAU OF CUSTOMS AND BORDER PROTECTION

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp95_en.pdf

Adopted on 22nd June 2004

66

Parere 7/2004 relativo all'inserimento di elementi biometrici nei permessi di soggiorno e nei visti, alla luce dell'istituzione del Sistema informativo europeo sui visti (VIS) (*)

ARTICLE 29 Data Protection Working Party

11224/04/EN
WP 96

OPINION NO 7/2004 ON THE INCLUSION OF BIOMETRIC ELEMENTS IN RESIDENCE PERMITS AND VISAS TAKING ACCOUNT OF THE ESTABLISHMENT OF THE EUROPEAN INFORMATION SYSTEM ON VISAS (VIS)

Adopted on 11 August 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp96_en.pdf

67 Parere 8/2004 sull'informazione dei passeggeri in merito al trasferimento di schede nominative dei passeggeri aerei (PNR) sui voli tra l'Unione europea e gli Stati Uniti d'America (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali



1173*30/04/IT*
WP 97

PARERE 8/2004 SULL'INFORMAZIONE DEI PASSEGGERI IN MERITO AL TRASFERIMENTO DI SCHEDE NOMINATIVE DEI PASSEGGERI AEREI (PNR) SUI VOLI TRA L'UNIONE EUROPEA E GLI STATI UNITI D'AMERICA

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp97_it.pdf

Adottato il 30 settembre 2004

68 Documento strategico (*)

ARTICLE 29 Data Protection Working Party

11648/04/EN
WP 98

STRATEGY DOCUMENT

Adopted on 29 September 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp98_en.pdf

69 Parere 9/2004 relativo ad una proposta di Decisione Quadro sulla memorizzazione di dati trattati e conservati allo scopo di fornire servizi pubblici di comunicazioni elettroniche o di dati disponibili su reti pubbliche di comunicazioni, ai fini della prevenzione, delle indagini, dell'accertamento e del perseguimento di atti criminali, compreso il terrorismo [Proposta presentata da Francia, Irlanda, Svezia e Gran Bretagna (Documento del Consiglio 8958/04 del 28 aprile 2004)] (*)

ARTICLE 29 Data Protection Working Party

11885/04/EN
WP 99

OPINION 9/2004 ON A DRAFT FRAMEWORK DECISION ON THE STORAGE OF DATA PROCESSED AND RETAINED FOR THE PURPOSE OF PROVIDING ELECTRONIC PUBLIC COMMUNICATIONS SERVICES OR DATA AVAILABLE IN PUBLIC COMMUNICATIONS NETWORKS WITH A VIEW TO THE PREVENTION, INVESTIGATION, DETECTION AND PROSECUTION OF CRIMINAL ACTS, INCLUDING TERRORISM. [PROPOSAL PRESENTED BY FRANCE, IRELAND, SWEDEN AND GREAT BRITAIN (DOCUMENT OF THE COUNCIL 8958/04 OF 28 APRIL 2004)]

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_en.pdf

Adopted on 9th November 2004

70 Parere relativo ad una maggiore armonizzazione delle informative (Allegato n. 1) (*)

Euro-Company

Short Privacy Notice

A complete privacy notice is available on request

Dated: October 2004

• We keep the personal information you give us to help provide you with the products and services you require

• We may also pass on your details to other companies who may contact you about their products. You can opt out of this byticking the box below

For the full privacy notice or for access or correction, contact:

• Privacy Department
Euro Company ******

•Call 00 ******

•Or go to the Privacy notice on our website at euro.com

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp100appendix1_en.pdf

71 Dichiarazione del Gruppo di lavoro *ex* art. 29 sulle attività di *enforcement* (*)

ARTICLE 29 Data Protection Working Party

12067/04/EN
WP 101

DECLARATION OF THE ARTICLE 29 WORKING PARTY ON ENFORCEMENT

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp101_en.pdf

Adopted on 25th November 2004

72 Lista di controllo Istanza di approvazione di norme aziendali vincolanti (*Binding Corporate Rules*)(*)

ARTICLE 29 Data Protection Working Party

12110/04/EN
WP 102

MODEL CHECKLIST
APPLICATION FOR APPROVAL OF BINDING CORPORATE RULES

Adopted on 25th November 2004

(*) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp102_en.pdf

Consiglio d'Europa

73 Principi guida per la protezione dei dati personali in relazione alle "carte intelligenti" (*smart card*) (*)

INTRODUZIONE

I comitati del Consiglio d'Europa che si occupano di questioni attinenti la protezione dei dati desideravano richiamare l'attenzione su alcuni aspetti specifici della tutela dei dati personali in relazione all'impiego di "carte intelligenti" (smart cards). Il Gruppo di progetto sulla protezione dei dati (CJ-PD) del Consiglio d'Europa ha, pertanto, chiesto ad un consulente, il dr. Karel Neuwirt (Presidente dell'Autorità ceca per la protezione dei dati), di redigere una Relazione sulla protezione dei dati in rapporto all'impiego di smart cards. Nella Relazione si riconosceva che qualunque studio in materia sarebbe stato necessariamente connesso agli sviluppi tecnologici e, pertanto, avrebbe dovuto essere collocato nel rispettivo contesto storico. Si esprimeva dunque l'auspicio di redigere un elenco di principi-guida specifici dei quali tenere conto in riferimento all'impiego di smart cards.

Dopo avere esaminato la Relazione del dr. Neuwirt ed i principi-guida ad essi allegati, il CJ-PD ha accettato di rivedere e specificare meglio alcuni di essi ed ha predisposto il documento di seguito riportato.

Ai fini dei presenti principi-guida, per "smart card" si intende un vettore mobile di dati personali dotato di funzioni automatiche di elaborazione, il quale viene rilasciato ad un interessato ed è in grado di trattare dati personali secondo le finalità e le specifiche del soggetto che lo rilascia in rapporto ad un sistema informativo cui tale vettore è collegato. La carta può essere utilizzata, ad esempio, al fine di identificare l'interessato, di svolgere operazioni che non possono essere effettuate in forma anonima, o di consentire l'accesso a luoghi o database specifici. È necessario distinguere la *smart card* dalle carte a banda magnetica o di memorizzazione, le quali non possono essere utilizzate per effettuare autonome operazioni sui dati secondo criteri logici ed aritmetici.

Le *smart card* trovano impiego crescente per una vasta gamma di applicazioni. Le caratteristiche e le potenzialità delle smart card sollevano numerosi interrogativi in termini di protezione dati, ai quali è necessario fornire risposta. Ad esempio, chi ha la titolarità dei dati personali utilizzati dal sistema? Chi è responsabile dell'accuratezza e della sicurezza dei dati qualora il sistema sia accessibile ad una pluralità di soggetti diversi? Come evitare il moltiplicarsi dei rischi di possibili violazioni della privacy dei cittadini a causa dell'impiego di tecnologie legate alle smart card? Chi deve accedere ai dati personali dell'interessato, ed a quali condizioni? ecc.

I sistemi d'informazione che utilizzino smart card associate al trattamento di dati personali ricadono nell'ambito di applicazione della Convenzione del Consiglio d'Europa per la protezione delle persone con riguardo al trattamento automatizzato di dati personali [ETS 108] (nel prosieguo, "Convenzione 108"). Tale Convenzione è stata elaborata quando ci si è resi conto che, al fine di garantire un'efficace tutela giuridica dei dati personali, sarebbe stato necessario sviluppare in modo più specifico ed organico il riferimento generico al rispetto per la vita privata contenuto nell'Articolo 8 della Convenzione per la tutela dei diritti umani e delle libertà fondamentali (nel prosieguo, "CEDU").

Diritti e garanzie ulteriori sono previsti in varie Raccomandazioni del Consiglio d'Europa, fra cui in particolare:

(*) Adottati dal CDCJ [Gruppo di progetto sulla cooperazione giuridica] in occasione della sua 79ma riunione plenaria (11-14 maggio 2004).

a) la Raccomandazione N. R(2002)9 sulla protezione dei dati personali raccolti e trattati per scopi assicurativi,
b) la Raccomandazione N. R(99)14 sul servizio universale, relativa ai nuovi servizi di comunicazione ed informazione,
c) la Raccomandazione N. R(99)5, per la tutela della privacy su Internet,
d) la Raccomandazione N. R(97)5, sulla protezione dei dati sanitari,
e) la Raccomandazione N. R(95)4, sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici,
f) la Raccomandazione N. R(90)19, sulla protezione dei dati personali utilizzati per operazioni di pagamento e per altre operazioni connesse,
g) la Raccomandazione N. R(89)2, sulla protezione dei dati personali utilizzati nel rapporto di lavoro,
h) la Raccomandazione N. R(86)1, sulla protezione dei dati personali utilizzati per scopi di previdenza sociale,
i) la Raccomandazione N. R(85)20, sulla protezione dei dati personali utilizzati per scopi di marketing diretto.

Numerosi sono i documenti e le attività del Consiglio d'Europa, in particolare attraverso i gruppi di esperti che si occupano di protezione dei dati personali, connessi indirettamente alle questioni sollevate dall'utilizzazione di smart card. In particolare, poiché le smart card possono essere utilizzate per la memorizzazione di dati biometrici, si richiama l'attenzione sui principi-guida relativi alla protezione dei dati personali sotto forma di dati biometrici attualmente in via di definizione da parte del T-PD. Le tecnologie moderne arrecano molteplici vantaggi alla vita quotidiana dei cittadini, ma comportano anche alcuni rischi legati alla possibilità di ingerenze nella privacy delle persone. Pertanto, il presente documento non si propone di descrivere i vantaggi dell'utilizzazione di smart card, bensì di specificare l'approccio da seguire per migliorare la tutela dei dati personali qualora si utilizzino tecnologie connesse alle smart card.

La raccolta ed il trattamento di dati personali in sistemi che utilizzino smart card devono rispettare tutti i principi fissati dalla normativa nazionale in materia di protezione dei dati personali.

I principi-guida che seguono non intendono fornire una risposta esauriente a tutti gli interrogativi concernenti la protezione dei dati che nascono dall'utilizzazione di smart card. Una smart card viene sempre utilizzata nell'ambito di un sistema d'informazione più ampio, e l'effettività della protezione complessiva dei dati personali utilizzati in un sistema del genere dipende da fattori e circostanze numerosi e di natura diversa. Anche la sicurezza del sistema dipende in larga parte dal comportamento di coloro che vi hanno a che fare. La tecnologia legata alle smart card sta attraversando una fase di rapidissimo sviluppo. I principi-guida in questione vogliono fissare alcuni principi fondamentali che non subiranno modifiche significative in rapporto alle innovazioni introdotte in campo tecnologico. Cionondimeno, può essere opportuno integrare tali principi alla luce degli incessanti sviluppi in questo settore.

È necessario ricordare che, nella misura in cui i presenti principi-guida contengano garanzie per i diritti e le libertà fondamentali di ognuno, ed in particolare per il diritto al rispetto della vita privata, sanciti negli Articoli 5, 6 ed 8 della Convenzione 108 e nell'Articolo 8 della CEDU, è possibile derogare a tali diritti, ai sensi dell'Articolo 9 della Convenzione 108, elaborato sulla base dell'Articolo 8 della CEDU, se ciò è previsto da norme di legge e costituisce una misura necessaria in una società democratica nell'interesse
a. della tutela della sicurezza dello Stato, della sicurezza pubblica, degli interessi economici dello Stato, o della repressione dei reati;
b. della tutela dell'interessato o dei diritti e delle libertà altrui.

Per quanto concerne tali deroghe, è opportuno sottolineare che esse vanno interpretate in maniera restrittiva e devono essere applicate solo in casi eccezionali, secondo le indicazioni fornite dalla giurisprudenza della Corte europea dei diritti umani relativa al comma 2 dell'Articolo 8 della CEDU.

I principi-guida sono rivolti precipuamente ai soggetti che rilasciano la carta, i quali hanno la responsabilità primaria della protezione dei dati personali in essa contenuti. I prin-

cipi si rivolgono, inoltre, a tutti gli altri soggetti che partecipano ai sistemi d'informazione: progettisti, gestori, operatori, e gli stessi interessati. Tutti i soggetti in questione dovrebbero tenere presenti i principi enunciati nel prosieguo. I principi elaborati dovrebbero essere applicati con la massima coerenza possibile; solo in tal modo sarà possibile contribuire alla diffusione di applicazioni basate su smart card che consentano la massima interoperabilità a livello internazionale e gli standard più elevati di sicurezza.

PRINCIPI GUIDA

1. La raccolta ed il trattamento di dati personali attraverso smart card devono avvenire in modo lecito e leale. Si deve prevedere di raccogliere e memorizzare sulla carta soltanto i dati personali necessari a raggiungere gli scopi per i quali la carta stessa è utilizzata. I sistemi che utilizzano smart card devono essere trasparenti[1] per gli interessati i cui dati personali siano oggetto di trattamento.

2. I dati personali devono essere raccolti e memorizzati su una smart card soltanto per scopi legittimi, specifici ed espliciti. Non devono essere utilizzati successivamente secondo modalità che siano incompatibili con tali scopi.

3. Gli obblighi attinenti la protezione dei dati personali pertengono al soggetto che determina gli scopi del sistema e gli strumenti utilizzati per raggiungere tali scopi. Ciò comporta, nel caso di carte multifunzionali, che titolari diversi siano responsabili ciascuno per la parte che gli compete.

4. Qualora una smart card sia utilizzata per scopi di tipo diverso, il trattamento deve essere organizzato in modo da non utilizzare i dati per scopi diversi da quelli per cui sono stati raccolti. Qualora gli stessi dati siano utilizzati per scopi di tipo diverso, essi devono limitarsi a quelli strettamente necessari.[2]

5. La raccolta di dati personali sensibili[3] da registrare nella memoria della carta deve essere effettuata soltanto se prevista da norme di legge oppure se l'interessato vi ha acconsentito esplicitamente.[4] Tali dati devono essere trattati soltanto nel rispetto di opportune garanzie previste per legge.[5] Qualora la raccolta ed il trattamento dei dati in questione si fondino sul consenso esplicito, l'interessato deve avere il diritto di ritirare tale consenso in qualsiasi momento. Il rifiuto o il ritiro del consenso non devono comportare conseguenze negative per l'interessato.[6]

6. I dati registrati su una smart card devono essere tutelati da accessi, alterazioni e/o cancellazioni non autorizzati o accidentali. La carta deve assicurare un livello adeguato di sicurezza alla luce delle conoscenze tecnologiche, della natura sensibile o non sensibile dei dati registrati, del numero e della tipologia delle applicazioni, e della valutazione dei possibili rischi.[7] È necessario stabilire in anticipo, relativamente a ciascuno dei diversi scopi per i quali la carta viene utilizzata, a quali condizioni sia consentito a soggetti terzi di accedere ai dati registrati sulla carta stessa.[8]

7. Qualora si raccolgano e memorizzino dati personali su una smart card, l'interessato deve essere informato delle finalità del trattamento, dell'identità del titolare, delle categorie di dati in oggetto e dei destinatari, o delle categorie di destinatari, dei dati memorizzati. L'interessato deve ricevere ulteriori informazioni[9] se ciò è necessario per garantire la lealtà del trattamento di dati personali.

8. All'atto del rilascio della carta, il titolare deve essere informato adeguatamente delle modalità di utilizzazione e dei passi da compiere in caso di frode o comunicazione non autorizzata.[10]

9. Ogniqualvolta si realizzi uno scambio di dati personali fra una smart card ed il sistema, l'interessato deve esserne informato, a meno che sia già in possesso di tale informazione. Ciò riveste particolare importanza con riguardo alle carte contactless, ossia qualora l'interessato non debba provvedere direttamente all'inserimento o alla presentazione della carta al sistema.

(1) Il concetto di trasparenza implica che l'interessato sia informato dei dati memorizzati e della loro utilizzazione.

(2) Ad esempio, nel caso di una smart card utilizzata da un'istituzione scolastica sia per i servizi di mensa sia per quelli di biblioteca, devono essere memorizzati soltanto i dati comuni alle due funzionalità, come il nome dell'alunno e la rispettiva classe di appartenenza.

(3) Ai sensi dell'Articolo 6 della Convenzione 108, per dati sensibili si intendono "i dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale [...] [e] i dati a carattere personale relativi a condanne penali". Si considerano dati sensibili anche gli altri dati definiti come tali dal diritto nazionale.

(4) Tuttavia, in taluni casi il diritto nazionale può prevedere che il consenso non è sufficiente a conferire liceità alla raccolta e/o al trattamento dei dati.

(5) Tali opportune garanzie atte a tutelare ulteriormente i dati possono trovare applicazione, ad esempio, attraverso la cifratura dei dati stessi, che attualmente rappresenta l'approccio più sofisticato. Tuttavia, è necessario tenere conto dei possibili sviluppi futuri in campo tecnologico.

(6) Se la memorizzazione di dati sensibili è necessaria per fornire un servizio all'interessato, e quest'ultimo rifiuta il proprio consenso esplicito ovvero ritira tale consenso, non sarà ovviamente più

segue nota 6, 7, 8, 9, 10

10. Gli interessati devono avere il diritto di accedere ai dati personali che li riguardano contenuti nella carta, e devono avere il diritto di farli correggere o, se necessario, aggiornare.[11]

11. I dati derivanti dall'utilizzazione di una smart card[12] devono essere cancellati se non sono più necessari per lo scopo specifico in relazione al quale la carta è stata utilizzata.

segue nota 6
possibile continuare la prestazione del servizio a favore dell'interessato.
(7) Ad esempio, se si utilizzano carte con un chip di memoria, è ammessa, in linea di principio, soltanto la registrazione di dati identificativi. Vi possono essere anche altri criteri da tenere presenti, come la quantità dei dati, il numero di potenziali lettori, le finalità del trattamento, ecc.
(8) Il rischio di utilizzazioni improprie dei dati registrati nella carta aumenta se quest'ultima è dotata di funzioni di pagamento. Si sconsiglia l'associazione fra funzioni di pagamento ed applicazioni che comportino la registrazione sulla carta di dati sensibili relativi al titolare della carta stessa.
(9) Le informazioni da fornire all'interessato possono comprendere anche le specifiche tecniche relative al sistema utilizzato.
(10) In particolare, è necessario richiamare l'attenzione del titolare della carta sulle possibili conseguenze in caso di utilizzazione impropria, comunicazione delle modalità di accesso ai dati (ad esempio, il codice) o comunicazione dei dati, nonché sulla circostanza che, in taluni casi, egli può essere chiamato a rispondere personalmente.
(11) Una possibilità per garantire l'accesso consiste nell'installazione di lettori di smart card.
(12) Ad esempio, le informazioni relative alla data ed al luogo di utilizzazione della carta.

26ª Conferenza internazionale sulla protezione dei dati Wroclaw (Polonia) 13-16 settembre 2004

74 Risoluzione della Conferenza europea per la protezione dei dati relativa all'istituzione di un *forum* comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia (protezione dei dati nel Terzo Pilastro)

Risoluzione della Conferenza europea per la protezione dei dati relativa all'istituzione di un forum comune dell'Unione europea sulla protezione dei dati nelle questioni attinenti alla cooperazione giudiziaria e di polizia (protezione dei dati nel Terzo Pilastro)

Il Trattato dell'Unione Europea (TUE), nella versione adottata il 2 ottobre 1997 (Trattato di Amsterdam) contiene, nel Titolo VI, ampie disposizioni relative alla cooperazione giudiziaria e di polizia in materia penale. Il Trattato di Nizza prevede che le autorità giudiziarie e di polizia degli Stati membri dell'UE intensifichino ulteriormente tale cooperazione. Si tratta di una delle priorità dell'Unione.

Le Autorità di protezione dei dati degli Stati Membri dell'Unione europea hanno piena coscienza della necessità di una cooperazione più stretta fra le autorità responsabili dell'azione penale negli Stati Membri, al fine di garantire ai cittadini dell'Unione un livello elevato di sicurezza in un'area di libertà, sicurezza e giustizia. Tuttavia, occorre garantire un equo bilanciamento fra tale esigenza e la difesa delle libertà civili, compresi i diritti di protezione dei dati, la cui tutela è sancita dalla Carta dei diritti fondamentali dell'Unione europea.

Uno dei compiti più importanti delle Autorità di protezione dei dati è rappresentato dall'attività consultiva in materia di protezione dei dati svolta per gli enti che si occupano di legiferazione; in tale ambito, le Autorità devono sottolineare i rischi che determinate iniziative di legge possono comportare per le libertà sopra ricordate, e proporre soluzioni più vicine ai cittadini. La Commissione, il Consiglio ed il Parlamento europeo usufruiscono di tale attività consultiva con sempre maggiore frequenza.

Naturalmente le Autorità di protezione dei dati sono liete di rispondere a tali richieste nella maniera migliore possibile. Tuttavia, è bene chiarire che, al momento, sono insuffi-

cienti o assenti le strutture organizzative necessarie all'adempimento di questa importante missione, e che pertanto le Autorità non possono garantire un intervento consultivo in fase precoce, sulla base di un'analisi condotta a livello paneuropeo e secondo i dovuti standard di qualità. Ciò dipende dall'inesistenza, all'interno del Terzo Pilastro, di un forum comune e della necessaria struttura organizzativa.

Questa situazione contrasta con quella rinvenibile nel Primo Pilastro, dove è stato costituito il Gruppo di lavoro "Articolo 29" che garantisce un'idonea struttura organizzativa alle Autorità di protezione dei dati. Tale struttura comprende un segretariato permanente (messo a disposizione dalla Commissione) e le risorse utili a consentire l'organizzazione di incontri periodici a Bruxelles con i necessari servizi di traduzione. Le autorità di controllo comuni all'interno del Terzo Pilastro (ad esempio per quanto riguarda Europol, Schengen, Eurojust) hanno un mandato specifico, ed occorre un approccio più ampio per garantire l'uniformità delle garanzie concernenti la protezione dei dati nell'intero settore della cooperazione giudiziaria e di polizia.

I partecipanti alla Conferenza attualmente stanno intensificando la propria collaborazione nelle materie giudiziarie e di polizia. A tal fine, un gruppo di lavoro "Polizia", costituito sotto l'egida della Conferenza delle Autorità europee di protezione dei dati, funge da forum strategico, analizzando tematiche che esulano dal mandato degli organismi attualmente esistenti a livello UE in materia di protezione dei dati. È stato inoltre costituito un altro sottogruppo della Conferenza. Tale gruppo di progetto, formato, fra gli altri, dai presidenti delle autorità comuni di controllo (Europol, Schengen, Dogane ed Eurojust), dal presidente del Gruppo di lavoro "Articolo 29", e dal Garante europeo per la protezione dei dati, ha il compito di sviluppare approcci strategici rispetto a nuove iniziative che riguardino l'utilizzazione di dati personali per scopi giudiziari e di polizia in una prospettiva europea.

Cionondimeno, sono necessarie ulteriori misure strutturali. In concomitanza con il rafforzamento e l'avanzamento dell'architettura europea di sicurezza nel Terzo Pilastro, è essenziale incorporare l'attività consultiva in materia di protezione dei dati nella struttura del Consiglio dell'Unione europea. Per tale motivo, la Conferenza delle Autorità europee di protezione dei dati invita il Consiglio e la Commissione ad attuare senza indugi le misure necessarie, in termini di risorse umane ed organizzative, onde consentire all'ente incaricato della protezione dei dati di iniziare l'importante attività di tutela degli interessi dei cittadini prima della fine dell'anno in corso. Il Garante europeo per la protezione dei dati, nominato ai sensi dell'Articolo 286(2) del Trattato delle Comunità europee, dovrebbe partecipare all'ente istituendo con un ruolo attivo.

La Conferenza, inoltre, invita il Consiglio e la Commissione a creare i presupposti giuridici per l'armonizzazione delle attività di controllo nell'ambito del Terzo Pilastro, in stretta cooperazione con i soggetti competenti.

La Presidenza è invitata a trasmettere la presente Risoluzione al Consiglio, alla Commissione ed al Parlamento.

Wroclaw, 14 settembre 2004

75 Risoluzione relativa alla proposta di uno standard-quadro ISO in materia di *privacy*

Sulla base di una proposta formulata dall'Autorità di Berlino per la protezione dei dati e l'accesso alle informazioni, l'Autorità per la protezione dei dati e l'accesso alle informazioni dello Stato di Brandeburgo, l'Autorità belga per la protezione dei dati, l'Information Commissioner del Regno Unito, l'Autorità federale tedesca per la protezione dei dati, il Centro indipendente per la protezione dei dati dello Schleswig-Holstein, l'Autorità per le informazioni e la *privacy* dello Stato di Ontario, l'Ispettore generale per la protezione dei dati personali della Polonia, l'Autorità per la protezione dei dati personali di Hong Kong, l'Autorità spagnola per la protezione dei dati, l'Ispettorato statale per la protezione dei dati della Repubblica di Lituania, e l'Autorità svizzera per la protezione dei dati propongono che la Conferenza internazionale adotti la seguente risoluzione:

Considerato che l'Organizzazione internazionale per la standardizzazione (ISO) ha istituito un Gruppo di studio sulle tecnologie della *privacy* (PTSG) nell'ambito del Comitato tecnico congiunto 1 (JTC1) con il compito di valutare la necessità di mettere a punto uno standard tecnologico in materia di *privacy* e, in caso affermativo, le modalità procedurali e la relativa portata, e quindi presentare una relazione entro il mese di novembre 2004;

Considerato che il Comitato tecnico congiunto 1 (JTC1) dell'ISO trasmette al Sottocomitato 27 (Sicurezza nelle tecnologie dell'informazione) le richieste di decisione su schemi attinenti alla *privacy* secondo una procedura accelerata;

Considerato che l'International Security, Trust, and Privacy Alliance (ISTPA, Alleanza internazionale per la sicurezza, la fiducia e la *privacy*) è un'alleanza mondiale di imprese, istituzioni e fornitori di tecnologie operanti congiuntamente allo scopo di chiarire e definire questioni attuali o in via di evoluzione connesse a sicurezza, fiducia e *privacy*;

Considerato che l'ISO ha ricevuto una proposta di standard internazionale (ISO/IEC (PAS) DIS 20886) relativa ad Quadro di riferimento per la *privacy*, presentata dall'ISTPA[1] nell'ambito di una procedura accelerata, sulla quale è aperto il voto per corrispondenza con scadenza all'11 dicembre 2004;

Considerato che il Privacy Enhancing Technology Testing and Evaluation Project (PETTEP[2], Progetto per la verifica e valutazione delle tecnologie di potenziamento della *privacy*) è una coalizione mondiale di autorità per la *privacy* e la protezione dei dati, esponenti del mondo universitario, autorità governative e organismi del settore privato, ed esperti in materia di *privacy*, la cui missione consiste nella definizione di criteri di verifica e valutazione riconosciuti a livello internazionale rispetto alle caratteristiche dichiarate da sistemi e tecnologie dell'informazione relativamente alla *privacy*;

Considerato che l'International Working Group on Data Protection in Telecommunications (Gruppo di lavoro internazionale sulla protezione dei dati nelle telecomunicazioni), in occasione del suo 35mo incontro tenutosi a Buenos Aires il 14 e 15 aprile 2004, ha adottato un Documento di lavoro su un futuro standard ISO in materia di *privacy*;[3]

Considerato che la Conferenza internazionale delle Autorità di protezione dati e della *privacy* (in appresso, la "Conferenza") desidera sostenere la definizione di uno standard internazionale delle tecnologie in materia di *privacy* efficace e riconosciuto su base globale, e mettere a disposizione dell'ISO le proprie competenze ai fini della definizione di tale standard;

Considerato che la Conferenza riconosce che la conformità a standard ISO attuali o futuri non comporta né surroga necessariamente la conformità a disposizioni di legge. La

(1) V. http://www.istpa.org
(2) Il PETTEP è un progetto condotto sotto la guida dell'Autorità per la privacy e le informazioni dello stato di Ontario, che ha svolto ricerche ed analisi finalizzate alla definizione di criteri di verifica e valutazione degli aspetti connessi alla privacy nei sistemi e nelle tecnologie dell'informazione.
(3) www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm

Conferenza in realtà considera la definizione degli standard IT in oggetto uno strumento che può essere d'ausilio onde rispettare le norme di legge in materia di protezione dati e *privacy*. La Conferenza riconosce senza alcun dubbio che, da un lato, i propri membri, ciascuno per il rispettivo ambito di giurisdizione, hanno e continueranno a mantenere in vigore norme di legge in materia di *privacy*, le quali in realtà si differenziano per alcuni profili, e che, d'altro canto, esiste complessivamente un grado elevato di concordanza fra le norme di legge in questione, il quale troverebbe il riconoscimento ottimale divenendo parte integrante di meccanismi basati sulle tecnologie dell'informazione attraverso la messa a punto di uno standard internazionale, o di più standard internazionali;

La conferenza adotta le seguenti Risoluzioni:

1. La Conferenza raccomanda rispettosamente che l'ISO metta a punto uno o più standard globali in materia di *privacy*, ed in particolare uno standard delle tecnologie in materia di *privacy*, tale da supportare l'attuazione di norme di legge in materia di *privacy* e protezione dei dati, se già esistenti, e la formulazione di tali norme ove esse non siano ancora definite.
2. La Conferenza ritiene che la definizione di uno standard internazionale in materia di *privacy* debba fondarsi sulle prassi di leale informazione e sui principi di parsimonia, necessità ed anonimizzazione nell'uso dei dati. Per essere efficace, uno standard relativo alle tecnologie dell'informazione deve
   - offrire criteri di valutazione e verifica riferiti alle funzionalità connesse alla *privacy* di qualsiasi sistema o tecnologia, onde facilitare il rispetto da parte dei titolari degli strumenti giuridici nazionali e internazionali in materia di protezione dei dati,
   - offrire assicurazioni sulle caratteristiche dichiarate di rispetto della *privacy* relativamente a tecnologie e sistemi utilizzati per la gestione di dati personali,
   - essere in grado di supportare le specifiche concernenti la *privacy* riferite ai dati personali relativi a una determinata persona, indipendentemente dalle combinazioni e dal numero di soggetti che possono intervenire nella gestione e nell'interscambio di tali dati personali.
3. La Conferenza appoggia la recente istituzione di un Gruppo di studio temporaneo sulle tecnologie della *privacy* (PTSG) con il compito di valutare l'esigenza di uno standard nonché gli ambiti e le metodologie di sviluppo di tale standard nel quadro dell'ISO.
4. La Conferenza sostiene con forza l'accelerazione, e non già il procrastinamento, dell'istituzione di un nuovo Sottocomitato permanente dell'ISO per la definizione di standard delle tecnologie dell'informazione riferiti alla *privacy*. Tale nuovo Sottocomitato dovrebbe tenere presente l'attività svolta attualmente nei Sottocomitati esistenti in rapporto a specifici temi connessi alla *privacy*.
5. La Conferenza sostiene con forza l'inserimento del *Privacy Enhancing Technology* Testing and Evaluation Project (PETTEP) quale organismo ufficiale di collegamento con il PTSG del JTC1 dell'ISO. In tal modo le Autorità di protezione dati potranno disporre di uno strumento per operare direttamente all'interno del PTSG dell'ISO, e si conferisce ai membri del PETTEP un ruolo ufficiale che consentirà loro di presentare, analizzare e contribuire all'attività del PTSG.
6. La Conferenza promuove e sostiene l'adesione al PETTEP delle Autorità di protezione dati interessate, il che consentirà loro, in quanto membri del PETTEP, di far sentire immediatamente la propria voce nel dibattito relativo alla definizione di uno standard ISO delle tecnologie della *privacy*.
7. La Conferenza riconosce che il PETTEP gode già di uno status ufficiale all'interno del PTSG, e chiede rispettosamente al PETTEP di adottare le risoluzioni della Conferenza e di presentarle quanto prima al PTSG.
8. La Conferenza, pur riconoscendo l'impegno e la determinazione dell'ISTPA nel settore della *privacy*, chiede rispettosamente il ritiro dello schema ISTPA quale specifica pubblica (PAS) fintanto che non siano state affrontate le questioni di seguito delineate:
   - Il concetto di *privacy* su cui si fonda la Proposta di standard-quadro in materia di *privacy*, ed il fatto che tale quadro deve tenere conto dell'esistenza di limiti alla raccolta di dati. Nella Proposta si definisce *privacy* "la

gestione ed utilizzazione corrette di dati personali per l'intero ciclo di vita di tali dati, conformemente a principi di protezione dati ed alle preferenze espresse dal soggetto".[4] Gli Autori della Proposta giudicano che la raccolta ed il trattamento di dati personali siano fondamentali ai fini del funzionamento corretto della società e delle relazioni commerciali moderne.[5] Tale considerazione si fonda sul presupposto che non ci siano limiti alla raccolta di dati personali. Possono sussistere circostanze in cui la raccolta ed il trattamento di dati personali sono fondamentali nel senso indicato; tuttavia, non si deve supporre che ciò costituisca la regola.

9. La Conferenza chiede rispettosamente all'ISO di sospendere eventuali richieste già avanzate per il riconoscimento di specifiche pubbliche tramite procedura accelerata di adozione nel settore della *privacy* e della protezione dei dati (ovvero di sospendere la presentazione di nuove richieste per il riconoscimento di specifiche pubbliche nel settore della *privacy* e della protezione dei dati), in quanto la definizione di uno standard in materia di *privacy* necessita di un approfondito dibattito.
10. La Conferenza chiede rispettosamente all'ISO di considerare le richieste di riconoscimento di specifiche pubbliche ed ogni altra richiesta concernente la protezione dei dati e la *privacy* come indicazioni e contributi utili alla definizione di un quadro generale nonché di potenziali standard futuri all'interno del quadro suddetto.

(4) Ibid., pag. 13.
(5) Ibid., pag. 10.

76 Versione emendata della Risoluzione della Conferenza internazionale del 2003 relativa agli aggiornamenti automatici di *software*

L'ufficio dell'Autorità australiana federale per la *privacy*, l'Autorità per l'informazione e la *privacy* dello stato di Ontario, l'Autorità per i dati personali di Hong Kong, e l'Autorità per la protezione dei dati e l'accesso alle informazioni dello stato di Brandeburgo propongono che la Conferenza Internazionale adotti la seguente risoluzione:

1. La Conferenza rileva con preoccupazione che le case produttrici di software in tutto il mondo fanno sempre più ricorso a meccanismi non trasparenti per trasferire aggiornamenti di software nel computer degli utenti.

Così facendo, esse
- sono in grado di leggere e raccogliere dati personali memorizzati nel computer dei singoli utenti (ad esempio, le impostazioni dei programmi di navigazione, e informazioni sulle abitudini di navigazione del singolo utente) senza che questi abbiano la possibilità di accorgersene, intervenire o impedirlo,
- possono assumere il controllo, almeno parziale, del *computer* terminale e, quindi, limitare la capacità dell'utente di far fronte agli obblighi ed alle responsabilità previsti dalla legge nei suoi riguardi, in quanto titolare del trattamento, al fine di garantire la sicurezza dei dati personali eventualmente oggetto di trattamento,
- modificano il *software* installato sul *computer*, che sarà quindi utilizzato senza essere collaudato o approvato nei modi previsti, e
- possono provocare malfunzionamenti del computer senza che sia possibile individuarne la causa nell'aggiornamento.

Tutto ciò può comportare particolari problemi per la pubblica amministrazione e le aziende private, nella misura in cui sussistano specifici obblighi di legge a loro carico relativamente alle modalità di trattamento dei dati personali.

2. La Conferenza, pertanto, invita le società produttrici di *software*
a. ad offrire procedure per l'aggiornamento online del *software* soltanto in associazione ad un'informativa, e ad effettuare l'aggiornamento una volta ottenuto il consenso dell'utente, senza travalicare o abusare di tale consenso, secondo modalità trasparenti e senza consentire accessi non controllati al computer dell'utente;
b. a chiedere la comunicazione di dati personali soltanto con il consenso informato dell'utente e nella misura in cui ciò risulti necessario per effettuare l'aggiornamento online. Gli utenti non dovrebbero essere obbligati a fornire le proprie credenziali di identificazione –anziché di autenticazione– per dare inizio alla procedura di caricamento remoto;
c. a prevedere servizi di aggiornamento che consentano di effettuare verifiche preventive su server separati prima di procedere all'installazione.

3. La Conferenza promuove la definizione e l'applicazione di tecnologie per l'aggiornamento del software che siano rispettose della *privacy* e dell'autonomia degli utenti.