ATTI PARLAMENTARI

XIII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **CXXXVI**
N. **1**

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 1997)

(Articolo 31, lettera n)*, della legge 31 dicembre 1996, n. 675)*

Presentata dal garante per la protezione dei dati personali
(RODOTÀ)

Trasmessa alla Presidenza il 5 maggio 1998

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

INDICE

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 1997)

PAGINA BIANCA

DISCORSO DEL PRESIDENTE STEFANO RODOTÀ

Signor Presidente della Repubblica,

per buona sorte e volontà del Parlamento, i componenti del Garante per la protezione dei dati personali hanno avuto la ventura di accompagnare l'avvio di una legge il cui significato profondamente innovatore, pur tra legittime differenze d'opinione, è ormai riconosciuto da tutti. Ma dalla legge 31 dicembre 1996, n. 675, non è venuto soltanto un mutamento dell'ordine giuridico: stanno cambiando l'organizzazione pubblica e quella privata, i rapporti tra i cittadini e i detentori delle informazioni trovano nuovi fondamenti, una cultura diffusa accompagna questa trasformazione.

Il linguaggio, si sa, dice cose che vanno oltre le parole. Il termine privacy, *piaccia o non piaccia, è ormai familiare al parlar comune, ricorre tutti i giorni nelle pagine dei giornali, ha una forza comunicativa che gli è riconosciuta dagli impieghi frequenti che ne fa la pubblicità. Se si considera il breve tempo trascorso dal giorno dell'entrata in vigore della legge sulla protezione dei dati personali, meno di un anno, potrebbe essere grande la tentazione di sostenere che, improvvisamente, si è aperto un orizzonte tutto nuovo.*

E' più ragionevole e realistico dire, piuttosto, che nella società italiana vi era un inespresso bisogno di rispetto, di un uso finalmente controllato dei dati personali, di redistribuzione del potere informativo. Così, l'adempimento di un obbligo istituzionale, il mettere al passo

anche il nostro Paese con quel che volevano una direttiva europea e le regole ormai comuni a tutti gli altri Stati dell'Unione, si è trasformato in una promessa che gli italiani stanno prendendo sul serio. Anche qui, come altrove, si può cogliere l'insofferenza per una condizione di sudditi, e la sacrosanta pretesa d'essere trattati come cittadini.

Come sempre accade quando si affermano diritti di portata universale, pure in questo caso l'innovazione ha messo in discussione assetti a lungo consolidati, provocando difficoltà e costi per chi doveva adeguare la propria mentalità e la propria organizzazione alla situazione mutata. Non sempre, anche perché non era facile, l'amministrazione pubblica e il settore privato hanno subito trovato il passo giusto. Si sono così manifestate incomprensioni, più che vere resistenze, che il Garante ha deciso di fronteggiare senza ricorrere agli strumenti coercitivi a sua disposizione, ma scegliendo la via della persuasione e della più ampia cooperazione con i soggetti chiamati ad applicare la legge.

E' stata una scelta ispirata dalla ragione, e non da una propensione alle concessioni. Proprio per il grandissimo ritardo accumulato nell'attuare una seria disciplina dei dati personali, l'Italia è di colpo passata da una protezione ridottissima ad una assai elevata, che realizza gran parte delle indicazioni contenute nella Direttiva europea 95/46 alla quale, con una scelta coraggiosa e lungimirante, il Parlamento ha deciso di dare immediata attuazione.

Il salto è stato grande: e per questo era necessario favorire un adattamento da parte di chi, da troppo tempo, era abituato a trattare le informazioni sulle persone come se si trattasse di cosa propria, della

cui utilizzazione non doveva rendere alcun conto. La linea della collaborazione, adottata dal Garante, ha così potuto promuovere una progressiva e spontanea adesione alla legge, senza per ciò sacrificare neppure per un momento i nuovi diritti dei cittadini. A questo risultato ha sicuramente contribuito l'attenzione prestata dal Garante e dal Governo alla riduzione degli oneri burocratici legati all'applicazione della legge, introducendo una opportuna normativa "di alleggerimento", anche attraverso autorizzazioni di carattere generale, che hanno consentito, ad esempio, di liberare milioni di cittadini e di imprese dall'obbligo delle notificazioni, che sono così potute scendere da alcuni milioni a poche centinaia di migliaia.

Ora si può dire che questa fase si sta concludendo. Non sarà certo abbandonato un metodo di cooperazione, che ha avuto manifestazioni significative nelle consultazioni, sia pure informali, degli interessati nelle fasi di preparazione di atti importanti, come il modello di notificazione. Nè verrà interrotto il lavoro di semplificazione che, grazie anche alla sensibilità ed all'iniziativa del Ministro di grazia e giustizia, si è concretato in tre importanti decreti legislativi, nelle autorizzazioni generali e in numerosi altri provvedimenti del Garante. Ma ormai il tempo per acclimatarsi è stato sufficiente, e tutti devono essere disponibili per l'attuazione piena della legge.

Si tratta di rendere operante in tutte le direzioni l'insieme dei principi fondativi della protezione dei dati personali, in primo luogo quel principio della dignità della persona che, con una scelta rivelatrice, si è voluto esplicitamente richiamare in apertura della legge. E bisogna rispettare la volontà quasi unanime del Parlamento, al quale presen-

tiamo oggi la nostra relazione non per adempiere burocraticamente ad un obbligo di legge, ma pure per richiamare la sua attenzione su qualche smagliatura istituzionale degli ultimi tempi, su qualche segno di insofferenza che si esprime in tentativi di ridurre non già il ruolo del Garante, ma la portata stessa della tutela dei cittadini resa concreta dalla nuova disciplina.

Non sarebbe saggio, e contrasterebbe sicuramente con la lettera stessa delle norme, favorire fenomeni, pur modesti, di "erosione", se non di vera e propria "fuga dalla legge n. 675", magari prevedendo deroghe in atti che sfuggono al controllo parlamentare. Al contrario, oggi l'obbligo è quello di completare l'introduzione della Direttiva europea, di attuare la delega che il Parlamento ha dato al Governo per specificare la protezione dei dati personali anche in campi nuovissimi come Internet, di proseguire sulla strada del rapido adeguamento della disciplina italiana alle prescrizioni europee, come già è stato fatto per la materia dei servizi di telecomunicazione, così confermando un primato dell'Italia nella materia delicatissima dei diritti dei cittadini nella società dell'informazione e della comunicazione.

In quest'impresa vi è posto larghissimo per la collaborazione istituzionale, nessuno per le gelosie. Il Garante ha sperimentato l'importanza determinante di questa collaborazione quando i suoi componenti si sono trovati a dover fronteggiare, quasi a mani nude, l'avvio di un lavoro che, fin dal primo momento, non permetteva esitazioni o pause, e per il quale, tuttavia, nulla era stato predisposto.

L'imprevidenza accompagna spesso, nel nostro Paese, le innovazioni istituzionali che, per la mancata predisposizione di strutture

adeguate, in molte occasioni hanno rischiato il fallimento, o subito comunque una drastica perdita di significato. Proprio per queste ragioni, è grande la nostra gratitudine per i Presidenti del Senato della Repubblica e della Camera dei deputati, che ci hanno messo immediatamente a disposizione quel minimo di personale e strutture che ha permesso alla nuova istituzione di rispondere fin dal primo giorno alle intensissime sollecitazioni che le venivano da tutta la società italiana, adottando anche uno stile comunicativo che consente di adempiere al compito di informare il cittadino sui contenuti della legge.

Non sono tra le mie abitudini la lamentazione o l'enfasi. Ma non rappresenterei i fatti nella loro realtà se non dicessi che solo a costo di veri sacrifici di tutti i nostri collaboratori, a partire dal Segretario Generale, è stato possibile fronteggiare una situazione nella quale urgenze ed emergenze sono state la vera normalità. In quest'anno di lavoro abbiamo così potuto valutare attraverso i fatti l'ampiezza del compito affidato al Garante, finora svolto con un organico di sole 45 persone. Questo organico, già insufficiente, si rivela del tutto inadeguato rispetto alla continua crescita del lavoro dei diversi settori di attività. Al Garante vengono affidati nuovi compiti, come quelli previsti dalla legge di conversione del decreto legge n. 23 del 1998 per quanto riguarda le prescrizioni mediche; dev'essere creata una efficiente struttura tecnologica e dei controlli; è indispensabile una organizzazione adeguata del settore della documentazione e della ricerca, rilevante soprattutto per la sempre più intensa attività di collaborazione internazionale.

Da ciò risultano con chiarezza la necessità e l'urgenza di un immediato adeguamento del personale e delle risorse finanziarie ai bi-

sogni reali di funzionamento del Garante, se non si vuol esporre anche questa nuova istituzione al rischio dei ritardi e delle inefficienze. Siamo sicuri che il Governo risolverà anche questo problema con lo stesso spirito di collaborazione manifestato in tutto il tempo dell'avvio.

Non è enfatico sottolineare, infatti, come la protezione dei dati personali incarni una disciplina pervasiva e capillare, trasversale se davvero ve n'è una, che tocca ogni aspetto dell'organizzazione pubblica e privata, e della stessa vita quotidiana. Basta scorrere i titoli dei paragrafi della Relazione al Parlamento, per rendersi immediatamente conto dell'ampiezza dei compiti e delle responsabilità del Garante. Nel corso d'un anno di lavoro ci siamo occupati di banche e di assicurazioni, di sanità e di archivi di polizia, di lavoro e di ricerca scientifica, di giornalismo e di trasparenza del settore pubblico, di telecomunicazioni e di videosorveglianza, di partiti e sindacati; e l'elencazione potrebbe continuare. Merita, tuttavia, un accenno particolare il potere fortemente innovativo attribuito dal Parlamento al Garante per quanto riguarda i dati personali trattati dai servizi di sicurezza, escludendo l'opponibilità del segreto di Stato: potere esercitato finora con la piena collaborazione dei servizi.

La portata del lavoro del Garante è ben rappresentata da una sola cifra: in dieci mesi sono state circa 25.000 le questioni prospettate, più

di ottanta al giorno. Questo non esaurisce, però, il numero dei casi in cui si è fatto ricorso alla legge. Il diritto di accesso alle raccolte di informazioni, infatti, si esercita nella quasi totalità dei casi senza alcun intervento del Garante, ma attraverso una richiesta diretta dell'interessato al detentore delle informazioni. Non sappiamo, quindi, quante volte quel diritto sia stato concretamente esercitato, anche se sappiamo che di questo strumento i cittadini italiani hanno cominciato a servirsi. Hanno immediatamente compreso, dunque, di avere in mano uno strumento di uso immediato, senza mediazioni burocratiche, nel quale si riflette una reale diffusione e distribuzione del potere sociale di controllo sulla raccolta e l'utilizzazione dei dati personali.

Bastano questi dati per mostrare come non corrisponda alla realtà la tesi di chi ha sostenuto che saremmo di fronte ad una legge fatta per tutelare solo i potenti, i personaggi influenti, le cosiddette figure pubbliche. Certo, alcune vicende clamorose possono aver spinto a questa frettolosa conclusione. Ma queste sono vicende percentualmente del tutto irrilevanti nella gran massa dell'attività del Garante, anche se le considero benvenute, perché hanno avuto l'effetto di richiamare l'attenzione sulla nuova legge con una ampiezza ed una immediatezza che nessuna campagna pubblicitaria avrebbe potuto realizzare.

Affidata com'è, in primo luogo, all'iniziativa degli stessi interessati, la protezione dei dati personali perde ogni connotazione burocratica, ed è lontanissima dal poter essere considerata oppressiva. Al contrario, in essa s'incarna la liberazione da un'antica servitù comunicativa, per la quale le persone erano senza voce, alla mercè di chiunque volesse raccogliere e far circolare informazioni sul loro conto.

Così non viene soltanto confermata la redistribuzione di potere che la nuova legge porta con sè. Emerge con nettezza anche l'effetto di trasparenza sociale che essa produce, dal momento che i detentori delle informazioni non possono più rispondere con l'indifferenza o con il rifiuto alla richiesta di conoscenza ed alla esigenza di controllo legittimamente manifestate dai soggetti ai quali le informazioni si riferiscono.

La tutela dei dati personali cammina ormai con due gambe: la riservatezza e il controllo. Alla prima si addice il silenzio, all'altra la trasparenza. Non basta rimanere al riparo dalle indiscrezioni altrui: poichè la natura stessa della società in cui viviamo rende quotidiani lo scambio e la cessione di informazioni personali, è indispensabile garantire a ciascuno il diritto di mantenere il controllo sulle proprie informazioni, sull'uso che altri possono farne.

Diritti individuali e trasparenza sociale si congiungono: i primi, anzi, diventano strumenti per rendere possibile la seconda. E proprio l'indicazione sulla trasparenza, che costituisce parte integrante del nuovo quadro istituzionale, è stata sempre ben presente nell'attività del Garante. Non solo sono stati rimossi gli ostacoli che, spesso in modo del tutto pretestuoso, venivano opposti alla conoscenza di determinate categorie di informazioni, invocando impropriamente la legge n. 675. Non solo sono stati ricostruiti i rapporti tra questa legge e le norme sull'accesso ai documenti amministrativi in modo da evitare ogni ingiustificata restrizione di queste ultime. Ma sono state valorizzate pure tutte le indicazioni normative che, in un corretto bilanciamento tra tutela della riservatezza e interesse alla conoscenza, consentono il

massimo controllo possibile delle attività svolte nel settore pubblico, dando così un contributo notevole alla trasparenza amministrativa.

Si è subito stroncato, dunque, il tentativo di utilizzare la normativa sulla tutela dei dati personali come via per mantenere o accrescere l'opacità sociale. In questo non vi è alcuna forzatura ricostruttiva, ma la corretta individuazione della logica complessiva che ovunque è alla base dei sistemi di tutela dei dati personali. Qui, infatti, s'intrecciano l'esigenza di tutela piena del diritto di costruire la propria sfera privata e la necessità di impedire la creazione e l'esercizio di poteri incontrollati. Gli equilibri tradizionali, tutti a favore di questo tipo di poteri, sono stati ribaltati dalla legge n. 675, ed è proprio questo il dato da tener presente tutte le volte che si deve ricostruire il sistema di tutela dei dati personali. Siamo in presenza di un vero e proprio cambiamento del paradigma sociale e giuridico.

Certo, il gioco dell'ombra e della luce ci propone anche immagini mutevoli, sfumature, incerti confini. Qui crescono le difficoltà e le responsabilità del Garante, chiamato non solo ad un impegnativo lavoro di bilanciamento di interessi, ma ad un'opera continua di adattamento delle indicazioni della legge a situazioni e contesti tra loro profondamente diversi. E' evidente, tanto per fare un solo esempio, che l'obbligo generale di trattare i dati "secondo correttezza", come dice l'art. 9, si specifica in modalità di comportamento diverse a seconda che ci si trovi di fronte ad un servizio di sicurezza, ad una banca, ad una istituzione ospedaliera.

Ma così non si rischia forse di giungere ad una pericolosa relati-

vizzazione della tutela dei dati personali? Credo che non si debba confondere la fermezza del quadro fondativo della tutela con le tecniche e gli strumenti che rendono flessibile la disciplina e in questo modo, anzi, la dotano di una elevata elasticità in contesti e tempi mutevoli, attribuendole una capacità di fronteggiare tutte quelle situazioni nuove o impreviste che sono tipiche delle dinamiche legate alle tecnologie dell'informazione e della comunicazione. In questo quadro, innovazione tecnologica e regola giuridica non sono più destinate ad una sorta di permanente conflitto, per lo scarto che può determinarsi tra i dati nuovi della realtà e la fissità della regola: questa, infatti, ricorre ormai a tecniche che le consentono un adeguamento continuo alle dinamiche sociali.

Di tutto questo è segno chiaro nell'impianto e nelle singole norme della legge n. 675. Essa si apre con un articolo impegnativo, che accoglie e arricchisce le indicazioni della Direttiva europea 95/46. L'art 1, infatti, stabilisce che "la presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale". Non si può dire, dunque, che la riservatezza costituisce il punto esclusivo d'incidenza della legge, presentandosi, al contrario, come uno soltanto dei diritti da prendere in considerazione, come una specificazione nient'affatto esaustiva in un quadro caratterizzato dall'esplicita rilevanza attribuita al complesso dei diritti e delle libertà fondamentali. Una lettura condotta unicamente in termini di riservatezza, allora, non sarebbe soltanto riduttiva, ma porterebbe pure ad una impropria ricostruzione di questo stesso concetto, che dev'essere inteso proprio nella più larga

dimensione fatta propria dalla legge italiana (e non dimentichiamo che questa è la prospettiva nella quale, alla fine del 1998, dovranno collocarsi tutte le legislazioni dei paesi membri dell'Unione europea).

Le variazioni della norma italiana rispetto allo schema di riferimento della Direttiva sono due, ed entrambe confermano la dilatazione della considerazione normativa. La prima riguarda l'arricchirsi del quadro dei principi con il rinvio alla dignità delle persone fisiche, secondo una linea generale di valorizzazione di questa nozione anche in ambienti culturali che non avevano finora attribuito ad essa una effettiva rilevanza costituzionale; la seconda consiste nell'aver affiancato alla riservatezza l'esplicita considerazione del diritto all'identità personale che, anzi, formalmente riceve lo stesso grado di considerazione della prima.

La nozione di dignità dev'essere tenuta presente tutte le volte che bisogna identificare il significato complessivo della protezione delle informazioni personali e, in questo quadro, della tutela della riservatezza e dell'identità, il cui esplicito riconoscimento legislativo si presenta come una manifestazione del processo di specificazione dei diritti fondamentali della persona. La protezione dei dati personali viene così proiettata al di là della sola nozione di riservatezza, e trova il suo sicuro fondamento nel quadro costituzionale, esplicitamente richiamato dall'art. 1 con i suoi riferimenti ai diritti ed alle libertà fondamentali.

La vera novità istituzionale, quindi, non può essere ritrovata esclusivamente nella forte tutela della riservatezza individuale che emerge

dalle indicazioni della legge. Non siamo di fronte ad una semplice disciplina di settore, anche se particolarmente significativa. Diritti, libertà fondamentali, dignità non costituiscono soltanto riferimenti assai impegnativi, ma definiscono un quadro generale nel quale la sfera privata appare come punto d'incidenza d'una molteplicità di diritti, dai quali discende uno statuto complessivo delle informazioni personali. Vengono così definite condizioni essenziali per quella libera costruzione della personalità di cui parla l'art. 2 della Costituzione. Il Garante si è mosso in questo campo più largo, e i suoi varii provvedimenti costituiscono un contributo alla concretizzazione di questa impegnativa dimensione dei diritti, dove spicca un generale diritto all'autodeterminazione informativa.

Naturalmente, il fatto che non ci si limiti a mettere l'accento sulla riservatezza, ma si dilati l'orizzonte con il riferimento all'intero quadro dei diritti e delle libertà fondamentali, pone problemi di bilanciamento tra i diversi valori sui quali diritti e libertà si fondano, e che possono trovarsi in contrasto con un diritto all'autodeterminazione informativa che pretendesse l'assolutezza. Il Garante ha già sperimentato questa difficoltà in relazione alla libertà della ricerca (art. 33 Cost.) e a quella di iniziativa economica privata (art. 41 Cost.), ma soprattutto per quanto riguarda la tradizionale questione dei rapporti tra tutela della sfera privata e attività giornalistica, intesa come momento della libertà di manifestazione del pensiero (art. 21 Cost.).

Su quest'ultimo terreno l'attività del Garante è stata particolarmente intensa, sia perché appariva indispensabile e urgente una rein-

terpretazione della legge n. 675 alla luce di precise indicazioni costituzionali, sia perché ad esso era assegnato il difficile compito di promuovere il codice di deontologia dei giornalisti previsto dall'art. 25 della legge. Partendo proprio dalla premessa, resa esplicita dall'art. 21 della Costituzione, che esclude che la stampa possa essere soggetta ad autorizzazioni o censure, sono stati così rimossi alcuni ostacoli all'attività giornalistica che potevano derivare da una inadeguata disciplina della raccolta delle informazioni e dalla previsione di una autorizzazione per il trattamento dei dati sensibili. Con lo stesso spirito, e valutando l'esperienza della prima fase di attuazione della legge, il Garante ha segnalato al Ministro di grazia e giustizia l'opportunità di una modifica dell'art. 25 della legge, là dove il trattamento dei dati sulla salute e la vita sessuale veniva subordinato al consenso dell'interessato: il testo dell'articolo è stato poi modificato da un recentissimo decreto legislativo.

Ma il fatto più significativo, e impegnativo, è sicuramente rappresentato dall'elaborazione insieme al Consiglio nazionale dell'Ordine dei giornalisti del codice di deontologia, che ora contiene una serie di significative disposizioni sul rispetto dei diritti e della dignità delle persone. Qui la novità istituzionale è notevole, perché la definizione di una normativa secondaria speciale è stata affidata ad un procedimento ed a soggetti "atipici", un'autorità indipendente ed un ordine professionale, sia pure in un quadro specificamente definito dalla legge. Le ragioni di questa scelta possono essere ricondotte alla volontà di evitare una disciplina di tipo autoritativo in una materia particolarmente delicata per un sistema democratico; ed all'esigenza di assicurare alla normativa quella flessibilità che può derivare dal fatto che

modifiche o integrazioni del codice di deontologia possono essere introdotte con estrema rapidità, sulla base di una semplice intesa tra le due istituzioni ricordate.

Al codice di deontologia dei giornalisti, inoltre si deve guardare come ad uno degli elementi che contribuiscono ad individuare una dimensione istituzionale caratterizzata da un elevato tasso di innovazione, e nella quale si può riconoscere uno dei tratti evolutivi degli attuali sistemi giuridici. Siamo in presenza, infatti, di una integrazione delle iniziative sovranazionali e di quelle nazionali, con un effetto di stimolo delle prime che, in Italia, è stato decisivo per sbloccare la situazione e vincere le resistenze che da anni facevano sempre rinviare una legge sulla protezione dei dati personali. Siamo di fronte ad una distribuzione del potere normativo tra soggetti diversi: alle competenze del legislatore sovranazionale e nazionale si aggiungono le funzioni integrative attribuite ad altri soggetti, all'autorità indipendente in primo luogo, e la rilevanza riconosciuta all'autodisciplina di settore (art. 31.1 h) legge n. 675). Si disegna un sistema con capacità di autocorrezione e di adeguamento, come risulta dalla previsione di decreti "correttivi" (art. 2.1 della legge 31 dicembre 1976, n. 676), dalla rilevanza attribuita ai codici deontologici, dalla presenza di clausole generali, da diffusi poteri del Garante. Si accrescono i poteri di autotutela dei cittadini.

Siamo, però, di fronte alla necessità di rispettare ulteriori impegni, volti proprio al coerente completamento del quadro normativo. E' il caso, in primo luogo, dei decreti legislativi previsti dalla legge di delega, che riguardano una serie assai ampia di materie. Si tratta di que-

stioni obiettivamente complesse, per alcune delle quali è necessario un intervento immediato.

E' in corso un lavoro di approfondimento e di progettazione, che richiede un impegno particolare e che investe temi per i quali è indispensabile tener conto anche della discussione in corso in tutti gli altri paesi dell'Unione europea. Valuterà il Parlamento, che ha già esteso la delega all'impegnativo campo delle prescrizioni mediche, se differire per alcune materie il termine del 23 luglio 1998, in modo da permettere la messa a punto di un quadro armonico e coerente con gli indirizzi europei, introducendo anche ulteriori elementi di semplificazione che lascino tuttavia intatto l'elevato grado di tutela previsto dalla legge.

La legge evoca una molteplicità di soggetti. Disegna uno scenario corale. Redistribuisce e diffonde poteri. Dall'insieme di questi elementi non risulta soltanto delineato un sistema più efficiente e più aperto. Vengono pure ridefiniti senso e portata della tutela della vita privata. Mutano, in Italia come ovunque nel mondo, la percezione e la richiesta di quel che dev'essere la privacy.

Non è certo scomparso il tradizionale "diritto ad essere lasciato solo", ma ormai si è passati a nozioni più complesse, che riflettono una realtà nella quale l'informazione è la più importante delle ma-

terie prime, di cui devono essere continuamente ridefinite le modalità d'uso. Non è in questione la possibilità di raccogliere dati personali, anche su larga scala. Si tratta di valutare le potenzialità positive e negative delle raccolte di dati, di considerarne le finalità, di individuare i criteri di controllo e i valori da privilegiare tra i quali, insieme al rispetto della dignità, emerge sempre più nettamente il rifiuto delle discriminazioni.

Cambiano simboli, esigenze, riferimenti. La privacy *si caratterizza in un quadro in cui assume rilevanza centrale il diritto di costruire liberamente la propria sfera privata, di scegliere i propri stili di vita al riparo da imposizioni esterne e stigmatizzazioni sociali.*

Si spiegano così l'attenzione del legislatore e l'impegno del Garante per la tutela dei dati sensibili, che più di altri possono appunto determinare mortificazioni della dignità e violazioni dell'eguaglianza. Può riuscire fastidiosa e pedante l'elencazione delle informazioni che la legge qualifica come sensibili, ma proprio questa analitica prolissità è rivelatrice. Si parla, infatti, dei dati "idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 22.1).

Colpisce, in questa elencazione, la rilevanza particolare attribuita ai dati che implicano un momento associativo, l'adesione ad un gruppo. La riservatezza, allora, non viene intesa come uno stru-

mento volto a favorire l'isolamento. Al contrario, solo attraverso la sua tutela è possibile stabilire liberamente legami sociali intensi e strutturati.

Nella norma sui dati sensibili, infatti, si manifesta uno dei tanti paradossi che accompagnano la nozione stessa di privacy. *Opinioni religiose a parte, quelle politiche o sindacali definiscono la sfera pubblica di un soggetto. Se ad esse si attribuisce uno statuto "privato" particolarmente forte, disciplinandone in modo rigoroso le possibilità di trattamento, la finalità è del tutto opposta a quella di assicurar loro segretezza, poichè si vuole, invece, creare la premessa della loro massima esplicazione pubblica, senza che ciò comporti per l'interessato il rischio di discriminazioni o stigmatizzazioni da parte di determinati soggetti o in particolari contesti.*

Quella che si può continuare a chiamare tutela della privacy, *allora, si presenta come condizione per il libero stabilirsi di relazioni sociali. E questo è ancora più vero quando le opinioni inducono all'adesione ad una qualsiasi forma associativa, perché questa scelta costituisce una "relazione" sociale formalizzata e, nella gran parte dei casi, la premessa di ulteriore "azione" sociale, perseguita appunto attraverso una struttura collettiva. Nella ricostruzione sistematica della tutela dei dati personali, in conclusione, devono essere tenuti presenti il momento della libera costruzione della personalità e quello dello stabilirsi del legame sociale, in una dimensione che vede congiunto il profilo della dignità (da intendere anche come dignità "sociale", secondo l'esplicita indicazione dell'art. 3 della Costituzione) e quello dell'eguaglianza.*

Senza forzare il significato della disciplina legislativa, si può ben dire che siamo di fronte ad un insieme di strumenti volti a consentire la libera collocazione della persona nella società. Costruzione della sfera privata, sovranità su di sè e determinazione dei legami sociali si congiungono.

Giungiamo così al cuore della condizione dell'uomo e del cittadino. Non è solo la "nuda vita" evocata da Walter Benjamin a costituire il punto di riferimento. Non s'invoca soltanto il potere del segreto, che consente il silenzio su di noi. Estremo paradosso, la privacy *non si presenta come momento di definitiva rottura del legame sociale, come strumento che scatena gli egoismi ed incita all'isolamento, ma come via per ricostruire liberamente quel legame, a partire dal controllo sui detentori delle informazioni, in una prospettiva caratterizzata da redistribuzione di potere sociale e da una conseguente trasparenza sociale. Tutto questo può determinare un integrale recupero della "sovranità su di sè", facendo della pienezza della sfera privata anche la condizione della pienezza della sfera pubblica.*

Per il Garante si è aperto così un cammino difficile, che già lo porta a confrontarsi con il tema dell'identità, richiamato nel primo articolo della legge n. 675 e che riguarda non la "riservatezza", ma la "rappresentazione" della persona. Anche qui siamo di fronte al problema della libera costruzione della sfera privata. Viviamo, infatti, in una società nella quale lasciamo continuamente tracce, cediamo informazioni in cambio di servizi. Basta usare una carta di credito, ed ecco che si forniscono dati non solo su un acquisto, ma sull'ora e il

luogo dove ci si trovava in un certo momento. I naviganti su Internet sanno che ogni loro passaggio, anche il più rapido, può essere colto, registrato, ritrovato in un momento successivo.

Queste informazioni finiscono nelle banche dati più diverse, che conservano implacabilmente tutto quel che riguarda abitudini al consumo, spostamenti, traffico telefonico, e via elencando. Ma la molteplicità dei luoghi, dove le informazioni sono conservate, porta con sè anche una frammentazione della persona, che in una banca dati compare con le sue malattie, in un'altra con i suoi gusti, in un'altra ancora con la sua capacità economica.

L'unità della persona viene spezzata. Al suo posto non troviamo un unico "clone elettronico", bensì tante "persone elettroniche", tante persone create dal mercato quanti sono gli interessi diversificati che spingono alla raccolta delle informazioni. Siamo di fronte ad un individuo "moltiplicato".

Nasce così un problema di identità. Che, tuttavia, non ha la sua radice soltanto nelle tendenze appena ricordate. Si manifesta anche per le possibilità offerte a qualsiasi navigante in rete di nascondersi dietro l'anonimato, di assumere nomi e identità diverse, continuamente variabili, intercambiabili. L'Io diviso esplode sullo schermo. Ognuno di noi può essere "uno, nessuno e centomila". Si è detto che il sé corrisponde alle molteplici "finestre" che possono essere aperte sullo schermo del computer: "queste finestre sono divenute una potente metafora per pensare il sé come un sistema multiplo, distribuito".

La vecchia dimensione della privacy *è lontana. Nuovi interrogativi accompagnano il modo d'intendere e di costruire la sfera privata. Come è possibile ritrovare la pienezza dell'identità di fronte ad un sistema di raccolta delle informazioni che frammenta, scompone, classifica? Come opporsi alla circolazione di profili automatizzati che amputano l'individuo di tratti caratteristici della sua personalità?*

Di fronte alla frammentazione, che la persona ormai subisce nella dimensione informativa, il riferimento all'identità costituisce lo strumento che può permettere di ricostituirne l'integrità. Molti sono i mezzi predisposti a tal fine dalla legge n. 675 e che bisognerà imparare ad usare: dal divieto di prendere decisioni giudiziarie e amministrative in base a valutazioni fondate esclusivamente su trattamenti automatizzati fino al diritto di ottenere l'integrazione delle informazioni raccolte. Il soggetto può così perseguire il fine d'essere presentato nella sua completezza, senza peraltro giungere ad un diritto di autorappresentazione.

Inoltre, il "diritto all'oblio" e quello di opporsi per motivi legittimi al trattamento di dati personali sono evidentemente funzionali alla libera costruzione della personalità, che certamente potrebbe essere resa più difficile o del tutto impedita da un implacabile permanere d'ogni informazione che riguardi fatti del passato. In ciò si potrebbe cogliere una contraddizione con l'esigenza di integrale rappresentazione della persona come connotato del diritto all'identità. Ma, come la costruzione della personalità è frutto di un processo selettivo e non di un puro accumularsi di vicende, così la proiezione nella dimensione giu-

ridica dell'identità personale esige il riconoscimento di una possibilità di selezione, affidata a criteri obiettivi (ad esempio, tempo di conservazione dei dati raccolti) ed alle decisioni dell'interessato.

L'irrompere nella vita sociale di una intensa tutela dei dati personali ha provocato pure moti di fastidio. L'essere sommersi da moduli, da informative e richieste di consenso, non costituisce proprio una violazione di quella sfera privata che si dice di voler tutelare? La protezione dei dati personali non rende più difficile l'opera di chi vuol scoprire criminali, evasori fiscali, profittatori del denaro pubblico? La privacy, *in definitiva, non rischia di divenire uno strumento di cui si servirà solo chi teme di dover mostrare in pubblico un volto poco pulito?*

L'argomento che evoca un cittadino retto e probo, che nulla avrebbe da nascondere e dunque non avrebbe bisogno d'alcuna norma a tutela della sua sfera privata, cela un'insidia. L'«uomo di vetro» è metafora totalitaria perché, reso un omaggio di facciata alle virtù civiche, nella realtà lascia il cittadino inerme di fronte a chiunque voglia impadronirsi di qualsiasi informazione che lo riguardi. Al contrario, il cittadino armato di potere di decisione e controllo sulle proprie informazioni, e garantito da un quadro istituzionale che esclude sopraffazioni, diventa il soggetto consapevole di una vicenda di libertà, anche se dovrà pagare il lieve pedaggio della lettura

d'una informativa e d'una firma sotto una richiesta di consenso, che rappresentano i primi strumenti per controllare chi, fino a ieri, certo non ci infastidiva, ma neppure ci informava del fatto che usava i nostri dati a suo piacimento.

Risulta altrettanto ingannevole, allora, l'argomento di chi, partendo dalla giusta premessa che oggi debba ritenersi attribuito a ciascuno un "diritto all'autodeterminazione informativa", sostiene poi che per la realizzazione di questo diritto sia sufficiente il gioco delle volontà in un mercato non irrigidito da regole. Tutto dovrebbe essere affidato alla scelta individuale, ciascuno dovrebbe poter scegliere la quota di privacy *di cui intende godere. Ma questa impostazione, da una parte, non tiene conto dell'antico argomento delle disparità di potere negoziale, dell'esistenza di contraenti deboli, che la pura logica di mercato potrebbe esporre persino al sacrificio della dignità; e, dall'altra, ignora proprio il delicatissimo bilanciamento di interessi che la disciplina dei dati personali porta con sè e che non può essere affidato soltanto alle dinamiche di mercato, poichè sono in gioco valori come l'eguaglianza, il rispetto della dignità individuale e sociale, la libertà d'informazione, la libertà della ricerca.*

Sono proprio questi valori di libertà che hanno già indotto il Garante a valutare con giusta severità le richieste perentorie di disporre di qualsiasi dato da parte di chi pensa che vi siano finalità d'interesse generale che devono essere perseguite anche con il sacrificio dei diritti di ciascuno sui propri dati personali. Ma si può davvero ritenere che l'altezza dei fini giustifichi il ricorso a tutti i mezzi che un'innovazione tecnologica sempre più sofisticata mette a disposi-

zione di chi vuol scrutare nelle pieghe dell'esistenza, seguire e registrare qualsiasi nostra traccia?

*Il cammino delle democrazie, il radicarsi dello Stato costituzionale dei diritti sono stati accompagnati proprio dall'interrogarsi, persino angoscioso, intorno alla legittimità dei mezzi che lo Stato, e qualsiasi detentore di potere, possono adoperare. L'*habeas corpus, *il diritto dell'imputato di non rispondere segnano da secoli la frontiera della civiltà. Non a caso, da anni s'invoca un* habeas data, *si sottolinea la necessità di un "Information Bill of Rights".*

La legislazione sulla protezione dei dati personali, soprattutto nella dimensione internazionale che ormai la caratterizza e dove si svolge una parte crescente del nostro lavoro, rappresenta un primo, significativo passo in questa direzione. Non sarebbe saggio, nè democraticamente accettabile, che qualcuno pensasse di incrinare una costruzione che si è appena cominciato ad edificare, magari invocando ragioni di Stato per moltiplicare indagini e controlli.

Proprio perché i problemi più acuti nascono dalla disponibilità di un arsenale tecnologico sempre più imponente, qui come altrove bisogna chiedersi se tutto quel che è tecnicamente possibile sia pure eticamente lecito, politicamente e socialmente accettabile, giuridicamente ammissibile. L'avvenire democratico si gioca sempre di più intorno alla capacità sociale e politica di trasformare le tecnologie dell'informazione e della comunicazione in tecnologie della libertà, e non del controllo.

In quest'anno, breve e intensissimo, abbiamo lavorato senza enfatiche rappresentazioni del nostro ruolo, ma con un tenace attaccamento all'idea che la protezione dei dati personali rappresenti non solo un fattore di promozione della persona, ma un elemento costitutivo della cittadinanza in tempi di vorticoso cambiamento. Di questo spirito, prima ancora che dei molti risultati concreti, vogliamo oggi dare testimonianza al Parlamento.

Roma, 30 aprile 1998

RELAZIONE

SULLO STATO DI ATTUAZIONE DELLA LEGGE CONCERNENTE LA PROTEZIONE DEI DATI PERSONALI

(Anno 1997)

La presente relazione al Parlamento e al Governo sull'attività svolta dal Garante e sullo stato di attuazione della legge n. 675/1996 (art. 31, comma 1, lett. n)) è riferita al primo anno di attività dell'organo collegiale, che è stato eletto il 5 marzo 1997 e si è insediato il successivo 17 marzo.

L'organo collegiale è così composto:

- *Prof. Stefano Rodotà, Presidente*
- *Prof. Giuseppe Santaniello, Vice Presidente*
- *Prof. Ugo De Siervo, componente*
- *Ing. Claudio Manganelli, componente*

PAGINA BIANCA

PREFAZIONE

Un nuovo orizzonte

1. Nella società della comunicazione è ormai luogo comune dire che le informazioni costituiscono la risorsa più importante e che hanno particolare pregio i dati personali, ai quali le crescenti possibilità di trattamento elettronico consentono di attribuire un sempre più sofisticato valore aggiunto. A questi dati personali, quasi che si trattasse di una inesauribile miniera a cielo aperto, nei decenni passati tutti hanno attinto a piene mani, poteri pubblici e soggetti privati.

La situazione è radicalmente e bruscamente cambiata l'8 maggio 1997, quando la nuova disciplina a tutela dei dati personali ha posto le condizioni formali perché anche i cittadini italiani possano esercitare quella "sovranità su di sé" che costituisce uno dei caratteri di una società democratica. E lo ha fatto in un modo intenso ed originale, che corrisponde all'affinamento della sensibilità culturale ed all'evoluzione giuridica, guardando non esclusivamente all'individuo singolo, bisognoso d'un "diritto a essere lasciato solo" ma al cittadino immerso nel flusso della comunicazione, che plasma in ogni momento anche le relazioni interpersonali e sociali. Così la tutela dei dati personali non recide il legame sociale, né uccide la trasparenza, ma si presenta come il luogo d'un difficile equilibrio sempre da verificare, tra valori diversi.

L'argomento che evoca un cittadino retto e probo, che nulla avrebbe da nascondere e dunque non avrebbe bisogno d'alcuna norma a tutela della sua sfera privata, cela un'insidia. L'"uomo di vetro" è metafora totalitaria perché, reso un omaggio di facciata alle virtù civiche, nella realtà lascia il cittadino inerme di fronte a chiunque voglia impadronirsi di qualsiasi informazione che lo riguardi.

Per altro verso, risulta altrettanto ingannevole l'argomento di chi, partendo dalla giusta premessa che oggi debba ritenersi attribuito a ciascuno un "diritto all'autodeterminazione informativa" sostiene poi che per la realizzazione di questo diritto sia sufficiente il gioco delle volontà in un mercato non irrigidito da regole. Tutto dovrebbe essere affidato alla scelta individuale, ciascuno dovrebbe poter scegliere la quota di privacy di cui intende godere. Ma questa impostazione, da una parte, non tiene conto dell'antico argomento delle disparità di potere negoziale, dell'esistenza di contraenti deboli, che la pura logica di mercato potrebbe esporre persino al sacrificio della dignità; e, dall'altra, ignora proprio il delicatissimo bilanciamento di interessi che la disciplina dei dati personali porta con sé e che non può essere affidato soltanto alle dinamiche di mercato, poiché sono in gioco valori come il rispetto della dignità individuale e sociale, la libertà d'informazione, la libertà della ricerca.

Non a caso, e non da oggi, insieme alla messa a punto di leggi sulla tutela della riservateza delle informazioni personali si sono invocati interventi più significativi e comprensivi, di portata costituzionale. Da anni si parla di un "Information Bill of Rights", di una

vera e propria dichiarazione dei diritti del cittadino nell'età elettronica. In questa più comprensiva dimensione si muovono i documenti internazionali che hanno via via arricchito la disciplina della materia.

A questa esigenza risponde l'art. 1 della legge 31 dicembre 1996, n. 675, che riprende e arricchisce l'indicazione contenuta nell'art. 1 della Direttiva europea n. 95/46/CE del 24 ottobre 1995. Questa norma mostra con chiarezza come la tutela dei dati personali sia irriducibile alla pur fondamentale dimensione della riservatezza che, infatti, costituisce uno soltanto dei riferimenti contenuti nell'articolo. La riservatezza, infatti, si pone, insieme all'identità personale, come una delle specificazioni d'una disciplina che colloca i dati personali in una dimensione propriamente costituzionale, visto che il loro trattamento deve svolgersi "nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche".

Non siamo di fronte, quindi, ad una semplice disciplina di settore, anche se particolarmente significativa. Diritti, libertà fondamentali, dignità non costituiscono soltanto riferimenti assai impegnativi, ma definiscono un quadro generale nel quale la sfera privata appare come punto d'incidenza d'una molteplicità di diritti, dai quali discende uno statuto complessivo delle informazioni personali.

L'Italia ha così di colpo raggiunto un livello di tutela particolarmente elevato, avendo dato attuazione alle parti più significative della Direttiva prima degli altri paesi dell'Unione europea. Il passaggio è stato senza dubbio brusco, dal momento che la situazione precedente conosceva solo discipline ridotte o parziali, talvolta affidate ad una incerta creazione ed attuazione giurisprudenziale, che pure aveva avuto il merito di forzare resistenze dottrinarie e disattenzioni legislative.

Si spiegano, allora, le difficoltà incontrate da molti soggetti per adattare la loro organizzazione, e la loro stessa cultura, ai criteri previsti dalla legge n. 675/1996. Si tratta di una difficoltà condivisa talvolta dagli stessi soggetti che più dovrebbero avvantaggiarsi dall'innovazione, dal cosiddetto cittadino comune. Non sempre, infatti, si è in condizione di percepire subito che quanto può apparire come un fastidio (la necessità di leggere un documento d'informazione, di sottoscrivere una dichiarazione di consenso) in realtà è il segno tangibile del passaggio da una situazione nella quale tutti potevano raccogliere informazioni su tutti, godendo di una sorta di franchigia totale, ad una situazione nella quale ciascuno si riappropria della possibilità di regolare la circolazione dei dati che lo riguardano.

Qui, come altrove, i costi dell'innovazione sono reali. Questo esige, non solo da parte del Garante, un lavoro paziente e non breve d'informazione, di alleggerimento di oneri, di chiarimento di linguaggi burocratici. Ma non si può denunciare il costo finanziario, che le imprese in particolare sopportano per l'attuazione della legge, come un aggravio ingiustificato, come un sopruso inaccettabile. Poiché si tratta di garantire diritti fondamentali della persona, di fondare addirittura una nuova forma di cittadinanza, è giusto che i costi della

tutela siano sopportati da chi utilizza le informazioni altrui, così come è giusto che sia l'imprenditore a sopportare i costi per la sicurezza del lavoro.

2. Cambiando profondamente i termini del problema, è naturale che sorgano diversi interrogativi, talvolta espressi in forme eccessivamente schematiche. Corriamo il rischio di un "imperialismo della privacy" o più semplicemente dobbiamo abituarci ad un "sano ascetismo informativo"? Dobbiamo usare come punto di riferimento l'utopia negativa del Grande Fratello o interrogarci realisticamente sui problemi della società della classificazione? Dobbiamo accettare l'integrale trasformazione delle informazioni personali in merce o deve prevalere la tutela dei valori fondamentali della persona? Vincerà l'Europa dei diritti dell'uomo o prevarranno gli interessi del mercato?

Intorno a queste dicotomie (e semplificazioni) si svolge ormai buona parte della discussione internazionale sulla privacy. Anche nei dibattiti più tecnici, infatti, si coglie una tensione tra valori e riferimenti diversi, tra la propensione a non porre alcun ostacolo al cammino vittorioso delle tecnologie e la riflessione sugli effetti che tutto ciò provoca sulla sfera privata di ciascuno, e sull'organizzazione sociale nel suo complesso. E, ancora una volta, è proprio la nozione tradizionale di privacy ad essere messa in discussione.

Dall'originario diritto "ad essere lasciato solo" si è passati a nozioni più complesse, che riflettono una realtà nella quale l'informazione è la più importante tra le materie prime e dove il problema dell'individuo non è solo quello di impedire la diffusione di determinate informazioni, ma pure quello di non perdere il controllo sulla massa di dati che lo riguardano e che si trovano ormai contenute in una miriade di banche dati. Così l'esigenza di tutela della privacy si diffonde su tutta la società, non è più un diritto tipico dell'"età dell'oro della borghesia". Il bisogno di tutela si è fatto acutissimo anche in paesi, come l'Italia, dove la stessa borghesia non aveva sentito il bisogno di una specifica tutela, come dimostra il silenzio del codice civile e di tutta la successiva legislazione speciale. Con un significativo rovesciamento, in Italia la privacy trova il suo primo riconoscimento, nel 1970, nello Statuto dei lavoratori: essa non è più solo uno scudo contro il pettegolezzo, ma un'arma contro le discriminazioni basate sulla raccolta di informazioni su opinioni politiche, sindacali, religiose.

Cambiano così simboli, esigenze e riferimenti. La privacy si definisce come il diritto di costruire liberamente la propria sfera privata, di scegliere i propri stili di vita al riparo da imposizioni esterne e stigmatizzazioni sociali.

La privacy cammina ormai con due gambe: la riservatezza e il controllo. Alla prima si addice il silenzio, all'altra la trasparenza. Non basta rimanere al riparo dall'indiscrezione altrui: è indispensabile non perdere il controllo sulle proprie informazioni. Viviamo, infatti, in una società nella quale lasciamo continuamente tracce, cediamo informazioni in cambio di servizi. Basta usare una carta di credito, ed ecco che si forniscono dati non solo su un acquisto, ma sul-

l'ora e il luogo dove ci si trovava in un certo momento. I naviganti su Internet sanno che ogni loro passaggio, anche il più rapido, può essere colto, registrato, ritrovato in un momento successivo.

Queste informazioni finiscono nelle banche dati più diverse, che conservano implacabilmente tutto quel che riguarda abitudini al consumo, spostamenti, traffico telefonico, e via elencando. Ma la molteplicità dei luoghi, dove le informazioni sono conservate, porta con sé anche una frammentazione della persona, che in una banca dati compare con le sue malattie, in un'altra con i suoi gusti, in un'altra ancora con la sua capacità economica.

L'unità della persona viene spezzata. Al suo posto non troviamo un unico "clone elettronico", bensì tante "persone elettroniche", tante persone create dal mercato quanti sono gli interessi diversificati che spingono alla raccolta delle informazioni. Siamo di fronte ad un individuo "moltiplicato".

Nasce così un problema di identità. Che, tuttavia, non ha la sua radice soltanto nelle tendenze appena ricordate. Si manifesta anche per le possibilità offerte a qualsiasi navigante in rete di nascondersi dietro l'anonimato, di assumere nomi e identità diverse, continuamente variabili, intercambiabili. L'Io diviso esplode sullo schermo. Ognuno di noi può essere "uno, nessuno e centomila". Si è detto che il sé corrisponde alle molteplici "finestre" che possono essere aperte sullo schermo del computer: "queste finestre sono divenute una potente metafora per pensare il sé come un sistema multiplo, distribuito".

La vecchia dimensione della privacy è lontana. Nuovi interrogativi accompagnano il modo d'intendere e di costruire la sfera privata. Come è possibile ritrovare la pienezza dell'identità di fronte ad un sistema di raccolta delle informazioni che frammenta, scompone, classifica? Come opporsi alla circolazione di profili automatizzati che amputano l'individuo di tratti caratteristici della sua personalità?

Al tempo stesso, però, rinasce la spinta verso la creazione di grandi raccolte d'informazioni per finalità di intervento e di controllo sociale. Lo stesso ridimensionamento dello Stato sociale, con l'abbandono del diritto universale a talune prestazioni, fa crescere la richiesta da parte delle amministrazioni pubbliche di dati personali sempre più analitici, per identificare coloro i quali hanno diritto a prestazioni che hanno ormai assunto un carattere selettivo (basta pensare a quelle sanitarie).

L'Europa vive questa e altre contraddizioni. Mentre si lavora per offrire alla privacy una tutela particolarmente intensa, soprattutto per motivi di polizia si costituiscono grandi banche dati sulle persone. E in Italia, in nome della lotta alla criminalità o all'evasione fiscale, si fa prepotente la richiesta di superare ogni barriera di riservatezza, e di tornare ad una situazione in cui qualsiasi soggetto pubblico possa raccogliere informazioni su tutti e su tutto.

Qui, a parte ogni considerazione sull'efficacia di interventi a tappeto al posto di iniziative mirate, si pone una questione più generale, che accompagna ormai l'innovazione scientifica e tecnologica in tutti i campi. Tutto quel che diventa tecnicamente possibile è pure eti-

camente accettabile? Più precisamente: le possibilità tendenzialmente illimitate di raccolta di informazioni sulle persone possono esonerare dall'obbligo di una valutazione in termini di rischi per la democrazia? La privacy, allora, non è questione da considerare come se in essa si esprimessero soltanto gli egoismi individuali. Diventa elemento essenziale della nuova cittadinanza nell'età della comunicazione.

Alla nuova disciplina dei dati personali, anzi, si accompagna anche un effetto notevole di trasparenza sociale. Da due punti di vista: da una parte, il diritto di accesso degli interessati ai loro dati porta con sé trasparenza e controllabilità di coloro che effettuano il trattamento, mentre questa attività in passato poteva essere circondata da una assoluta segretezza; e la precisazione degli ambiti di applicazione della legge n. 675 sta progressivamente implicando una parallela precisazione delle situazioni che, invece, esigono una effettiva pubblicità, com'è già accaduto, ad esempio, grazie agli interventi del Garante relativi agli stipendi in alcuni settori, ai redditi di taluni soggetti, all'accesso ai dati personali contenuti in documenti trasmessi al Parlamento.

Più netto ancora è l'effetto di trasparenza sociale determinato dal fatto che al Garante non può essere opposto neppure il segreto di Stato. Per la prima volta, l'insieme delle istituzioni di sicurezza è sottoposto ad un controllo che, finalizzato alla garanzia di posizioni individuali, tuttavia elimina una situazione di opacità che ha certamente contribuito, in passato, a determinare frequenti occasioni di uso di quelle istituzioni per finalità radicalmente diverse da quelle per le quali sono state create è vengono mantenute.

Unico caso di segreto che continua a poter essere opposto allo stesso Garante, è quello che riguarda le fonti del giornalista. Ma qui la finalità del segreto è radicalmente diversa dalla creazione di situazioni di opacità. Al contrario: esso può consentire una informazione più libera, rimanendo fermi i diritti dei cittadini nella fase di diffusione della notizia.

3. Per affrontare questo insieme di questioni, davvero una delle grandi sfide del nuovo millennio, è stata avviata la costruzione d'un sistema normativo complesso, di cui la legge n. 675/1996 costituisce il nucleo, ma non l'unica componente. La disciplina contenuta in questa legge, infatti, viene progressivamente integrata e completata dai decreti legislativi di attuazione della delega prevista dalla legge 31 dicembre 1996, n. 676, che riguarda materie tutte di grande rilevanza. Inoltre, il sistema viene progressivamente ampliato dalla legislazione attuativa di altre direttive comunitarie, ultima quella riguardante le telecomunicazioni.

Siamo allora in presenza di un sistema non solo complesso, ma caratterizzato da una dinamica continua, che si esprime anche in strumenti di correzione, più propriamente di autocorrezione, e di adattamento. Il sistema, dunque, si presenta connotato al tempo stesso da nettezza dei princìpi e da flessibilità.

Al suo interno è possibile cominciare ad individuare, sulla base dell'esperienza attuativa e delle riflessioni sempre più intense degli studiosi, tendenze generali e nodi problematici. Emerge il carattere non retorico del riferimento alla dignità, evidente soprattutto in tutte le questioni che riguardano la salute e la comunicazione di fatti alla cui riservatezza si annette un particolare significato (come le ricette mediche o l'invio di atti giudiziari in forme che li rendono leggibili da chiunque abbia con essi anche un fuggevole contatto). Qui si coglie con particolare nettezza il bisogno di rispetto che i cittadini manifestano nei confronti di chiunque tratti informazioni.

Questa cultura del rispetto, che davvero costituisce uno dei grandi obiettivi della legge n. 675/1996, fonda anche l'altra situazione alla quale si è dato particolare rilievo, il diritto all'identità. Qui siamo certamente al di là di un pur significativo ampliamento della tradizionale tutela della reputazione e dell'onore, e della stessa esigenza di impedire che il cittadino venga rappresentato in forme che diano "falsa luce agli occhi del pubblico". Di fronte alla frammentazione, che la persona ormai subisce nella dimensione informativa, il riferimento all'identità costituisce lo strumento che permette di ricostituire l'integrità della persona.

Molti sono i mezzi predisposti a tal fine, dal divieto di prendere decisioni giudiziarie e amministrative in base a valutazioni fondate esclusivamente su trattamenti automatizzati fino al diritto di ottenere l'integrazione delle informazioni raccolte. Il soggetto può così ottenere d'essere presentato nella sua completezza, senza peraltro giungere ad un diritto d'autorappresentazione.

Inoltre, il "diritto all'oblio" e quello di opporsi per motivi legittimi al trattamento di dati personali sono evidentemente funzionali alla libera costruzione della personalità, che certamente potrebbe essere resa più difficile o del tutto impedita da un implacabile permanere d'ogni informazione che riguardi fatti del passato. In ciò si potrebbe cogliere una contraddizione con l'esigenza di integrale rappresentazione della persona come connotato del diritto all'identità. Ma, come la costruzione della personalità è frutto di un processo selettivo e non di un puro accumularsi di vicende, così la proiezione nella dimensione giuridica dell'identità personale esige il riconoscimento di una possibilità di selezione, affidata a criteri obiettivi (tempo di conservazione dei dati raccolti) ed alle decisioni dell'interessato.

Torna così il tema della scelta individuale. Questo principio, tuttavia, trova una ovvia limitazione nelle situazioni in cui si manifestano esigenze collettive o bisogno di più intensa protezione delle stesse posizioni individuali. Il primo caso si evidenzia, ad esempio, in relazione al trattamento dei dati da parte della pubblica amministrazione, che non richiede il consenso degli interessati. Naturalmente, sulla base dell'esperienza anche futura di applicazione della legge, il legislatore potrà valutare l'opportunità di modificare le disposizioni in materia, individuando forme di autorizzazione ulteriori rispetto alla legge e introducendo in casi specifici forme di consenso. Diversa è la ragione di esclusione del consenso degli interessati per ciò che riguarda

il trattamento dei dati relativi alle loro attività economiche, esclusione giustificata dalla necessità di assicurare al mercato la necessaria trasparenza, anche al fine di evitare distorsioni nella concorrenza.

Significativa poi è la disciplina dei dati sensibili trattati dai privati fuori dal settore sanitario, dove la regola generale esclude che il consenso dello stesso interessato sia sufficiente per la legittimità del trattamento, esigendo anche l'autorizzazione del Garante, per evitare che pressioni dirette o condizionamenti ambientali inducano a consentire al trattamento dei dati sensibili anche in situazioni in cui sarebbe violata la dignità della persona. Qui la funzione di garanzia della nuova Autorità si coglie con particolare nettezza. E, allo stesso modo, l'area individuata dalla legge n. 675/1996 si presenta come un luogo di permanente confronto tra valori fondamentali.

Da questo, e dal fatto che la nuova disciplina investe tutti i soggetti e si dilata su una straordinaria molteplicità di materie, nasce la difficoltà del compito del Garante, chiamato anche a dare evidenza concreta al modo in cui si opera il bilanciamento tra interessi tutti rilevanti in quella dimensione costituzionale nella quale si è voluto porre pure lo statuto dei dati personali. Il Garante ha operato in modo da evitare ogni compressione di libertà fondamentali, come quelle d'informazione e di ricerca, ad esempio adoperandosi fin dall'avvio dell'applicazione della legge per eliminare ostacoli al libero esercizio dell'attività d'informazione. E questa consapevolezza della rilevanza degli interessi fondamentali in gioco lo ha guidato anche nell'impegnativo (e nuovissimo sul terreno delle fonti del diritto) compito di cooperare con l'Ordine dei giornalisti per l'adozione di un codice di deontologia.

In tutta la difficile e complessa fase d'avvio della legge il Garante è stato ben consapevole che il compito suo era quello di promuovere una cultura prima ancora che di applicare puntigliosamente un insieme di norme. È stato così in ogni momento perseguito il dialogo con tutti i soggetti, nelle forme più aperte e meno formalizzate, con continue consultazioni di tutti gli interessati, che sono state percepite all'esterno anche come un segno di un diverso e più rispettoso modo d'agire delle istituzioni pubbliche.

Il Garante ha svolto questo compito in condizioni di straordinarie difficoltà materiali, superate grazie alla collaborazione di tutte le istituzioni, di quelle parlamentari in primo luogo, e alla dedizione dei collaboratori. Consegna oggi al Parlamento un bilancio ed una riflessione. Sa di non compiere un atto formale, rivolgendosi all'unica istituzione dalla quale tutti i suoi componenti traggono legittimazione. Si augura, quindi, che la riflessione parlamentare, anche critica, contribuisca a meglio orientare l'attività futura.

4. Ma la dimensione del futuro appartiene già alla dimensione del Garante, così come la dimensione internazionale. L'art. 29 della Direttiva europea 95/46/CE ha istituito un gruppo, composto dai rappresentanti delle autorità nazionali e delle istituzioni comunitarie e incaricato, tra l'altro, di esaminare le questioni riguardanti le applicazioni nazionali delle direttive europee e di dare pareri alla Commis-

sione in tutta la delicata materia della tutela dei diritti e delle libertà per quanto riguarda il trattamento dei dati personali. Tuttavia, questo compito, pur importantissimo, non esaurisce il campo dell'azione del Garante, che davvero abbraccia ormai, e con continuità, tutti i continenti, per i rapporti necessari con l'area più avanzata, Stati Uniti e Canada, e per le novità anche organizzative, che si colgono nell'America latina e nell'est dell'Asia: fatti, questi, che impongono una riflessione quotidiana sulle modalità degli interventi del Garante, che non possono certo svolgersi come se la tutela dei dati personali avesse come unico riferimento il cortile di casa.

Così vuole lo sviluppo stesso delle tecnologie, che in Internet trova la sua più nota manifestazione. Questo impongono le novità nei più diversi settori, dal commercio elettronico alla proprietà intellettuale. Corre lungo questa frontiera un'azione che deve sempre considerare il futuro come già presente.

Si leggono ogni giorno le più diverse, e sovente fantasiose, descrizioni delle modalità di raccolta delle informazioni, dei controlli a distanza, delle utilizzazioni più varie dei dati personali. Se questo non implica necessariamente la nascita di una società del controllo totale, con il moltiplicarsi di Piccoli e Grandi Fratelli, sicuramente spinge verso il progressivo instaurarsi di una società della classificazione che pone questioni sempre nuove non solo per la classica tutela delle libertà individuali, che il riferimento alla privacy continua a simboleggiare, ma per la salvaguardia degli stessi caratteri democratici dell'organizzazione sociale.

Quali sono le vie istituzionali per perseguire questo fine? Sappiamo già che l'insieme dei fenomeni nuovi non può essere affrontato con vecchi strumenti. Le tecnologie della rete sfidano lo Stato nazionale: ma la complessità degli abituali strumenti internazionali impone processi lunghi, in attesa dei quali sono indispensabili modalità di intervento rapido, capaci almeno di colmare il tempo d'attesa di più comprensive regolamentazioni. La velocità del cambiamento sfida la regola giuridica tradizionale, che rischia ad ogni momento d'essere superata da una realtà in movimento, che esige strumenti giuridici di disciplina. La platea di soggetti tendenzialmente coinvolti sfida le abituali forme autoritative di regolazione, ed impone il ricorso a forme partecipative e consensuali nel definire le normative e le forme della loro attuazione.

Rappresentare questa situazione in termini di alternativa tra legge e autodisciplina, di scontro tra legge statale e regola di mercato, rischia di costruire nuove gabbie ideologiche, che la realtà fluida non tollera. Al tempo stesso, però, il rinvio d'una seria e comprensiva strategia istituzionale rischia di abbandonare l'individuo alla forza dei condizionamenti, o addirittura a forme di violenza, sottili e pervasive; e di aprire la strada a forme di organizzazione sociale nella quale si insediano poteri fondati sul possesso di dati personali e di nuovo non controllabili, dunque contraddittori con la linea di trasparenza e controllo che le direttive europee e le legislazioni nazionali cercano di seguire.

La strategia istituzionale non può che essere una strategia "integrata" sia dal punto di vista degli strumenti che da quello degli attori. L'impraticabilità della regola rigida non implica l'abbandono della legge, ma l'adozione di un fermo quadro di princìpi generali, all'interno del quale possono trovare posto strumenti diversi (legislazioni nazionali o di settore; codici di autodisciplina; tecniche contrattuali; tecnologie volte ad assicurare il rispetto della privacy).

Questo porta al coinvolgimento di una molteplicità di soggetti, favorendo processi di partecipazione e di responsabilizzazione; costituisce un antidoto alle ricorrenti pretese di instaurare forme di censura, o comunque di limitazione delle libertà; favorisce il passaggio da tecnologie "sporche", fondate sull'indiscriminata raccolta e permanenza delle informazioni, a tecnologie "pulite", che non lasciano tracce o le limitano a tempi e finalità preventivamente determinati.

Ma una buona strategia istituzionale esige una buona cultura dell'uso delle informazioni. Nella società civile (se è lecito usare questa espressione), questo vuol dire cultura del reciproco rispetto. Nella società politica, questo vuol dire anche rinuncia a ritenere che ogni possibilità tecnologica possa essere colta per trattare qualsiasi dato. L'esperienza comincia a mostrarci che uno Stato democratico è anche uno Stato capace di sobrietà nella raccolta e nell'uso delle informazioni sui cittadini.

Stefano Rodotà
Presidente dell'Autorità Garante
per la protezione dei dati personali

PAGINA BIANCA

1. LA TUTELA DEI DATI PERSONALI: UNA NOVITÀ NELLA LEGISLAZIONE ITALIANA

1.1. Le linee-guida delle leggi 31 dicembre 1996 n. 675 e n. 676.

1.1.1. Premessa.

Le leggi nn. 675 e 676 del 31 dicembre 1996 hanno innovato profondamente la legislazione italiana in materia di diritti della personalità, colmando una lacuna avvertita da più parti nel corso degli anni.

Il Parlamento, nel dare attuazione alla convenzione n. 108/1981 del Consiglio d'Europa e ad altri atti internazionali e comunitari, tra cui la direttiva n. 95/46/CE del 24 ottobre 1995, ha mostrato particolare sensibilità alla protezione della riservatezza e dell'identità personale, intervenendo con una disciplina di ampio respiro.

L'*iter* delle due leggi si è sviluppato nel corso di più legislature, sin dal primo progetto presentato nel 1984. In particolare, a partire dal 1992, si sono succeduti alcuni disegni di legge che le interruzioni anticipate delle legislature non hanno permesso di approvare tempestivamente, considerato anche il vivace dibattito suscitato.

Gli interventi normativi del 1996 si sono articolati in una pluralità di innovazioni e sono destinati ad incidere in maniera significativa sull'assetto dei diritti garantiti costituzionalmente, favorendone un corretto bilanciamento.

La legge n. 675/1996 mira infatti ad introdurre una tutela efficace e tempestiva dei vari aspetti nei quali si articolano i diritti fondamentali della personalità, attraverso un processo normativo sviluppato in diverse disposizioni alcune delle quali sono già in vigore, mentre altre verranno introdotte dal Governo in attuazione delle deleghe legislative contenute nella legge n. 676/1996.

Analogamente a quanto avvenuto nelle legislazioni straniere più recenti, la tecnica normativa ha valorizzato solennemente il diritto alla riservatezza e il diritto all'identità personale, e si è poi articolatata in una disciplina dell'attività di raccolta e di elaborazione delle informazioni che, in varia forma, attengono alla persona.

Di conseguenza, in linea con quanto previsto dalla citata direttiva europea, l'approccio normativo ha posto come oggetto della nuova disciplina, il "trattamento" di qualunque informazione di carattere personale, anche se non riguardante la sfera più intima della persona.

Il legislatore ha posto l'accento sulla trasparenza che deve caratterizzare la raccolta e l'elaborazione di informazioni, sulle finalità perseguite dai soggetti che elaborano dati personali nonché sul diritto degli interessati di ricevere tutela prima ancora che l'elaborazione possa aver provocato un danno.

Superando l'esperienza delle legislazioni in materia di tutela dei dati ("Datenschutz") di prima e seconda generazione, la legge n. 675/1996 ha evitato di porre eccessiva enfasi sul consenso dell'interessato o sulla necessità, per chi raccoglie ed elabora informazioni, di ottenere il rilascio di un'autorizzazione preventiva, ed ha preferito regolare in maniera

complessiva i flussi delle informazioni, individuando limiti e garanzie e tenendo conto di altri interessi pubblici e privati meritevoli di considerazione.

In questo quadro, in luogo di un'autorizzazione preliminare al trattamento che, come si dirà tra breve, è stata prevista solo in alcune ipotesi, sono stati posti a carico dei soggetti che elaborano i dati alcuni oneri di informazione agli interessati e di dichiarazione ad un'autorità indipendente.

Si è evitato, così, un sovraccarico di adempimenti e di procedure che avrebbero comportato un inutile impianto burocratico, e si è adottata una soluzione tale da garantire un progressivo aggiornamento delle normative attraverso integrazioni e correzioni, che, pur mantenendo un elevato grado di tutela delle persone, permette di semplificare il più possibile gli oneri a carico dei soggetti impegnati a diverso titolo in un'attività di informazione.

In tal modo, la concezione "statica" del diritto alla riservatezza ha ceduto il passo ad una visione dinamica, che è legata all'odierna intensità della circolazione dei dati e che al tempo stesso non esaurisce il diritto alla riservatezza in un mero "diritto all'indennizzo".

Tale visione si incentra nel riconoscimento all'interessato del diritto di essere informato sui trattamenti di dati che lo riguardano e sulle relative finalità, nella possibilità di esprimere o meno il consenso in diversi casi, nonché nel diritto di verificare la correttezza dell'elaborazione anche attraverso l'accesso alle informazioni raccolte nei suoi confronti. Per alcune categorie di dati definiti dalla legge "sensibili", al consenso scritto dell'interessato si aggiunge l'ulteriore garanzia rappresentata da un'autorizzazione rilasciata al soggetto che intende raccogliere ed elaborare dati.

Il Parlamento ha così dotato l'Italia di un modello legislativo moderno che offre un'ampia tutela riferita alle informazioni concernenti, oltre che le persone fisiche, gli enti collettivi (persone giuridiche, associazioni, fondazioni, organismi pubblici). E ciò, anche quando le stesse sono elaborate con mezzi non automatizzati o non sono inserite in vere e proprie banche dati.

La legge n. 675/1996 è obiettivamente complessa, in quanto abbraccia un arco notevole di attività pubbliche e private e tende ad assicurare un livello elevato di tutela della persona.

Come si vedrà, l'intento del Garante nella prima fase di applicazione della nuova legge è stato quello di interpretare ed attuare le norme in modo da assicurare la piena applicazione delle garanzie snellendo, al tempo stesso, adempimenti e modalità.

Analogamente a quanto avvenuto in altri Paesi, l'innesto di un corpo così articolato di princìpi comporta alcune difficoltà applicative fisiologiche, che l'esperienza e gli eventuali correttivi possono permettere di risolvere in un quadro di corretto bilanciamento dei diritti e delle libertà.

1.1.2. Nuove forme di tutela dei diritti della personalità.

Per effetto della legge n. 675/1996, che si pone come disciplina generale sul trattamento dei dati personali, il diritto alla riservatezza assume connotati del tutto nuovi rispetto all'originario nucleo del "diritto ad es-

sere lasciato solo", definito in via prevalentemente giurisprudenziale e solo nell'ambito di alcuni settori, come quello dell'attività giornalistica o dell'attività di impresa.

Senza entrare nel merito del dibattito che ha appassionato la dottrina circa l'esistenza di un unico, complesso diritto della personalità o di più diritti, oggi il diritto alla riservatezza e il diritto all'identità personale son assistiti da nuove forme di tutela che mirano a garantire il complesso "dei diritti e delle libertà fondamentali nonché della dignità delle persone fisiche" (art. 1 legge n. 675/1996).

Tali posizioni sostanziali sono ora tutelate, per effetto della nuova legge, in ogni settore della vita sociale, pubblica o privata, e nel contesto di qualunque attività nella quale si effettui un trattamento di dati personali.

Questa trasversalità aumenta il grado di tutela della persona, in quanto la protezione dei dati si innesta, talora in modo problematico, con varie discipline di settore che troveranno una sistemazione più armonica e compiuta attraverso i decreti delegati previsti dalla legge n. 676/1996.

Il binomio riservatezza-identità personale è valorizzato, non a caso, nell'art. 1 della legge.

Da un lato, la solenne formula che indica le finalità della legge elimina ogni dubbio sulla piena cittadinanza nel nostro ordinamento del diritto all'identità personale, che la dottrina e la giurisprudenza anche costituzionale avevano già inserito nel "catalogo" dei diritti fondamentali e inalienabili della persona.

Dall'altro, la medesima formula testimonia una linea di tendenza che, mentre permette che una fascia di informazioni personali possa circolare anche in assenza di un previo consenso dell'interessato, accentua il diritto di quest'ultimo ad una tutela "forte" della sua legittima aspettativa ad essere "rappresentato" dagli altri in una maniera corrispondente al proprio modo d'essere.

In altre parole, l'ordinamento fornisce adeguata protezione anche alla dimensione sociale della persona e alla sua partecipazione alla vita di relazione nelle multiformi manifestazioni morali, culturali e professionali.

1.1.3. La protezione multiforme dei dati personali.

Sul piano della tecnica normativa, il legislatore ha previsto forme di protezione differenziata della riservatezza, al fine di contemperarla con interessi pubblici e privati meritevoli di una qualche tutela (art. 3 legge n. 675/1996: trattamenti per finalità esclusivamente personali; art. 4: attività per scopi di difesa, di sicurezza dello Stato, di giustizia e di tutela della sicurezza dei cittadini; art. 12, comma 1, lett. f): trasparenza delle attività economiche; art. 27: trattamenti effettuati dalla pubblica amministrazione).

Questa differenziazione della tutela dei dati e delle modalità della loro circolazione è collegata al progressivo abbandono dell'originaria matrice "proprietaria" del diritto alla riservatezza, intesa come bene ad uso rigorosamente esclusivo del soggetto al quale avrebbe dovuto riconoscersi il diritto di estromettere chiunque altro dalla propria sfera privata.

Ci si è invece indirizzati verso una protezione di tipo dinamico e procedimentale, che rappresenta il nucleo forte della nuova legge, in base alla quale i trattamenti dei dati sono disciplinati secondo procedure

e requisiti corrispondenti ad uno schema tipico, senza esclusione, però, di alcune particolarità che modellano la disciplina rispetto ad esigenze di maggior tutela della riservatezza o di protezione di interessi contrapposti, riscontrabili in alcuni settori.

1.1.4. Le scelte del legislatore e il margine di manovra comunitario.

Il recepimento della direttiva comunitaria n. 95/46/CE (c.d. "direttiva-quadro") ha rappresentato per il legislatore l'occasione per offrire una risposta capace di soddisfare in termini di più ampio respiro le esigenze che avevano originato il fervido dibattito in materia di tutela nei confronti delle banche dati, sfociato dapprima nella costituzione del "Comitato di studi per le libertà individuali e l'informatica" (1975) e, di seguito, nella Commissione "Mirabelli" (1980).

Parallelamente al disposto della direttiva-quadro, la disciplina italiana presenta due cardini fondamentali.

Dal punto di vista sostanziale, la legge collega la tutela della riservatezza al "trattamento" dei dati personali, e considera secondaria la circostanza dell'inserimento delle informazioni in una "banca dati" o in un "archivio" (circostanza centrale per alcune legislazioni straniere approvate prima dell'adozione della direttiva), che avrebbe impedito una tutela efficace dei dati "dispersi", non organizzati, cioè, in un insieme sistematico.

Sotto il profilo procedimentale, il nuovo quadro di trasparenza dell'attività di raccolta dei dati si basa, anzitutto, sugli obblighi di informativa all'interessato e di acquisizione, ove necessario, del consenso, nonché sul "diritto di accesso" che il più delle volte può essere esercitato direttamente nei confronti del soggetto che elabora i dati.

Tale trasparenza è rafforzata da un regime di pubblicità dei trattamenti, che trova il suo fulcro nella "notificazione" al Garante (art. 7) prevista dalla legge n. 675/1996. Il decreto legislativo n. 255/1997 ha, poi, opportunamente circoscritto la notificazione ai soli trattamenti caratterizzati da maggiori rischi di danno all'interessato riducendo, così, il rischio di un eccessivo impatto amministrativo (art. 1, comma 1, lett. f), legge n. 676/1996).

Il livello elevato di tutela dei diritti che il Parlamento ha voluto assicurare con voto pressoché unanime traspare, in particolare, dalle seguenti scelte:

a) sono stati ricompresi nell'ambito di applicazione della legge anche i trattamenti non automatizzati di dati personali elaborati al di fuori di archivi o banche dati, che la direttiva-quadro non considera nell'ambito del processo di armonizzazione delle legislazioni europee. Si è prevenuto, così, il rischio di una facile elusione della normativa, e al tempo stesso si è rispettato il dettato costituzionale che non avrebbe permesso una differenziazione della tutela basata sulle modalità di organizzazione dei dati. Di converso, è stata prestata attenzione alla sfera di libertà di chi elabora dati per fini esclusivamente personali (art. 3), e si è previsto che qualunque individuo possa utilizzare dati nell'ambito della propria vita di relazione, comunicandoli anche a terzi purché in maniera non sistematica, senza la necessità di osservare i vari adempimenti previsti dalla legge;

b) il trattamento dei dati "sensibili" è assistito da particolari cautele che si basano su prescrizioni analitiche contenute in un'autorizzazione rilasciata dal Garante al privato o all'ente pubblico economico che elabora i dati, ovvero (se a trattare i dati è una pubblica ammini-

strazione) in una puntuale disposizione di legge (art. 22, comma 3). Tale assetto risulta più attento ai rischi di discriminazione e di lesione dei diritti, se confrontato con quello imposto, come grado minimo di tutela, dall'articolo 8 della direttiva;

c) l'ambito di applicazione della tutela della riservatezza risulta esteso, sotto il profilo soggettivo. Infatti, la legge include nella definizione dell'interessato, oltre alla persona fisica, la persona giuridica, l'ente o associazione cui si riferiscono i dati personali (art. 1, comma 2, lett. f)). Di conseguenza, le informazioni che si riferiscono a tali enti collettivi godono di varie garanzie dalle quali sarebbero state escluse ove il legislatore si fosse limitato ad attuare pedissequamente la direttiva-quadro, la quale tutela le sole persone fisiche. In tal modo, il Parlamento ha confermato l'orientamento giurisprudenziale che riconosce il diritto all'identità anche alle persone giuridiche, ed ha anticipato una soluzione che un'ulteriore direttiva europea rende necessaria per tutti i dati in circolazione nelle reti e che siano relativi ad abbonati, persone fisiche o giuridiche (direttiva n. 97/66/CE, in materia di tutela della vita privata nel settore delle telecomunicazioni).

1.2. I DIRITTI DELL'INTERESSATO: RIFLESSI IN TEMA DI TUTELA SOSTANZIALE E PROCEDIMENTALE.

1.2.1. I diritti garantiti dall'art. 13 della legge.

La chiave di volta della nuova disciplina risiede nella previsione della possibilità per il cittadino o per qualunque altro soggetto di esercitare i diritti di cui all'art. 13 della legge, e nei correlati adempimenti posti a carico del "titolare" e del "responsabile" del trattamento.

Fin dalla fase della raccolta dei dati, e nel corso del loro ulteriore trattamento, è assicurata tutela all'interesse della persona a vedere difesa la propria sfera di riservatezza - aspetto della propria libertà che si concreta nella reazione ad aggressioni altrui attraverso il ricorso all'autorità giudiziaria o al Garante - nonché al diritto di proporre un'azione in via preventiva, facoltà che rappresentano un aspetto "attivo" della libertà, e cioè un immanente potere di controllo delle informazioni e dei dati personali.

Tale tempestiva possibilità di controllo determina lo spostamento del fulcro della tutela dei diritti della personalità, dal momento della loro possibile lesione a quello, anteriore, del coinvolgimento dell'interesse stesso. Ciò comporta un effetto positivo, sotto almeno due aspetti:

a) attraverso il diritto di accesso, rettifica, integrazione e cancellazione dei dati, nonché di opposizione al trattamento "per motivi legittimi", si raggiunge il risultato di diminuire al minimo il rischio di lesioni;

b) conseguentemente, si favorisce un'apprezzabile diminuzione del contenzioso amministrativo e giudiziario.

Va rilevato, peraltro, che la nuova legge non dovrebbe comportare un incremento dei conflitti proposti avanti all'autorità giudiziaria per la violazione dei diritti della personalità, in quanto ha introdotto un sistema di "doppio binario" per la tutela dei diritti, rendendo alternativi al ricorso giurisdizionale i rimedi amministrativi dinanzi al Garante, i quali ultimi si sviluppano secondo procedure più snelle, destinate a concludersi in tempi rapidi (artt. 29 e 31).

1.2.2. L'accesso al registro dei trattamenti.

Per effetto della nuova disciplina, chiunque sia interessato al trattamento di dati personali ha, anzitutto, il diritto di accedere gratuitamente al registro dei trattamenti, che è tenuto presso il Garante e che include le notificazioni obbligatorie per legge (art. 31, comma 1, lett. a)).

Il registro, ovviamente, non contiene i nominativi delle persone oggetto dei vari trattamenti, ma reca una serie di indicazioni generali che possono essere utili agli interessati per comprendere le principali caratteristiche dei trattamenti in corso e per facilitare l'eventuale esercizio del diritto d'accesso, che può essere fatto valere gratuitamente presso i singoli titolari o responsabili.

Queste misure si affiancano a quelle, ben note, che la legge 7 agosto 1990, n. 241, ha introdotto in tema di trasparenza del procedimento amministrativo, e favoriscono la trasparenza nel trattamento dei dati personali, da chiunque effettuato, in ambito sia pubblico sia privato. Ad esse, si somma la scelta operata con il decreto legislativo n. 255/1997 in sintonia con la direttiva comunitaria, volta a garantire che i soggetti che non notificano il trattamento al Garante, in quanto si avvalgono di una causa di esonero, forniscano egualmente a chiunque ne faccia richiesta le notizie che andrebbero riportate nella notificazione (art. 7, comma 5-quinquies legge n. 675/1996).

In tal modo si fornisce un ulteriore strumento di tutela contro i trattamenti illeciti, in particolare nei confronti di quelli che possono essere effettuati senza l'informativa o il consenso dell'interessato.

In questa prima fase applicativa, l'attività del Garante è stata orientata a favorire la capacità di assorbimento dei nuovi adempimenti da parte dei titolari. In questa direzione, il Garante ha valutato con favore la proposta di introdurre le forme semplificate e gli esoneri previsti dalla legge-delega (sanciti poi dal d.lg. n. 255/1997) e il contestuale differimento "ragionato" delle scadenze previste in tema di notificazione.

Gli esoneri e le semplificazioni previsti dal decreto legislativo n. 255/1997 hanno introdotto una notevole deflazione rispetto ai trattamenti di cui in genere è nota l'esistenza (si pensi, tra l'altro, a quelli necessari per assolvere un compito previsto dalla legge, da un regolamento o dalla normativa comunitaria, ovvero per adempiere ad obblighi contabili, retributivi, previdenziali, assistenziali o fiscali).

Scaduti i nuovi termini previsti per le notificazioni al Garante, graduati fino al 30 giugno 1998, tutto ciò permetterà una più agevole istituzione e consultazione del registro delle notificazioni, ponendosi in armonia con le esigenze di semplificazione dell'azione amministrativa e senza contraddire l'esigenza di un'omogeneità del grado di tutela dei diritti della persona.

Contemporaneamente a queste iniziative, il Garante si è adoperato per semplificare in altro modo la notificazione dovuta per legge, ed ha predisposto a tal fine un modello unico - su supporto informatico e cartaceo - che ha distribuito mediante vari canali, in particolare attraverso gli uffici postali.

1.2.3. Le richieste rivolte al titolare e al responsabile del trattamento.

Le posizioni attive degli interessati comprendono, anzitutto, il diritto di ottenere direttamente dai soggetti che elaborano i dati la conferma dell'esistenza o meno delle informazioni che li riguardano nonché, tra l'altro, delle finalità del trattamento.

Rientra inoltre nelle prerogative dell'interessato la possibilità di veder prontamente rispettati i requisiti di liceità e correttezza del tratta-

mento dei dati, anche attraverso la cancellazione delle informazioni trattate in violazione di legge, l'aggiornamento, la rettifica o l'integrazione dei dati stessi.

La garanzia di effettività di tali diritti, nel caso in cui il titolare del trattamento non adempia alle richieste dell'interessato, è rimessa inoltre ai provvedimenti inibitori e coercitivi che l'Autorità garante può adottare anche su ricorso dell'interessato e che sono assistiti dal presidio della sanzione penale.

Particolarmente degna di nota è l'introduzione del diritto di rettifica, attraverso il quale si può ottenere concreta soddisfazione dell'interesse alla correttezza e alla veridicità dei dati prima ancora della loro eventuale messa in circolazione, interesse che rimaneva assolutamente pretermesso nel sistema di tutela antecedente alla legge n. 675/1996, il quale assicurava la sola tutela civile risarcitoria senza alcuna possibilità di un'effettiva riparazione o di una garanzia contro il ripetersi dell'evento dannoso.

Da un lato, quindi, l'interessato ha acquisito il diritto di chiedere ed ottenere senza ritardo l'aggiornamento, la rettificazione e l'integrazione dei dati erronei, inesatti, incompleti o non aggiornati (artt. 9 e 13 della legge). Dall'altro, nel caso di inadempimento anche parziale da parte del titolare o del responsabile, l'interessato può beneficiare dei poteri autoritativi del Garante, connotati in termini di assoluta novità nella materia della tutela dei diritti della persona.

Il Garante, infatti, oltre a inibire in termini più tradizionali quei comportamenti che consistono in un fare illecito, può indicare "le misure necessarie a tutela dei diritti dell'interessato" (art. 29, comma 4), e dunque impartire qualunque prescrizione atta a tutelare l'interessato da un comportamento omissivo o elusivo.

1.2.4. Altre prerogative previste dalla legge n. 675 a tutela della riservatezza e bilanciamento con altri interessi.

La legge n. 675/1996 offre una varietà di strumenti che permettono all'interessato di adire il Garante mediante segnalazioni, reclami e ricorsi, nonché con richieste volte ad accedere ai dati per i quali non è previsto l'accesso in forma diretta (artt. 14 e 32, comma 6).

Questa pluralità di strumenti ha favorito un quadro di garanzie anche nelle more della disciplina più compiuta contenuta nel regolamento sull'organizzazione e il funzionamento dell'Ufficio del Garante (approvato dal Consiglio dei ministri il 19 dicembre 1997 e di imminente pubblicazione), che fissa nel dettaglio le regole del contraddittorio relative ai ricorsi e cioè ai mezzi di tutela che presuppongono una trattazione secondo una procedura più articolata.

Il numero e l'importanza delle questioni sinora esaminate dal Garante (vedi cap. 4) rivela la diffusa sensibilità che la legge n. 675/1996 ha stimolato nella società civile.

Le pronunce del Garante si sono articolate, soprattutto, in segnalazioni con le quali sono state rappresentate ai titolari del trattamento le modifiche da apportare (art. 31, comma 1, lett. c)), oppure, per alcuni casi di accertata violazione di legge, in provvedimenti con i quali si è vietata la prosecuzione del trattamento (art. 31, comma 1, lett. l)).

L'entrata in vigore del citato regolamento offrirà un quadro più completo che permetterà all'interessato di modulare meglio le proprie azioni (ferma restando la possibilità di adire la magistratura civile e penale, nelle forme ordinarie). Si potrà infatti scegliere con maggiore consapevolezza tra gli strumenti di tutela che offrono flessibilità in termini di forme e di tempi di trattazione (si allude alle segnalazioni e ai reclami: art. 31, comma 1, lett. d)) e i mezzi che, nonostante una procedura mi-

nutamente regolata, possono risultare maggiormente incisivi, considerata l'immediata "esecutività" dei provvedimenti anche cautelari del Garante e la tutela penale prevista a sostegno del loro rispetto (artt. 29 e 37).

Il Garante ha valorizzato nei propri provvedimenti un approccio non autoritativo e ispirato alla "persuasione", attraverso "segnalazioni" dirette ai titolari e ai responsabili dei trattamenti. Si è invece circoscritto l'intervento più propriamente interdittivo ai casi di manifesta violazione di legge, nei quali si è applicato l'art. 31, comma 1, lett. l) (divieto del trattamento dei dati in ragione del concreto rischio del verificarsi di un pregiudizio per uno o più interessati).

Un rilievo notevole ha assunto, ad esempio, la facoltà dei cittadini di inoltrare segnalazioni al Garante concernenti, in particolare, l'inosservanza anche parziale degli obblighi di informativa e di richiesta del consenso, a seguito delle quali il Garante ha invitato vari titolari a modificare i formulari o modelli da loro predisposti, concedendo più volte un termine congruo per l'adeguamento.

Questa complessiva impostazione è sembrata in linea con le esigenze manifestate da più parti volte ad individuare, anche con la collaborazione dell'Ufficio del Garante, le modalità più idonee e snelle per applicare i princìpi di garanzia nei diversi, e spesso articolati settori, considerate le obiettive difficoltà di introdurre una nuova disciplina in contesti della vita economica nei quali si erano consolidate prassi che appaiono inadeguate; difficoltà che in alcuni casi rendono comprensibile l'aspirazione all'introduzione graduale delle nuove regole.

Particolare attenzione è stata data dal Garante alla tutela dei diritti collegati alla riservatezza e, segnatamente, al bilanciamento dei diritti della personalità con la concorrente esigenza, avvertita anche dall'opinione pubblica, intesa ad evitare un arretramento della qualità e del livello di circolazione delle informazioni, specie di quelle detenute da organi pubblici ed accessibili in base alla legge n. 241/1990.

Le decisioni del Garante hanno evidenziato che il maggior grado di tutela apprestato al diritto alla riservatezza dalla legge n. 675/1996 non ha in alcun modo diminuito le prerogative di trasparenza e di libertà di informazione sia nei procedimenti della pubblica amministrazione, sia nei vari settori della vita sociale. Ad esempio, in risposta ad istanze e quesiti proposti anche da organi pubblici, il Garante ha riconosciuto la compatibilità delle nuove disposizioni con le norme di legge che prevedono:

a) la possibilità di rendere conoscibili al pubblico, in vario modo, alcune informazioni concernenti le classi stipendiali, le retribuzioni e le altre indennità corrisposte ad amministratori, dirigenti e lavoratori dipendenti ed autonomi da parte dei concessionari dei pubblici servizi (provvedimento del 16 settembre 1997);

b) la pubblicità della situazione patrimoniale dei titolari di determinate cariche pubbliche elettive o di incarichi direttivi (provvedimento dell'8 gennaio 1998);

c) la conoscibilità e la fruibilità da parte dei parlamentari dei dati personali contenuti nelle dichiarazioni e nei documenti forniti dall'AIMA, in applicazione della legge n. 204/1997 sulle quote-latte (provvedimento del 10 febbraio 1998).

Peraltro, sotto un altro versante, il Garante ha ribadito che la disciplina dell'accesso ai trattamenti prevista dalla legge n. 675/1996 non ha ampliato il regime della conoscibilità degli atti e dei documenti delineato da altre disposizioni legislative. Specificatamente, si è constatato che non sono stati attenuati i limiti all'accesso derivanti dalla legge n. 241/

1990, la quale collega la conoscibilità degli atti detenuti dalle amministrazioni all'esistenza di un interesse personale e concreto in relazione alla tutela di situazioni giuridicamente rilevanti; e ciò in occasione di pareri richiesti, ad esempio, in tema di conoscibilità dei verbali di commissioni consultive presso la Presidenza del Consiglio dei ministri (provvedimento del 22 gennaio 1998).

1.3. I NUOVI STRUMENTI DI TUTELA.

1.3.1. Tre sedi di tutela del diritto alla riservatezza.

Il settore dove si possono evidenziare meglio le scelte fondamentali del legislatore, e dunque verificare ricadute del tutto peculiari della normativa sull'ordinamento giuridico e sull'assetto degli interessi coinvolti, è quello del sistema delle garanzie e dei controlli apprestati per l'effettività della tutela.

Si registra, in definitiva, il superamento dello schema di tutela del diritto alla riservatezza imperniato unicamente sulla repressione dei comportamenti illeciti attraverso gli ordinari strumenti giurisdizionali, a favore di forme differenziate e progressive di tutela anche cautelare:

a) in una prima fase, affidata all'esercizio dei diritti di cui all'art. 13 della legge, il cittadino è posto in grado di esercitare il diritto di accesso direttamente nei confronti dei soggetti che trattano i dati a lui riferibili, e dunque innesca un primo meccanismo che è collegato all'obbligo di informativa da parte del titolare e del responsabile del trattamento, i quali devono attivarsi anche per dare riscontro alle richieste dell'interessato (artt. 10, 11 e 13);

b) nel caso in cui l'interessato non veda soddisfatte le sue richieste, la tutela dell'effettività delle situazioni giuridiche può spostarsi nella sede giurisdizionale o, attraverso il ricorso al Garante, in quella amministrativa (art. 29 della legge), la quale comporta l'eventuale esercizio dei poteri interdittivi del Garante anche sul piano cautelare.

Particolarmente significativa risulta la previsione di forme specifiche di tutela coercitiva e inibitoria, collegate agli obblighi di fare e non fare posti dalla legge n. 675/1996 e incanalate nel solco di un procedimento amministrativo avanti al Garante, ma "rafforzate" dalla contestuale previsione di sanzioni penali per l'inosservanza degli atti che le concretano.

Tale previsione non intacca minimamente la competenza del giudice ordinario, ma è frutto dell'avvertita opportunità di destinare forze e competenze specifiche in capo ad una Autorità caratterizzata da un forte connotato di indipendenza ed autonomia, al fine di creare forme immediate ed efficaci di tutela complementari e non in contraddizione con l'ordinario processo civile che resta, peraltro, l'unica sede esclusivamente "competente" per determinati aspetti (ad esempio, per il risarcimento del danno).

Ciò corrisponde all'esigenza di far fronte alla velocità di propagazione e alla potenziale ampiezza dei destinatari della diffusione dei dati, specie nel caso di trattamenti per via telematica, nonché all'opportunità di non inflazionare ulteriormente il già gravoso carico di lavoro della giustizia ordinaria.

L'istituzione e i poteri del Garante, con la contestuale previsione di meccanismi a garanzia sia dell'osservanza delle forme procedimentali, sia dei provvedimenti adottati, rappresentano una scelta "forte" del legislatore a favore di un sistema coerente, e denotano una novità assoluta

nella tutela dei dati personali, affidata fino ad oggi alla sola garanzia giurisdizionale del risarcimento del danno alla riservatezza e, sotto il profilo penale, sostanzialmente limitata alla punibilità di alcune fattispecie.

Va inoltre osservato che gli artt. 21, comma 3 e 31, comma 1, lett. l) della legge n. 675/1996 estendono i poteri coercitivi del Garante, in sede cautelare o "definitiva", dall'ambito della garanzia amministrativa su ricorso all'attivazione di procedimenti - che possono iniziare anche d'ufficio - a tutela di uno o più interessati ovvero di rilevanti interessi della collettività non individualizzati;

c) la tutela successiva alla lesione della riservatezza è affidata al risarcimento del danno e alla previsione di alcune sanzioni anche penali. Tali sanzioni sono state previste in considerazione degli obblighi nascenti da convenzioni e atti comunitari, a seguito di un raffronto con le legislazioni degli altri Paesi e con le disposizioni sanzionatorie già vigenti in Italia che tutelano in varia forma il diritto alla riservatezza e la segretezza della corrispondenza. Particolarmente significativa è, oggi, la conferma della configurabilità di una responsabilità civile per trattamento illecito di dati personali (evidenziata dagli articoli 18 e 29, comma 9, della legge) che dimostra, sul versante delle sanzioni civili, la preferenza del legislatore (in atto anche per altre attività socialmente rilevanti) per i rimedi inibitori, riparatori e sanzionatori, anziché per i controlli preventivi.

La risarcibilità del danno "da computer", in assenza di una normativa specifica che inquadrasse la relativa responsabilità, era materia oggetto dell'elaborazione dottrinaria e giurisprudenziale, nel cui ambito si erano prospettate distinte ipotesi di utilizzazione di norme applicate analogicamente, quali l'art. 2050 del codice civile in tema di "attività pericolose" e l'art. 2049 del medesimo codice sulla responsabilità del produttore.

La legge n. 675/1996 ha ampliato la possibilità di riparazione del danno morale, che viene ad essere oggi risarcibile anche nei casi di inosservanza dei requisiti di liceità dei trattamenti, indipendentemente dalla presenza di fattispecie penalmente rilevanti.

Dal punto di vista processuale, invece, la prova liberatoria dinanzi al giudice civile è stata disciplinata in conformità all'art. 2050 del codice civile.

La legge, così, ha tenuto presente la necessità di agevolare la riparazione dei danni subiti per effetto della gestione dei dati, attività che per la sua potenziale invasività, velocità ed ampiezza di diffusione, è equiparata alle c.d. "attività pericolose" senza che ciò ne comporti, però, una valutazione negativa. Al contrario, l'ordinamento tiene conto dell'importanza sociale delle attività particolarmente rischiose, e si limita ad evitare che i danneggiati possano incorrere in difficoltà nel provare determinati elementi del fatto illecito.

Al tempo stesso, il legislatore ha avvertito la necessità di riconoscere il diritto al risarcimento del danno morale proprio nei casi che non sono sanzionati sul piano penale e che comportano più frequentemente un danno alla persona, in particolare nei casi di violazione dei princìpi di qualità, esattezza, completezza ed aggiornamento delle informazioni (art. 9).

Si è voluto quindi assicurare protezione a qualsiasi lesione della *privacy* collegata alla violazione delle disposizioni della legge, indipendentemente dalla rilevanza penale della fattispecie e si è superato così (in termini particolarmente innovativi per la tradizione giuridica italiana) lo schema risarcitorio tipico del danno non patrimoniale.

Il sistema di garanzie offerte dalla nuova normativa è integrato, infine, dalla previsione di alcune sanzioni penali, temperate dalla rilevanza, di regola, delle sole condotte dolose e dall'introduzione, per alcuni casi, di un dolo specifico rappresentato dal fine di trarre un profitto per sé o per altri o di recare ad altri un danno (artt. 34, 35, 36, 37 e 38).

PAGINA BIANCA

2. L'EVOLUZIONE DELLA DISCIPLINA SULLA RISERVATEZZA.

2.1. LE SEMPLIFICAZIONI APPORTATE DAL LEGISLATORE IN UN QUADRO DI RAFFORZATE GARANZIE.

2.1.1. Gli obblighi di informativa.

La legge n. 675/1996 ha previsto per coloro che intendono raccogliere ed utilizzare dati personali l'obbligo di fornire alcune informazioni all'interessato o, comunque, alle persone presso le quali i dati sono raccolti. L'informativa deve precedere la raccolta delle informazioni e, quando i dati sono raccolti presso terzi, deve essere fornita all'interessato al momento della registrazione dei dati o, qualora sia prevista la loro comunicazione, non oltre la prima operazione di comunicazione (art. 10).

L'informativa riguarda, in particolare, i seguenti aspetti:

a) le finalità e le modalità del trattamento dei dati;

b) l'obbligo o meno di fornire le informazioni richieste;

c) le conseguenze dell'eventuale rifiuto di fornire le informazioni;

d) i soggetti o le categorie di soggetti alle quali possono essere comunicati i dati e l'ambito di diffusione nazionale e internazionale dei dati;

e) i diritti riconosciuti alla persona alla quale i dati si riferiscono, ai sensi dell'art. 13 della legge;

f) il nominativo e le coordinate del titolare nonché, se designato, del responsabile.

L'obbligo dell'informativa, che trova riscontro in varie raccomandazioni del Consiglio d'Europa, ed è puntualmente disciplinato dalla direttiva n. 95/46/CE (artt. 10 e 11), rappresenta una delle principali novità introdotte dalla legge n. 675/1996, in quanto permette al soggetto che fornisce i dati di comprendere appieno le motivazioni della richiesta di informazioni, di scegliere se aderirvi o meno (e, ove necessario, di manifestare il proprio consenso "informato"), nonché di poter controllare meglio, successivamente, l'utilizzazione e la destinazione dei dati.

Il legislatore ha facilitato l'adempimento dell'obbligo, stabilendo che:

a) l'informativa possa non contenere, in tutto o in parte, gli elementi già conosciuti dall'interessato;

b) nell'informativa si possano non inserire gli elementi suscettibili di ostacolare lo svolgimento di funzioni pubbliche ispettive o di controllo (peraltro circoscritte a casi precisamente individuati);

c) le informazioni di cui all'art. 10 non debbano essere fornite quando i dati sono utilizzati in base ad un obbligo normativo;

d) nel caso di raccolta dei dati presso terzi, si possa richiedere al Garante di valutare i casi in cui l'adempimento sia, di fatto, impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto dell'interessato di essere informato personalmente sull'esistenza di un trattamento di dati che lo riguardano.

Con il decreto legislativo n. 123 del 1997, il Governo, anche su sollecitazione del Garante, ha introdotto una modifica significativa all'art. 10 della legge n. 675/1996, prevedendo che l'informativa possa essere data anche oralmente, oltre che in forma scritta.

Questa modifica, che riguarda la raccolta di dati sia presso l'interessato sia presso terzi, ha reso più armoniche le disposizioni normative sull'informativa e il consenso (che può essere prestato anche oralmente, se i dati non hanno natura sensibile, ferma restando la necessità di documentarlo per iscritto anche a cura del soggetto che raccoglie i dati).

A parte l'evidente semplificazione, la novità permette in alcuni casi di tutelare meglio le stesse persone interessate, consentendo ad esse di ottenere una spiegazione orale immediata ed esauriente delle principali caratteristiche della raccolta, la quale può essere, a volte, più efficace rispetto ad una informativa scritta, riportata - magari - in un modello-tipo.

Il Garante ha chiarito poi che l'informativa non deve essere fornita caso per caso, in occasione di ogni singola operazione di utilizzazione dei dati. Inoltre, ha specificato che le due informative (quella fornita per i dati raccolti presso l'interessato e quella resa per i dati acquisiti da terzi), sono cumulabili e possono essere effettuate contestualmente, qualora il titolare del trattamento precisi chiaramente che l'informativa è in relazione ad entrambe le situazioni previste dall'art. 10 (il che può avvenire predispondendo, ad esempio, un modello cartaceo nel quale siano riportate distinte caselle corrispondenti alle due informative previste da tale disposizione, caselle che il titolare potrebbe barrare a seconda dei casi).

2.1.2. I termini per il rilascio delle autorizzazioni e per le notificazioni.

L'entrata in vigore della legislazione sulla *privacy* ha implicato due importanti adempimenti, specie per le imprese e le pubbliche amministrazioni: la richiesta di autorizzazione al Garante per poter trattare alcuni dati personali e l'obbligo di notificare alcuni trattamenti alla medesima Autorità.

Il primo adempimento è connesso alla particolare tutela che la legge n. 675/1996 attribuisce ad alcune categorie di dati definiti "sensibili" (art. 22, comma 1) o attinenti a taluni provvedimenti giudiziari (art. 24).

Sono ritenuti "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 idonei a rivelare lo stato di salute e la vita sessuale.

Nei riguardi dei trattamenti di questi dati, la legge prevede una disciplina differenziata a seconda che ad effettuarli siano soggetti pubblici o privati.

Il trattamento dei dati sensibili da parte dei soggetti pubblici, esclusi gli enti pubblici economici, deve essere autorizzato da un'espressa disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite (art. 22, comma 3). Il legislatore si è mostrato consapevole della circostanza che l'ordinamento prevedeva poche disposizioni di questo tipo, ed ha perciò fissato il termine transitorio di un anno (cioè, fino al 7 maggio 1998), permettendo alle pubbliche amministrazioni di continuare a trattare i dati sensibili già elaborati anche in assenza di disposizioni di legge del genere poc'anzi indicato, sulla base di una semplice comunicazione al Garante.

Lo stesso trattamento può essere effettuato anche da privati o da enti pubblici economici, che sono tenuti a richiedere il consenso scritto dell'interessato e l'autorizzazione preventiva del Garante (art. 22, comma 1).

In termini generali, qualora vi sia una richiesta di autorizzazione, il Garante deve pronunciarsi entro trenta giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, o successivamente, il Garante può prescrivere misure ed accorgimenti a garanzia dell'interessato, che il titolare del trattamento deve adottare (art. 22, comma 2).

Un'autorizzazione del Garante è altresì necessaria quando, in assenza di un'esplicita disposizione di legge che abbia caratteristiche analoghe a quelle sopra descritte per i dati sensibili, si intendano trattare dati personali idonei a rivelare determinati provvedimenti giudiziari (art. 24 legge n. 675/1996; art. 686, commi 1, lettere *a)* e *d)*, 2 e 3, del codice di procedura penale). Anche in questo caso, una disposizione transitoria ha permesso di non pregiudicare la prosecuzione dei trattamenti che soggetti pubblici e privati effettuano, talvolta anche per il perseguimento di rilevanti finalità pubbliche.

Per il rilascio di tutte queste autorizzazioni la legge aveva fissato il termine di trenta giorni successivi all'entrata in vigore della legge n. 675/1996, che è apparso subito insufficiente e che per questo è stato prorogato al 30 novembre 1997 (art. 4, comma 1, d.lg. 9 maggio 1997, n. 123; art. 41, comma 7, l. n. 675). Con questo intervento correttivo, si è inoltre ribadito che il Garante può rilasciare tali autorizzazioni - anche d'ufficio - non solo in favore di singoli titolari, ma anche attraverso provvedimenti-tipo o di ordine generale nei confronti di intere categorie di titolari o di trattamenti.

L'Autorità ha utilizzato ampiamente tale facoltà ed ha emanato, come si vedrà, sei autorizzazioni generali, nel periodo compreso fra il 19 novembre e il 29 dicembre 1997.

Ciò ha permesso non solo di semplificare enormemente le procedure altrimenti insostenibili che si sarebbero attivate dinanzi al Garante, ma ha facilitato l'armonizzazione delle prescrizioni impartite con carattere di generalità a tutti coloro che rientrano in una determinata categoria (ad esempio, i liberi professionisti iscritti in albi o elenchi) o che elaborano certi dati (ad esempio, quelli di carattere medico).

Per quanto riguarda, invece, l'obbligo di notificazione, va ricordato che esso grava sul titolare che intenda effettuare o cessare un trattamento di dati personali oggetto di applicazione della legge (artt. 7 e 16). Analogamente, l'articolo 28 stabilisce che il trasferimento di dati personali fuori dal territorio nazionale, anche se temporaneo, debba essere notificato previamente al Garante, qualora sia diretto verso Paesi non appartenenti all'Unione europea ovvero, se si tratta di dati sensibili o attinenti a taluni provvedimenti giudiziari, anche quando sia diretto verso Paesi dell'Unione europea.

L'art. 41, comma 2, prevedeva che i trattamenti iniziati prima dell'8 maggio 1997 e fino al successivo 7 agosto avrebbero dovuto essere notificati entro sei mesi dalla pubblicazione nella *Gazzetta Ufficiale* del decreto del Presidente del Consiglio dei ministri relativo alla determinazione del contingente di personale posto alle dipendenze del Garante.

Il decreto legislativo 28 luglio 1997, n. 255, ha modificato tali termini, non tanto per esigenze di mera proroga, ma per permettere ai titolari dei trattamenti di valutare attentamente le numerose ipotesi di esonero e di semplificazione introdotte dal medesimo decreto.

In particolare, si è prevista la possibilità di dichiarare i trattamenti iniziati prima del 1 gennaio 1998 nel periodo intercorrente dal 1 gennaio al 31 marzo 1998, ferma restando la necessità di dichiarare preventivamente, a partire dal 1 gennaio 1998, le attività del tutto nuove di trattamento intraprese a decorrere da tale data.

Nella medesima ottica di gradualità già seguita dalla legge n. 675/1996, si è differito al periodo intercorrente tra il 1 aprile e il 30 giugno 1998 il termine per notificare i trattamenti:

a) non automatizzati di dati diversi da quelli sensibili;

b) effettuati per ragioni di giustizia presso gli uffici giudiziari, il C.S.M. e il Ministero di grazia e giustizia;

c) effettuati presso il servizio del casellario giudiziale o per il servizio carichi pendenti nella materia penale;

d) posti in essere da alcuni soggetti pubblici per finalità di difesa o di sicurezza dello Stato, ovvero di prevenzione, accertamento o repressione dei reati (art. 4, comma 1, lett. *e)*).

2.1.3. Esenzioni e semplificazioni delle notificazioni.

Sono state sollevate alcune perplessità nei confronti della "notificazione", essendosi paventato da più parti che si volesse costituire una sorta di "Grande Fratello" informatico nel quale far confluire tutti i dati trattati nel Paese.

In realtà, questo obiettivo non è presente nelle norme e nello spirito della legislazione sulla *privacy*.

L'obiettivo della notificazione e della conseguente istituzione di un registro generale dei trattamenti - già esistente in tutti i Paesi europei - è quello di predisporre uno strumento semplice ed aggiornato, attraverso il quale il soggetto che abbia il sospetto di un trattamento illecito di dati che lo riguardano o intenda comunque effettuare una verifica, possa individuare con maggiore facilità i possibili titolari e responsabili nei confronti dei quali esercitare i propri diritti.

In altre parole, il registro non conterrà i nominativi dei soggetti ai quali si riferiscono i dati elaborati dai vari titolari, e recherà piuttosto una serie di indicazioni generali utili per comprendere le modalità complessive dei trattamenti e le relative finalità.

Inoltre, la consapevolezza di evitare inutili appesantimenti burocratici era ben presente nell'idea del legislatore, il quale, nell'approvare le leggi nn. 675 e 676, ha bilanciato l'esigenza di rendere pubblici e facilmente individuabili i trattamenti di dati personali con la necessità di non gravare gli operatori di inutili adempimenti.

Infatti, nei riguardi della notificazione, la legge n. 676 ha previsto la possibilità di introdurre forme semplificate e di esonero per le notificazioni sia del trattamento dei dati sia del loro trasferimento all'estero, laddove questi non presentino rischi di danno all'interessato (art. 1, comma 1, lett. *f)*).

Lo snellimento previsto da tale legge è in linea, peraltro, con l'articolo 18 della direttiva n. 95/46/CE, il quale stabilisce che gli Stati membri *"... possono prevedere una semplificazione o l'esonero dall'obbligo di notificazione soltanto qualora si tratti di categorie di trattamento che non siano tali da recare pregiudizio ai diritti e alle libertà della persona interessata ..."*.

Peraltro, quest'ultima disposizione prevede che per ogni trattamento sottoposto ad una notificazione semplificata o che benefici di un esonero, lo Stato membro debba precisare necessariamente ".. *le finalità,*

i dati o le categorie di dati trattati, la categoria o le categorie di persone interessate, i destinatari o le categorie di destinatari cui sono comunicati i dati e il periodo di conservazione dei dati".

Tali "condizioni", fissate su base comunitaria, hanno imposto una descrizione non sintetica di ciascuna situazione presa in considerazione. L'art. 1 del decreto legislativo n. 255/1997 ha perciò individuato analiticamente i casi di esonero e quelli nei quali è possibile effettuare la notificazione in forma semplificata.

In particolare, sono stati esonerati dalla notificazione alcuni trattamenti il cui "tasso di rischio" per la violazione della sfera di riservatezza del cittadino è sembrato minore (trattamenti di dati necessari per assolvere un compito previsto dalle leggi; trattamenti di dati contenuti o provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque; trattamenti effettuati esclusivamente per la gestione del protocollo; tenuta di rubriche telefoniche o analoghe; trattamenti collegati strettamente a specifiche prestazioni di liberi professionisti o all'attività di piccoli imprenditori; tenuta di albi o elenchi professionali; trattamenti effettuati esclusivamente per l'ordinaria gestione di biblioteche, musei e mostre, nonché per l'organizzazione di iniziative culturali o sportive o per la formazione di cataloghi e bibliografie; trattamenti effettuati da associazioni, fondazioni, comitati; trattamenti effettuati temporaneamente, per esclusive finalità di raccolta di adesioni a proposte di legge d'iniziativa popolare, a richieste di referendum, a petizioni o ad appelli; trattamenti finalizzati all'amministrazione dei condomini).

È stata inoltre riconosciuta ad alcune categorie la possibilità di notificare in forma semplificata, e precisamente: *a)* ai soggetti pubblici, relativamente al trattamento di dati sensibili o attinenti a determinati provvedimenti giudiziari, autorizzato da una norma di legge o da un provvedimento del Garante; *b)* ai giornalisti, ai pubblicisti e agli iscritti al registro dei praticanti, riguardo ai trattamenti relativi all'esercizio della loro professione e per l'esclusivo perseguimento delle relative finalità; *c)* ai soggetti pubblici e privati che trattano dati non sensibili o attinenti a taluni provvedimenti giudiziari, in via temporanea e senza l'ausilio di mezzi elettronici o automatizzati, per finalità strettamente collegate all'organizzazione interna della propria attività.

Il decreto legislativo n. 255 ha quindi previsto che la notificazione in forma semplificata debba contenere in ogni caso l'indicazione delle coordinate del titolare e del responsabile, l'ambito di comunicazione e di diffusione dei dati, la descrizione generale delle misure di sicurezza (che hanno un rilievo particolare secondo la nuova normativa), nonché la menzione della qualità e della legittimazione del soggetto che effettua la notificazione.

Relativamente ai restanti elementi che compongono la notificazione "ordinaria", si è stabilito che il Garante, in conformità al regolamento previsto dall'art. 33, comma 3, della legge 675/1996, debba individuare le notizie che possono essere omesse nella notificazione semplificata, il che è avvenuto attraverso la predisposizione di un modello semplificato.

Il Garante, nelle more dell'entrata in vigore del regolamento in corso di pubblicazione, ha così avvertito la necessità di predisporre un modello che agevolasse e rendesse più omogenee le notificazioni, ed ha contestualmente individuato, quale elemento informativo da indicare comunque, anche per la forma semplificata (oltre a quelli appena citati) i luoghi ove sono custoditi i dati.

È appena il caso di precisare che le semplificazioni e gli esoneri introdotti, conformemente a quanto previsto dalla legge-delega, attengono unicamente al profilo della notificazione e non incidono sugli altri ob-

blighi previsti dalla legge n. 675/1996, quali ad esempio quelli relativi all'attuazione delle misure di sicurezza, all'acquisizione del consenso e all'esercizio dei diritti.

Anche per quanto riguarda le modalità concrete per la notificazione, il Garante si è ispirato da subito alle indicazioni previste dal regolamento *in itinere*, che denotano, in particolare, una preferenza per l'impiego di tecniche informatiche per la redazione della dichiarazione.

2.1.4. Estensione della disciplina applicabile ai giornalisti.

Il legislatore delegato ha attuato tempestivamente il principio di delega che prevedeva eventuali norme corettive e l'estensione delle deroghe per i giornalisti contenute nella legge n. 675/1996, ed ha applicato le deroghe stesse, come si vedrà, ai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti giornalisti (artt. 26 e 33, legge n. 69/1963), nonché a coloro che trattano dati ai fini della pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero (art. 25, comma 4-*bis*, legge n. 675/1996).

Si è così attuata la garanzia della libertà di informazione e dell'espressione letteraria ed artistica, prevista dallo stesso art. 9 della direttiva europea, in termini che comprendono anche la notificazione, ma che vanno oltre questo adempimento, in quanto espandono in favore dei predetti soggetti anche le altre disposizioni della legge che bilanciano i diritti della personalità con il fondamentale diritto di informare e di manifestare liberamente il proprio pensiero.

2.2. Le iniziative in corso.

2.2.1. L'individuazione delle misure minime di sicurezza.

Le disposizioni che in varia forma regolano la raccolta, l'elaborazione e la divulgazione delle informazioni personali risulterebbero inefficaci qualora non fossero assistite da un'idonea politica della sicurezza che porti a custodire i dati e a gestire i sistemi riducendo al minimo il rischio della perdita anche accidentale delle informazioni o di un'accesso non corretto o non consentito.

La legge n. 675/1996 è stata approvata nella consapevolezza dei costi che ciò può comportare, ma ha segnato un'inversione di tendenza nella materia, orientando i titolari delle banche dati, specie automatizzate, verso la convinzione che le spese sostenute rappresentano non tanto un'inutile dispendio di danaro, quanto un prezioso investimento che riduce i danni che possono derivare dalla vulnerabilità dei sistemi o dalla dispersione di dati spesso sensibili.

La sicurezza dei dati e dei sistemi non è più un argomento di mero interesse militare e finisce per interessare anche i soggetti che dispongono di una base limitata di dati.

Il legislatore ha avvertito l'esigenza di una certa gradualità, ed ha perciò previsto alcune disposizioni transitorie che hanno effetti anche sul piano dell'eventuale responsabilità per danno (art. 41, comma 3).

La legge ha poi preso atto della necessità di delimitare per quanto possibile la responsabilità penale, in termini di *extrema ratio*, ed ha pertanto stabilito che la sanzione penale ora prevista dall'art. 36 della legge non riguarda le condotte lesive del generale obbligo di sicurezza posto dall'art. 15, comma 1, della legge (rilevanti sul piano della responsabilità civile e, se del caso, contabile o disciplinare), ma attiene alla sola inosservanza di alcune circoscritte prescrizioni contenute nel regola-

mento di prossima emanazione (il quale deve individuare, tra le più ampie regole di sicurezza fissate dal citato comma 1, alcune prescrizioni "minime" ritenute talmente essenziali da comportare, in ottemperanza dell'obbligo sanzionatorio nascente dalla direttiva europea e dalla Convenzione di Strasburgo, la previsione di una sanzione penale).

Più precisamente, la legge n. 675/1996 ha previsto l'individuazione mediante regolamento del Governo di alcune *"misure minime di sicurezza da adottare in via preventiva"* per la sicurezza dei dati e dei sistemi (art. 15, comma 2), richiamate armonicamente nella stessa legge n. 249/1997 istitutiva dell'Autorità per le garanzie nelle comunicazioni (art. 1).

Tale indicazione si inquadra nell'ambito delle norme sulla sicurezza contenute, oltre che nella Convenzione di Strasburgo e nella direttiva europea, nella raccomandazione N. R (87) 15 del 17 settembre 1987 del Consiglio d'Europa e nella Convenzione di applicazione dell'Accordo di Schengen.

Il Ministero di grazia e giustizia ha diramato il 17 marzo 1998 lo schema di regolamento predisposto dalla "Commissione Fanelli", sottoponendolo al parere dell'Autorità per l'informatica nella pubblica amministrazione e del Garante, il quale si è espresso favorevolmente formulando alcuni suggerimenti.

La materia è apparsa complessa e delicata, in quanto la molteplicità dei sistemi informativi, le differenti configurazioni e le applicazioni informatiche presenti sui diversi sistemi (unitamente alla vastità dei campi di applicazione indagati), hanno richiesto un provvedimento che chiarisse anzitutto i termini del linguaggio (misure minime di sicurezza, strumenti utilizzati, amministratore di sistema, ecc.) e desse indicazioni chiare sulle linee di principio cui deve ispirarsi la sicurezza informatica, senza addentrarsi in elencazioni puntuali di tecniche o di adempimenti che, oltre a richiedere una certa autonomia d'azione, non possono essere ingabbiate in soluzioni che privilegerebbero determinati fornitori o produttori o che diverrebbero rapidamente obsolete in ragione del progresso tecnologico.

Le disposizioni transitorie che graduano il rispetto delle future disposizioni regolamentari (art. 41, commi 3 e 4) contribuiranno a favorire un'applicazione consapevole di prescrizioni che peraltro risultano già osservate di fatto presso strutture pubbliche e private attente alla tematica della sicurezza.

2.2.2. Attività parlamentari.

Il Garante ha seguìto i lavori parlamentari relativi ad alcuni provvedimenti, formulando suggerimenti che hanno sottolineato l'opportunità di apportare integrazioni e modifiche a disegni e a progetti di legge *in itinere*, in considerazione dei riflessi che le relative scelte comportavano sui diritti della personalità e, in particolare, sulle garanzie previste dalla legge n. 675/1996.

In particolare:

a) il Garante ha fornito alcuni spunti di riflessione nel corso dell'*iter* di approvazione della legge n. 249/1997 istitutiva dell'Autorità per le garanzie nelle comunicazioni, ed ha constatato con soddisfazione la successiva approvazione di alcuni emendamenti che armonizzano la normativa sulle telecomunicazioni con quella relativa ai dati personali, anche per ciò che attiene al coordinamento tra l'operato delle due autorità indipendenti e al ruolo dei pareri e delle proposte che il Consiglio nazionale degli utenti delle telecomunicazioni può ora sottoporre al Garante, qualora attengano alla tutela dei diritti indicati nell'art. 1 della legge n. 675/1996;

b) un'ulteriore significativa cooperazione con le commissioni parlamentari ha riguardato la ratifica della Convenzione istitutiva dell'Ufficio europeo di polizia (Europol), di recente varata definitivamente dal Parlamento, e che conferma la scelta già operata dalla legge n. 675/1996 di individuare nel Garante l'autorità nazionale di garanzia rispetto ai trattamenti di dati personali, analogamente a quanto previsto dalla Convenzione di applicazione dell'Accordo di Schengen;

c) il Garante è stato inoltre richiesto di esprimere il proprio punto di vista in occasione della conversione del decreto-legge 17 febbraio 1998, n. 23, recante disposizioni in materia di sperimentazioni cliniche in campo oncologico. Al riguardo, nel richiamare il quadro introdotto dalla legge n. 675/1996, il Garante ha rappresentato la necessità di tutelare meglio la riservatezza dei pazienti interessati alle terapie, omettendo l'annotazione del relativo nominativo sulle ricette mediche e ogni altra indicazione che potesse rendere conoscibile la patologia. Il Garante ha formulato altre osservazioni in modo da valorizzare il principio del "consenso informato" e da rendere più chiaro al paziente l'uso dei dati personali da parte delle autorità sanitarie pubbliche. Il Parlamento ha recepito, nella sostanza, le descritte indicazioni, accogliendo con la legge di conversione due proposte emendative tendenti, l'una, a far omettere, nella compilazione delle ricette, le generalità del paziente, sostituendole con riferimenti numerici collegati a dati d'archivio; l'altra, ad assicurare all'interessato un "consenso informato" sulla circostanza che i dati personali possono essere utilizzati presso gli organismi sanitari pubblici a fini di verifiche amministrative e per scopi epidemiologici o di ricerca;

d) il Garante ha inoltre constatato con soddisfazione che il Parlamento ha ritenuto opportuno far acquisire il suo parere in ordine agli schemi dei decreti legislativi previsti dalla legge n. 449/1997 di accompagnamento alla legge finanziaria, relativamente alla fissazione dei criteri di valutazione della situazione economica dei cittadini che richiedono determinate prestazioni sociali (c.d. "riccometro"), nonché per ciò che riguarda il sistema della partecipazione alla spesa sanitaria e delle relative esenzioni. Il 26 marzo 1998, il Garante ha formulato un parere articolato, invitando il Governo a perfezionare lo schema preliminare sul "riccometro" esaminato dal Consiglio dei ministri il 4 marzo scorso, in sostanziale sintonia con alcune osservazioni formulate in Parlamento. In particolare, il Garante ha richiamato l'attenzione sulla necessità di individuare meglio: 1) le prestazioni sociali agevolate oggetto di disciplina; 2) le modalità di acquisizione delle informazioni da parte degli enti erogatori e per lo svolgimento dei controlli successivi; 3) la natura giuridica, regolamentare o meno, di alcuni provvedimenti attuativi; 4) una forma di incisivo coordinamento dell'operato delle amministrazioni e degli enti impegnati nell'attuazione del decreto legislativo, anche per consentire al Garante di formulare una compiuta valutazione dei provvedimenti attuativi in sede di espressione dei pareri che l'art. 31, comma 2, della legge n. 675/1996 prevede riguardo ai provvedimenti che interessano la tematica dei dati personali; 5) maggiori garanzie per il trattamento dei dati sensibili, quali quelli relativi ai portatori di handicap; 6) l'ambito dei controlli, che non è apparso possibile autorizzare genericamente in deroga alle norme vigenti, come pure ipotizzato, considerata anche la non praticabilità del consenso dell'interessato (che lo schema di decreto aveva previsto anche in riferimento all'operato di organi pubblici, nonostante la diversa impostazione seguita, in termini più generali, dalla legge n. 675/1996). Il Garante è inoltre in procinto di esprimersi sul parere che il Governo ha richiesto in materia di spesa sanitaria;

e) nell'ambito dei prossimi impegni, il Garante continuerà a seguire i lavori parlamentari relativi al disegno di legge comunitaria 1995/1997, nonché quelli relativi alla legge comunitaria per il 1998, con particolare riferimento, quanto a quest'ultima, all'eventuale necessità di completare il recepimento delle direttive comunitarie nn. 95/46/CE e 97/66/CE (concernente specificamente il settore delle telecomunicazioni) per le parti eventualmente non considerate in sede di attuazione della legge-delega n. 676/1996;

f) sempre nell'intento di contribuire alla coerenza degli strumenti normativi collegati alla cooperazione europea in materia di giustizia e affari interni il Garante seguirà ulteriormente i lavori relativi al disegno di legge di ratifica della Convenzione sull'uso dell'informatica nel settore doganale (SID), già approvato dalla Camera in prima lettura;

g) sono inoltre all'attenzione del Garante altri provvedimenti attinenti all'obiezione di coscienza, alla tematica delle intercettazioni telefoniche e della tutela dei consumatori, come pure il disegno di legge (A.S. n. 3095), che reca modifiche alle leggi n. 59 e 127/1997 (c.d. "leggi Bassanini") nonché disposizioni sul lavoro a distanza e sui documenti di riconoscimento su supporto magnetico.

2.3. Le semplificazioni apportate dal Garante.

2.3.1. La predisposizione dei modelli per le notificazioni e le richieste di autorizzazione.

Come si è detto, nelle more dell'entrata in vigore del regolamento sull'organizzazione dell'Ufficio, e nell'ottica di semplificare al massimo l'adempimento della notificazione, il Garante ha ritenuto opportuno predisporre un apposito modello che è stato realizzato su supporto cartaceo e su supporto informatico.

Il modello, predisposto interamente dall'Ufficio, è stato sottoposto previamente al giudizio e ai suggerimenti del pubblico mediante la sua diffusione su organi di stampa specializzati.

Questa scelta, che intendeva rappresentare un ulteriore passo verso una collaborazione più proficua tra pubblica amministrazione e cittadini, ha stimolato vari apprezzamenti per l'impostazione seguìta. Sono pervenuti diversi suggerimenti, dei quali si è tenuto conto prima di avviare la prima stampa del modello cartaceo, che l'Istituto Poligrafico e Zecca dello Stato ha curato per n. 500.000 esemplari.

Dal punto di vista grafico, il modello è stato realizzato in due distinti fascicoli, contenenti l'uno le istruzioni per la compilazione e, l'altro, i riquadri da compilare e da inviare al Garante.

È stato compiuto ogni sforzo per contenere il numero delle pagine allo stretto indispensabile (comprensive di vari spazi per consigli, istruzioni, grafici ed altre precisazioni) e per agevolarne la redazione (la quasi totalità delle informazioni richieste può essere inserita barrando alcune caselle o inserendo codici numerici di riferimento).

Il modello è utilizzabile per notificare, a seconda dei casi: *a)* l'esistenza di trattamenti da dichiarare in forma ordinaria o semplificata; *b)* la loro cessazione; *c)* il trasferimento dei dati all'estero; *d)* le eventuali modifiche da apportare a precedenti notificazioni, che non sono soggette a variazioni temporali.

Il modello si articola in riquadri che corrispondono agli elementi necessari richiesti dalla legge. Il primo fa riferimento all'indicazione del titolare; il secondo ai luoghi ove sono custoditi i dati; il terzo all'ambito di comunicazione e di diffusione dei dati; il quarto alla descrizione gene-

rale delle misure adottate per la sicurezza dei dati; il quinto è da compilare nel caso in cui si intenda notificare la cessazione di un trattamento; il sesto, invece, si riferisce ai dati relativi ai responsabili, se designati.

È stato inserito, poi, un apposito riquadro da compilare facoltativamente, relativo a notizie volte a facilitare i rapporti con il Garante. Tra queste, alcune sono di mero carattere strumentale (numeri di telefono o di telefax e indirizzi di posta elettronica relativi a titolari, contitolari ed eventuali responsabili del trattamento). Altre, invece, tendono ad evitare o a semplificare nuove notificazioni in relazione alle informazioni aggiuntive che dovranno essere inserite nella notificazione entro il 1998 per effetto del pieno recepimento della direttiva comunitaria n. 95/46/CE (si tratta, in particolare, delle indicazioni relative alle categorie di servizi, di organismi e di persone fisiche e giuridiche preposte ai trattamenti oggetto di notifica, nonché all'eventuale designazione del titolare quale rappresentante in Italia da parte di altro titolare, stabilito fuori dall'Unione europea, che si avvalga per il trattamento di strumenti situati nel territorio italiano).

La prima parte del modello si conclude con la sottoscrizione da parte delle persone fisiche che notificano in forma semplificata o che dichiarano la cessazione del trattamento.

I riquadri successivi, quindi, devono essere compilati solo dai soggetti tenuti a notificare in forma ordinaria o a dichiarare il trasferimento dei dati all'estero; tali riquadri si riferiscono alle finalità e modalità del trattamento, alla natura dei dati oggetto del trattamento, alle categorie di interessati cui si riferiscono i dati, alla banca o banche dati cui è collegato il trattamento (quest'ultima informazione deve essere fornita anche nelle notificazioni semplificate relative ai giornalisti, pubblicisti e praticanti). Un apposito riquadro riguarda infine il trasferimento di dati all'estero, mentre l'ultimo raccoglie le sottoscrizioni di chi effettua la notificazione in forma ordinaria.

La predisposizione del modello ha permesso anche al Garante di fornire qualche chiarimento riguardo alle figure del titolare e del responsabile, alla nozione di banca dati, a quelle di contitolarità di trattamento e di trattamenti con "finalità correlate", che sono state oggetto nei primi mesi di applicazione della legge di diversi dubbi interpretativi da parte del pubblico.

Per la realizzazione del modello in versione informatica si è fatto ricorso alla collaborazione di una società esterna, incaricata in conformità alle norme di contabilità e di spesa.

Per raggiungere l'obiettivo della massima diffusione del modello nei suoi due supporti, è stata stipulata una convenzione "principale" con l'Ente poste italiane, che li ha distribuiti attraverso la propria rete di uffici presenti sull'intero territorio nazionale.

L'Ufficio ha poi sottoscritto numerose convenzioni dello stesso tipo con vari soggetti (in particolare con associazioni, anche di categoria, editori, liberi professionisti e Internet provider), che sono stati autorizzati a duplicare e a rendere disponibili i modelli sui siti Web, ovvero a distribuirli gratuitamente o dietro corrispettivo di modica entità (£. 6.000 max).

Per quanto riguarda le autorizzazioni al trattamento dei dati sensibili, si è già osservato che il Garante, attraverso le autorizzazioni generali, ha cercato di disciplinare la maggior parte dei trattamenti di questo tipo, individuando precise regole a garanzia degli interessati.

Le prescrizioni sono state delineate previa consultazione di diverse parti interessate, ed è stato fissato il termine di scadenza delle autorizzazioni generali al 30 settembre 1998, in considerazione del fatto che entro il 23 luglio 1998 dovranno essere previste alcune norme integrative in attuazione della legge-delega n. 676.

Di conseguenza, si sono sollevati i soggetti privati, le autorità pubbliche sanitarie e gli enti pubblici economici dall'onere di richiedere di volta in volta un'apposita autorizzazione al Garante, fatte salve le ipotesi in cui la specificità del caso o di alcuni trattamenti giustifichi la puntuale e diversa considerazione da parte del Garante di talune circostanze del tutto particolari o di situazioni eccezionali rappresentate dal richiedente.

Più precisamente, non devono richiedere l'autorizzazione:

a) gli esercenti le professioni sanitarie e gli organismi sanitari pubblici che trattano dati personali idonei a rivelare lo stato di salute dell'interessato, limitatamente ai dati e alle operazioni indispensabili per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato medesimo; l'autorizzazione è però necessaria se tali finalità riguardano un terzo o la collettività e l'interessato non abbia fornito il proprio consenso (art. 23);

b) i soggetti pubblici diversi dagli enti pubblici economici, i quali possono trattare dati sensibili o relativi ai provvedimenti indicati in talune disposizioni dell'articolo 686 del codice di procedura penale, qualora ciò sia previsto da un'espressa disposizione di legge nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite (artt. 22, comma 3, 24 e 41, comma 5).

Non sono altresì tenuti a richiedere l'autorizzazione i giornalisti, i pubblicisti, i praticanti iscritti nell'apposito registro e i soggetti che effettuano trattamenti temporanei finalizzati esclusivamente alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero, in conformità a quanto previsto dall'articolo 25 della legge n. 675/1996.

Fuori da questi casi, qualunque soggetto privato o ente pubblico economico che intenda trattare dati sensibili o relativi ai provvedimenti giudiziari cui fa riferimento l'art. 24 della legge n. 675/1996, è tenuto a richiedere un'apposita autorizzazione al Garante. Per facilitare tale adempimento, l'Ufficio ha predisposto anche in questo caso, sulla falsariga di quanto avvenuto per la notificazione, un modello semplificato contenente i dati ritenuti necessari per valutare il trattamento oggetto della richiesta di autorizzazione.

In particolare, il modello richiede di precisare a quale tipo di dati sensibili e a quali categorie di interessati il trattamento si riferisce; per quali finalità e con quali modalità questo viene effettuato, in quali luoghi e con quali misure di sicurezza sono custoditi i dati oggetto del trattamento. Si chiede poi di conoscere se i dati sono comunicati o diffusi o in connessione con altri trattamenti o banche dati in Italia o in altri Paesi, quali sono le categorie di titolari verso i quali avviene tale flusso e, infine, l'indicazione degli eventuali responsabili del trattamento.

2.3.2. Le autorizzazioni "generali" al trattamento dei dati sensibili.

Le autorizzazioni del Garante in materia di trattamento dei dati sensibili rappresentano uno dei punti-cardine del sistema delineato dalla legge n. 675/1996, essendo rivolte a tutelare il "nucleo centrale" della riservatezza e dell'identità personale.

La prima radice di una protezione rafforzata si rinviene nell'art. 6 della Convenzione di Strasburgo del 28 gennaio 1981 (ratificata con

legge 21 febbraio 1989 n. 98), che prospetta l'esigenza (nell'ambito del diritto interno degli Stati aderenti) di adeguate garanzie concernenti l'elaborazione di categorie speciali di dati, senza però indicarle nel dettaglio.

Successivamente, l'art. 8 della direttiva n. 95/46/CE ha fissato in linea generale il principio del divieto del trattamento di categorie particolari di dati, enumerando, tuttavia, sei ipotesi di eccezioni e di deroghe, le quali sono condizionate ad un presupposto fondamentale quale la previsione di opportune garanzie da parte degli Stati membri.

In realtà, le norme di fonte comunitaria recepiscono ed ampliano orientamenti che già precedentemente erano affiorati, pur se in forme embrionali, in alcune legislazioni contenenti disposizioni particolari sui dati sensibili. Norme antesignane si ritrovano, ad esempio, nell'art. 4 della legge svedese del 1973, nell'art. 3 della legge norvegese del 1978 e nell'art. 31 della legge francese del 1978.

Il nocciolo duro della riservatezza e dell'identità personale, che troviamo racchiuso nell'art. 22 della legge n. 675/1996, si presenta come uno dei capisaldi della sistematica dei dati personali, quale si è venuta enucleando nel suo complesso itinerario di sviluppo.

Già da tempo era *communis opinio* che i dati concernenti le opinioni e gli orientamenti politici, religiosi, e precipuamente quelli c.d. "supersensibili" inerenti allo stato di salute e alla vita sessuale, dovessero essere posti al riparo della conoscenza altrui. In un sistema moderno di idonei mezzi di salvaguardia, la riservatezza e l'identità personale si configurano come una situazione giuridica a struttura concentrica, nel cuore della quale emergono con particolare risalto i dati sensibili, mentre nei cerchi più distanti si collocano quelli ordinari (o non sensibili).

Non avendo le normative di fonte comunitaria tipizzato nel dettaglio tutte le garanzie specifiche cui devono attenersi i diritti interni in materia di dati sensibili, le legislazioni di tipo europeo possono distinguersi a seconda che la liceità del trattamento dipenda precipuamente dal consenso dell'interessato o dall'autorizzazione di un organo di garanzia o da una formula che abbini entrambi questi presupposti (ci si basa, ovviamente, su una visione comparatistica di ordine generale che non può tener conto, ovviamente, delle norme che saranno previste negli altri Paesi in attuazione della direttiva). La prima forma si riscontra, ad esempio, nella legge francese del 1978.

La legge spagnola adopera una formula binaria, secondo cui la liceità del trattamento dei dati individuanti l'ideologia e la religione è condizionata al consenso scritto dell'interessato, mentre la raccolta, il trattamento e la cessione dei dati che fanno riferimento all'origine razziale, alla salute e alla vita sessuale possono aver luogo solo quando lo disponga una legge per ragioni di interesse generale o quando l'interessato vi acconsenta espressamente.

La legge italiana introduce una tutela rafforzata, fondata sulla duplicità dei momenti legittimanti: l'autorizzazione e il consenso.

È da ricordare che, secondo il *memorandum* allegato alla Convenzione del Consiglio d'Europa n. 108 del gennaio 1981 (*"Rapport explicatif concernant la Convention pour la protection des personnes à l'egard du traitement automatisé des données à caractére personnel"*), "le garanzie appropriate" di cui all'art. 6 della Convenzione possono essere previste, se del caso, con strumenti diversi da un atto di rango legislativo, purché risultino specifiche ed idonee ad assicurare un *elevato* livello di protezione.

La scelta del nostro legislatore è rivolta a tale obiettivo, tenendo conto degli ulteriori presupposti fissati dalla direttiva e aggiungendo al consenso dell'interessato l'autorizzazione del Garante.

Notevole è il significato di questa opzione legislativa, in quanto l'art. 22, comma 1, rende non interamente disponibile il trattamento curato da privati ed enti pubblici economici.

L'introduzione dell'autorizzazione consegue all'affievolimento del "mito del consenso", in base alla considerazione che la manifestazione di volontà non è sempre frutto di libera autodeterminazione, e può apparire obbligata per effetto di un rapporto nel quale l'interessato sia in una posizione di debolezza e di svantaggio. Di qui un intreccio di garanzie che non si limitano all'autorizzazione e che si esprimono in misure ed accorgimenti che il Garante può prescrivere anche dopo il rilascio dell'autorizzazione.

L'atto amministrativo di autorizzazione è inserito in una sequenza procedimentale che trae inizio dalla richiesta del titolare interessato e che si conclude con la decisione adottata dal Garante nel termine di trenta giorni (decorsi i quali la mancata pronuncia equivale a rigetto).

Sostanzialmente, la norma originaria disegnava l'autorizzazione come atto inerente principalmente a fattispecie singole, portate di volta in volta a cognizione dell'organo di garanzia.

La formula della decisione resa caso per caso, episodicamente, è apparsa subito inadeguata, sicché attraverso l'attuazione della delega legislativa contenuta nella legge n. 676/1996, (d.lg. 9 maggio 1997, n. 123) è stata introdotta la modifica del comma 7 dell'art. 41 della legge n. 675/1996, in modo da precisare che le autorizzazioni del Garante possono essere rilasciate anche per determinate categorie di titolari o di trattamenti.

Ciò ha segnato un momento altamente innovativo nelle modalità di esercizio dei poteri del Garante, e ha configurato un modello istituzionale ispirato a criteri progrediti e avanzati di disciplina e di gestione degli interessi in gioco e delle molteplici posizioni soggettive presenti nel multiforme settore dei dati personali.

I tratti distintivi della nuova disciplina sono i seguenti:

a) le autorizzazioni per categorie o "collettive" permettono all'organo di garanzia di svolgere la propria azione di tutela con organicità, procedendo attraverso ampie aggregazioni di attività omogenee e rivolgendosi non più in maniera frammentaria e parcellizzata a singoli soggetti, ma ad intere categorie. La generalità dell'approccio valorizza lo strumento autorizzativo, che da provvedimento di disciplina di specifiche situazioni diviene una fonte di regolamentazione più ampia di interessi di rango quasi-normativo;

b) tale metodo conferisce alla formula autorizzatoria la possibilità di individuazione di momenti unitari, che rendono agevole e snella la salvaguardia di princìpi inderogabili connessi ai dati sensibili;

c) l'autorizzazione collettiva non soltanto si ispira ai princìpi di snellimento dell'azione amministrativa, ma comporta una notevole semplificazione degli adempimenti spettanti ai soggetti preposti al trattamento e incide positivamente sui loro profili economici, implicando un risparmio nei costi di gestione. Sicché il provvedimento collettivo ben può ricomprendersi in quella formula che la dottrina tedesca definisce come "norme di alleggerimento".

Molti sono i pregi inerenti a tale *modus procedendi*; e poiché oggi trova credito la formula definitoria del giusrealismo, va inoltre osservato come in una visuale di concretezza della vasta realtà economico-sociale sottostante al trattamento dei dati, e particolarmente a quelli sensibili, il metodo delle autorizzazioni di ampia portata sia rispondente alle esi-

genze del settore e dotato di efficacia operativa. Altrimenti, il governo degli interessi in gioco diverrebbe difficoltoso, con forte rischio di appesantimento e di inefficienza.

Il ritmo evolutivo del diritto alla riservatezza e all'identità personale sta rivelando un'espansione crescente. L'applicazione di tale diritto nel suo ciclo storico ha lambito dapprima pochi settori, ma ha pervaso poi una molteplicità sempre più fitta di comparti e di ambiti produttivi, professionali, economico-sociali o culturali. Il mercato dei dati conosce spazi sempre più vasti, essendo i confini superati in modo agevole da sofisticate tecniche telematiche ed informatiche.

Tenendo presenti questi criteri, il Garante ritiene che le autorizzazioni collettive rappresentino una prima risposta soddisfacente, realizzando una metodologia moderna ed efficiente.

Le sei autorizzazioni emanate nel 1997 presentano alcuni elementi caratterizzanti che le accomunano in un modello giuridico sostanzialmente omogeneo. Più precisamente:

a) le autorizzazioni sono provvisorie, con validità fino al 30 settembre 1998, poiché sono in fase di predisposizione i citati decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, che dovranno prevedere norme integrative in tema di dati sensibili, anche in attuazione delle raccomandazioni del Consiglio d'Europa;

b) ciascuna autorizzazione consta dei seguenti elementi strutturali: ambito di applicazione; interessati ai quali i dati si riferiscono; finalità del trattamento; categorie di dati; modalità di trattamento; conservazione, comunicazione e diffusione dei dati;

c) un elemento fortemente innovativo risiede nel fatto che l'autorizzazione è rilasciata anche senza richiesta di parte, in correlazione con i caratteri della categorialità e della collettività, i quali rendono superfluo l'atto di impulso del singolo.

Tutte le autorizzazioni sono rivolte a settori di grande ampiezza, quali quelli in cui operano datori di lavoro, medici, organismi sanitari pubblici, organismi di tipo associativo e fondazioni, liberi professionisti, imprese e società concernenti attività bancarie o assicurative, organismi di gestione di fondi o di strutture turistiche e del trasporto, investigatori privati. Va anzi rilevato che mentre alcune autorizzazioni sono monosettoriali, altre sono plurisettoriali fino a coinvolgere vere e proprie costellazioni di comparti aventi tra loro connessioni ed interrelazioni come pure rapporti di integrazione o di complementarietà;

d) un profilo comune alle sei autorizzazioni rilasciate è l'inserimento di un "considerando" concernente la necessità di garantire (anche nell'attuale fase transitoria) il rispetto dei princìpi relativi ai diritti e alle libertà fondamentali nonché alla dignità delle persone, "specie per quanto riguarda la riservatezza e l'identità personale". Nella prima fase di applicazione della legge n. 675/1996, l'attenzione del pubblico si era concentrata prevalentemente sull'aspetto della tutela della riservatezza, prestando minore considerazione ad altri aspetti inscindibilmente connessi: eppure l'art. 1 della legge medesima fa riferimento ad un binomio, riservatezza e identità personale. Le autorizzazioni collettive mostrano di tener conto di tale esigenza di completezza della tutela, e di tener presenti entrambi gli aspetti;

e) infine, un tratto caratterizzante delle autorizzazioni è costituito dal rilievo che viene dato, fra i soggetti destinatari, all'impresa.

Com'è noto, nella direttiva europea del 1995 si fa menzione più volte dell'attività economica in generale e, specificamente, dell'impresa.

La direttiva evidenzia il progressivo aumento dello scambio di dati tra imprese stabilite negli Stati membri e sottolinea che il divario di tutela dei diritti e delle libertà personali, garantiti negli Stati membri relativamente al trattamento dei dati personali, potrebbe costituire un ostacolo all'esercizio di una serie di attività economiche su scala comunitaria, falsando la concorrenza. Enuncia poi che gli Stati membri possono precisare le condizioni alle quali i dati personali possono essere utilizzati e comunicati a terzi nell'ambito di attività lecite di gestione corrente delle imprese o di altri organismi.

Nel contesto della legge n. 675/1996, la figura dell'impresa assume un ruolo importante dal lato passivo, essendo i dati che si riferiscono all'impresa stessa tutelati nella loro qualità e genuinità. Sul piano opposto (con riferimento, cioè, ai dati che l'impresa raccoglie) vi sono alcuni spunti interessanti. Tuttavia nelle autorizzazioni del Garante l'impresa assume un rilievo più nitido e viene indicata esplicitamente (assieme ad altri soggetti) fra i destinatari dei provvedimenti stessi.

In particolare, fra i tanti soggetti destinatari dell'autorizzazione n. 5/97, si distinguono le imprese autorizzate all'esercizio dell'attività bancaria o assicurativa e quelle che svolgono attività strettamente connesse e strumentali, nonché le imprese finalizzate a compimenti di sondaggi di opinione, di ricerche di mercato o campionarie. Anche l'autorizzazione n. 1/1997 ricomprende, fra i vari soggetti, le imprese che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche e parziali.

In conclusione, può dirsi che le formule autorizzatorie a carattere collettivo esprimono un duplice valore: quello di salvaguardare i diritti fondamentali della persona e quello di considerare gli interessi socialmente rilevanti di strutture portanti della società produttiva e del suo tessuto organizzativo.

Per quanto riguarda l'esame in dettaglio delle autorizzazioni rilasciate, il Garante, come si è detto, alla data del 31 dicembre 1997, ne ha emanate sei: si tratta della n. 1/97 relativa ai rapporti di lavoro (pubblicata sulla *Gazzetta Ufficiale* della Repubblica italiana n. 272 del 2 novembre 1997), della n. 2/97 attinente ai dati sulla salute e sulla vita sessuale, della n. 3/97 relativa ad associazioni e fondazioni (entrambe pubblicate sulla *Gazzetta Ufficiale* n. 279 del 29 novembre 1997), della n. 4/97 applicabile ai liberi professionisti (in *Gazzetta Ufficiale* n. 281 del 2 dicembre 1997), della n. 5/97 concernente diverse categorie di titolari di trattamento - settore bancario, assicurativo, turistico, del trasporto, dei sondaggi, ricerche ed elaborazione dati, della selezione del personale e della mediazione a fini matrimoniali (in *Gazzetta Ufficiale* n. 294 del 18 dicembre 1997) e la n. 6/97 riguardante gli investigatori privati (in *Gazzetta Ufficiale* n. 1 del 2 gennaio 1998).

La prima autorizza al trattamento dei dati sensibili di cui all'art. 22 della legge: *a) le persone fisiche e giuridiche, le imprese, gli enti, le associazioni e gli organismi che sono parte di un rapporto di lavoro* o che utilizzano prestazioni lavorative anche atipiche o temporanee, o che comunque conferiscono un incarico professionale; *b)* gli organismi paritetici e quelli che gestiscono osservatori in materia di lavoro; *c)* i medici competenti in materia di igiene e di sicurezza del lavoro.

I dati sensibili che possono essere trattati sono quelli attinenti a: a) lavoratori dipendenti, associati e ai relativi familiari; b) consulenti, liberi professionisti, agenti, rappresentanti e mandatari; c) lavoratori autonomi; d) candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti; e) persone fisiche che ricoprono cariche sociali.

Il trattamento dei dati sensibili deve essere necessario: *a)* per adempiere o per esigere l'adempimento o per eseguire specifici compiti previsti da leggi, regolamenti o da contratti collettivi anche aziendali, ovvero dalla normativa comunitaria in materia di previdenza e assistenza; *b)* ai fini della contabilità o della corresponsione di stipendi ed altri emolumenti; *c)* per il perseguimento delle finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo; *d)* per far valere o difendere un diritto in sede giudiziaria.

I dati oggetto del trattamento, così come la loro conservazione e le logiche di trattamento, non possono eccedere gli obblighi o le finalità sopradescritti.

La diffusione dei dati idonei a rivelare lo stato di salute è consentita solo se ciò è necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia. I dati idonei a rivelare la vita sessuale non possono essere diffusi. Gli altri dati sensibili possono essere comunicati e, ove necessario diffusi, nei limiti strettamente pertinenti agli obblighi, ai compiti e alle finalità sopra ricordati.

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 dei dati personali, con particolare riferimento all'art. 8 della legge n. 300/1970 (divieto per il datore di lavoro di effettuare indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione della sua attitudine professionale), all'art. 6 della legge n. 135/1990 (divieto per il datore di lavoro di effettuare indagini sul lavoratore tese ad accertare l'esistenza di uno stato di sieropositività), alle norme in materia di pari opportunità o volte a prevenire discriminazioni.

Il provvedimento n. 2/97, invece, autorizza al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale: *a)* gli esercenti le professioni sanitarie, qualora tale trattamento sia indispensabile per tutelare l'incolumità di un terzo o della collettività e l'interessato non abbia prestato il proprio consenso per iscritto; *b)* gli organismi e le case di cura private, nonché ogni altro soggetto privato, purché gli interessati abbiano prestato il consenso; *c)* gli organismi sanitari pubblici, compresi i soggetti pubblici che agiscano nella qualità di autorità sanitarie, qualora ricorrano alcune particolari condizioni.

L'autorizzazione, in particolare, viene rilasciata: *a)* ai medici-chirurghi, agli odontoiatri e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi; *b)* al personale sanitario infermieristico, tecnico e della riabilitazione che eserciti 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, ad alcune particolari condizioni; *d)* 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; *e)* alle organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi previsti nelle rispettive norme statutarie; *f)* alle comunità di recupero e di accoglienza, alle case di cura e di riposo; *g)* agli enti, alle associazioni e alle organizzazioni religiose riconosciute, ivi comprese le confessioni religiose e le comunità religiose, relativamente ai dati e alle operazioni indispensabili per perseguire scopi previsti nelle rispettive norme statutarie, se esistenti; *h)* alle persone fisiche o giuridiche, alle imprese, agli enti, alle associazioni e agli altri organismi, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precon-

trattuali derivanti da un rapporto di fornitura all'interessato di beni, di prestazioni o di servizi; *i)* ai gestori di impianti e strutture sportive, limitatamente ai dati e alle operazioni indispensabili per accertare l'idoneità fisica alla partecipazione ad attività sportive o agonistiche; *l)* ai fini dello svolgimento delle investigazioni di cui all'art. 38 delle norme di attuazione del codice di procedura penale; *m)* per far valere o difendere un diritto in sede giudiziaria, sempreché tale diritto sia di rango pari a quello dell'interessato.

Il trattamento può avere per oggetto i dati strettamente pertinenti agli obblighi, ai compiti o alle finalità sopra menzionate, e può comprendere le informazioni relative a stati di salute pregressi.

Particolare attenzione è stata riservata, attraverso stringenti limitazioni, alle informazioni relative ai nascituri nonché ai dati genetici, anticipando le più articolate regole che dovranno essere dettate anche in attuazione della Raccomandazione N. R (97) 5 del Consiglio d'Europa.

Per le modalità di trattamento, la conservazione dei dati e la loro comunicazione vengono impiegate previsioni e formule analoghe a quelle utilizzate per l'autorizzazione n. 1/97; unica eccezione di rilievo è l'introduzione della possibilità di diffondere i dati idonei a rivelare la vita sessuale, nel caso in cui tale diffusione riguardi dati resi manifestamente pubblici dall'interessato e per i quali il medesimo non abbia manifestato successivamente la sua opposizione per motivi legittimi.

Anche in questo caso, 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 dei dati personali, con particolare riferimento all'art. 5, comma 2, della citata legge n. 135/1990 (obbligo di effettuare la rilevazione statistica dell'infezione da HIV con modalità che non consentano l'identificazione della persona), all'art. 11 della legge n. 194/1978 (obbligo per l'ente ospedaliero nel quale si sia effettuata un'interruzione di gravidanza di inviare al medico provinciale una dichiarazione che non faccia menzione dell'identità della donna), all'art. 734-*bis* del codice penale (divieto di 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.

Con il provvedimento n. 3/97 è stato poi autorizzato il *trattamento di dati sensibili da parte di organismi di tipo associativo e fondazioni*, con particolare riferimento a: *a)* associazioni anche non riconosciute, ivi comprese le confessioni religiose e le comunità religiose, i partiti e i movimenti politici, le associazioni e le organizzazioni sindacali, i patronati, le associazioni di categoria, le organizzazioni assistenziali o di volontariato, nonché le federazioni e confederazioni nelle quali tali soggetti sono riuniti; *b)* le fondazioni, i comitati ed 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)* le cooperative sociali e le società di mutuo soccorso.

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, nonché per far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato.

Qualora tali soggetti, per perseguire le predette finalità, si avvalgano di persone giuridiche o di altri organismi con scopo di lucro (es. società editoriali o centri di assistenza fiscale), l'autorizzazione opera anche nei confronti di questi ultimi.

Il trattamento può riguardare i dati sensibili attinenti: *a)* agli associati, ai soci e, se necessario, ai relativi familiari e conviventi; *b)* agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesioni o che hanno contatti regolari con l'associazione, la fondazione o l'organismo; *c)* ai soggetti che ricoprono cariche sociali o onorifiche; *d)* ai beneficiari, agli assistiti e ai fruitori delle attività dei servizi prestati dall'associazione.

L'autorizzazione riguarda i dati sensibili, ad eccezione di quelli idonei a rivelare lo stato di salute e la vita sessuale ai quali si riferisce l'autorizzazione n. 2/97.

Per quanto concerne le modalità del trattamento e la conservazione dei dati, si fa sostanzialmente riferimento a quanto già previsto per le precedenti autorizzazioni.

I dati sensibili trattati possono essere comunicati e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi sopra individuati.

Restano anche in questi casi fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento dei dati personali, nonché le norme volte a prevenire discriminazioni, con particolare riferimento a quelle contenute nel decreto-legge n. 122/1993, convertito, con modificazioni, dalla legge n. 205/1993, in materia di discriminazioni per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio.

Con il provvedimento n. 4/97 è stato poi autorizzato *il trattamento dei dati sensibili da parte dei liberi professionisti* tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale in forma individuale o associata.

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.

Il trattamento 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 n. 12/1979 che disciplina la professione di consulente del lavoro; *b)* per far valere o difendere un diritto in sede giudiziaria, anche da parte di terzi; *c)* ai fini dello svolgimento da parte del difensore nel procedimento penale delle investigazioni di cui all'art. 38 delle norme di attuazione del codice di procedura penale, anche a mezzo di sostituti e di consulenti tecnici.

Le informative da inviare agli interessati devono permettere loro di comprendere agevolmente se il titolare del trattamento è un singolo professionista, ovvero se ricorre un'ipotesi di contitolarità fra più liberi professionisti.

Anche in questo caso, per quanto riguarda le modalità di conservazione, comunicazione e diffusione dei dati vengono mantenuti gli accorgimenti già indicati con le altre autorizzazioni generali.

L'autorizzazione n. 5/97 ha riguardato invece il *trattamento dei dati sensibili*, fatta eccezione per quelli idonei a rivelare la vita sessuale, *effettuato da categorie operanti in diversi settori.*

In particolare, nell'ambito delle *attività bancarie, assicurative, di gestione di fondi e del settore turistico o del trasporto*, sono state considerate le seguenti realtà: *a)* imprese autorizzate all'esercizio dell'attività bancaria o assicurativa ed organismi che le riuniscono; *b)* società ed altri organismi che gestiscono fondi pensione o di assistenza, ovvero fondi o casse di previdenza; *c)* società ed altri organismi che gestiscono 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.

Nei loro confronti, l'autorizzazione è rilasciata per adempiere agli obblighi anche precontrattuali assunti nei rispettivi settori di attività, nonché per adempiere o esigere l'adempimento ad obblighi previsti dalla legge, dai regolamenti, dalla normativa comunitaria o dai contratti collettivi, ovvero prescritti da autorità di vigilanza o di controllo.

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.

Entro tali limiti di pertinenza, i dati possono essere comunicati a soggetti pubblici o privati, nonché, ove necessario, ai familiari dell'interessato. I titolari del trattamento devono conservare un elenco dei destinatari delle comunicazioni effettuate recante un'annotazione delle specifiche categorie di dati comunicati. Non è possibile diffondere i dati sensibili trattati.

Nel settore dei *sondaggi* e delle *ricerche*, con il medesimo provvedimento n. 5/97 sono state autorizzate le imprese, le società, gli istituti e gli altri organismi o soggetti privati che effettuano tali trattamenti ai soli fini del compimento di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie. Questi devono essere effettuati per scopi puntualmente determinati e legittimi, noti all'interessato.

I dati personali di natura sensibile possono essere trattati solo se il trattamento di dati anonimi non permette di raggiungere i suoi scopi.

Il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente mediante un riferimento a qualsiasi altra informazione. I dati personali, individuali o aggregati, devono essere distrutti o resi anonimi subito dopo la raccolta, salvo un brevissimo periodo entro il quale possono essere utilizzati per verificare la veridicità o l'esattezza dei campioni.

In linea di principio, i dati sensibili autorizzati da questo provvedimento non possono essere comunicati o diffusi. È possibile comunicare o diffondere i campioni del sondaggio o della ricerca in forma individuale o aggregata, sempreché non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili.

Nel campo dell'*attività di elaborazione di dati*, sono stati autorizzati gli istituti, le imprese, le società e gli 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.

Per tali trattamenti è stato fatto esplicito riferimento alle precedenti autorizzazioni n. 1/97 e n. 4/97 in materia di rapporti di lavoro e liberi professionisti.

Nel settore dell'*attività di selezione del personale*, l'autorizzazione è stata rilasciata alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di un'attività svolta nell'interesse di terzi ai soli fini dalla ricerca o della selezione di personale.

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute 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. Sono esclusi dall'autorizzazione, oltre i trattamenti dei dati idonei a rivelare i dati sensibili diversi da quelli inerenti allo stato di salute, quelli relativi a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore e quelli effettuati in violazione delle norme in materia di pari opportunità o volte a prevenire discriminazioni.

I dati possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità sopra ricordate a soggetti pubblici o privati che siano specificamente menzionati nella dichiarazione di consenso dell'interessato. I dati non possono essere diffusi.

Sempre con il medesimo provvedimento, sono stati autorizzati al trattamento di dati sensibili le imprese, le società, gli istituti e gli 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.*

Il trattamento è autorizzato ai soli fini dell'esecuzione dei singoli incarichi conferiti, e può riguardare i dati sensibili attinenti alle persone direttamente interessate al matrimonio o alla convivenza. Tali dati devono essere forniti personalmente dai medesimi interessati e possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti. I titolari 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 richiesta di autorizzazione al Garante.

Il provvedimento n. 5/97 detta, poi, norme comuni a tutti i trattamenti autorizzati, per quanto riguarda le modalità di trattamento e la conservazione dei dati, sostanzialmente conformi a quelle delle precedenti autorizzazioni.

L'ultimo provvedimento adottato, il n. 6/97, si applica al trattamento di alcuni dati sensibili da parte degli *investigatori privati* effettuato unicamente: *a)* 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 un diritto della personalità o un altro diritto fondamentale; *b)* su incarico di un difensore nell'ambito del procedimento penale, per ricercare ed individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova.

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità sopra menzionate.

Gli investigatori non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di tali dati se non sulla base di un apposito incarico conferito per iscritto, anche da un difensore, per far valere o difendere in sede giudiziaria un diritto di rango pari a quello del soggetto al quale si riferiscono i dati.

Il trattamento dei dati, oltre ad una serie di precise indicazioni contenute nell'autorizzazione, deve rispettare le prescrizioni di un apposito codice di deontologia e di buona condotta che il Garante è in procinto di promuovere ai sensi degli artt. 22, comma 4 e 31, comma 1, lett. *h)* della legge n. 675/1996.

I dati in questione possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto. Conclusa l'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.

PAGINA BIANCA

3. IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

3.1. L'ELEZIONE E L'INSEDIAMENTO DEL COLLEGIO.

Il corpo sostanziale delle disposizioni contenute nella legge n. 675/1996 è entrato in vigore l'8 maggio 1997, ma alcune disposizioni concernenti l'attuazione dell'Accordo di Schengen e la nomina della nuova autorità indipendente ("Garante per la protezione dei dati personali") hanno trovato applicazione fin dal 9 gennaio 1997.

Ciò ha permesso al Parlamento di dar vita all'organo collegiale, che è formato da quattro componenti eletti con voto limitato, per una metà dalla Camera dei deputati e per l'altra dal Senato della Repubblica.

L'elezione dei componenti, che la legge prevede — in termini solenni e innovativi — direttamente a cura delle Assemblee parlamentari, è avvenuta in entrambi i rami il 5 marzo 1997.

La Camera dei deputati ha eletto il prof. Ugo De Siervo e l'ing. Claudio Manganelli, mentre il Senato della Repubblica ha eletto il prof. Stefano Rodotà e il prof. Giuseppe Santaniello.

L'organo collegiale si è insediato il 17 marzo 1997, procedendo all'elezione del Presidente nella persona del prof. Stefano Rodotà e del Vice Presidente in persona del prof. Giuseppe Santaniello.

Dopo l'insediamento dell'organo, la sua originaria denominazione ("Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"), è stata poi semplificata con il d.lg. n. 123 del 9 maggio 1997, che ha introdotto la più sintetica formula "Garante per la protezione dei dati personali".

3.2. L'INDIPENDENZA DELL'ORGANO NEL QUADRO COSTITUZIONALE.

L'art. 30, comma 2, della legge, statuendo che il Garante opera con "*piena autonomia e con indipendenza di giudizio e di valutazione*", ha collocato il nuovo organo nel novero delle c.d. autorità amministrative indipendenti, e più specificamente in quelle di garanzia.

Tali autorità riflettono un modello organizzativo della pubblica amministrazione che si allontana notevolmente dal tradizionale assetto ministeriale che tuttora caratterizza in larga misura la struttura dell'amministrazione centrale.

Il nuovo assetto organizzativo mutua alcuni aspetti dalle esperienze degli ordinamenti giuridici di derivazione anglosassone (si pensi anche al ruolo significativo esercitato negli USA, fin dagli anni '30, dalle *Indipendent Regulatory Commission*), ma assume oggi connotati originali.

Com'è noto, le autorità indipendenti (la cui denominazione come categoria non ha esplicite basi normative ma è di ricostruzione dottrinale) sono dotate di soggettività giuridica propria e oltre ad essere istituite per lo svolgimento di funzioni di garanzia e di vigilanza sull'attua-

zione di valori costituzionali, sono caratterizzate in misura più o meno ampia dai connotati di indipendenza e di autonomia che le svincolano da qualsiasi riferimento al circuito dell'indirizzo politico.

Nel caso del Garante per la protezione dei dati personali, i predetti connotati di indipendenza, imparzialità e terzietà sono valorizzati ulteriormente.

Tale organo, infatti, oltre a ricevere un'investitura direttamente e integralmente dalle assemblee parlamentari (circostanza che rafforza l'investitura stessa in termini di imparzialità e terzietà), vede garantita la sua indipendenza anche per effetto della direttiva europea (art. 28) e di altri strumenti internazionali (Europol, Schengen, Sistema informativo doganale) i quali vincolano lo Stato italiano ad assicurare ad autorità come il Garante un'indipendenza piena, rafforzata dalla previsione di poteri effettivi di intervento nella materia.

La legittimazione democratica dell'organo e dei suoi componenti deriva anche dai criteri di nomina dei componenti stessi, scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza nelle materie del diritto o dell'informatica, in modo da garantire nell'organo la presenza di entrambe le qualificazioni.

Ad arricchire questo quadro, rileva anche la disposizione che regola l'incompatibilità della nomina nel collegio (efficace per quattro anni e confermabile per una volta) con qualsiasi attività professionale o di consulenza, con la funzione di amministratore o di dipendente pubblico o privato e con cariche elettive (art. 30, comma 4).

L'emergere delle autorità indipendenti nell'ordinamento italiano è fenomeno abbastanza recente e significativo di un processo più generale di trasformazione dell'organizzazione dello Stato contemporaneo (che trova traccia anche nei lavori della Commissione bicamerale per le riforme costituzionali), in relazione ad un duplice ordine di esigenze.

Da un lato, la necessità di approntare strutture operative caratterizzate dalla garanzia di imparzialità e da una conoscenza tecnico-giuridica più specifica, in settori della vita economico-sociale che richiedono l'esercizio di poteri di garanzia, di vigilanza e di bilanciamento di interessi che rivestono un preminente interesse per la collettività.

Dall'altro, il bisogno, cui risponde più propriamente il Garante per la protezione dei dati personali, di predisporre una struttura snella, dotata di adeguati mezzi di tutela e di garanzie di operatività, a presidio di valori costituzionali di grande rilievo, non sempre oggetto di sufficiente attenzione nel quadro normativo previgente.

In questa prospettiva, appare significativo richiamare nuovamente il principio contenuto nell'art. 1 della legge n. 675/1996, il quale, nel sottolineare l'esigenza che il trattamento dei dati personali deve svolgersi "*nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale*", si colloca nel solco della diretta attuazione degli articoli 2 e 3 della Costituzione, in armonia con altri parametri costituzionali.

Senza entrare nel merito delle scelte parlamentari, sembra quindi legittimo osservare che l'art. 109 del progetto di legge costituzionale di riforma della seconda parte della Costituzione, presentato alle Camere il 4 novembre 1997, pone opportunamente nel dibattito il tema della natura e del rilievo costituzionale dell'istituzione di autorità create "*per l'esercizio di funzioni di garanzia o di vigilanza in materia di diritti e libertà garantiti dalla Costituzione*".

3.3. Compiti e poteri del Garante.

Con poteri propri, e con una configurazione indipendente rispetto alla pubblica amministrazione intesa nella sua accezione tradizionale, il Garante si pone come organo di garanzia del rispetto dei diritti della personalità per ciò che riguarda le multiformi attività di trattamento di dati personali.

Attraverso una pluralità di funzioni di impulso, di indirizzo, di vigilanza e, ove sia necessario esercitarli, interdittivi o sanzionatori, l'Autorità è chiamata a promuovere un rapporto più corretto tra i soggetti pubblici e privati che elaborano informazioni personali e gli interessati, che in passato non erano sempre consapevoli dei rischi connessi alla gestione di banche dati ed archivi.

La legge n. 675/1996 orienta questo ruolo di garanzia della trasparenza della Società dell'Informazione secondo modalità rispettose dei diritti costituzionali concernenti le libertà di manifestazione del pensiero, di iniziativa economica e di uso della corrispondenza, la tutela della salute e del domicilio e gli altri valori fondamentali della società.

Le attribuzioni conferite al Garante si muovono nell'ambito delle seguenti prospettive:

— *la tutela dei diritti dell'interessato, individuati dall'art. 13 della legge n. 675/1996, di fronte all'elaborazione dei dati che lo riguardano da parte di soggetti pubblici o privati.*

In tale solco, si colloca la funzione di risoluzione dei conflitti tra l'interessato e il titolare del trattamento (specie in sede di trattazione dei ricorsi proposti ai sensi dell'art. 29 della legge, delle segnalazioni e dei reclami). Vi si inseriscono anche i poteri decisori e i connessi poteri cautelari e definitivi, che possono comportare anche il blocco o il divieto di prosecuzione di alcune operazioni o dell'intero trattamento.

Le medesime funzioni conformative ed interdittive sono esercitabili d'ufficio, ovvero su segnalazione o reclamo (art. 31, comma 1, lett. *d)* ed *l)*).

Strumentali alla funzione di tutela dei diritti sono l'attribuzione all'Autorità dei poteri ispettivi e di accertamento (art. 32), finalizzati alla prevenzione e alla repressione degli illeciti in materia, nonché la previsione di alcune sanzioni amministrative che possono essere applicate dal Garante (art. 39).

L'Autorità ha infatti il potere di disporre l'accesso a banche-dati (se ritenuto necessario, avvalendosi della collaborazione di altri organi dello Stato), acquisendo con le modalità previste dal regolamento in corso di pubblicazione l'autorizzazione del presidente del tribunale ordinario competente per territorio in relazione al luogo dell'accertamento.

Tali controlli possono interessare la generalità dei trattamenti di dati soggetti per intero all'ambito applicativo della legge n. 675/1996, o ai quali la legge stessa si applica, sino alla data di attuazione della legge delega n. 676, per alcune parti soltanto.

Procedure specifiche sono previste per determinati trattamenti rispetto ai quali il diritto di accesso del cittadino può essere esercitato solo per il tramite di una richiesta al Garante (art. 14 legge n. 675/1996, ad esempio rispetto ai dati raccolti a fini antiriciclaggio o da commissioni parlamentari d'inchiesta).

Garanzie apposite sono previste, poi, per determinati trattamenti aventi finalità di giustizia, di difesa dello Stato o di tutela della sicurezza pubblica, sia sul piano della procedura osservata dal Garante, sia sotto il profilo dei riscontri forniti all'interessato (art. 32, comma 6).

Nella medesima ottica di tutela dei diritti del cittadino, l'art. 31, comma 1, lett. *b)*, *f)* e *p)* affida al Garante un generale potere di controllo della liceità e della correttezza dei trattamenti, che devono essere conformi sia alle disposizioni che ne disciplinano i requisiti e i presupposti, sia al quadro di trasparenza evidenziato nelle informative all'interessato e nella notificazione. Anche questo potere può comportare la prospettazione di alcune modificazioni opportune che la segnalazione al titolare del trattamento (art. 31, comma 1, lett. *c)*) permette di veicolare in termini non autoritativi, ma pur sempre efficaci per far adeguare i trattamenti alle norme vigenti;

— *la ricerca degli strumenti più efficaci di bilanciamento dei diritti della personalità con diritti e interessi anche di settore sottesi al trattamento.*

Sotto tale profilo, possono essere collocati i poteri di promozione e di raccordo indicati dall'art. 31, comma 1, lett. *h)* in relazione alla sottoscrizione dei codici di deontologia professionale;

— *la divulgazione tra il pubblico della conoscenza delle disposizioni che regolano la materia dei dati personali (art. 31, comma 1, lett. i)), al fine di favorirne l'osservanza e formare una coscienza collettiva sulla definizione, in capo ad ogni soggetto, del nuovo diritto alla riservatezza;*

— l'attività di *relazione al Parlamento sullo stato di attuazione della legge, e il compito di segnalazione al Governo* dell'opportunità di adottare provvedimenti normativi richiesti dalla evoluzione di settore (art. 31, comma 1, lett. *m)* ed *n)*) che sottolineano il raccordo tra la funzione esercitata dal Garante e il suo inquadramento nel complessivo assetto istituzionale.

Infine, il Garante si pone come centro di riferimento per una serie di funzioni di rilevanza fondamentale in materia di diritto alla riservatezza. In particolare spetta ad esso:

— curare *l'attività di assistenza sulla protezione dei soggetti rispetto al trattamento dei dati personali,* secondo quanto previsto dalla Convenzione n. 108 del Consiglio d'Europa, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della stessa Convenzione (l'art. 14 della Convenzione prevede che l'Autorità presti assistenza alle persone interessate residenti all'estero);

— *esercitare le funzioni già di competenza del Comitato di controllo sui servizi di informazione e di sicurezza riguardanti il controllo sui trattamenti effettuati dal Centro elaborazione dati del Dipartimento di pubblica sicurezza;*

— *operare in collaborazione con altre autorità di vigilanza competenti per il settore creditizio, per le attività assicurative e per le comunicazioni, nonché con l'AIPA.*

Entro un anno dall'istituzione del registro generale dei trattamenti di dati, il Garante promuoverà intese con le province ed eventualmente con altre amministrazioni pubbliche, allo scopo di assicurarne la consultazione mediante sistema informatico almeno su base provinciale (art. 31, comma 3).

Il Garante è chiamato infine a intrattenere intensi e proficui rapporti di collaborazione con le corrispondenti autorità istituite in altri Stati, sia bilateralmente sia nell'ambito delle varie istituzioni e organismi comuni che fungono anche da veicolo per un intreccio di esperienze. A tal fine il Garante valuterà d'intesa con tali autorità la possibilità di disporre uno scambio temporaneo di funzionari per brevi missioni da curare presso altre autorità europee.

3.4. La consultazione da parte del Governo.

L'art. 31 della legge prevede che il Garante sia consultato dal Presidente del Consiglio dei ministri e dai singoli ministri all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla legge.

Il contesto di ampia delegificazione, e quindi di centralità dell'attività di normazione secondaria, rende tale funzione consultiva di particolare rilievo specie per quanto attiene agli atti di natura regolamentare.

Non meno significativa è la previsione della consultazione del Garante nella predisposizione degli atti amministrativi.

Senza entrare nel merito del vizio che determina la mancata richiesta di parere, si vuole sottolineare che la legge ha ritenuto necessario sottoporre tali atti ad una valutazione preventiva del Garante, proprio per prevenire il possibile insorgere di contrasti con la disciplina in materia di riservatezza.

Il rilievo di tali previsioni è accresciuto dall'impatto dei princìpi e delle disposizioni della legge n. 675/1996 sulla situazione preesistente, che richiede mutamenti ed adattamenti sul piano del costume e della prassi amministrativa.

L'art. 31 pone l'accento sull'idoneità dei provvedimenti a spiegare effetti nelle materie disciplinate dalla legge, e si applica, quindi, anche agli atti che provocano tale effetto in via mediata.

Sulla richiesta delle competenti amministrazioni, ovvero di propria iniziativa, il Garante ha espresso un avviso in relazione a diversi atti, tra i quali:

— lo schema di regolamento del Ministero delle comunicazioni recante disposizioni per il rilascio delle licenze individuali;

— lo schema di regolamento governativo sui compiti, l'organizzazione e il funzionamento del Centro tecnico per l'assistenza ai soggetti che utilizzeranno la rete unitaria della pubblica amministrazione;

— lo schema di regolamento del Ministero del lavoro e della previdenza sociale concernente le modalità di tenuta della documentazione sulla protezione dalle radiazioni ionizzanti;

— lo schema di regolamento governativo in materia di attività statistica;

— lo schema di regolamento del Ministero delle comunicazioni sull'istituzione di una commissione interministeriale per la sicurezza dei dati.

Si deve peraltro osservare che il Garante non è stato consultato in occasione dell'emanazione di alcuni decreti presidenziali e ministeriali, tra i quali:

a) il d.P.R. 16 dicembre 1997, n. 486, in materia di certificazioni antimafia;

b) il d.P.R. 4 dicembre 1997, n. 465, in materia di ordinamento dei segretari comunali e provinciali;

c) il d.P.R. 19 settembre 1997, n. 318, di attuazione di recenti direttive comunitarie in materia di telecomunicazioni.

In altra occasione, relativa all'emanazione del regolamento sui contratti di locazione e acquisto delle apparecchiature informatiche e sulle licenze d'uso dei programmi per elaboratore, l'Autorità non è stata consultata tempestivamente.

Peraltro, il Garante è stato investito di numerosi quesiti concernenti l'attività di pubbliche amministrazioni e, in particolare:

— la trasmissione all'INPS, da parte dei datori di lavoro, dei dati necessari ai fini della corresponsione dei trattamenti di integrazione salariale; in proposito, è stata segnalata al Ministero del lavoro e della previdenza sociale l'opportunità di disciplinare con legge o regolamento tale flusso di dati;

— il trattamento dei dati idonei a rivelare lo stato di salute nel procedimento per il riconoscimento dell'invalidità civile;

— la pubblicità delle situazioni patrimoniali dei titolari di determinate cariche elettive e di cariche direttive presso alcuni enti;

— l'anagrafe delle prestazioni dei dipendenti pubblici;

— l'individuazione della figura del titolare del trattamento di dati personali nell'ambito della pubblica amministrazione;

— la pubblicità della relazione conclusiva della commissione ministeriale per l'esame dei contratti in materia di circolazione delle quote-latte;

— la presentazione delle dichiarazioni dei redditi tramite intermediari. Sull'argomento, ad una prima risposta fornita al Ministero delle finanze, ha fatto seguito una serie di incontri ed un'ulteriore collaborazione per individuare alcune soluzioni operative;

— la richiesta del Dipartimento per la protezione civile della Presidenza del Consiglio dei Ministri di acquisire alcuni dati relativi all'attività di volo di velivoli CANADAIR.

È stata inoltre segnalata al Governo la disponibilità del Garante a cooperare alla definizione di garanzie d'interesse generale riguardanti l'attribuzione alle persone di carte o documenti personali contrassegnati da numeri d'identificazione.

È stata altresì segnalata, con riferimento alla circolare del Ministero dei lavori pubblici n. 3816 del 21 luglio 1997, in materia di tariffazione degli accessi alle zone urbane a traffico limitato, l'opportunità di ulteriori misure e cautele in relazione allo sviluppo del patrimonio informativo pubblico in materia.

È stata quindi rappresentata al Ministero di grazia e giustizia l'esigenza di una disciplina più puntuale delle forme di conoscibilità degli albi e degli elenchi dei liberi professionisti.

Prescindendo in questa sede dal contenuto dei singoli pareri (di alcuni dei quali si dà conto nel seguito della presente relazione) si osserva che il Garante ha cercato di contemperare le esigenze di funzionalità proprie dei settori di volta in volta considerati con le finalità di tutela e di garanzia proprie dell'Autorità.

In alcuni casi, ciò ha comportato la prospettazione di modificazioni ai testi esaminati, mentre in altri è emersa l'opportunità di integrare il quadro di riferimento con atti di indirizzo o direttive a contenuto non precettivo, per favorire ulteriori riflessioni, anche non definitive, dirette a valutare in modo adeguato una pluralità di interessi.

3.5. L'Ufficio del Garante.

3.5.1. Costituzione dell'Ufficio.

La legge n. 675/1996 ha posto alle dipendenze del Garante un contingente di personale non superiore a 45 unità, composto da dipendenti dello Stato e di altre amministrazioni pubbliche collocati fuori ruolo nelle forme previste dai rispettivi ordinamenti.

Il Segretario generale è stato nominato con provvedimento del Garante del 12 maggio 1997 nella persona del dott. Giovanni Buttarelli. L'articolazione delle figure o qualifiche è stata invece operata con il d.P.C.M. del 27 giugno 1997, che ha fissato il contingente in 45 unità.

Nonostante la collaborazione prestata da varie amministrazioni e le semplificazioni previste in materia di collocamento fuori ruolo (art. 3, comma 3, d.lg. 9 maggio 1997, n. 123; art. 17 l. 15 maggio 1997, n. 127), il distacco delle singole unità ha richiesto un congruo periodo che non ha facilitato l'espletamento dei numerosi compiti che gravano sull'Ufficio sin dal periodo antecedente l'8 maggio 1997.

Attualmente, anche per i ritardi registrati presso talune amministrazioni di provenienza, prestano servizio presso il Garante n. 40 unità, selezionate sulla base di una valutazione dei singoli profili professionali utili e delle specifiche esperienze, nonché degli elementi pertinenti per una valutazione del carattere fiduciario della collaborazione con una struttura che è preposta, con evidenza, alla cura di delicate questioni.

È in fase di definizione la modifica del predetto d.P.C.M., sulla base di una recente proposta del Garante che il 16 gennaio 1998 ha prospettato una diversa distribuzione di alcune qualifiche, al fine di tener conto di talune esigenze e di determinate difficoltà emerse nel corso della formazione del contingente.

Grazie ad alcuni locali messi cortesemente a disposizione dalla Camera dei deputati e dal Senato della Repubblica, l'Ufficio ha potuto organizzare la prima fase di attività in attesa di poter fruire della sede provvisoria stabilita in Roma, Largo del Teatro Valle n. 6, che si è resa praticabile solo nel mese di febbraio del corrente anno.

Per le spese di funzionamento dell'Ufficio è stato stanziato un apposito fondo nel bilancio dello Stato, pari a 8 miliardi circa di lire per il 1997 e in 12 miliardi circa di lire a decorrere dal 1998.

Nelle more dell'approvazione del regolamento sul funzionamento dell'Ufficio, l'art. 5, comma 3, del d.lg. 9 maggio 1997, n. 123, ha permesso di applicare provvisoriamente il regolamento sulla gestione delle spese occorrenti per il funzionamento dell'AIPA (d.P.R. 6 ottobre 1994, n. 769).

Si è resa possibile, così, l'individuazione delle modalità per la prima fase di gestione economica dell'Ufficio, nella quale si è prestata particolare attenzione ai contratti necessari ai fini della realizzazione del *software* per il programma di notificazione dei trattamenti, per la duplicazione di alcuni supporti e per l'acquisizione di talune dotazioni informatiche.

Per quanto riguarda le dotazioni di apparecchiature telefoniche e di altri strumenti di servizio, ivi comprese la disponibilità di autoveicoli, l'Ufficio si è ispirato immediatamente ai recenti criteri di orientamento che il Governo ha indicato per la pubblica amministrazione.

In sintonia con gli obblighi di segretezza e di riservatezza previsti dall'art. 33, comma 6, della legge, nonché con le analoghe iniziative adottate presso altre autorità indipendenti, il Garante ha adottato un codice etico che mira a rafforzare la trasparenza e la correttezza del proprio operato.

3.5.2. Il regolamento sull'organizzazione e il funzionamento.

Le norme di organizzazione e sul funzionamento dell'Ufficio del Garante sono state demandate dalla legge ad un apposito regolamento (art. 33, comma 3).

Tale atto normativo deve contenere, oltre ai profili attinenti più strettamente all'organizzazione dell'Ufficio medesimo, le norme relative alla riscossione dei diritti di segreteria, alla gestione delle spese (per le quali è prevista la possibilità di derogare alle norme della contabilità generale dello Stato), allo svolgimento del procedimento dinanzi al Garante — previsto dall'art. 29, commi da 1 a 5 della legge n. 675/1996 — nonché alle modalità della notificazione del trattamento dei dati personali.

Il citato art. 33 ha fissato le modalità per l'adozione di tale regolamento, prescrivendo che lo stesso, in base all'art. 17, comma 1, lettera *b)* della legge 23 agosto 1988, n. 400, sia emanato con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato, su proposta del Presidente del Consiglio dei ministri, di concerto con i Ministri del tesoro, di grazia e giustizia e dell'interno. È richiesto anche il parere conforme del Garante. L'articolato, elaborato dalla "Commissione Fanelli" istituita presso il Ministero di grazia e giustizia, ricevuto il parere conforme del Garante, è stato sottoposto alla sezione consultiva per gli atti normativi del Consiglio di Stato (che si è espresso il 17 novembre 1997), nonché al Consiglio dei ministri (che lo ha approvato il 19 dicembre 1997).

Il regolamento consterà di 46 articoli ripartiti in 8 capi.

Il capo I fissa alcune linee di funzionamento generale del collegio del Garante e delinea i compiti del Presidente, del Vice Presidente, dei componenti e del Segretario generale.

L'art. 4 si occupa della materia delle incompatibilità. Vengono poi previste le modalità di svolgimento delle riunioni e della formazione dell'ordine del giorno.

Il capo II è dedicato all'Ufficio e prevede uno sviluppo dell'organizzazione interna attraverso ulteriori atti (artt. 8 e 9), sulla base del criterio della speditezza dell'azione amministrativa e tenendo conto della necessità di organizzare le strutture secondo parametri di flessibilità.

In attesa dei decreti legislativi previsti dall'art. 1, comma 1, lett. *c)* e *m)* della legge n. 676/1996, che dovranno definire lo stato giuridico ed economico del personale dipendente, l'art. 9 demanda ad un'ulteriore disciplina da parte del Garante la tematica dell'organizzazione, della prestazione del lavoro, del conferimento delle funzioni e dell'attribuzione dell'indennità di funzione.

Si disciplina poi la creazione di un'apposita segreteria di sicurezza per la custodia degli atti riservati, e la fissazione dell'ammontare dei diritti di segreteria per gli atti e per i provvedimenti per i quali tali diritti possono essere richiesti (notificazioni, autorizzazioni e ricorsi).

Il capo III dedicato al registro generale dei trattamenti, fissa all'art. 12 alcuni dettagli tecnici per la notificazione e per l'impiego della relativa modulistica, e prevede nel successivo art. 13 le modalità per consentire a chiunque l'accesso al registro medesimo.

Nel capo IV sono considerate sia le modalità di pubblicazione delle autorizzazioni generali, sia la previsione di autorizzazioni *ad hoc* per singoli casi. L'art. 15 fissa poi le modalità per gli accessi, le ispezioni e le altre verifiche di cui all'art. 32 della legge.

L'art. 17 (capo V) individua le modalità per l'accesso ai dati personali di cui all'art. 13 della legge n. 675/1996, avendo cura di assicurare la massima snellezza ed economicità di procedure.

Particolarmente significativo è il capo VI del regolamento, che agli artt. 18, 19 e 20 reca la disciplina attuativa dell'art. 29 della legge 675 in tema di ricorso al Garante, fissando le modalità per la presentazione, il contenuto necessario del ricorso e i casi di inammissibilità, nonché le necessarie regole procedimentali.

Nel capo VII sono raggruppate varie disposizioni concernenti la pubblicazione del bollettino dell'Autorità e la difesa in giudizio del Garante da parte dell'Avvocatura generale dello Stato.

Infine, il capo VIII (artt. 23-46) contiene tutte le disposizioni attinenti alla gestione delle spese, con particolare riguardo alla contabilità speciale, alla modalità dei pagamenti, alla conservazione delle somme, alle spese per i servizi in economia, al funzionamento del servizio cassa, alla rendicontazione e alle procedure contrattuali applicabili.

3.5.3. Attività di informazione e di relazione con il pubblico.

Tra i vari compiti che la legge affida al Garante vi è anche quello di "*curare la conoscenza tra il pubblico delle norme che regolano la materia e delle relative finalità*" (art. 31, comma 1, lett. *i)*).

La funzione di comunicazione e diffusione, ma anche di spiegazione e chiarificazione delle norme che tutelano la riservatezza delle persone, riveste quindi un carattere primario e investe l'intero quadro dei diritti fondamentali degli individui.

Per adempiere a questo compito essenziale, il Garante ha provveduto sin dalla sua istituzione a portare a conoscenza dei cittadini la propria attività e i diversi aspetti della nuova legge, attraverso vari strumenti.

L'Ufficio ha aderito, anzitutto, alle diffuse richieste di chiarimenti provenienti dai cittadini, dagli organi pubblici e dalle imprese, attraverso una massiccia opera di assistenza, anche telefonica.

Ancor prima dell'entrata in vigore della legge, le utenze telefoniche dell'Autorità sono state interessate continuamente da chiamate, fax e note di richiesta di chiarimenti. Le centinaia di telefonate pervenute giornalmente al Garante in questi mesi appaiono la testimonianza di un interesse e di un'attenzione diffusi e senz'altro nuovi rispetto ai comportamenti tipici tenuti nei confronti di nuove normative che si innestano nell'ordinamento.

I comunicati-stampa, data la loro particolare natura di linguaggio diretto e semplificato, hanno permesso di portare a conoscenza con immediatezza, attraverso gli organi di informazione, le decisioni e le deliberazioni assunte dal Garante, i pareri formulati, le indicazioni e i contributi forniti.

L'uso dei comunicati-stampa ha inoltre consentito al Garante di spiegare più volte il contenuto della legge, di evidenziare alcune interpretazioni non corrette, di intervenire con tempestività su vicende nelle quali la tutela della *privacy* dei cittadini assumeva un carattere di emergenza.

La modalità comunicativa adottata con i comunicati-stampa è derivata da una scelta consapevole finalizzata alla diffusione dell'attività di un'istituzione che, per le finalità per le quali è stata istituita, deve

essere in grado di rendere comprensibile il reale significato dei propri provvedimenti alla società nel suo complesso e nelle sue diverse articolazioni.

Si è ritenuto opportuno, quindi, ricorrere ad alcune conferenze-stampa e ad interviste per fare di volta in volta il punto sull'attuazione della legge e l'attività del Garante, sulle problematiche sollevate, sui cambiamenti intervenuti nelle procedure burocratiche così come nei comportamenti collettivi.

A queste forme più tradizionali di comunicazione, si sono aggiunte le possibilità offerte dalla pubblicazione di un bollettino e dei Quaderni di documentazione. Il bollettino, di cui sono usciti già i primi tre numeri e che può essere inviato a chiunque ne faccia richiesta, raccoglie, oltre alla normativa sulla *privacy*, i provvedimenti del Garante adottati in seguito a ricorsi, segnalazioni o reclami, nonché le risposte ai quesiti e alle richieste di parere, i comunicati-stampa, ecc.

I Quaderni di documentazione, invece, nascono con l'obiettivo di fornire analisi, testi e studi specifici riguardo all'ampio contesto storico, politico e tecnologico in cui si inscrive oggi la nozione di *privacy*. Risulta palese che la documentazione di tipo strettamente giuridico sulla nascita e sull'evoluzione della *privacy* si dimostra insufficiente per valorizzare l'importanza e il peso crescente della tutela degli spazi individuali nella nascente Società dell'informazione. Pertanto, la varietà e la complessità di questi fenomeni richiedono un approfondimento in ambito culturale, letterario e scientifico, allo scopo di produrre chiavi esegetiche adeguate e costantemente aggiornate.

Di tali Quaderni è in pubblicazione il primo numero, che si apre con un saggio inedito di William Faulkner sulla *privacy* e raccoglie interventi di studiosi italiani e stranieri.

Da ultimo, va ricordata l'intensa partecipazione dei componenti dell'Autorità e dell'Ufficio a numerosi convegni e seminari promossi, in particolare, da organismi associativi, organizzazioni di categoria, gruppi sociali e imprese.

3.5.4. Le iniziative intraprese per il futuro assetto.

Al termine del suo primo anno di operatività, l'Ufficio del Garante ha iniziato a potenziare la propria attività di informazione e di relazione con il pubblico, programmando la costituzione di una banca dati giuridica informatizzata. Ciò in armonia con gli articoli del regolamento in fase di pubblicazione, i quali prevedono che l'Ufficio debba operare, di regola, con strumenti informatici e telematici, sia nel lavoro interno, sia nei rapporti con i cittadini (artt. 5, 7, 12 e 13).

Tale banca dati, che sarà consultabile anche per mezzo di un sistema di classificazione dei documenti, conterrà i principali provvedimenti adottati in materia dal Garante e dall'autorità giudiziaria (art. 40 legge n. 675).

L'archivio sarà aperto alla libera consultazione in collegamento con l'istituendo sito *Web* del Garante, il quale faciliterà l'accesso ad altra documentazione e che in una seconda fase permetterà anche al cittadino di dialogare con l'ufficio attraverso strumenti telematici.

Un ruolo complementare in questa attività di comunicazione sarà svolto tramite l'ANCI, che è in procinto di stipulare con il Garante una convenzione in base alla quale l'ANCI stessa potrà veicolare attraverso la rete ANCITEL il materiale informativo nei settori di più stretto interesse per le comunità locali.

4. TEMI DI MAGGIOR RILIEVO NELL'ATTIVITÀ DEL GARANTE

4.1. PREMESSA.

Il Garante, privilegiando, come già detto, il profilo del dialogo e della persuasione, ha fornito numerose indicazioni a singoli cittadini, operatori economici, enti, associazioni e pubbliche amministrazioni, al fine di agevolare una corretta applicazione dei nuovi princìpi introdotti dalla legge n. 675/1996.

Sin dai primi giorni di costituzione dell'Autorità sono pervenute innumerevoli richieste di chiarimenti, in forma di quesiti scritti e telefonici, sulla disciplina normativa, sulle modalità di consultazione o di attivazione dei poteri del Garante e sugli adempimenti previsti dalla legge. Ad esempio, sulla base di una stima che si riferisce al periodo agosto 1997 - marzo 1998, si è calcolato un numero di chiarimenti telefonici superiori a 25.000. Oltre alle risposte fornite per iscritto, molti interrogativi hanno trovato riscontro in appositi comunicati-stampa (in tutto, i comunicati diffusi dal Garante sono stati 67).

Nel 1997 sono pervenute diverse notificazioni effettuate in modo erroneo e prima del decorrere dei termini previsti. Ad esse, l'Ufficio ha fornito un riscontro con lettere circolari che, oltre ad illustrare la normativa in materia, hanno allegato anche un esemplare del supporto magnetico realizzato dal Garante per la notificazione.

Sono inoltre pervenute 8889 richieste di autorizzazione al trattamento dei dati sensibili, ai sensi dell'art. 22, comma 1, della legge 675/1996, alle quali si è provveduto, come già precisato, con le autorizzazioni generali pubblicate sulla Gazzetta ufficiale, nonché con comunicati-stampa e, ove possibile, con singole missive.

Oltre agli innumerevoli reclami e segnalazioni pervenuti, unitamente a 86 ricorsi, l'Ufficio ha ricevuto varie comunicazioni da parte di soggetti pubblici effettuate in adempimento delle apposite prescrizioni normative. In particolare 268 comunicazioni hanno riguardato l'ipotesi del trattamento di dati sensibili da parte di un soggetto pubblico in assenza di un'espressa disposizione di legge, secondo il disposto dell'art. 41, comma 5.

Circa 320 comunicazioni sono pervenute, invece, riguardo all'ipotesi di cui all'art. 27, comma 2, che prescrive tale adempimento qualora la comunicazione o la diffusione di dati tra soggetti pubblici avvenga in carenza di disposizioni normative, ma risulti comunque necessaria per lo svolgimento delle funzioni istituzionali delle amministrazioni interessate.

Va rilevato, inoltre, che prima ancora dell'entrata in vigore della legge n. 675/1996, l'Autorità Garante si è subito impegnata in una delicata attività volta a fornire alcuni indirizzi operativi, a richiamare l'attenzione sui comportamenti cui uniformarsi e ad assicurare un confronto proficuo con i soggetti interessati.

In questa prospettiva, si è ritenuto utile operare anche attraverso lo strumento delle audizioni dei gruppi e delle categorie interessate su vari problemi di interpretazione e di applicazione della legge n. 675.

Le audizioni hanno avuto inizio già alla data del 17 aprile 1997, e hanno interessato vari interlocutori istituzionali e imprenditoriali, a cominciare dai rappresentanti della Federazione italiana degli editori giornali, della Federazione nazionale della stampa, dell'Associazione nazionale tra le imprese di informazione commerciale, nonché dell'Arcigay-Arcilesbica.

I primi hanno richiamato l'attenzione sulle delicate implicazioni nascenti dall'applicazione della legge n. 675 al settore dei *media*, nonché sull'esigenza di assicurare qualità e trasparenza all'informazione nel mondo dell'impresa e del commercio.

Dal canto suo, l'Arcigay-Arcilesbica ha chiesto di appurare se le autorità di polizia utilizzino appositi elenchi di omosessuali. Il Garante ha chiesto ai Ministri dell'interno e della difesa di fornire assicurazioni circa l'assenza di un'illecita schedatura di omosessuali. Il Ministro dell'interno (con nota del 23 dicembre 1997) e il Comando generale dell'Arma dei carabinieri (con nota del 25 febbraio 1998) hanno escluso che tale pratica sia in atto. L'Arcigay-Arcilesbica hanno inoltre lamentato una prassi invalsa presso alcune testate giornalistiche e televisive che obiettivamente discrimina l'omosessualità specie quando è collegata a fatti di cronaca.

Dopo l'8 maggio 1997, data di entrata in vigore della legge n. 675/1996, l'attività di consultazione dei gruppi e delle categorie interessate ha avuto una sua, ovvia, evoluzione tematica, sviluppandosi anche in numerosi incontri anche informali con esperti e istituzioni, impegnati, tra l'altro, nel settore della statistica, della ricerca epidemiologica e delle telecomunicazioni.

Il 20 maggio 1997 si sono tenute le audizioni dell'Adusbef, del Movimento di difesa del cittadino e della Banca nazionale del lavoro.

Le prime due organizzazioni hanno rappresentato una prassi in atto presso alcuni istituti di credito relativa all'informativa all'interessato e all'acquisizione del consenso, non conforme alle disposizioni di cui agli artt. 10 e 11 della legge n. 675.

Di seguito alla prima decisione adottata dal Garante il 28 maggio 1997, che ha riguardato, come si vedrà, i modelli inviati alla clientela dalla Banca nazionale del lavoro, il Garante ha fornito a vari soggetti, e in particolare ad istituti di credito e imprese di assicurazione, alcune indicazioni generali utili per il rispetto del principio del consenso libero e informato.

Considerata la vastità e la complessità della catena dei trattamenti in atto in tali ambiti, il Garante ha avviato una proficua consultazione con la Banca d'Italia, l'ISVAP, l'Associazione bancaria italiana (ABI) e l'Associazione italiana delle imprese di assicurazione (ANIA), anche per individuare i profili su cui la prevista legislazione integrativa e, se del caso, correttiva, dovrebbe intervenire anche in attuazione delle Raccomandazioni del Consiglio d'Europa citate nella legge delega n. 676.

L'attività di consultazione e di collaborazione con le categorie interessate è proseguita con gli incontri che si sono tenuti, a partire dal 23 giugno 1997, in particolare con la Federazione nazionale dell'Ordine dei medici, e, nella stessa giornata, con l'ANIA.

Altra audizione che ha avuto come esito una decisione del Garante è stata quella con il Comitato promotore dei *referendum*, svoltasi il 9 luglio 1997. Il Comitato è stato sentito in ordine ai moduli per la raccolta di firme relative alle iniziative referendarie, nei quali si prospettava l'utilizzazione dei dati anche per altre finalità.

La successiva decisione adottata dal Garante ha precisato, come si vedrà, che il trattamento dei dati, qualora abbia finalità diverse da quelle proprie della legittima iniziativa referendaria, richiede il consenso dell'interessato manifestato in forma specifica.

Sempre il 9 luglio 1997, si è tenuto un primo incontro con una delegazione del Consiglio nazionale dell'Ordine dei giornalisti, al fine di individuare, in un quadro di cooperazione, le linee-guida e i tempi di preparazione del codice di deontologia dei giornalisti previsto dall'articolo 25 della legge n. 675/1996, sollecitata dal Garante con nota del 26 maggio 1997.

Nella seconda settimana di luglio, si è tenuto un incontro con due delegazioni della Banca d'Italia e dell'ABI per analizzare congiuntamente le problematiche organizzative derivanti dall'applicazione della legge, anche alla luce della menzionata decisione sui modelli di informativa e sulla manifestazione del consenso in ambito bancario.

Nell'incontro sono state individuate alcune tematiche da approfondire per agevolare la piena applicazione dei princìpi in materia di tutela della riservatezza nel quadro della complessa attività bancaria, tenendo conto, anche e soprattutto, delle nuove funzioni che caratterizzano la "banca del futuro". In tal modo si è inteso quindi avviare una proficua collaborazione, informata a quello spirito di "promozione della legge" che ha caratterizzato l'attività del Garante nel periodo di prima applicazione della nuova normativa.

Dei successivi incontri con altre categorie, relativi anche al rilascio delle autorizzazioni generali, è fatta menzione in altri paragrafi.

4.2. Giornalismo e attività di informazione.

Tra i problemi più delicati in materia di trattamento dei dati personali vi è quello che si pone con riguardo al giornalismo e all'espressione letteraria ed artistica. Sempre più spesso, accade infatti che si sviluppi un conflitto tra la tutela della persona e la garanzia della libertà di stampa e della libera manifestazione del pensiero.

Il problema dell'individuazione di un punto soddisfacente di equilibrio tra queste due istanze è stato affrontato a livello comunitario con la direttiva n. 95/46/CE del 24 ottobre 1995. L'art. 9 (*"Trattamento di dati personali e libertà di espressione"*) demanda agli Stati membri il compito di prevedere, in favore del giornalismo e dell'espressione artistica o letteraria, determinate deroghe o esenzioni a talune disposizioni di attuazione della direttiva stessa, qualora ciò si riveli necessario per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione.

L'indirizzo perseguito in sede comunitaria è stato tradotto, nella legge 675/1996, in una serie di norme che fanno riferimento ai giornalisti e ai soggetti ad essa equiparati per effetto del d.lg. n. 123/1997 (pubblicisti, praticanti e autori di saggi, articoli e altre manifestazioni del pensiero). Tra queste, assumono particolare importanza gli articoli 12, 20 e 25 e 28, comma 6.

Al trattamento effettuato nell'esercizio della professione giornalistica o nel più generale esercizio della libertà di manifestazione del pensiero si applicano con le semplificazioni contenute nel codice di deontolgia di prossima emanazione le norme concernenti le informazioni che vanno rese al momento della raccolta (art. 10). Non si applicano, invece, le disposizioni che prescrivono l'acquisizione del consenso dell'interes-

sato, quando il trattamento è effettuato per l'esclusivo perseguimento delle finalità giornalistiche e nel rispetto del codice di deontologia (art. 12, comma 1, lett. e)).

Inoltre, è ammessa la comunicazione e la diffusione dei dati (senza il consenso dell'interessato) quando il trattamento è effettuato nell'esercizio della professione giornalistica e per l'esclusivo perseguimento delle relative finalità, nei limiti del diritto di cronaca posti a tutela della riservatezza e in particolare, dell'essenzialità dell'informazione riguardo a fatti d'interesse pubblico (art. 20, comma 1, lett. d)). In ogni caso, è necessario rispettare le prescrizioni del codice deontologico.

Le disposizioni in materia di flusso transfrontaliero dei dati non si applicano al trasferimento di dati personali all'estero effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità: un'esplicita deroga è sancita infatti dal comma 6 dell'art. 28, che prevede la disciplina generale di tale aspetto.

L'art. 25 individua le condizioni da osservare per considerare lecito il trattamento dei dati sensibili da parte del giornalista e dei soggetti ad esso parificati; al tempo stesso, questa disposizione fissa la procedura da seguire per l'adozione del codice deontologico, che deve precisare alcune garanzie (che si applicano sia ai dati sensibili, sia alle altre categorie di dati) e, individuate dal Consiglio nazionale dell'Ordine dei giornalisti, anche sulla base delle indicazioni fornite dal Garante.

La stessa disposizione stabilisce inoltre un regime di deroga al sistema altrimenti vigente per i dati sensibili e che ruota attorno al binomio consenso-autorizzazione. Tale deroga non operava, tuttavia, con riferimento ai dati idonei a rivelare lo stato di salute e la vita sessuale dell'individuo. Queste informazioni finiscono spesso per svelare la sfera più intima, delicata e vulnerabile della vita privata, e l'eventuale diffusione di simili informazioni può risultare estremamente pericolosa per il soggetto cui si riferiscono. In ragione di tutto ciò, la legge guardava all'interessato come all'unico soggetto legittimato, in via di principio, ad autorizzare la circolazione della "propria" proiezione sociale relativa ai dati sulla salute e alla vita sessuale, ma presentava alcuni difetti in quanto, qualora fosse stata applicata alla lettera, avrebbe impedito irragionevolmente la diffusione non consensuale di ogni qualsivoglia dato sulla salute, anche in relazione a fatti o a circostanze rese evidenti da comportamenti in pubblico dell'interessato o da un fatto di cronaca. Il difetto è stato rimosso dal decreto legislativo approvato il 9 aprile u.s. durante la fase di stampa della presente relazione.

A differenza di quanto avveniva per i dati idonei a rivelare lo stato di salute e la vita sessuale dell'individuo, le altre categorie di dati sensibili previste dall'art. 22 (comprese le informazioni concernenti l'origine razziale ed etnica, le opinioni politiche e religiose, l'adesione a partiti o ad altre organizzazioni politiche, religiose, filosofiche, sindacali) potevano e possono essere oggetto di trattamento senza necessità del consenso scritto dell'interessato e dell'autorizzazione del Garante. Infatti, il comma 1 dell'articolo 25 stabilisce che il consenso dell'interessato non è richiesto nel caso di trattamento *effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità, nei limiti del diritto di cronaca, e in particolare dell'essenzialità dell'informazione riguardo a fatti d'interesse pubblico.* Analoga soluzione è prevista per il trattamento di dati personali idonei a rivelare determinati provvedimenti di carattere giudiziario.

Il decreto del 9 aprile ha perfezionato l'art. 25 in modo da ribadire, anzitutto, che in materia di attività giornalistica non è prevista un'autorizzazione del Garante. Il decreto, oltre a sottolineare la cooperazione tra il Garante e il Consiglio nazionale dell'Ordine dei giornalisti per ciò che riguarda l'adozione del codice, ha previsto anche la pubblicazione sulla *Gazzetta Ufficiale* del codice stesso. Il codice dovrà specificare misure ed accorgimenti particolari per i dati sulla salute e la vita sessuale, per i quali la previgente formulazione dell'art. 25 fissava un limite più rigido nel consenso dell'interessato.

È da segnalare anche che il decreto ha modificato gli artt. 12, 20 e 25 della legge, evitando che la sola inosservanza dei limiti al diritto di cronaca o delle disposizioni del codice deontologico comporti automaticamente, di per se sola, l'applicazione di una sanzione penale, che rimane invero riservata alle norme penali comuni, in particolare in tema di lesione dell'onore e della reputazione.

Da ultimo, il decreto (sul quale il Garante ha espresso formalmente un parere favorevole) ha introdotto una precisazione che previene ancor più i dubbi che potevano sorgere circa la possibilità di raccogliere dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico.

Sotto altri profili, contestualmente all'entrata in vigore della legge, il Governo è intervenuto inserendo nel decreto legislativo n. 123 una disposizione che permette al giornalista di fornire le informative previste dall'art. 10 secondo le forme semplificate previste dal codice deontologico.

Oltre all'equiparazione ai giornalisti dei pubblicisti, dei praticanti e degli autori di saggi, articoli e altre manifestazioni del pensiero, il Governo ha operato successivi interventi esonerando dalla notificazione gli autori medesimi, e rendendo possibile la notificazione in forma semplificata da parte di giornalisti, pubblicisti e praticanti (art. 7, commi 5 bis e 5 ter, legge n. 675/1996, introdotti dal d.lg. n. 255/1997).

Al tempo stesso, anche sulla base di alcune indicazioni fornite dal Garante, il Governo si è riservato di valutare ulteriori correttivi in materia a seguito di una prima verifica del funzionamento della legge.

Dal canto suo, il Garante ha seguìto da subito un'interpretazione dell'art. 25 in linea con l'art. 21 della Costituzione, precisando nella lettera circolare n. 2/GAR (inviata a tutti i giornalisti che hanno richiesto l'autorizzazione al trattamento dei dati sensibili) che per i giornalisti stessi non è necessaria alcuna autorizzazione del Garante.

Il Garante, con nota del 26 maggio 1997, diretta al Consiglio nazionale dell'Ordine dei giornalisti, ha promosso l'adozione del codice deontologico, la cui elaborazione si è poi sviluppata in un quadro di proficua cooperazione, articolatasi anche in diversi incontri e iniziative pubbliche di confronto.

Essendo tenuto ad impartire eventuali misure ed accorgimenti a garanzia degli interessati sin dalla fase di formazione del codice, il Garante ha inviato al Consiglio nazionale una prima segnalazione il 18 dicembre 1997. Quest'ultimo, avvalendosi del più ampio termine che aveva chiesto al Garante di poter utilizzare, ha approvato un primo testo alla fine del mese di dicembre, sul quale il Garante si è nuovamente pronunciato il 23 gennaio 1998, formulando alcune osservazioni.

In particolare, il Garante ha ricordato che: il codice reca non solo precetti deontologici sanzionabili in via disciplinare, ma riveste rango di normativa secondaria speciale indirizzata a chiunque eserciti funzioni

informative mediante mezzi di comunicazione di massa; che il codice deve conformarsi, senza possibilità di deroghe, sia alla legge n. 675/1996, sia alle altre norme primarie vigenti da tempo a tutela della riservatezza, come quelle per le vittime di violenze sessuali, per i minori coinvolti in procedimenti penali, per i malati di Aids; che il codice stesso deve determinare misure adeguate a garanzia degli interessati rapportate alla natura dei dati utilizzati, sia ordinari sia sensibili.

Al tempo stesso, il 15 gennaio 1998 il Garante ha richiamato l'attenzione del Ministro di grazia e giustizia, ritenendo realizzate le condizioni ritenute necessarie per la modifica dell'art. 25, considerati i progressi maturati nella fase di formazione del codice.

Come già riferito, il Ministro e il Governo hanno raccolto l'indicazione del Garante provvedendo il 9 aprile 1998 al varo del citato decreto legislativo.

Una volta adottato per tutti gli organi competenti, il codice costituirà un parametro importante in materia. Peraltro, il comma 3 dell'art. 25 attribuisce al Garante una potestà sanzionatoria di tipo inibitorio, in caso di violazione delle prescrizioni contenute nel codice di deontologia, che si estrinseca nel potere di vietare il trattamento dei dati, a norma dell'art. 31, comma 1, lett. l), qualora in considerazione della loro natura o delle modalità del trattamento, o degli effetti che esso può determinare, vi sia il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati.

D'altra parte, vanno sottolineate alcune ulteriori misure di garanzia.

Il comma 4-bis dell'art. 25, aggiunto dal d.lg. n. 123/1997, allo scopo di consentire l'applicazione delle deroghe in esso disposte ha, come si è visto, esteso la nozione di "trattamento nell'esercizio della professione di giornalista" ai trattamenti effettuati dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti, nonché a quelli temporaneamente effettuati per la finalità esclusiva della pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero.

È opportuno evidenziare che il Garante ha sollecitato il Consiglio nazionale dell'Ordine a introdurre nel codice una norma che prescriva ai quotidiani e ai periodici di indicare gli eventuali responsabili del trattamento dei dati, anche con riferimento ai trattamenti finalizzati seppur occasionalmente all'espressione del pensiero. Tale misura appare di particolare importanza, in quanto consentirà un più agevole esercizio dei diritti di cui all'art. 13 da parte del soggetto cui i dati si riferiscono.

Peraltro, la legge n. 675/1996, nel testo aggiornato con le modifiche apportate nel corso del 1997, disciplina il trattamento dei dati effettuato nell'esercizio della professione giornalistica anche con riguardo a profili diversi da quelli toccati dall'art. 25 e che comportano peculiarità procedimentali che semplificano gli oneri di notifica al Garante.

Restano fermi, in ogni caso, i diritti riconosciuti in capo all'interessato dall'art. 13, nonché gli obblighi che la legge stabilisce con riferimento all'adozione di adeguate misure di sicurezza (art. 15), poiché essi risultano incomprimibili anche di fronte al trattamento giornalistico dei dati personali inteso come espressione sia della libertà di stampa, sia della libertà di manifestazione del pensiero, ferma restando l'esigenza della tutela del segreto professionale del giornalista per ciò che riguarda la confidenzialità della fonte della notizia.

4.3. Trasparenza dell'attività amministrativa.

Altro delicato problema di cui si è dovuto occupare il Garante specie nei primi mesi della propria attività è stato quello di verificare l'incidenza della legge n. 675/1996 sul trattamento dei dati personali ad opera dei soggetti pubblici. La delicatezza del compito va rinvenuta nel fatto che la legge si è innestata in un assetto normativo e giurisprudenziale già articolato in materia di trasparenza e accesso ai documenti amministrativi. Ciò ha indotto alcuni a sollevare qualche interrogativo circa il rapporto tra le esigenze di riservatezza e le misure a garanzia della trasparenza nella pubblica amministrazione. Il punto di equilibrio tra le predette situazioni giuridiche risiede nel garantire comunque ai soggetti privati le prerogative loro accordate dalla legge circa il corretto trattamento dei propri dati personali ancorché questi siano in possesso della pubblica amministrazione.

Il tema è venuto in rilievo, in particolare, nel parere reso il 30 giugno 1997 a proposito della pubblicità degli albi professionali dei medici e degli odontoiatri. In tale parere sono state distinte quattro situazioni possibili per quanto concerne la pubblicità dei documenti detenuti dai soggetti pubblici: *a)* documenti da ritenere pienamente pubblici, ovvero conoscibili da chiunque; *b)* documenti la cui conoscibilità è circoscritta ad alcune pubbliche amministrazioni, oppure a talune categorie professionali; *c)* documenti accessibili ai sensi dell'art. 22 della legge n. 241/1990 (procedimento amministrativo) da parte di chi ha un interesse personale e concreto e per la tutela di situazioni giuridicamente rilevanti; *d)* documenti accessibili alla sola amministrazione che li detiene, soggetti cioè al segreto d'ufficio. Sulla base di tali premesse, il Garante ha analizzato la normativa riguardante l'albo dei medici (la quale prevede che ciascun albo sia pubblicato nel mese di febbraio di ciascun anno, con contestuale trasmissione di una copia ad alcune amministrazioni anche ai fini della sua affissione nelle prefetture), ed ha ritenuto che il caso rientrasse nell'ipotesi indicata alla lettera *a)*. Ciascun ordine è stato quindi ritenuto legittimato ad autorizzare la visione dell'albo presso l'ordine stesso e, quanto alle richieste di nominativi dei professionisti specializzati in talune discipline, a valutarne la meritevolezza e la praticabilità.

L'Autorità è stata richiesta di precisare, poi, se la RAI S.p.A., concessionaria del pubblico servizio radiotelevisivo, fosse tenuta a comunicare nel dettaglio e nominativamente gli stipendi dei suoi dirigenti e giornalisti, nonché i compensi dei suoi collaboratori esterni, e se fosse legittimo o meno, alla luce della legge n. 675/1996, divulgare, da parte di periodici o quotidiani, i dati personali relativi alle retribuzioni del suddetto personale, senza il consenso degli interessati.

Con il parere del 16 settembre 1997, l'Autorità ha ritenuto che la R.A.I. S.p.A. abbia formalmente una struttura societaria, ma, in quanto concessionaria esclusiva del servizio pubblico di diffusione radiotelevisiva, assuma la particolare connotazione di soggetto "pubblicistico" autonomo, in quanto la "concessione" determina "l'impianto" di un ufficio, che per un verso compie attività pubblicistica ed è soggetto a controlli da parte dell'amministrazione concedente e, per un altro, compie attività di diritto privato, operando secondo le norme privatistiche e in base alle regole del mercato. Nei suoi confronti, si è quindi ritenuta applicabile la legge n. 241/1990 per quanto concerne il diritto di accesso, conformemente a quanto ritenuto dal Consiglio di Stato (Sez. IV, 17

giugno 1997 n. 649), in quanto la società concessionaria pubblica rientra nel più ampio concetto di organo indiretto di amministrazione. Pertanto si applicano i medesimi princìpi elaborati per la pubblica amministrazione in senso stretto anche in relazione alla documentazione custodita presso gli uffici della concessionaria pubblica.

All'atto di questa decisione e di altre successive, il Garante ha tenuto conto di alcuni princìpi espressi dalla giurisprudenza amministrativa, in base ai quali, tra l'altro:

— ai fini della legittimazione all'accesso agli atti della pubblica amministrazione, ai sensi dell'art. 22 della legge n. 241/1990, non è necessario possedere tutti i requisiti che legittimerebbero il ricorso giudiziale, essendo sufficiente che l'istante sia titolare di una posizione giuridicamente rilevante e che il suo interesse alla richiesta si fondi su tale posizione (Consiglio di Stato Sez. IV, 11 gennaio 1994 n. 21; Sez. VI, 15 luglio 1994 n. 1243);

— l'interesse all'accesso non è limitato alla titolarità di una posizione strettamente personale di diritto soggettivo o interesse legittimo ed è azionabile anche indipendentemente dall'esistenza di una lesione della posizione giuridica del richiedente;

— il diritto di accesso configurato dalla legge n. 241 del 1990, è correlato non tanto agli atti amministrativi quanto all'attività amministrativa, la quale comprende nel suo ambito anche l'attività di diritto privato (si pensi all'attività contrattuale e all'evidenza pubblica), essendo anch'essa volta alla cura concreta di interessi della collettività non meno dell'attività amministrativa in senso stretto.

Ai princìpi suddetti va aggiunto quanto statuito dall'Adunanza plenaria del Consiglio di Stato (n. 5 del 4 febbraio 1997), la quale ha ricordato che il diritto di accesso ai documenti amministrativi riconosciuto dalla legge n. 241/1990, allorché la conoscenza di determinati documenti sia necessaria per curare o per difendere l'interesse giuridico del richiedente, prevale sul diritto alla riservatezza e comporta la necessità di garantire comunque al richiedente stesso la visione degli atti dei procedimenti amministrativi necessari per perseguire tali finalità.

In questo quadro, il provvedimento del 16 settembre 1997 ha esaminato la questione se le informazioni riguardanti le retribuzioni e le altre indennità corrisposte dai concessionari di pubblici servizi fossero conoscibili e potessero essere oggetto di diffusione attraverso i mezzi di comunicazione. Il Garante, dopo aver premesso che l'art. 43 della legge n. 675/1996 non ha abrogato le disposizioni concernenti la pubblicità degli atti parlamentari, dei contratti collettivi di lavoro e dei documenti amministrativi, nonché quelle che riguardano il controllo da parte della Corte dei Conti o il legittimo esercizio del diritto di cronaca, ha stabilito che i dati personali concernenti le classi stipendiali, le indennità e gli altri emolumenti corrisposti ad amministratori, dirigenti e lavoratori da concessionari di pubblici servizi (quali le Ferrovie dello Stato S.p.A. e la R.A.I. S.p.A.) sono conoscibili. Più precisamente, ha stabilito che sono conoscibili da parte delle competenti autorità pubbliche e da chiunque vi abbia interesse, attraverso:

a) la lettura degli atti parlamentari nei quali sono documentate le doverose risposte fornite ad interrogazioni e ad interpellanze parlamentari;

b) l'esame dei contratti collettivi, destinati per loro stessa natura ad un regime di diffusa conoscibilità;

c) l'accesso ai documenti amministrativi che la legge 7 agosto 1990 n. 241 rende accessibili da parte di chiunque vi abbia un interesse giuridicamente rilevante personale e concreto (art. 22 legge n. 241/1990;

art. 2 d.P.R. n. 352/1992), nonché da parte di amministrazioni, associazioni e comitati portatori di interessi pubblici o diffusi (art. 9 d.P.R. n. 352/1992);

d) in sede di esercizio del diritto di cronaca da parte di chi esercita la professione di giornalista o collabora occasionalmente ai mezzi di informazione (artt. 12, 20 e 25 legge n. 675/1996).

Nella decisione, si è preso in esame il delicato rapporto tra diritto di cronaca e diritto alla riservatezza, e si è stabilito che l'esposizione di cifre e classi stipendiali, benché accostate a determinate persone fisiche, soddisfa pur sempre l'interesse pubblico alla conoscenza della prassi in atto presso soggetti che, pur operando, di regola, secondo norme privatistiche e in base a logiche di mercato, svolgono attività aventi una particolare connotazione pubblicistica.

Successivamente, il Garante è stato chiamato a pronunciarsi sui rapporti esistenti tra i princìpi espressi dalla legge n. 675/1996 e il diritto di accesso ai documenti amministrativi anche con riferimento all'attività dell'Agenzia Spaziale Italiana (ASI). Quest'ultima ha chiesto di sapere se fosse possibile consegnare la documentazione relativa allo svolgimento di un concorso ad un concorrente che non aveva superato la selezione effettuata dall'Agenzia ai fini dell'assunzione di personale altamente specializzato. L'Autorità, con la decisione 21 ottobre 1997, ha ribadito i princìpi giurisprudenziali (già riferiti) in materia di accesso ai documenti amministrativi, precisando in particolare che, per quanto concerne i *curricula vitae* dei partecipanti alla selezione, la normativa sull'accesso prevede che spetta alle singole amministrazioni individuare i documenti amministrativi che possono essere sottratti all'accesso in relazione all'esigenza di salvaguardare la riservatezza dei terzi. Sicché possono essere esclusi quei documenti o parti di documenti che riguardano la vita privata o la riservatezza di persone fisiche, con particolare riferimento ai profili sanitari, professionali ecc... Si è ricordato ancora, quindi, che deve essere garantita, comunque, la possibilità di visionare gli atti relativi ai procedimenti amministrativi, ivi compresi i *curricula*, qualora la conoscenza dei singoli documenti sia effettivamente necessaria per curare o difendere gli interessi giuridici dei concorrenti (art. 24, comma 2, lett. d), legge n. 241/1990; art. 8, comma 5, lettera d), d.P.R. n. 352/1992).

Un'altra importante occasione in cui l'Autorità è intervenuta su questi delicatissimi temi è stata originata dalla richiesta di parere della Presidenza del Consiglio dei ministri in ordine ai rapporti tra la legge n. 675/1996 e la legge n. 441 del 1982, in tema di pubblicità della situazione patrimoniale relativa ai titolari di talune cariche elettive o direttive. In particolare, la Presidenza ha chiesto di conoscere se fosse legittima la contestazione da parte di taluni interessati (titolari di determinate cariche direttive, quali i presidenti, i vicepresidenti, gli amministratori delegati di istituti ed enti pubblici o partecipati), cui pure era stata estesa l'applicazione della legge (con conseguente raccolta delle dichiarazioni patrimoniali dei titolari delle predette cariche direttive, poi pubblicate in un apposito bollettino diffuso presso i prefetti ed altri organismi, ai sensi degli articoli 12 e 8 della legge n. 441/1982). Alcuni interessati sostenevano che l'interpretazione della norma testé indicata da parte della Presidenza del Consiglio dei ministri era errata e, comunque, non più rispondente ai princìpi contenuti nella nuova legge sulla riservatezza dei dati personali.

Il Garante, con il parere dell'8 gennaio 1998, ha chiarito che la disciplina del trattamento dei dati personali da parte di soggetti pubblici è prevista dall'art. 27 della legge n. 675/1996, che permette a tali soggetti di raccogliere e di utilizzare le informazioni di carattere personale

qualora ciò sia necessario ai fini dello svolgimento di funzioni istituzionali, nel rispetto dei limiti eventualmente stabiliti da norme di legge o di regolamento. La medesima norma stabilisce che la divulgazione dei dati ad altre amministrazioni pubbliche è possibile non solo in presenza di norme espresse che lo consentano, ma anche in via residuale, qualora sia necessario per lo svolgimento di funzioni istituzionali. Al contrario, la comunicazione e la diffusione dei dati personali a soggetti privati, si è ricordato, è possibile solamente quando tali operazioni siano previste da un'espressa disposizione normativa.

Nel caso di specie (ove vi era una espressa normativa rinvenibile negli artt. 12, 13, 14 e 15 della legge n. 441/1982), l'Autorità non ha ravvisato alcuna incompatibilità di fondo tra le nuove disposizioni in materia di dati personali e le norme in tema di trasparenza nella pubblica amministrazione.

Nel parere, il Garante ha esaminato in particolare il problema della legittimità della pubblicazione dei dati relativi alla situazione patrimoniale degli alti dirigenti di aziende ed organismi pubblici, in quanto tale possibilità non è oggetto di un preciso richiamo nell'ambito degli articoli di legge sopra ricordati. L'Ufficio ha ritenuto che il comma 2 del citato art. 14 della legge n. 441/1982, benché formulato in maniera asistematica, debba essere considerato come una norma di chiusura volta a prevedere, in relazione alla situazione patrimoniale dei soggetti di cui all'art. 12 della medesima legge, la conoscibilità e la pubblicità dei dati contenuti nelle dichiarazioni e negli atti da essi presentati, attraverso un bollettino edito a cura della Presidenza del Consiglio dei ministri.

In altri termini, l'Autorità ha ritenuto che il problema interpretativo specifico dovesse armonizzarsi con lo spirito complessivo della legge n. 441/1982, che ha voluto prevedere uno speciale regime di trasparenza per quanto riguarda alcuni dati economici relativi agli individui che ricoprono determinati incarichi pubblici o di rilievo.

Nel parere, infine, si è affermato che il regime così come delineato vale anche per la situazione patrimoniale relativa al personale dirigenziale o equiparato alle amministrazioni pubbliche, nonché al personale di magistratura ordinaria, amministrativa, contabile e militare, al quale, per effetto della legge n. 127/1997, attualmente si applicano le disposizioni dell'art. 12 della legge n. 441/1982 (vedasi in particolare l'art. 17, comma 22, legge 15 maggio 1997, n. 127).

A tale proposito, va segnalato che il Consiglio di presidenza della giustizia amministrativa ha chiesto al Garante di poter acquisire il predetto parere al fine di uniformarsi a quanto ivi statuito, in relazione alla pubblicazione delle situazioni patrimoniali dei magistrati amministrativi.

4.4. Consenso e correttezza nella raccolta delle informazioni.

Con l'entrata in vigore della legge n. 675/1996, sono emersi numerosi problemi in ordine alla corretta esecuzione degli obblighi di informativa agli interessati e di acquisizione del relativo consenso da parte di coloro che raccolgono ed utilizzano i relativi dati personali.

L'Autorità, spesso, su segnalazione di cittadini, si è attivata per garantire il pieno rispetto delle disposizioni vigenti e per rendere più semplice e comprensibile l'apposita modulistica predisposta, ad esempio, da banche, compagnie di assicurazione e da altre imprese per la clientela o per il personale dipendente.

Il primo caso affrontato a questo proposito dal Garante, e senza dubbio quello di maggior rilievo, riguarda il settore bancario.

Immediatamente dopo l'entrata in vigore della legge n. 675/1996, alcuni cittadini ed associazioni a difesa dei consumatori hanno presentato all'Autorità segnalazioni e reclami nei confronti dei modelli di informativa e consenso che la Banca nazionale del lavoro aveva inviato ai propri clienti prima dell'8 maggio 1997.

In tali modelli era stato richiesto un consenso "generale" per un'ampia serie di trattamenti dei dati personali, anche sensibili, e si prospettava, in caso di mancato rilascio del consenso da parte del cliente, la chiusura del conto corrente o, comunque, l'estinzione del rapporto bancario.

In seguito alle denunce degli interessati, il Garante è intervenuto, facendo sospendere la trasmissione dei modelli ritenuti non conformi ai princìpi della legge n. 675/1996 ed avviando una procedura di verifica nel corso della quale sono stati raccolti documenti ed osservazioni da parte dei soggetti coinvolti nella vicenda.

Sulla base degli elementi acquisiti, è stata adottata, il 28 maggio successivo, una decisione con cui la banca è stata invitata a riformulare la modulistica inviata alla clientela e a non tener conto delle dichiarazioni di consenso o di rifiuto di prestazione del consenso già manifestate dagli interessati.

Nella decisione il Garante ha fornito alcuni criteri generali in materia di informativa e di richiesta del consenso all'interessato, utili non solo per il mondo degli istituti di credito ma anche per altri soggetti ed operatori di diversi settori economici e produttivi, ai quali è stata fornita comunque la massima collaborazione, anche attraverso consultazioni ed incontri informali, per agevolare l'attuazione delle nuove regole poste a garanzia dei cittadini.

In particolare, è stato affermato anzitutto il principio secondo il quale l'informativa di cui all'art. 10 della legge n. 675/1996 non deve essere fornita all'interessato caso per caso in occasione di ciascuna operazione bancaria.

Nell'informativa, si è detto, occorre inoltre: *a)* specificare se la stessa riguarda i dati raccolti presso la persona a cui questi si riferiscono o presso soggetti diversi, oppure entrambi i casi; *b)* individuare finalità e modalità senza l'utilizzo di formule generiche o tautologiche; *c)* chiarire con riferimento ai soggetti ai quali la banca demanda alcuni compiti, quelli che agiscono come "responsabili" (ai sensi dell'art. 8 della legge n. 675/1996) e quelli che svolgono invece questi compiti in completa autonomia; *d)* indicare direttamente i soggetti o, quantomeno, le categorie di soggetti ai quali i dati possono essere comunicati o diffusi senza procedere a mere elencazioni esemplificative o a semplici richiami all'esistenza presso la banca di un elenco di tali categorie (che spesso non permettono al cliente di avere un'effettiva conoscenza di queste informazioni).

Il difetto principale delle comunicazioni trasmesse dalla banca era comunque quello di prospettare al cliente in maniera generalizzata, nel caso di rifiuto a fornire i propri dati personali, l'eventuale interruzione dell'intero rapporto contrattuale, la mancata esecuzione di singole operazioni o la mancata instaurazione di nuovi rapporti.

Un'indicazione di questo tipo è risultata in contrasto con la normativa sulla *privacy*, la quale invece richiede anzi di distinguere le ipotesi in cui il conferimento dei dati abbia un carattere obbligatorio, perché derivante da obblighi di legge (ad es., per individuare operazioni di riciclaggio) o strettamente connesso all'esecuzione del rapporto contrattuale (in questi due casi non è necessario acquisire il consenso del cliente), oppure facoltativo, quando si riferisce allo svolgimento di ulteriori attività da parte dell'istituto di credito (subordinate invece ad uno specifico consenso dell'interessato).

È evidente che i vizi riscontrati nel modello di informativa spiegano riflessi immediati sulla successiva manifestazione di consenso richiesta agli interessati.

Un modulo di consenso generalizzato e fondato su informazioni generiche ed insufficienti, accompagnate da un'esplicita minaccia di rottura dei rapporti contrattuali, risulta una negazione dei diritti sanciti dalla stessa legge n. 675/1996.

In base ai princìpi dell'ordinamento giuridico e alle regole dettate a livello comunitario, il consenso può essere ritenuto effettivamente libero solo se è prestato al riparo da qualsiasi pressione e non è condizionato dall'accettazione di clausole che determinino uno squilibrio nelle posizioni delle parti del contratto. Pertanto, la richiesta di un consenso generale ed incondizionato, proveniente da un soggetto in posizione contrattuale più forte rispetto al destinatario dell'informativa, si risolve in una violazione della libertà contrattuale di quest'ultimo.

È risultato inoltre impraticabile un consenso richiesto nei confronti dei trattamenti effettuati da un'ampia serie di soggetti individuati solo genericamente od indirettamente. Il consenso deve essere prestato "in forma specifica" e deve fare quindi riferimento ad un preciso genere di trattamento effettuato a cura di un ben individuato titolare del trattamento. Quando la banca o un altro soggetto titolare di trattamento intende acquisire il consenso dell'interessato anche per l'utilizzazione dei suoi dati da parte di altri soggetti, questi ultimi devono essere indicati puntualmente, altrimenti la dichiarazione di consenso deve considerarsi circoscritta soltanto ai trattamenti e alle comunicazioni di dati effettuati dall'istituto di credito.

Sono apparse, altresì, in aperto contrasto con le disposizioni della legge n. 675/1996 determinate richieste di consenso per i dati sensibili, il cui trattamento generalizzato non può certo ritenersi connaturato alle esigenze nascenti da un comune contratto bancario, e deve essere collegato a specifiche finalità o a particolari prestazioni richieste dall'interessato.

Come precisato anche nelle successive decisioni del Garante (relative anch'esse a società che svolgono attività bancaria o che emettono carte di credito), l'interessato deve essere a conoscenza di tutte le informazioni richieste dall'art. 10 e deve essere libero di esprimere il consenso per uno o più trattamenti, soprattutto quando gli stessi riguardino operazioni non funzionali al rapporto bancario (per fini commerciali, indagini di mercato, iniziative di *marketing*, ecc.) o attività svolte non dalla banca ma da altre imprese appartenenti al gruppo bancario o terze.

Dunque, la formula di consenso, preceduta da una chiara e corretta informativa, deve essere precisa e ben articolata, con la previsione, se necessario, di particolari opzioni per l'interessato, le quali dovranno essere di tipo "positivo" (possibilità di esprimere o di negare un consenso) anziché "negativo" (possibilità di esercitare a posteriori un diniego).

A seguito di queste prime indicazioni, i cui contenuti sono stati ampiamente diffusi dagli organi di informazione, è iniziata una consultazione — cui si è già accennato — tra il Garante, le banche, l'ABI e la Banca d'Italia, al fine di risolvere le numerose problematiche relative all'applicazione della disciplina sulla protezione dei dati personali al settore bancario. Inoltre, alcune imprese ed istituti di credito hanno riformulato i modelli già distribuiti ai propri clienti, e le altre banche, che non avevano ancora assunto iniziative al riguardo, hanno provveduto a predisporre e a inviare modelli di informativa e consenso alla clientela.

Negli ultimi mesi dell'anno, sono continuate però a pervenire all'Autorità segnalazioni di comportamenti non rispondenti ai princìpi della legge n. 675/1996 ed è stato necessario fornire ulteriori indicazioni. La legge, infatti, rende obbligatorio per la banca richiedere il consenso dell'interessato anche per operazioni di comunicazione dei suoi dati connesse all'adempimento di obblighi contrattuali sia per la clientela in essere sia per i nuovi clienti, quantomeno per quanto riguarda le comunicazioni sul territorio nazionale.

Il Garante ha inoltre indicato una soluzione del tutto transitoria in base alla quale, qualora gli attuali clienti non diano riscontro all'informativa inviata ai fini dell'acquisizione del consenso, l'esecuzione di una specifica operazione potrebbe essere considerata come manifestazione provvisoria di consenso in attesa di una sua successiva ed esplicita formalizzazione.

Altro caso di grande rilievo, affrontato in questo primo anno di attività del Garante in relazione agli aspetti della correttezza della raccolta dei dati personali, è quello relativo ad un questionario diffuso prima dell'entrata in vigore della legge attraverso un quotidiano a tiratura nazionale, e diretto alla raccolta di alcune informazioni personali ai fini di una ricerca sui consumi.

Attraverso il questionario, segnalato all'Autorità da alcuni cittadini e da una Associazione dei consumatori, una società di *marketing* intendeva acquisire dati personali per effettuare analisi di mercato indirizzate ad aziende produttrici di beni e servizi, permettendo al compilatore di partecipare ad un concorso a premi. L'attività di rilevazione dei dati teneva parzialmente conto delle nuove regole introdotte dalla legge n. 675/1996, ma sotto diversi aspetti appariva lesiva dei diritti degli interessati.

In particolare, il modello prevedeva una informativa insufficiente, formulata e collocata, assieme alla formula di consenso, in maniera non conforme alle disposizioni vigenti. Inoltre, conteneva alcune richieste di informazioni personali di carattere sensibile, riguardanti, in particolare, la salute degli interessati e la raccolta di dati relativi anche ai familiari del compilatore, senza che agli stessi fosse richiesto un consenso ad utilizzare tali informazioni.

Con una prima pronuncia, adottata il 19 giugno 1997, il Garante ha dato precise istruzioni in ordine alla riformulazione del questionario, fissando un termine per l'invio del documento appositamente modificato; ha poi inibito temporaneamente il trattamento da parte della società dei dati raccolti dopo l'8 maggio.

Dopo questa decisione, la società in questione ha apportato alcune importanti correzioni al questionario, consistenti nella predisposizione di una nuova informativa secondo quanto richiesto dall'art. 10 della legge n. 675/1996, nell'eliminazione di domande relative ad informazioni di natura sensibile e nella previsione di un apposito spazio per la manifestazione del consenso da parte degli altri componenti il nucleo familiare.

La società si è inoltre impegnata a non utilizzare, per quanto riguarda le informazioni già raccolte, dati sensibili o relativi a soggetti diversi dai compilatori.

Fermo restando quanto stabilito con il precedente provvedimento, l'Autorità ha pertanto ritenuto che la stessa società potesse proseguire il trattamento delle informazioni non aventi carattere sensibile, e relative ai compilatori del questionario, ai soli fini dello svolgimento del concorso e delle iniziative a questo funzionali il Garante ha ritenuto possibile comunicare i dati alle aziende interessate soltanto in forma anonima.

Anche nell'ambito del rapporto tra datore di lavoro e dipendenti sono emersi alcuni delicati problemi inerenti all'adempimento degli obblighi di informativa e di acquisizione del consenso.

La disciplina dei trattamenti di dati personali nell'ambito del rapporto di lavoro è particolarmente delicata e, com'è noto, dovrà essere completata con i decreti legislativi previsti dalla legge n. 676/1996.

Allo stato attuale, la normativa sulla *privacy* impone al datore di lavoro di acquisire il consenso informato del dipendente in due specifici casi: per le operazioni di raccolta e di utilizzazione dei dati sensibili anche se connesse all'adempimento di obblighi di legge o di contrattazione collettiva, nonché per la comunicazione a terzi dei suoi dati non sensibili. Ciò comporta in ogni caso l'attuazione da parte delle aziende dei predetti obblighi di informativa e richiesta del consenso nei riguardi del personale dipendente, che in alcuni casi, in questa fase di prima applicazione della legge, sono stati congegnati con modalità tali (ad esempio, linguaggio burocratico, atteggiamento vessatorio, formulazioni generiche o generalizzate, assenza di precisi elementi richiesti dalla legge, ecc.) da determinare un rifiuto dei dipendenti a prestare il consenso al trattamento dei dati personali anche quando quest'ultimo sia effettuato nel loro esclusivo interesse.

Il caso più rilevante tra quelli, numerosi, esaminati dal Garante, riguarda alcuni reclami presentati da dipendenti dell'ENEL e da un'organizzazione sindacale, i quali lamentavano la non rispondenza ai princìpi sanciti dalla normativa sulla protezione dei dati personali delle comunicazioni inviate dalle società subito dopo l'entrata in vigore della legge.

La modulistica inviata agli interessati, redatta nella fase di prima applicazione della legge (prima che il Garante, con il provvedimento relativo al caso BNL, indicasse taluni princìpi essenziali), conteneva alcuni passaggi non sufficientemente chiari e precisi in ordine ai trattamenti svolti dalla società titolare nell'ambito del rapporto di lavoro e alle ipotesi di manifestazione del consenso del dipendente.

L'Autorità ha ritenuto pertanto opportuno effettuare un'immediata verifica presso il titolare del trattamento e segnalare gli aggiustamenti necessari per semplificare la modulistica e renderla più comprensibile agli interessati.

I modelli di informativa e di consenso sono stati quindi riesaminati dall'ENEL e sottoposti nuovamente all'attenzione del Garante, il quale, nel fornire alcune ulteriori indicazioni, ha invitato nell'ottobre '97 la società ad inviare la nuova informativa a tutti i dipendenti (compresi quelli che avevano già prestato il proprio consenso), e a reiterare le richieste di consenso, sulla base di questa comunicazione, per i dipendenti che non lo avevano ancora prestato o che si erano rifiutati di prestarlo.

In conclusione, si osserva che anche per altri settori continuano ad arrivare all'Ufficio numerose segnalazioni di mancato o non corretto adempimento degli obblighi di informativa e di consenso.

Molti soggetti che si accingono a raccogliere o gestire dati personali ancora non forniscono alcuna informativa agli interessati (limitandosi il più delle volte ad un mero richiamo della legge n. 675/1996) o non comunicano alcune specifiche informazioni previste dall'art. 10. Nei casi più gravi rilevati dall'Autorità sarà necessario provvedere all'applicazione delle sanzioni amministrative pecuniarie di cui all'art. 39 della legge n. 675/1996.

Più in generale, il Garante sarà impegnato nel corso del prossimo anno nel fornire ulteriori chiarimenti per la corretta esecuzione degli adempimenti connessi alla raccolta ed al trattamento di informazioni personali, anche attraverso la predisposizione di alcuni modelli-tipo che, siano sintetici, semplici e più comprensibili, pur mantenendo ferme sostanziali ed adeguate garanzie a tutela dei diritti degli interessati.

4.5. Salute.

Il quadro normativo in materia di protezione dei dati personali idonei a rivelare lo stato di salute presenta caratteristiche di specialità rispetto al complesso delle disposizioni concernenti i dati personali cosiddetti "ordinari" o "comuni".

Tale "specialità", dovuta alla delicatezza che contraddistingue questi dati e al concreto pericolo della loro utilizzazione a fini discriminatori, si rinviene già nella normativa europea di riferimento.

L'art. 6 della Convenzione n. 108, adottata dal Consiglio d'Europa il 28 gennaio 1981 (Convenzione di Strasburgo), detta linee-guida per la disciplina di alcune "categorie speciali di dati". In particolare, stabilisce il divieto di elaborazione automatica dei dati personali relativi, fra l'altro, allo stato di salute e alla vita sessuale, fatto salvo il loro trattamento in presenza di garanzie adeguate previste in modo specifico dal diritto interno.

Successivamente, l'articolo 8 della direttiva 24 ottobre 1995, n. 95/46/CE, rafforzando le indicazioni contenute nella Convenzione di Strasburgo, ha individuato una serie di garanzie in mancanza delle quali il trattamento di "particolari categorie di dati" deve essere vietato.

Tali princìpi generali, meglio precisati nella Raccomandazione N. R (81) 1 relativa alle banche di dati sanitari automatizzate del 23 gennaio 1981 (recentemente sostituita dalla Raccomandazione N. R (97) 5 del 13 febbraio 1997 sulla protezione dei dati sanitari), sono stati recepiti nel nostro Paese dalla legge 31 dicembre 1996, n. 675/1996, la quale ha riservato ai dati cosiddetti "sensibili", tra i quali anche quelli idonei a rivelare lo stato di salute, una disciplina giuridica più severa (artt. 22 e 23 della legge n. 675/1996).

L'articolo 22, quale norma generale in materia di dati sensibili, stabilisce che tali dati possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.

Fa eccezione a questa regola il trattamento dei dati sensibili da parte dei soggetti pubblici, per i quali l'art. 22, comma 3, rende superflua l'acquisizione del consenso e dell'autorizzazione del Garante, demandando a norme primarie il compito di specificare, caso per caso, l'ambito di operatività del trattamento, ovvero "*i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite*".

Ciò comporta che le pubbliche amministrazioni dovranno rivedere la normativa in base alla quale hanno finora raccolto ed elaborato le informazioni sensibili nei diversi settori di competenza.

Il nuovo regime introdotto dalla legge n. 675/1996 per i soggetti pubblici che trattano dati sensibili è stato temperato, tuttavia, da una disposizione transitoria che consente di proseguire il trattamento fino al 7 maggio 1998, anche in assenza di una espressa disposizione di legge, previa comunicazione al Garante che può esperire gli opportuni controlli (art. 41, comma 5, della legge n. 675/1996).

Tale facoltà può essere esercitata anche quando il trattamento sia iniziato prima dell'8 maggio 1997 e riguardi dati raccolti in epoca successiva. Così ha precisato il Garante nel parere reso in data 12 novembre 1997, nel quale ha chiarito alcune questioni relative all'applicazione degli articoli 22 e 23 della legge n. 675 agli organismi sanitari pubblici.

L'articolo 23, infatti, che riguarda specificamente i "dati inerenti alla salute", integra, per alcuni aspetti, la regolamentazione contemplata nell'articolo precedente. In particolare, stabilisce che il trattamento dei dati personali idonei a rivelare lo stato di salute da parte degli esercenti le professioni sanitarie e gli organismi sanitari pubblici può avvenire:

a) anche senza l'autorizzazione del Garante, ma sempre con il consenso scritto dell'interessato, quando il trattamento è finalizzato alla tutela dell'incolumità fisica e della salute dell'interessato;

b) con l'autorizzazione del Garante, qualora il consenso scritto non sia o non possa essere prestato dall'interessato, se le medesime finalità riguardano un terzo o la collettività.

Rimane pertanto fermo che, al di fuori di queste ipotesi, ovvero nei casi di trattamenti non autorizzati dalla legge o non indispensabili per la tutela della salute dell'interessato, di un terzo o della collettività, deve essere osservata la regola generale della doppia condizione del consenso scritto dell'interessato e dell'autorizzazione del Garante. Quest'ultima, salvo casi di particolare urgenza, è rilasciata sentito il Consiglio superiore di sanità.

Il Garante, tuttavia, in questa prima fase transitoria di applicazione della legge n. 675/1996, allo scopo di garantire il rispetto dei diritti e delle libertà fondamentali della persona e, al tempo stesso, di semplificare gli adempimenti prescritti, si è avvalso, come si è visto in precedenza, della facoltà prevista dall'art. 41, comma 7 (come modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123), di rilasciare autorizzazioni mediante provvedimenti di carattere generale nei confronti di determinate categorie di titolari o di trattamenti.

Con l'autorizzazione n. 2/97, già illustrata nelle sue linee generali al paragrafo 2.3.2, il Garante ha autorizzato il trattamento dei dati idonei a rivelare lo stato di salute anche da parte dei soggetti pubblici che agiscano nella qualità di autorità sanitarie, ogniqualvolta il trattamento non sia previsto da una specifica disposizione di legge, sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività e manchi il consenso scritto dell'interessato, che non lo abbia prestato o non possa prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere.

Di tale provvedimento si è avvalso, ad esempio, il Ministro della sanità in sede di emanazione dell'ordinanza 23 dicembre 1997, con cui ha disposto per tutti coloro che ne fossero in possesso, di provvedere alla consegna della documentazione clinica inerente il trattamento di patologie oncologiche secondo il c.d. metodo Di Bella.

Particolare attenzione è stata dedicata, nella citata autorizzazione, ai dati genetici e alle informazioni relative ai nascituri, stabilendo - per i primi - esclusioni soggettive e limitazioni nelle finalità (i dati genetici possono essere trattati, sulla base del consenso scritto dell'interessato, soltanto per fini di prevenzione, di diagnosi o terapia o per finalità di ricerca scientifica), nonché il divieto di comunicazione, e rinviando, per i secondi, ai criteri delineati nella raccomandazione N. R (97) 5 del Consiglio d'Europa.

La disciplina in materia di protezione dei dati inerenti alla salute è, pertanto, articolata in un intreccio di ipotesi ed eccezioni tali da sollevare alcuni problemi interpretativi sui quali il Garante è stato invitato a pronunciarsi.

Il primo parere, reso da questa Autorità in data 30 giugno 1997, riguarda alcuni quesiti posti dalla Federazione nazionale dell'Ordine dei medici riguardo alla pubblicità degli albi professionali dei medici e degli odontoiatri e ad alcune modalità applicative della legge n. 675 in riferimento ai medici di medicina generale.

Il Garante ha affrontato, in quel contesto, alcuni aspetti inerenti alla trasparenza dei dati personali rilevabili dagli albi dei medici (v. paragrafo 4.3) e, per quanto concerne specificatamente i dati inerenti alla salute, ha chiarito che il medico che sostituisce formalmente un collega può utilizzarne lo schedario dei pazienti, ove vi sia stato uno specifico consenso degli interessati.

Tale consenso, che deve essere prestato per iscritto, deve intendersi necessario (salvo che si persegua una finalità di tutela dell'incolumità fisica e della salute di un terzo o della collettività: art. 23, comma 1, legge n. 675), sia per i dati raccolti successivamente all'entrata in vigore della legge sia, nel caso in cui siano comunicati o diffusi, per le informazioni acquisite anteriormente.

In relazione agli studi professionali, il Garante ha precisato che i professionisti che si associano per l'esercizio della professione medica possono regolare i propri rapporti nel trattamento dei dati personali in modi diversi, realizzando, a seconda dei casi:

a) una gestione individuale e separata dei dati in possesso di ciascun professionista, che assume, conseguentemente, la qualità di "titolare" del trattamento;

b) una contitolarità da parte di tutti o di alcuni dei professionisti, i quali vengono a condividere a titolo personale le prerogative e le responsabilità del "titolare" del trattamento;

c) un'unica attività di elaborazione dei dati personali effettuata nell'ambito di un'associazione o di un organismo che assuma di per se stesso la qualità di titolare del trattamento.

Con il medesimo provvedimento si è chiarito, infine, che le certificazioni rilasciate dai laboratori di analisi o dagli altri organismi sanitari, anche per quanto riguarda le cartelle cliniche, possono essere ritirati anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante consegna dei documenti in busta chiusa.

In ordine alle modalità di esercizio dell'attività di intermediazione del medico, il solo che possa rendere noti all'interessato i dati personali idonei a rivelare lo stato di salute (art. 23, comma 2, legge n. 675/1996), il Garante ha precisato che questa funzione di intermediazione può essere svolta in vario modo: *a)* attraverso la consegna dei dati al medico di fiducia designato dall'interessato, il quale a sua volta li renda noti a quest'ultimo; *b)* attraverso una spiegazione orale ovvero

un giudizio scritto, da parte di un medico designato dal laboratorio di analisi o dall'organismo sanitario titolare del trattamento dei dati personali.

Proseguendo nell'intento di chiarire il più possibile i dubbi interpretativi e di semplificare l'applicazione della legge in ambito sanitario, l'Autorità, rispondendo a numerosi quesiti ricevuti da parte di medici, farmacisti e di loro organizzazioni rappresentative, ha fornito ulteriori indicazioni e suggerimenti nella pronuncia del 13 febbraio 1998.

In tale provvedimento, in cui sono state affrontate in particolare le tematiche dell'informativa e del consenso, si è ribadito che gli esercenti le professioni sanitarie che intendono trattare i dati sullo stato di salute dei loro pazienti devono informare preventivamente gli interessati circa l'utilizzazione che desiderano farne, specificando tutti i trattamenti che saranno effettuati e la loro natura obbligatoria o facoltativa, in modo da porre gli assistiti nella condizione di poter esprimere un consenso "specifico", ovvero differenziato in relazione a ciascun trattamento.

A tal fine, si è detto, i sanitari possono operare autonomamente o sulla base di informative e di modelli di consenso elaborati dagli ordini professionali.

Peraltro, in un'ottica di semplificazione, il Garante ha ipotizzato che la raccolta del consenso, per i medici di famiglia, possa eventualmente avvenire per il tramite delle aziende sanitarie locali all'atto della scelta del medico di fiducia, se del caso anche in relazione ai relativi sostituti. In tal caso, le aa. ss. ll. potrebbero successivamente inviare ai medici la relativa documentazione, analogamente a quanto avviene per i modelli di scelta e di revoca del medico.

Problematiche analoghe sono state segnalate in relazione al trattamento delle ricette mediche necessarie per l'acquisto dei farmaci, le quali vengono conservate presso i farmacisti ed inviate, in copia, alle aziende sanitarie locali per ottenerne il corrispettivo.

Ferme restando le decisioni che sono state adottate dal Parlamento per ciò che riguarda le ricette mediche nel loro complesso (legge di conversione del c.d. "decreto Di Bella"), una soluzione potrebbe essere ravvisata inserendo nell'informativa e nella richiesta di consenso, sottoposte all'assistito prima dell'inizio dei trattamenti da parte degli esercenti le professioni sanitarie, un riferimento puntuale alle operazioni di trattamento effettuate dal farmacista.

In alternativa, si potrebbe prevedere l'inserimento dell'informativa e di una formula per la richiesta del consenso nei moduli utilizzati per le ricette mediche, che potrebbero essere sottoscritti dall'interessato prima della consegna al farmacista.

Infine, nel medesimo provvedimento, il Garante si è pronunciato sulla questione, già sollevata dall'Ordine dei medici di Pescara all'indomani dell'entrata in vigore della legge n. 675/1996, relativa all'omissione della diagnosi o del sospetto diagnostico sulla certificazione sanitaria destinata alle aziende sanitarie locali.

A tale riguardo, il Garante ha ritenuto che le amministrazioni interessate debbano individuare i trattamenti per i quali gli adempimenti di carattere amministrativo impongono di indicare le patologie riscontrate negli assistiti e che, d'altra parte, debbano predisporre formulari e modelli differenziati per i casi in cui questa indicazione non risulti indispensabile per il perseguimento delle finalità amministrative connesse al servizio sanitario.

Nelle more della predisposizione di questi moduli, è stato suggerito ai medici di omettere fin d'ora l'indicazione della patologia specifica nella copia dei certificati destinati al trattamento da parte del personale non medico.

Questa posizione è stata ulteriormente ribadita nelle osservazioni che questa Autorità ha ritenuto di dover sottoporre alla Presidenza della Commissione igiene e sanità del Senato, in relazione al decreto-legge in materia di sperimentazioni cliniche in campo oncologico e altre misure in materia sanitaria (cosiddetto "decreto Di Bella", decreto-legge 17 febbraio 1998, n. 23).

In tale occasione la Commissione ha recepito, attraverso appositi emendamenti, i suggerimenti del Garante in materia di compilazione e conservazione delle ricette mediche, nonché in tema di consenso informato, come risulta anche dalla legge di conversione.

Il rispetto della dignità e della riservatezza dei pazienti interessati al "multitrattamento Di Bella" ha suggerito una nuova misura di salvaguardia dell'anonimato, mediante l'omissione dell'annotazione del loro nominativo sulle ricette. Le esigenze delle verifiche amministrative possono essere soddisfatte apponendo sulla ricetta un riferimento numerico o alfanumerico in collegamento a dati d'archivio in possesso del medico e che consentono di risalire all'identità del paziente trattato qualora l'autorità sanitaria ne faccia richiesta.

L'indicazione della diagnosi deve essere omessa nel caso della visita medica effettuata ai fini dell'iscrizione nelle liste di collocamento e per il riconoscimento dell'invalidità civile. In questo senso si è espresso il Garante in data 19 dicembre 1997, rispondendo ad un quesito relativo alla compatibilità delle norme della legge n. 675/1996 con quelle stabilite dalla legge 5 giugno 1990, n. 135, in materia di prevenzione e lotta contro l'AIDS.

In tale provvedimento il Garante, sulla base della premessa che la legge n. 675/1996 si pone in armonia con le finalità perseguite dalla legge n. 135/1990, soprattutto per quanto riguarda l'intento del legislatore di evitare che si pongano in essere comportamenti discriminatori nei confronti dei soggetti sieropositivi o affetti da HIV, ha chiarito che per poter iscrivere una persona nelle liste di collocamento è sufficiente l'indicazione della percentuale di invalidità riscontrata.

Soltanto in vista dello svolgimento di un'attività lavorativa che possa comportare un serio rischio di contagio per i terzi, la persona affetta da HIV sarà tenuta a fornire le indicazioni relative alla malattia, conformemente a quanto ritenuto dalla Corte Costituzionale nella sentenza n. 218 del 1994.

Le richieste di chiarimenti e le segnalazioni pervenute in numero assai elevato a questa Autorità, evidenziano che la disciplina della riservatezza in ambito sanitario presenta un ampio quadro di problematiche che necessitano di essere risolte in sede di decreti delegati.

4.6. Lavoro.

Anche la problematica dell'incidenza del trattamento dei dati personali nell'ambito del rapporto di lavoro trova una disciplina di riferimento nelle linee-guida desumibili dalla Convenzione del Consiglio d'Europa n. 108 del 28 gennaio 1981. Le relative norme in materia di qualità

dei dati, orientate ai princìpi di trasparenza, finalità e pertinenza dei dati rispetto agli scopi perseguiti, si applicano al datore di lavoro in termini significativi.

Una rilevanza più specifica riguardo all'uso dei dati personali nel rapporto di lavoro è assunta dalla Raccomandazione N. R (89) 22 del 18 gennaio 1989, che raccomanda agli Stati membri di recepire i princìpi del rispetto della dignità della vita privata e della dignità umana del lavoratore, come pure della possibilità di profique relazioni sociali ed individuali nei luoghi di lavoro, che dovranno trovare tutela anche in riferimento al profilo della raccolta e dell'utilizzo dei dati a carattere personale nel lavoro.

La Raccomandazione introduce la definizione di dati finalizzati al lavoro ritenendo tali i dati, relativi a tutti i rapporti tra i lavoratori e i datori di lavoro, raccolti ed utilizzati nella fase della costituzione e della gestione del rapporto di lavoro, compresi quelli utilizzati per l'attività di mediazione tra domanda e offerta di lavoro dagli uffici di collocamento pubblici e privati.

La disciplina contenuta nella Raccomandazione è significativa in quanto evidenzia le problematiche connesse con la raccolta, il trattamento e la circolazione dei dati personali nel rapporto di lavoro, prefigurando un diritto di accesso non solo individuale ma anche collettivo.

In tal senso è importante rilevare che la legge 31 dicembre 1996, n. 676, conferisce al Governo la delega ad emanare, entro diciotto mesi, decreti legislativi volti a garantire la piena attuazione dei princìpi previsti dalla legislazione in materia di dati personali nell'ambito dei diversi settori di attività e nel rispetto dei criteri direttivi e dei princìpi affermati dalle Raccomandazioni adottate dal Consiglio d'Europa, fra le quali, appunto, figura quella del 18 gennaio 1989 (art. 1, comma 1, lett. *b*), n. 4, legge n. 676/1996 citata).

Ulteriori e vincolanti riferimenti alla disciplina del rapporto di lavoro in relazione al trattamento dei dati personali sono contenuti nella direttiva 24 ottobre 1995, n. 95/46/CE, la quale, oltre ai princìpi "orizzontali" sulla qualità dei dati (determinazione delle finalità, adeguatezza, pertinenza e non eccedenza dei dati, ecc.) reca nell'art. 8, in tema di dati sensibili, due importanti disposizioni; una di queste, nel prevedere che gli Stati membri possano considerare insufficiente il solo consenso dell'interessato quale parametro per il trattamento dei dati, tiene implicitamente ma certamente conto di disposizioni come quelle dello Statuto dei lavoratori italiano che pongono alcune garanzie che vanno oltre la dimensione del consenso. L'altra richiede la precisione di adeguate garanzie per il caso in cui il trattamento serva per assolvere obblighi e diritti specifici del titolare in materia di diritto del lavoro.

Inoltre, l'art. 15, par. 1, della medesima direttiva impone agli Stati membri di riconoscere a qualsiasi persona il diritto di non essere sottoposta ad una decisione fondata esclusivamente su un trattamento automatizzato dei dati personali destinato a valutare taluni aspetti della sua personalità, quali, ad esempio, il rendimento professionale, il credito, l'affidabilità, il comportamento, a meno che tale decisione sia presa nel contesto della conclusione o dell'esecuzione di un contratto, ovvero sia autorizzata da una legge la quale precisi i provvedimenti atti a salvaguardare un interesse legittimo della persona interessata.

La legge 31 dicembre 1996, n. 675/1996, non disciplina in maniera dettagliata il trattamento dei dati personali nell'ambito del rapporto di lavoro, ma è affiancata da una previsione di delega contenuta nella legge n. 676 che preannuncia alcune regole più specifiche in attuazione della citata Raccomandazione. Peraltro, la legge n. 675 ha raccolto la

sentita esigenza di evitare che l'applicazione di alcune regole quali quelle in tema di consenso e di sicurezza potesse comportare l'effetto non voluto di derogare alle disposizioni dello Statuto dei lavoratori sui controlli a distanza e sulla pertinenza dei dati.

D'altro canto, l'esonero previsto dal d.lg. n. 25/97 per ciò che riguarda la notificazione al Garante dei trattamenti finalizzati all'adempimento di obblighi contabili, retributivi, previdenziali, assistenziali e fiscali ha introdotto un'opportuna semplificazione nell'ambito della gestione dei rapporti di lavoro che evita, sia pure nell'ambito della sola notificazione, un approccio generalizzato e privo della necessaria modulazione.

La legge stabilisce, in linea generale, che il trattamento dei dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato; tale principio subisce una deroga nel caso in cui il trattamento riguardi dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (si pensi alla disciplina in materia di documentazione dello svolgimento della prestazione lavorativa e in materia previdenziale ed assistenziale) ovvero nel caso in cui la raccolta e l'elaborazione siano necessarie per eseguire obblighi derivanti da un contratto del quale è parte l'interessato.

In linea con l'articolo 15 della direttiva 95/46/CE, la legge n. 675/1996 stabilisce, all'articolo 17, il principio secondo cui, qualsiasi atto o provvedimento giudiziario o amministrativo il quale implichi una valutazione del comportamento umano, non può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

Nell'ambito del rapporto di lavoro, la norma suddetta vieta al datore di lavoro di fondare il proprio atto (si pensi alla concessione di benefici economici o all'individuazione di lavoratori da promuovere) esclusivamente su procedure automatizzate le quali, anche attraverso un'interconnessione di dati, sia pure lecitamente raccolti, consentano di costruire il profilo professionale del lavoratore.

Con riguardo alla comunicazione e alla diffusione dei dati, l'art. 20 della legge n. 675/1996 richiede, in alternativa al consenso dell'interessato, che la comunicazione sia imposta in adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. Quindi, in relazione a tale disciplina, il datore di lavoro può, senza richiedere il consenso dei lavoratori, rendere noti i dati personali dei medesimi laddove una norma glielo imponga (si pensi alle comunicazioni dell'avvenuta assunzione del lavoratore ai sensi dell'art. 9-bis, della legge 28 novembre 1996, n. 608, ovvero alle comunicazioni dei nominativi dei lavoratori per i quali vengono avviate le procedure di mobilità ai sensi dell'art. 4 della legge 23 luglio 1991, n. 223).

Proprio quest'ultimo profilo ha caratterizzato una pronuncia di questa Autorità in materia di integrazione salariale. Il Garante ha infatti constatato che in assenza dell'integrazione normativa che l'Autorità stessa ha poi suggerito, l'INPS può raccogliere i dati personali dei lavoratori che beneficiano del trattamento di integrazione salariale, in quanto il trattamento medesimo è correlato allo svolgimento delle funzioni istituzionali dell'Istituto (art. 27, primo comma, della legge n. 675/1996); il datore di lavoro invece deve acquisire il consenso dei singoli lavoratori interessati, in quanto l'obbligo di trasmettere i predetti dati all'INPS non si rinviene ancora nella legge o in un regolamento (art. 20, primo comma, lett. c) della legge n. 675/1996).

Il Garante ha perciò provveduto a segnalare al Ministro del lavoro e della previdenza sociale l'opportunità che il suddetto flusso di dati che i datori di lavoro devono trasmettere all'INPS sia menzionato specificamente dalla legge o dai regolamenti che disciplinano i compiti dell'INPS in materia. Ciò renderebbe superflua l'acquisizione da parte dei datori di lavoro del consenso dei lavoratori interessati nell'ambito di una procedura che è disciplinata già, per altri aspetti, dalle leggi o dai regolamenti, e che si svolge nel diretto interesse dei lavoratori stessi.

Un aspetto di particolare importanza nel trattamento di dati personali nell'ambito del rapporto di lavoro è, certamente, quello che riguarda i dati sensibili che, come noto, benché riferiti ad aspetti strettamente connaturati al rapporto di lavoro (si pensi ai dati relativi alle rappresentanze sindacali) possono essere trattati solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.

La legge n. 675/1996 incentra la legittimità del trattamento dei suddetti dati sul provvedimento autorizzatorio del Garante, assegnando una rilevanza non esclusiva alla manifestazione del consenso scritto dell'interessato, tenuto conto della delicatezza della categoria dei dati.

Come già riferito in precedenza, il Garante si è avvalso della possibilità di rilasciare un'autorizzazione generale al fine di semplificare gli adempimenti che la legge n. 675/1996 pone a carico dei datori e di altri titolari di trattamenti finalizzati alla gestione dei rapporti di lavoro, e ciò nella considerazione che un ampio numero di trattamenti di dati sensibili è effettuato ai soli fini dell'adempimento di obblighi contabili, retributivi, previdenziali, assistenziali e fiscali.

A tale scopo, con la citata autorizzazione n. 1/97 del 19 novembre 1997 (in G.U. del 21 novembre 1997, n. 272), emanata dopo la consultazione di alcune parti sociali, il Garante ha inteso facilitare la gestione dei rapporti di lavoro nel rispetto dei diritti e delle libertà fondamentali dei lavoratori dipendenti ed autonomi, dedicando a tale materia la prima delle autorizzazioni generali complessivamente rilasciate.

Appare opportuno richiamare ancora l'attenzione sulla circostanza che il Garante, nel tenere conto del fatto che la disciplina legislativa della tutela dei diritti della persona nel mondo del lavoro dovrà essere completata entro il 23 luglio 1998 in attuazione della legge delega n. 676/1996, ha emanato il suddetto provvedimento autorizzatorio attenendosi a un criterio di massima valido anche per le altre autorizzazioni generali, volto ad evitare che l'innesto di ulteriori garanzie rispetto a quelle già previste dalla legge n. 675 comportasse inutili contraccolpi nell'ordinaria gestione delle aziende.

Non può non rilevarsi che, secondo un'indicazione contenuta nella citata Raccomandazione del Consiglio d'Europa (principio 1.4), occorrerà far fronte ai nuovi scenari che si sono aperti, ad esempio con l'ingresso di agenzie fornitrici di prestazioni di lavoro temporaneo, ai sensi della legge 24 giugno 1997, n. 196, scenari che richiederanno la predisposizione di adeguate tutele per il trattamento dei dati personali. In questa prospettiva, l'autorizzazione n. 1/97 individua alcune prime regole, ricomprendendo nel proprio ambito di applicazione i soggetti che utilizzano prestazioni lavorative temporanee ai sensi della legge n. 196/1997.

Un'ulteriore problematica si è presentata con riferimento al trattamento dei dati sensibili da parte del datore di lavoro, sulla base di espressa delega, che riscuota, le ritenute sindacali. Sul punto, il Garante è intervenuto con una riflessione di cui si è dato atto con un comunicato stampa nel quale si è ricordato che l'adesione all'organizzazione sindacale deve essere accompagnata dalla manifestazione del consenso af-

finché i dati riguardanti l'iscrizione sindacale vengano comunicati al datore di lavoro e, da quest'ultimo, siano trattati nella misura necessaria all'adempimento di obblighi previsti dalla legge e dai contratti.

Peraltro, il Garante ha suggerito una formula di espressione del consenso che oltre ad essere sintetica e riproducibile con facilità su moduli e tessere sindacali, permette anche di "autorizzare" in un'unica soluzione anche l'ulteriore trattamento dei dati da parte del datore di lavoro finalizzati alla gestione dei contributi.

4.7. Ricerca scientifica e statistica.

La legge n. 675/1996 si occupa della ricerca scientifica e della statistica nell'articolo 12, comma 1, lett. *d)*, ove si prevede che il consenso non è richiesto quando il trattamento è finalizzato unicamente a scopi di ricerca scientifica o di statistica e si tratta di dati anonimi, nonché all'articolo 21, comma 4, lett. *a)*, il quale stabilisce che la comunicazione e la diffusione dei dati personali sono comunque permesse qualora siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi, a prescindere dalla veste pubblica o privata del "titolare del trattamento".

Le eccezioni poste dagli articoli sopra ricordati, relative ai soli dati anonimi, evidenziano la circostanza che la ricerca scientifica e la statistica non sono escluse dall'applicazione delle norme in materia di protezione dei dati personali.

Naturalmente, a seconda della figura del titolare del trattamento, muta la disciplina di riferimento. Il soggetto pubblico che elabora dati comuni non deve chiedere il consenso dell'interessato; se oggetto del trattamento sono i dati sensibili devono essere rispettate, poi, le maggiori garanzie previste dagli articoli 22, comma 3, 23 e 24.

I privati e gli enti pubblici economici che trattano i dati comuni (non anonimi) devono richiedere necessariamente il consenso dell'interessato (v. art. 12, comma 1, lett. *d)* e art. 21, comma 4, lett. *a)* citati). Per i dati sensibili, invece, valgono le regole generali di cui agli articoli 22 e 23 che prevedono maggiori garanzie.

Alla luce della disciplina sopra richiamata, appare evidente che i tradizionali metodi di ricerca scientifica e di analisi statistica operati in ambito sia pubblico sia privato devono essere oggetto di riflessione da parte degli operatori, al fine di prevedere, anzitutto, un maggior utilizzo di dati anonimi anziché personali, e di individuare, al tempo stesso, alcune linee direttrici dell'intervento normativo complementare che dovrà affrontare nel dettaglio le diverse problematiche sottese alla ricerca storica e scientifica e alla statistica, riducendo l'impiego di dati che non siano anonimi e prevedendo, nel contempo, idonee garanzie a favore dell'interessato.

Giova infatti evidenziare che le stesse disposizioni del d.lg. 6 settembre 1989, n. 322, in tema di statistica, pur non ponendosi in un contrasto di fondo con la legge n. 675/1996, meritano alcune integrazioni e rettificazioni anche perché sono state fatte salve dalla stessa legge solo in quanto "compatibili" con la nuova disciplina in materia di protezione dei dati personali (art. 43, comma 2, legge n. 675/1996).

È di tutta evidenza che l'attuazione mediante decreto delegato della Raccomandazione N. R (93) 10 nelle materie storiche o della ricerca e della statistica potrà tener conto dell'ulteriore e recente Racco-

mandazione N. R (97) 18 del 30 settembre 1997 che il Consiglio d'Europa ha varato in tema di protezione di dati a carattere personale utilizzati a fini di ricerca scientifica e di statistica, poiché il Parlamento, nell'approvare la legge-delega n. 676, ha consapevolmente inserito nella legge stessa un riferimento ("e successive modificazioni" art. 1, comma 1, lett. *a)*) al chiaro scopo di permettere al legislatore delegato di tener conto della nuova e citata Raccomandazione all'epoca *in itinere* presso il Consiglio d'Europa.

Le disposizioni della legge n. 675 suscettibili di incidere sulla ricerca dovranno essere quindi oggetto di attenta riflessione per verificare se, ed in quale misura, occorrano ulteriori misure per bilanciare i diritti della personalità e lo sviluppo della ricerca, anche epidemiologica, in particolare sotto il profilo delle garanzie adeguate da osservare rispetto ai dati raccolti originariamente per altri scopi e che si intenda conservare per motivi statistici o scientifici.

Il Garante ha già iniziato l'esame di questi aspetti, in particolare allorchè ha emanato l'autorizzazione n. 2/97 sui dati idonei a rivelare lo stato di salute e la vita sessuale.

Più precisamente, nel definire con il suddetto provvedimento autorizzatorio l'ambito di applicazione e le finalità del trattamento, si è fatto riferimento 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, ha aggiunto il Garante, "occorre acquisire il consenso (fermo restando quanto previsto dall'articolo 23, comma 1, ultimo periodo, della legge n. 675/1996), 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".

Questo primo assetto della materia è, ovviamente, parziale e temporaneo, e dovrà essere rivisto alla luce delle prossime novità normative.

Da ultimo, si ritiene opportuno evidenziare un'importante novità intervenuta in materia. Il Consiglio dei ministri, nella seduta del 27 febbraio 1998, ha approvato uno schema di decreto legislativo recante norme in materia di ricerca scientifica e tecnologica, sottoposto all'esame del Parlamento, nel quale sono state dettate alcune disposizioni volte a promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico. Più precisamente, s'intende prevedere che le pubbliche amministrazioni, ivi comprese le università e gli enti di ricerca, ferme restando le disposizioni della legge n. 675/1996 sulla tutela dei diritti dell'interessato, possano, con autonome determinazioni, comunicare e diffondere, anche a privati e per via telematica, i dati relativi all'attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei dati sensibili o attinenti a provvedimenti giudiziari; tali dati potrebbero essere successivamente trattati per le sole finalità in base alle quali saranno comunicati o diffusi.

4.8. TELEFONIA E SERVIZI DI TELECOMUNICAZIONE.

Il Garante, nel suo primo anno di attività, ha dedicato particolare attenzione alla tematica della protezione dei dati personali nel settore dei servizi della multimedialità e delle telecomunicazioni e, in particolare, della telefonia.

Nel 1997, in attuazione della direttiva 96/2/CE sulle comunicazioni mobili e personali, è stata introdotta una normativa sulla liberalizzazione di tali servizi (decreto legge 1 maggio 1997, n. 115, convertito con legge 1 luglio 1997, n. 189) ed è stata avviata una revisione della disciplina legislativa del settore, che per gli aspetti relativi alla riservatezza e alla sicurezza dei dati dovrebbe rifluire, però, nei decreti delegati previsti dalla legge-delega n. 676/1996.

Tale legge, tra gli altri profili della delega alla quale si è accennato più volte, include nelle tematiche oggetto dei decreti delegati anche l'attuazione della Raccomandazione del Consiglio d'Europa N. R (95) 4 del 7 febbraio 1995, in materia di protezione della vita privata nel settore delle telecomunicazioni, che a sua volta è strettamente connessa alla citata direttiva comunitaria n. 97/66/CE del 15 dicembre 1997.

Nei primi mesi del suo funzionamento, l'Autorità ha seguito, come si è detto, l'*iter* legislativo di approvazione della legge n. 249/1997 istitutiva dell'Autorità per le garanzie nelle comunicazioni, guardando con favore, come già accennato, all'adozione da parte del Parlamento di alcune modifiche che hanno garantito una maggiore armonizzazione con la disciplina sulla tutela della sfera personale e un coordinamento, per quanto riguarda tale disciplina, dei poteri della nuova *authority* con le attribuzioni che la normativa comunitaria e la legge n. 675/1996 affidano in via primaria al Garante per la protezione dei dati personali.

Successivamente, il Garante ha affrontato i delicati problemi scaturiti dall'approvazione del d.P.R. 19 settembre 1997, n. 318, recante il "*Regolamento per l'attuazione di direttive comunitarie nel settore delle telecomunicazioni*", che ha introdotto nuove regole in materia di esercizio e fornitura delle reti di telecomunicazioni e di prestazione dei servizi accessibili al pubblico.

Tale regolamento, all'art. 15, rinvia espressamente, per ciò che riguarda la protezione dei dati, la tutela della riservatezza e le misure di sicurezza, alle disposizioni contenute nelle leggi 31 dicembre 1996, nn. 675 e 676, o a quelle che saranno inserite nei relativi decreti di attuazione. Analogo rinvio è previsto dall'art. 17, comma 1, lett. *b)*, per ciò che riguarda i diritti degli abbonati in ordine all'inserzione nei relativi elenchi.

Tuttavia, l'art. 17, comma 3, del d.P.R. ha inoltre previsto l'obbligo per ogni organismo di telecomunicazione di "*rendere disponibili, anche telematicamente, al centro elaborazione dati del Ministero dell'interno gli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile*".

Sotto vari profili, quest'ultima disposizione è apparsa in contrasto con la legge n. 675/1996 ed è stata oggetto, subito dopo la sua emanazione, di specifiche segnalazioni all'Autorità, provenienti dalla TIM S.p.a.-Telecom Italia Mobile, da associazioni di difesa dei cittadini e da singoli utenti del servizio telefonico.

Nelle segnalazioni pervenute all'Ufficio del Garante sono state evidenziate la genericità e la mancanza di motivazione della disposizione regolamentare, con particolare riferimento alle funzioni e alle finalità isti-

tuzionali del soggetto pubblico (che avrebbero dovuto giustificare la lesione del diritto di riservatezza degli abbonati e degli utenti del servizio telefonico) dovuto, nonché alle adeguate garanzie.

Il 1 ottobre 1997, in sede di risposta ad alcune interrogazioni parlamentari presentate presso la VIII Commissione (Lavori Pubblici, Comunicazioni) del Senato, il Governo ha dichiarato che il citato art. 17, comma 3, sarebbe divenuto operativo solo dopo l'emanazione dei decreti legislativi previsti dalla legge n. 676/1996, i quali dovranno disciplinare organicamente la materia della sicurezza e del trattamento dei dati personali nel settore delle telecomunicazioni; al tempo stesso, ha fatto notare che la citata disposizione non permette la divulgazione delle notizie attinenti al traffico telefonico e alla sfera privata delle persone.

Alla luce di queste dichiarazioni, il Garante ha deciso di differire l'esame delle segnalazioni pervenute.

Con successivo decreto ministeriale del 25 novembre 1997, il Ministro delle comunicazioni ha dettato alcune disposizioni integrative sul rilascio delle licenze individuali di telecomunicazione, con le quali si è ribadita l'inoperatività dell'obbligo previsto dal già citato art. 17, comma 3, del d.P.R. n. 318/1997.

In base a tale d.m., infatti, i titolari dei servizi di telefonia vocale hanno l'obbligo di rendere disponibile agli utenti e al pubblico l'elenco degli abbonati, anche al fine di permettere la realizzazione di elenchi telefonici generali. Al contrario, il medesimo decreto non riproduce tra gli obblighi dei titolari dei servizi quello di fornire gli elenchi al Ministero dell'interno.

In tal modo, è stata recepita una precisa indicazione che il Garante, consultato preventivamente ai sensi dell'art. 31, comma 2, della legge n. 675/1996, ha fornito con il proprio parere sullo schema normativo trasmesso dal Ministro delle comunicazioni.

Nello stesso schema di d.m., inoltre, venivano riprodotte in maniera pressochè meccanica, alcune disposizioni della recente direttiva comunitaria sulla tutela della vita privata nel settore delle telecomunicazioni attinenti alla sicurezza del trattamento dei dati di fatturazione. Poiché questo genere di disposizioni dovrebbe essere oggetto di una legislazione di rango primario anziché regolamentare, il Ministro ha recepito il suggerimento del Garante e le ha di seguito congegnate come una disciplina transitoria destinata a perdere efficacia alla data di entrata in vigore dei decreti legislativi previsti dalla legge n. 676/1996, cui è stata riservata la materia.

Nel mese di gennaio, dopo l'emanazione del d.m. sul rilascio delle licenze individuali, il Garante ha ritenuto necessario formalizzare una decisione, sia pure di carattere interlocutorio, in ordine alle segnalazioni sopraindicate, considerando fondati alcuni rilievi. Ai sensi dell'art. 31, comma 1, lett. *m)* della legge n. 675/1996, è stata pertanto segnalata al Governo l'opportunità che la materia venisse nuovamente esaminata sul piano normativo sulla base di alcune specifiche considerazioni.

Nel provvedimento, si è precisato infatti che l'art. 17 comma 3, del citato d.P.R. n. 318/97, una volta applicato, obbligherebbe i titolari dei servizi di telefonia fissa o mobile a rendere disponibili al C.e.d. del Dipartimento di pubblica sicurezza gli elenchi di tutti gli abbonati, nonché degli acquirenti del traffico prepagato, a prescindere dalla volontà degli interessati. Gli elenchi comprenderebbero anche le utenze per le quali gli abbonati manifestano la volontà di mantenerle riservate, e che non sono conoscibili al pubblico.

La disposizione finirebbe inoltre per introdurre in maniera surrettizia l'obbligo per i fornitori dei servizi di telefonia mobile di identificare per il tramite degli esercizi commerciali tutti gli acquirenti del traffico prepagato, sebbene per tale categoria di utenti non sia prevista, allo stato, la creazione di appositi elenchi resi disponibili al pubblico.

Si deve quindi ritenere che la creazione di un siffatto complesso di informazioni personali, e la sua messa a disposizione del C.e.d. del Dipartimento di pubblica sicurezza, contrasti con i princìpi previsti dalla legge n. 675/1996, richiamati dallo stesso d.P.R. n. 318, nonché con i diritti riconosciuti agli abbonati in ordine alla riservatezza dell'utenza e all'inserzione del proprio nominativo negli elenchi.

Non è stata messa in discussione l'esigenza dell'autorità giudiziaria o di polizia di disporre, in caso di indagine o per specifiche esigenze connesse alla difesa, alla sicurezza dello Stato o alla prevenzione dei reati, degli elementi necessari per identificare rapidamente il titolare di un'utenza anche riservata. Non è stata ritenuta parimenti pregiudicata la facoltà delle predette autorità di individuare un determinato abbonato e di disporre un'intercettazione telefonica a norma di legge.

Ciò che ha suscitato ampie perplessità è stato in primo luogo, l' inserimento automatico e indistinto di una moltitudine di informazioni, anche riservate, relative a cittadini che non hanno pendenze di giustizia, in un centro elaborazione dati (nonché, di conseguenza, negli archivi giudiziari o di polizia eventualmente interconnessi) che ha precise finalità di raccolta dei dati che devono essere forniti in materia di tutela dell'ordine, della sicurezza pubblica e di prevenzione o repressione della criminalità (art. 6, primo comma, lett. *a)*, legge n. 121/1981).

In sintonia con il complessivo quadro di garanzie che si prefigura anche in ambito internazionale rispetto agli archivi utilizzati per fini di polizia, non è apparso sufficiente finalizzare la tenuta per via telematica degli elenchi degli abbonati e degli acquirenti del traffico prepagato a generiche esigenze di tutela della sicurezza pubblica o di prevenzione dei reati.

E' risultato invece necessario individuare in maniera più precisa alcune finalità collegate, ad esempio, alla prevenzione di gravi reati o di specifici illeciti a danno di uno o più soggetti (es.: molestie o procurato allarme per via telefonica) per il tramite degli esercizi commerciali.

E' apparso inoltre indispensabile valutare altri profili delicati, quali quelli relativi alla reale necessità di far confluire i dati nel C.e.d. del Dipartimento di pubblica sicurezza anziché in un separato archivio, e alle garanzie per gli interessati, con particolare riguardo alla disciplina degli accessi alle utenze riservate.

Infine, si è osservato che la natura dei diritti coinvolti rende insostituibile l'utilizzo di un atto di rango legislativo anziché regolamentare. Questa conclusione appare peraltro confermata dall'insieme delle recenti disposizioni che attengono alla materia (art. 4 legge n. 675/1996; artt. 15 e 17, comma 1, d.P.R. n. 318/1997).

Il ricorso ad una disposizione normativa secondaria, quale l'art. 17, comma 3, del d.P.R. n. 318, risulta in contrasto anche con le previsioni della legge-delega n. 676/1996, che riservano ad un decreto legislativo la puntuale ricognizione dei trattamenti per finalità di polizia ai quali la disciplina sul trattamento dei dati personali si applica con alcuni adattamenti (art. 1, comma 1, lett. *i)*, legge n. 676).

In conclusione, il Garante ha ritenuto opportuno che la tematica fosse nuovamente affrontata nell'ambito dei decreti legislativi di imminente emanazione volti a recepire la direttiva comunitaria n. 97/66/CE

del 15 dicembre 1997 in materia di protezione della vita privata nel settore delle telecomunicazioni, con conseguente abrogazione della disposizione contenuta nell'art. 17, comma 3, del d.P.R. n. 318.

Il citato decreto legislativo del 9 aprile 1998, approvato durante la fase di stampa della presente relazione, ha attuato la predetta direttiva. Nell'esprimere il proprio parere favorevole al riguardo, il Garante ha constatato che le tematiche da ultimo citate, riguardanti le utenze riservate e le carte telefoniche, è stato implicitamente differito ad un successivo provvedimento legislativo per cui rimangono al momento ferme le considerazioni formulate dal Garante nel menzionato provvedimento di gennaio.

4.9. Rete unitaria della pubblica amministrazione.

Il Garante segue con particolare attenzione gli sviluppi che si registrano sul piano dell'attuazione della rete unitaria della pubblica amministrazione, che permetterà a vari soggetti pubblici di dialogare con facilità, nel rispetto di alcune regole di riservatezza e di sicurezza che trovano già negli artt. 15, 22 e 27 della legge n. 675 un preciso punto di riferimento.

Il d.P.R. 10 novembre 1997, n. 513 ("Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59") pone le leggi nn. 675 e 676 del 1996 come un parametro puntuale per la realizzazione e la revisione dei sistemi informativi pubblici, confermando la tesi della compatibilità tra un'infrastruttura tecnica che agevoli i flussi di dati con una contemporanea ed attenta modulazione degli scambi delle informazioni, rispettosa dei princìpi di pertinenza dei dati, di compatibilità delle finalità perseguite e di svolgimento degli scopi istituzionali delle amministrazioni interessate.

4.10. Consiglio Superiore della Magistratura.

Il Garante ha risposto a vari quesiti posti dal Consiglio Superiore della magistratura, relativi all'applicazione della legge n. 675/1996 ai trattamenti dei dati effettuati dallo stesso organo.

Il 2 dicembre 1997, anche a seguito di alcuni incontri tenuti con i rappresentanti del Consiglio, il Garante ha ricordato che una distinzione puntuale dei trattamenti effettuati dal C.S.M. sarà operata dal legislatore delegato (ai sensi dell'art. 1, comma 1, lett. i), n. 3 della legge 676/1996) e che l'art. 4 della legge n. 675/1996 prevede che solo parte dei trattamenti in atto presso il Consiglio siano assoggettati per intero, al momento, alle disposizioni di legge.

Nella pronuncia si ricorda infatti, che ai trattamenti effettuati dal C.S.M per "ragioni di giustizia", si applicano, al momento, solo alcune delle disposizioni della legge 675/1996 che riguardano, più precisamente, la notificazione, le misure di sicurezza, il divieto delle c.d. decisioni automatizzate sui profili individuali o sulla personalità, la responsabilità per danno e i compiti del Garante (art. 4, comma 2).

Il Garante ha osservato che l'espressione "ragioni di giustizia" rappresenta, fino all'entrata in vigore dei decreti delegati, il criterio-guida per verificare quali siano i trattamenti sottoposti per intero all'applicazione della legge.

Il Garante ha ritenuto problematico ricomprendere tra le "ragioni di giustizia" l'intera sfera delle attribuzioni del C.S.M., e ha suggerito al Consiglio di procedere ad una ricognizione delle categorie dei trattamenti effettuati che potrà essere utile anche per il legislatore delegato.

Ciò anche in quanto i trattamenti non ricompresi nella categoria "ragioni di giustizia", devono osservare già oggi le prescrizioni applicabili alle comuni attività poste in essere dalle pubbliche amministrazioni.

Il Garante ha condiviso l'orientamento del C.S.M. inteso a considerare i propri regolamenti (regolamento interno e regolamento sulla gestione delle spese) rispondenti alle caratteristiche delle fonti che in vari articoli della legge vengono citate quale presupposto per il trattamento dei dati o per l'applicazione di alcune eccezioni. In particolare, si è osservato che il regolamento del C.S.M., a differenza di quello previsto da altri organi, viene considerato dalla dottrina quale fonte secondaria in grado di produrre effetti all'esterno.

Si è poi precisato che il C.S.M. può continuare a trattare i dati sensibili fino alla data del 7 maggio 1998, entro la quale una puntuale disposizione di legge - anche delegata - dovrà individuare le rilevanti finalità di interesse pubblico perseguite dal C.S.M., i dati trattati e le operazioni eseguibili; l'Autorità ha ritenuto inoltre adempiuto da una nota del settembre scorso l'obbligo di comunicazione richiesto dalla disciplina transitoria prevista dall'art. 41, comma 5, della legge 675/1996

L'obbligo di notifica spetta al C.S.M. unicamente per quei trattamenti che non sono "esonerati" in quanto, ad esempio, non sono necessari per assolvere ai compiti previsti dalla legge o da un regolamento.

Oltre ad alcune osservazioni relative alla notificazione, il Garante ha ricordato che in tema di accesso occorre diversificare l'ipotesi in cui ricorrono "ragioni di giustizia", da quella in cui l'interessato chiede di accedere ai propri dati trattati per altre finalità. Nel primo caso, infatti, l'interessato non può esercitare direttamente il diritto, ma può investire il Garante per verificare se il trattamento risponde ai requisiti stabiliti dalla legge o dai regolamenti (artt. 31, comma 1, lett. *p)*, 32, commi 6 e 7, l. 675/1996). Nel secondo, invece, l'interessato può chiedere direttamente di esercitare l'accesso nei confronti del C.S.M., e in tal caso vi ha diritto a prescindere dalle eventuali eccezioni previste da norme regolamentari vigenti.

Simile differenziazione va operata anche per la comunicazione a terzi: nell'ipotesi in cui ricorrano le "ragioni di giustizia" non si ravvisano particolari limitazioni nella disciplina vigente, mentre nel caso di trattamenti "ordinari" occorre una fonte normativa idonea (quale il regolamento interno del C.S.M.) per legittimare la comunicazione dei dati ad altre pubbliche amministrazioni o a terzi.

Per quanto concerne infine l'adozione delle misure di sicurezza, si è fatto presente che il C.S.M. è chiamato a rispettare gli obblighi previsti in via ordinaria per ogni altro trattamento. Compito dell'organo sarà quello di distinguere il profilo civilistico da quello penale. Sul piano della responsabilità civile, infatti, fino all'adozione del regolamento che individuerà le misure minime di sicurezza, il C.S.M. dovrà adottare, al pari di altri soggetti, gli accorgimenti necessari per evitare che i trattamenti in atto alla data dell'8 maggio 1998 non siano sottoposti a rischi

di maggiore entità; sul piano penale, invece, le eventuali responsabilità deriveranno solo dalla violazione delle specifiche disposizioni regolamentari che saranno emanate con il d.P.R. previsto dall'art. 15 della legge.

Il Garante ha infine segnalato l'opportunità che il Consiglio richiami l'attenzione degli uffici giudiziari sulle problematiche derivanti dall'applicazione della legge, sottolineando agli stessi l'importanza della comunicazione al Garante, ai sensi dell'art. 40 della 675/1996, dei provvedimenti giudiziari emessi in relazione alla legge stessa e alla legge n. 547/1993, in modo da poter tenere aggiornata l'istituenda banca dati di informazione giuridica che sarà accessibile al pubblico e agli uffici giudiziari; come confermato da una nota del C.S.M. del 27 gennaio 1998, tale invito è stato prontamente formalizzato nella seduta del C.S.M del 26 gennaio.

Infine, con proprio decreto pubblicato nella Gazzetta Ufficiale del 3 marzo u.s., il C.S.M. ha modificato alcuni articoli del proprio regolamento, con particolare riferimento al tema della pubblicità delle sedute del Consiglio ed alla tutela della riservatezza della vita privata del magistrato o di terzi.

4.11. Legislazione sociale.

Anche questo vasto settore pone problematiche significative dal punto di vista della legislazione sulla *privacy*, integrandosi con la tutela della salute.

Il Garante ha adottato alcune decisioni, una parte delle quali è menzionata anche in altri punti della presente relazione.

Una prima questione, affrontata fin dallo scorso mese di giugno, ha riguardato le modalità della trasmissione - dal datore di lavoro all'INPS - dei dati personali relativi ai lavoratori posti in cassa integrazione, allo scopo di assicurare agli stessi la corresponsione del trattamento di integrazione salariale (vedi paragrafo 4.6).

Tale situazione, prospettata da alcune società interessate, configura un' ipotesi di comunicazione di dati e pertanto presuppone l'acquisizione del consenso dei lavoratori interessati, che per i dati relativi allo stato di salute va manifestato necessariamente per iscritto.

Il Garante, attesa la rilevanza della questione e considerata l'opportunità di semplificare una procedura che si svolge nel diretto interesse dei lavoratori, ha interessato il 18 giugno 1997 il Ministro del lavoro e della previdenza sociale, evidenziando l'opportunità che tale flusso di dati venga previsto da un'apposita disposizione normativa, rendendo così superflua l'acquisizione del consenso dei lavoratori, in conformità a quanto previsto dall'art. 20, comma 1, lett. *c)*, della legge n. 675.

Il 17 settembre 1997, il Garante si è espresso su una richiesta di parere pervenuta dall'Associazione nazionale mutilati e invalidi civili (ANMIC). Alla luce della normativa che attiene specificamente alla materia, si è ritenuto che la disposizione che impone ai segretari delle commissioni sanitarie provinciali (incaricate di procedere all'accertamento della sussistenza di minorazioni invalidanti) di trasmettere all'ANMIC gli elenchi dei soggetti sottoposti a visita, risponda ai requisiti di specificità previsti dall'art. 22, comma 3, della legge n. 675.

Tali dati consistono nei nominativi dei soggetti visitati, corredati, secondo quanto indicato dal Ministero dell'interno - Direzione generale dei servizi civili - nel parere reso in data 10 settembre 1997, dai rispettivi indirizzi.

Naturalmente, per gli ulteriori trattamenti svolti dalla citata associazione nell'ambito delle rispettive finalità statutarie, si è ritenuta necessaria l'informativa e l'acquisizione del consenso scritto degli interessati, ai sensi dell'art. 22, comma 1, della legge n. 675.

Il Garante ha seguito con attenzione le iniziative governative e le proposte parlamentari che allo scopo di contenere la spesa pubblica in materia di previdenza e assistenza, hanno ipotizzato l'attribuzione ai cittadini interessati di una carta sanitaria personale o di un documento contrassegnato da un numero di identificazione.

In questo quadro, si collocano le già illustrate disposizioni contenute nella legge collegata alla finanziaria per il 1998 che delegano il Governo ad emanare un decreto legislativo recante la fissazione dei criteri per valutare la situazione economica dei soggetti che richiedono prestazioni sociali agevolate nei confronti delle pubbliche amministrazioni (cd. "riccometro").

Alla luce di quanto disposto in merito dalla direttiva comunitaria 95/46/CE e dalla legge n. 675/1996, il Garante ha anzitutto ricordato, con nota in data 16 settembre 1997 indirizzata al Presidente del Consiglio dei ministri, che tali strumenti riguardano strettamente la sfera privata delle persone, e richiedono la previsione di idonee garanzie a tutela dei dati personali oggetto di trattamento.

In particolare, occorre valutare la pertinenza dei dati che si intendono acquisire rispetto agli obiettivi da perseguire e alle finalità per le quali i dati stessi possono essere utilizzati.

La materia è in continua evoluzione. Il Garante, investito della richiesta di parere sul "riccometro", si è pronunciato nei termini indicati nel precedente paragrafo 2.2.2.

4.12. Pubbliche amministrazioni.

In conformità con i princìpi fissati dal legislatore comunitario, la legge n. 675/1996 disciplina anche i trattamenti di dati personali effettuati dalle amministrazioni pubbliche.

La tutela dei diritti alla riservatezza e all'identità personale non trova, infatti, un limite nella circostanza che il titolare del trattamento è un soggetto pubblico anziché privato.

La legge n. 675/1996, pur disciplinando in modo differenziato il settore pubblico da quello privato, garantisce un grado equivalente di tutela ad entrambe le tipologie di trattamento.

Le amministrazioni pubbliche possono infatti utilizzare i dati personali, automatizzati e cartacei, soltanto per lo svolgimento delle funzioni istituzionali e nei limiti stabiliti dalle specifiche leggi e dai regolamenti vigenti nei settori di riferimento (art. 27, comma 1).

Una disciplina più rigorosa è prevista per il trattamento dei dati sensibili concernenti l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione a partiti politici, sindacati, associazioni, lo stato di salute e le abitudini sessuali (art. 22, comma 1).

Infatti, i soggetti pubblici possono effettuare tali trattamenti solo se sono autorizzati da un'espressa disposizione di legge (art. 22, comma 3).

Da ciò discende, per ciascuna Amministrazione, la duplice necessità di verificare in modo puntuale la corrispondenza tra le attribuzioni istituzionali e i dati utilizzati e di analizzare in maniera ancora più attenta le fonti normative che sorreggono la propria attività.

Il Garante è intervenuto in materia in varie occasioni.

Tra le numerose pronunce relative ai trattamenti effettuati dalle pubbliche amministrazioni, meritano di essere segnalate le seguenti.

— *Rapporti con la normativa riguardante lo stato civile, gli atti anagrafici e le liste elettorali.*

Nel luglio del 1997, su sollecitazione di alcuni Comuni, il Garante ha chiarito che il rilascio a terzi dei certificati concernenti la residenza o lo stato di famiglia è conforme alla legge sulla protezione dei dati personali. Tale ipotesi è, infatti, disciplinata da specifica normativa non abrogata o modificata dalla legge n. 675/1996.

Al tempo stesso, tenendo conto delle norme previgenti alla legge n. 675/1996 e non abrogate da quest'ultima, il Garante ha ritenuto illegittima, in base alla legge vigente, la prassi di fornire dati ed elenchi a terzi, in particolare alle redazioni dei giornali, al di fuori delle modalità previste dalla normativa dei registri dello stato civile, degli atti anagrafici e da altre specifiche norme di legge.

E' stata, infine, dichiarata legittima la comunicazione e la diffusione dei dati riportati nelle liste elettorali in quanto espressamente prevista dall'attuale normativa di settore: chiunque può, infatti, copiare, stampare o mettere in vendita le liste elettorali (art. 51 d.P.R. 223/1967).

— *Applicazioni della L. 675/1996 al settore universitario.*

Su richiesta di alcune Università, nel mese di luglio 1997 il Garante ha fornito chiarimenti riguardanti l'applicazione della legge n. 675/1996 al settore universitario.

L'Autorità ha ritenuto che le Università possano comunicare e diffondere ad imprenditori, associazioni di categoria e altri soggetti privati i dati personali relativi a studenti e laureati solo sulla base della normativa generale che regola il settore universitario o sulla base degli ordinamenti dei singoli atenei.

La comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati è consentita solo se prevista da norme di legge o di regolamento (art. 27, comma 3). Il Garante ha, pertanto, segnalato la necessità, in caso di assenza di previsioni normative, di regolamentare la prassi della trasmissione di dati ed elenchi di studenti e laureati.

Ha, altresì, giudicato legittima la pubblicazione dei dati dei dipendenti nell'annuario dell'Università, in quanto già disciplinata da specifica disposizione normativa (regio decreto n. 674 del 1924).

— *Costituzione di una banca dati relativa all'immigrazione extra comunitaria.*

Su richiesta della Prefettura di Prato, nel dicembre 1997 l'Autorità ha espresso un parere sulla legittimità di un progetto istitutivo di una banca dati relativa agli immigrati extracomunitari.

Al riguardo il Garante ha richiamato l'attenzione sulla "sensibilità" di alcuni dati oggetto di un trattamento iniziato prima dell'8 maggio 1997, (nazionalità e luogo di nascita), essendo gli stessi, nel caso concreto, idonei a rivelare l'origine razziale ed etnica degli interessati (art.

22, legge n. 675/1996). Ha segnalato pertanto la necessità di intervenire sulle fonti normative di tipo primario che regolano l'attività del Ministero dell'interno a livello centrale e periferico.

L'Autorità ha suggerito, infine, di raccogliere i dati relativi agli immigrati in forma anonima, in attesa dell'emanazione di un'apposita disciplina legislativa.

— *Utilizzabilità dei dati relativi agli utenti Enel ai fini del controllo e della manutenzione degli impianti termici.*

Nel mese di febbraio 1998, il Garante ha adottato un parere sull'utilizzabilità dei dati relativi agli utenti Enel ai fini del controllo e della manutenzione degli impianti termici da parte di un'azienda privata convenzionata con la Provincia di Udine.

Il Garante ha preso in considerazione le norme di legge e di regolamento che autorizzano la provincia a svolgere determinati controlli in materia di impianti termici, e ha constatato l'inesistenza di un esplicito l'obbligo dell'Enel di fornire alla provincia i dati dei propri utenti.

Tale incompletezza normativa è stata segnalata al Ministero dell'industria, del commercio e artigianato e all'Autorità di regolamentazione per l'energia elettrica e il gas, allo scopo di sollecitare un'apposita integrazione della normativa (legge n. 10/1991 e d.P.R. n. 412/1993).

— *Utilizzabilità di informazioni di carattere giudiziario relative ad appartenenti ad una comunità zingara.*

Su richiesta della prefettura di Rimini, il Garante si è pronunciato sulla richiesta presentata da uno studente universitario volta ad acquisire dalla prefettura e dalle forze di polizia alcuni dati sulle denunce e sui procedimenti penali pendenti nei confronti degli appartenenti ad una comunità nomade.

Il Garante ha ritenuto che i dati richiesti rivestano solo apparentemente un carattere anonimo, in quanto suscettibili, se connessi ad altre informazioni, di rendere identificabili gli interessati. Tali dati sono stati ritenuti di carattere "personale", nonostante siano privi delle generalità degli interessati.

Il Garante ha infine richiamato l'attenzione sull'illegittimità della comunicazione a privati se non prevista da una norma di legge o di regolamento (art. 27, comma 3).

— *Pubblicazione dell'annuario dell'Accademia dei Lincei.*

Nel gennaio 1998, a seguito di una richiesta di parere dell'Accademia nazionale dei Lincei, il Garante si è pronunciato sulla legittimità della pubblicazione di un annuario contenente i dati anagrafici, le qualifiche dei soci, nonché indirizzi e recapiti privati.

L'Autorità, esaminato lo statuto e il regolamento dell'Accademia e constatata la natura giuridica pubblica dell'istituzione, ha ritenuto legittima la pubblicazione dell'annuario in quanto connessa alle finalità istituzionali dell'ente.

Ha, però, rilevato la mancanza nello statuto di una specifica disposizione relativa alla pubblicazione nell'annuario dei dati personali relativi ai soci, ed ha pertanto segnalato la necessità di promuovere una modificazione dello Statuto al fine di inserirvi tale previsione.

— *"Titolari del trattamento" nei concessionari di pubblici servizi.*

Particolarmente significativo è stato il caso relativo al quesito inoltrato dalle Ferrovie dello Stato S.p.A., che, in qualità di concessionaria pubblica, ha chiesto di conoscere se la legge predetta consenta di individuare il "titolare del trattamento" non tanto dell'azienda in quanto

tale, quanto tra le persone fisiche che ricoprono incarichi di vertice o che coordinano i diversi settori dell'azienda stessa (amministratore delegato, direttori generali e responsabili di aree).

Nella decisione del 9 dicembre 1997, il Garante ha ricordato che, ai sensi della legge n. 675/1996, il "titolare del trattamento" è la persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente cui competano le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza. Il titolare, quindi, anche quando si tratti di una pubblica amministrazione, è l'entità nel suo complesso anziché talune delle persone fisiche che operano nella relativa struttura. Tali soggetti, potrebbero assumere, semmai, la qualifica di responsabile (v. art. 8 legge n. 675/1996). Nel caso di specie il titolare è stato quindi individuato nelle Ferrovie S.p.A., che possono designare alcuni soggetti quali "responsabili" del trattamento, delineandone analiticamente e per iscritto i compiti attribuiti e individuandone al loro interno, se del caso, ulteriori livelli di responsabilità in base all'organizzazione delle divisioni e degli uffici o alle tipologie di trattamenti, di archivi e di dati. Analoga decisione del Garante è stata adottata in riferimento all'Amministrazione delle finanze.

4.13. Investigazione privata.

L'investigazione privata è al centro di varie riflessioni che riguardano la configurazione professionale della categoria, il relativo stato giuridico e le regole previste dalla legislazione di pubblica sicurezza.

Senza entrare nel merito della scelta di fondo che tutto ciò implica, il legislatore del 1996 si è dimostrato consapevole dell'utilità sociale che una corretta esplicazione di questa attività può avere nella società contemporanea, non solo nei tradizionali confini del diritto di famiglia e della raccolta di elementi utili a fini di prova in un giudizio, ma anche nel sempre più importante ambito della trasparenza e correttezza delle iniziative economiche, della concorrenza e della tutela dei segreti aziendali e industriali.

La legge n. 675/1996, prima in Europa, prevede un'attenta considerazione dell'attività di raccolta di informazioni personali finalizzata alla tutela giudiziaria di un diritto, ancorchè esercitata al di fuori degli adempimenti derivanti da un mandato difensivo conferito nell'ambito di un procedimento penale.

Durante l'*iter* parlamentare della legge si era creata l'aspettativa di una totale esclusione dall'ambito di applicazione della normativa dell'intera attività investigativa o, quantomeno, l'introduzione di una serie più ampia di deroghe a vari istituti disciplinati dalla legge.

Si è però, giustamente, osservato che una simile esclusione non è prevista in nessun Paese europeo e non è consentita dalla direttiva, la quale non permette eccezioni in favore della categoria delle investigazioni private in quanto tale, benchè la legislazione di pubblica sicurezza rechi già alcune disposizioni che regolano tale attività. La direttiva autorizza semmai, deroghe "mirate" e giustificate non tanto dalla qualifica soggettiva del beneficiario, quanto dal legame di interdipendenza che collega la raccolta di alcuni dati all'esercizio di un diritto in sede giudiziaria.

Del resto, avrebbe rappresentato una netta contraddizione l'introdurre precisi limiti in materia di raccolta dei dati operanti per qualunque operatore pubblico o privato, e permettere al tempo stesso a chiunque di eluderli rivolgendosi ad un investigatore privato che avrebbe operato *de facto,* in una "zona franca". Ogni investigatore avrebbe goduto di prospettive non riconosciute neanche alle forze dell'ordine, e si sarebbe legittimata una prassi sicuramente pericolosa che avrebbe potuto permettere a qualunque soggetto in possesso dell'autorizzazione prevista dal t.u.l.p.s., di raccogliere dati di propria iniziativa e senza un'adeguata tutela degli interessati.

Tutto ciò non ha impedito di bilanciare il diritto alla riservatezza con i diritti di chi deve poter raccogliere i dati per potersi difendere o tutelare dinanzi all'autorità giudiziaria.

La legge n. 675/1996 reca varie disposizioni che tengono conto della c.d. indagine difensiva e della tutela dei diritti in sede giudiziale.

Il comma 4 dell'articolo 10 riporta la prima delle diverse eccezioni riferite allo svolgimento delle indagini difensive e alla difesa di un diritto in sede giudiziaria.

La soluzione adottata permette di non informare l'interessato dell'avvenuta raccolta dei dati reperiti presso terzi, ad una duplice condizione:

— qualora i dati siano utilizzati per "far valere" o "difendere" un diritto in sede giudiziaria o ai fini dello svolgimento di un'indagine difensiva nel procedimento penale;

— qualora il trattamento si protragga per il tempo necessario al perseguimento di tali fini.

In riferimento al procedimento penale l'eccezione risulta congrua dal punto di vista soggettivo, ed è utilizzabile dal difensore dell'imputato o di un'altra parte privata, come pure da investigatori privati autorizzati ed incaricati dal difensore medesimo.

Peraltro, l'istituto può trovare larga applicazione anche in sede civile (ad es.: controversie per concorrenza sleale, violazione del segreto industriale, cause di separazione e divorzio ecc.) e nella materia del lavoro, come pure dinanzi agli uffici giudiziari di ogni ordine e grado. Inoltre, l'espressione "far valere un diritto in giudizio" è risultata opportunamente comprensiva delle diverse azioni costitutive, dichiarative, ecc. esercitate dinanzi ad un giudice.

L'eccezione all'obbligo dell'informativa è, peraltro, temporanea, in quanto, come precisata dal Garante nell'autorizzazione generale n. 6/97, l'informativa diviene necessaria se i dati sono trattati per un periodo superiore a quello necessario per perseguire i predetti fini, o per ulteriori finalità.

Tale deroga trova il suo presupposto nel fatto che l'interessato, una volta che eserciti il diritto in sede giudiziaria, viene a conoscenza dei trattamenti che lo riguardano attraverso le carte processuali, ed è in quella sede informato dei dati e notizie a lui riferibili.

Per i dati sensibili sono previste garanzie analoghe, in quanto l'ordinario regime basato sull'autorizzazione e il consenso è temperato da una regola secondo cui è sufficiente l'autorizzazione del Garante (già rilasciata con il provvedimento n. 6/97) quando per l'esercizio del diritto di difesa occorre raccogliere dati relativi allo stato di salute e alla vita sessuale (ad es. per accertamenti finalizzati all'instaurazione di una causa di separazione o di divorzio). Questa eccezione non si estende, quindi, ai dati della persona idonei a rivelare l'origine razziale ed etnica, la sfera religiosa, politico-sindacale o filosofica.

Sempre nel caso dei dati sulla salute e la vita sessuale, il soggetto che raccoglie i dati deve perseguire le sole finalità che giustificano la deroga e utilizzarla per il solo periodo strettamente necessario per lo svolgimento dell'indagine difensiva, ovvero per l'esercizio del diritto in sede giudiziaria.

Il soggetto che si avvale della deroga deve rispettare anche le misure e gli accorgimenti prescritti dal Garante nel provvedimento di autorizzazione.

Inoltre, l'incarico conferito ad un investigatore privato non può avere ad effetto l'elusione dei limiti posti dallo "Statuto dei lavoratori" (legge n. 300/1970) alla raccolta di determinati dati da parte del datore di lavoro.

Come già esposto nella presente relazione, il Garante si è avvalso della facoltà concessagli dalla legge di emanare autorizzazioni generali al trattamento dei dati sensibili per categorie ben individuate.

Con il provvedimento datato 29 dicembre 1997 è stata emanata l'autorizzazione n. 6/97 "*al trattamento di alcuni dati sensibili da parte degli investigatori privati*". L'autorizzazione è diretta: 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 (articolo 134 del regio decreto 1931 n. 773, e successive integrazioni e modificazioni).

Oltre a quanto già illustrato, va ricordato che tale autorizzazione precisa che il trattamento deve rispettare le ulteriori prescrizioni contenute nell'autorizzazione generale n. 2/97, in particolare per ciò che riguarda le informazioni relative ai nascituri e ai dati genetici.

4.14. Liberi professionisti.

La disciplina sulla protezione dei dati personali prevede (art. 7, comma 5-ter, lettera f), legge n. 675/1996) l'esonero dall'obbligo di notifica al Garante del trattamento di dati effettuato dai liberi professionisti iscritti in albi o elenchi professionali, purché finalizzato all'adempimento di specifiche prestazioni e fermo restando il segreto professionale.

L'esonero è chiaramente teso a non gravare tali soggetti di ulteriori adempimenti, ma non incide sugli altri obblighi previsti dalla legge n. 675/1996 a carico dei titolari del trattamento: in particolare gli stessi sono tenuti, ai sensi del medesimo art. 7, comma 5-*quinquies*, a comunicare a chiunque ne faccia richiesta le notizie che dovrebbero essere inserite nella notifica al Garante.

Questo obbligo scaturisce dal principio indicato nell'art. 21, par. 3, della direttiva 95/46/CE che impone agli Stati membri di garantire in ogni caso la pubblicità dei trattamenti oggetto di esonero.

Il Garante ha emanato, ai sensi dell'art. 41, comma 7, della legge 675/1996, l'autorizzazione generale n. 4 del 29 novembre 1997 diretta, appunto, ai liberi professionisti iscritti in albi o elenchi professionali, che trattano dati sensibili per lo svolgimento di determinate attività professionali.

Questa autorizzazione non riguarda le figure professionali e le attività già considerate in altre autorizzazioni o che non necessitano di un atto autorizzatorio, quali la gestione dei rapporti di lavoro o di collabo-

razione prestata dal libero professionista (autorizzazione n. 1/97), i medici e il personale sanitario (autorizzazione n. 2/97) nonché i giornalisti, pubblicisti o praticanti giornalisti.

L'autorizzazione ricomprende, invece, i soggetti che collaborano professionalmente con il libero professionista, quali i sostituti, gli ausiliari, i praticanti e i tirocinanti.

Il trattamento dei dati sensibili è autorizzato purché rientri nei limiti strettamente indispensabili per l'esecuzione delle prestazioni professionali richieste dal cliente e ai soli fini dell'espletamento dell'incarico ricevuto.

La stessa autorizzazione n. 4/97, contiene precise indicazioni relative alle modalità di raccolta e di trattamento dei dati, all'idoneità delle misure di sicurezza e all'adempimento degli obblighi di informativa all'interessato e di raccolta del suo consenso.

Per quanto attiene ai quesiti, pervenuti principalmente dagli ordini professionali, il Garante ha chiarito alcuni aspetti applicativi della legge n. 675/1996, ponendo in evidenza che la legge non ha modificato la disciplina relativa al regime di pubblicità degli albi, e che occorre pertanto rispettare le norme di legge e di regolamento che regolano la conoscibilità e la pubblicità di tali atti. Tali norme sono spesso ispirate, per loro stessa natura e funzione, ad un regime di piena pubblicità, anche in funzione della tutela dei diritti di coloro che, a vario titolo, hanno rapporti con gli iscritti agli albi. Pertanto, gli ordini professionali possono trattare dati personali, per la tenuta degli albi nonché per l'espletamento di altri compiti, ai soli fini dello svolgimento delle proprie funzioni istituzionali.

4.15. Associazioni e partiti politici.

L'utilizzazione dei dati personali da parte delle organizzazioni di tipo associativo non aventi fini di lucro, quali i partiti e i movimenti politici, i sindacati, le organizzazioni di volontariato, le confessioni religiose ed altri, è stata oggetto di particolare attenzione.

Sia l'intervento normativo (d.lg. 28 luglio 1997, n. 255) sia quello attuato dal Garante (autorizzazione generale n. 3/97) hanno mirato a semplificare le procedure previste a tutela del diritto alla riservatezza, anche in ragione dell'importante funzione sociale svolta nei vari settori.

Il legislatore delegato ha esonerato dall'obbligo di notificazione i trattamenti effettuati da tali organismi, relativamente ai dati inerenti agli associati e ai soggetti che hanno contatti regolari con l'associazione (art. 7, comma 5 ter, lettere *l)* ed *m)*).

Analogamente, il Garante ha esonerato tali organizzazioni dall'obbligo di richiedere singolarmente l'autorizzazione per il trattamento dei dati sensibili, autorizzando con il ricordato provvedimento generale l'uso dei dati sensibili relativi agli iscritti e ai sostenitori, ferme restando alcune necessarie garanzie a tutela degli interessati.

Nel mese di ottobre del 1997 il Garante ha, altresì, fornito chiarimenti riguardanti l'applicazione della legge sulla *privacy* in merito alle procedure di rinnovo delle adesioni degli associati.

Come già riferito, il Garante ha chiarito, anche attraverso un comunicato stampa, che la procedura di rinnovo delle adesioni degli associati non è soggetta all'ambito di applicazione della legge 675/1996, in quanto

relativa a dati personali raccolti prima della data di entrata in vigore della citata legge, mentre l'informativa e il consenso sono obbligatori nel caso di nuove adesioni.

Peraltro, in tale occasione, sono state suggerite alcune formule di acquisizione del consenso collegate alle finalità statutarie sia per le organizzazioni associative in generale, sia per quelle sindacali e politiche.

In più occasioni il Garante ha fornito risposte a quesiti formulati in particolare dal Partito democratico della sinistra sull'applicazione della legge sulla protezione dei dati personali ai partiti politici, su aspetti che interessano anche altri partiti.

Il Garante ha ribadito che i partiti e i movimenti politici non sono obbligati ad effettuare la notificazione né per il trattamento dei dati relativi ai propri associati, né per quello relativo ai propri dipendenti.

Le associazioni politiche sono state autorizzate con un provvedimento generale a trattare i dati sensibili sia dei propri associati sia dei dipendenti, salva la necessità di acquisire il consenso scritto.

Si è precisato che il consenso può, eventualmente, essere esteso alla possibilità di pubblicare, anche via Internet, gli elenchi dei sostenitori e dei dipendenti dell'associazione.

Su sollecitazione del Gruppo parlamentare Lega nord per l'indipendenza della Padania, il Garante si è occupato inoltre della diffusione di dati sensibili a scopo di propaganda politica.

Nel caso di specie, poiché gli opuscoli informativi sono stati curati da alcuni giornalisti, è stata ritenuta applicabile la disciplina derogatoria relativa al giornalismo che prescinde dall'acquisizione del consenso.

4.16. Ricerche di mercato.

La Raccomandazione del Consiglio d'Europa 25 ottobre 1985, N. R (85) 20, relativa alla protezione dei dati personali utilizzati per fini di *marketing* diretto, qualifica come "*marketing diretto*" "*l'insieme delle attività, nonché ogni servizio ausiliario ad esse, che permettano di offrire prodotti e servizi o di trasmettere ogni altro messaggio pubblicitario a segmenti di popolazione mediante la posta, il telefono o altri mezzi diretti, a scopo di informazione o al fine di sollecitare una reazione da parte della persona interessata*"*(1.2)*.

Tutte le fasi in cui si articolano tali attività, dalla selezione del prodotto allo studio del potenziale mercato, fino all'individuazione dei soggetti ai quali dirigere il messaggio e dai quali attendere risposte, comportano un trattamento di dati personali; pertanto, dovranno essere effettuate nel rispetto delle norme della legge n. 675.

Nelle more dell'attuazione della citata Raccomandazione, il trattamento per scopi di *marketing* risulta disciplinato da regole comuni ad altri trattamenti.

Devono essere osservate, pertanto, le disposizioni degli articoli 10, 11 e 20 della legge n. 675/1996, relative all'obbligo di informativa degli interessati e all'acquisizione del consenso, ove necessario. La legge prevede, infatti, alcune ipotesi in cui il trattamento può essere legittimamente effettuato anche indipendentemente dal consenso degli interessati (ad esempio, nel caso di dati acquisiti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque art. 12, lett. *c)*, della legge n. 675/1996).

Anche in queste ipotesi resta fermo, tuttavia, l'obbligo di informare preventivamente, gli interessati, oralmente o per iscritto, circa le finalità e le modalità del trattamento, nonché in ordine alla possibilità di esercitare i diritti di opposizione di cui all'articolo 13 della legge n. 675/1996.

Proprio con riferimento ai diritti di opposizione, il legislatore italiano, in linea con quanto disposto dalla direttiva 95/46/CE, ha dettato, per il settore del *marketing*, una norma specifica.

Nella legge n. 675/1996, infatti, l'art. 13, lettera *e)*, sancisce il diritto dell'interessato di opporsi al trattamento di dati che lo riguardano, (nel suo complesso ovvero con riferimento alla sola divulgazione) previsto *"a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva"*.

A differenza dell'opposizione prevista dall'articolo 13, lettera *d)*, la fattispecie in esame rappresenta una "figura speciale di opposizione", in quanto l'interessato che non intende essere inserito in un indirizzario pubblicitario non deve addurre alcun motivo a supporto dell'opposizione, né una specifica violazione di legge, né l'esistenza di un motivo legittimo.

L'attività di *marketing* è stata oggetto di un provvedimento del Garante il quale, anche in questa materia, ha emanato un'autorizzazione generale per il trattamento dei dati sensibili.

L'autorizzazione n. 5/97, consente nel Capo II il trattamento dei dati sensibili di cui all'articolo 22 della legge n. 675/1996, fatta eccezione di quelli idonei a rivelare la vita sessuale, da parte di imprese, società, istituti ed altri organismi o soggetti privati che effettuano ricerche di mercato o altre ricerche campionarie, per scopi determinati e legittimi, noti all'interessato che abbia manifestato il suo consenso per iscritto.

Nel provvedimento, il Garante ha stabilito che i dati sensibili possono essere trattati per compiere sondaggi di opinione o ricerche di mercato, solo se il trattamento di dati anonimi non consente di raggiungere gli scopi perseguiti. In ogni caso, il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente, mediante un riferimento ad una qualsiasi altra informazione. A tal fine, sono previste alcune regole sulla registrazione dei dati.

Ulteriori aspetti relativi al *marketing* saranno regolamentati più analiticamente nel decreto legislativo che il Governo è stato delegato ad emanare, ai sensi dell'art. 1, comma 1, lett. b), n. 2, della legge n. 676/1996, per garantire la piena attuazione dei princìpi sanciti in materia dal Consiglio d'Europa.

4.17. VIDEO-SORVEGLIANZA.

Anche in Italia, il tema della video-sorveglianza e della tecno-sicurezza, e dei problemi che esse pongono sul piano della riservatezza dei singoli, inizia ad essere avvertito con chiara consapevolezza dai cittadini e dai mezzi d'informazione.

L'utilizzo di telecamere allo scopo di favorire la sicurezza sociale in strade, piazze, luoghi pubblici o l'accesso selettivo a zone di traffico limitato, comincia a diffondersi, soprattutto nelle grandi città. Il dibattito sulla legittimità di tali forme di controllo e sui rischi che possono derivarne alla riservatezza e alla libertà dei singoli si è avviato in Italia già da qualche tempo.

Analoghe riflessioni vengono a maturazione per la video-sorveglianza interna a edifici e luoghi aperti al pubblico (quali esercizi pubblici, supermercati e banche).

In Italia, a differenza di altri Paesi europei come ad esempio la Francia, non esiste ancora un'apposita normativa sulla video-sorveglianza.

La direttiva 95/46/CE e la Convenzione n. 108/1991 del Consiglio d'Europa rendono obbligatoria l'applicazione della disciplina sul trattamento dei dati personali anche ai suoni e alle immagini, qualora queste consentano di identificare un soggetto anche attraverso il collegamento con altre informazioni, come ad esempio foto segnaletiche, *identikit* o archivi di polizia contenenti immagini. La legge, quindi, si applica anche ai trattamenti di suoni e di immagini effettuati attraverso sistemi di video-sorveglianza, a prescindere dalla circostanza che tali informazioni siano eventualmente registrate in un archivio elettronico o comunicate a terzi, dopo il loro temporaneo monitoraggio in un circuito di controllo.

La complessiva regolamentazione della materia sarà oggetto di uno dei decreti legislativi previsti dalla legge n. 676 del 1996, che dovrà definire regole specifiche per trovare il giusto bilanciamento tra gli interessi perseguiti nel settore della pubblica sicurezza, della prevenzione dei reati, dell'accesso nei centri storici, con il diritto alla riservatezza degli interessati.

Pur non essendo presente nel nostro Paese una normativa specifica per la video-sorveglianza, le prescrizioni contenute nella legge n. 675 peraltro costituiscono un preciso riferimento normativo e sono applicabili anche alle informazioni di tipo visuale.

L'installazione di telecamere presso istituti bancari, esercizi commerciali o strade e piazze, finalizzata a sorvegliare luoghi pubblici o ad aiutare le forze dell'ordine nella lotta alla criminalità, è già stata oggetto di esame da parte del Garante, che ha richiamato l'attenzione sugli aspetti connessi alla violazione della *privacy* fornendo alcune indicazioni.

Nella risposta al quesito presentato da un ente locale, il Garante ha, anzitutto, posto l'accento sulla necessità che vi sia una legittimazione giuridica che consenta l'installazione delle telecamere, che siano individuate le relative finalità e che l'iniziativa risponda alle funzioni istituzionali demandate all'ente pubblico. In secondo luogo, il Garante ha precisato che l'attenzione deve essere rivolta anche a singole disposizioni della legge n. 675/1996 riguardanti le misure di sicurezza (art. 15), la conservazione, la pertinenza e la non eccedenza dei dati raccolti rispetto agli scopi perseguiti (art. 9, comma 1, lett. *d)*), le procedure e le modalità volte a fornire agli interessati le informazioni dovute (art. 10), nonché, in caso di comunicazione e diffusione, alle singole disposizioni diverse a seconda della natura dei soggetti che intendono procedere alla comunicazione o alla diffusione.

4.18. Accesso ai centri storici.

Per quanto riguarda l'accesso ai centri storici, è stata segnalata l'esigenza generale di non utilizzare impropriamente i dati acquisiti dalle amministrazioni pubbliche per regolare gli accessi, in particolare i dati relativi allo stato di salute dei titolari di permessi di accesso.

In un caso specifico (ove un'Amministrazione comunale ha preteso l'esposizione sui contrassegni necessari per l'accesso delle generalità dell'intestatario dell'autovettura) sono state richieste al Comune ulteriori informazioni, richiamando il principio in base al quale i dati trattati dalle pubbliche amministrazioni devono essere pertinenti e non eccedenti rispetto alle finalità perseguite, principio che costituisce applicazione dei criteri generali di ragionevolezza e proporzionalità.

Ciò nella consapevolezza, che ha ispirato altri pareri forniti dall'Autorità, che le esposizioni dell'immagine e dei dati delle persone, non necessarie né correlate allo svolgimento di funzioni pubbliche, favoriscono interferenze che contribuiscono a limitare la sfera di effettiva autodeterminazione del singolo.

4.19. Trasferimento di dati all'estero.

Per essere incisiva, la protezione dei dati personali non può trascurare il fenomeno della circolazione transfrontaliera dei dati.

Questo profilo ha occupato un posto centrale sia nella Convenzione del Consiglio d'Europa, sia nella direttiva comunitaria n. 95/46/CE.

La Convenzione n. 108 del 1981, intesa a "garantire nel territorio degli Stati contraenti, ad ogni persona fisica, indipendentemente dalla sua nazionalità e dalla sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, con particolare riferimento al diritto alla vita privata, in relazione alla elaborazione automatica dei dati a carattere personale che lo riguardano" (art. 1), si occupa del flusso transfrontaliero dei dati, prevedendo, da un lato, la definizione in ciascun Paese di un sistema normativo quanto più possibile uniforme, in modo da ridurre il pericolo di abusi nell'utilizzazione di tali flussi e la conseguente elusione delle rispettive legislazioni nazionali. D'altro lato, si è proibito o sottoposto ad una autorizzazione speciale, salve eccezioni espressamente stabilite, il flusso transfrontaliero dei dati a carattere personale destinato al territorio di un'altra parte contraente.

Con l'approvazione della direttiva comunitaria n. 95/46/CE, il legislatore comunitario ha dettato regole e criteri uniformi per la protezione dei dati nel territorio comunitario, al fine di evitare che la disciplina comune possa essere elusa dal mero spostamento fisico dell'attività disciplinata nella direttiva. Il capo IV della direttiva è interamente dedicato al trasferimento dei dati verso Paesi terzi.

In particolare l'art. 28 fissa un principio importante secondo cui il trasferimento dei dati personali è consentito soltanto se il Paese terzo garantisce un livello di protezione "adeguato". La Commissione Europea svolge un ruolo centrale nella valutazione sull'adeguatezza del livello di tutela esistente negli Stati membri.

L'art. 26 della direttiva individua le condizioni in base alle quali il principio dell'adeguatezza può trovare eccezioni. In tali casi (esistenza del consenso dell'interessato, conclusione o esecuzione di un contratto, salvaguardia di interessi pubblici; utilizzo di informazioni estraibili da un elenco pubblico o accessibile al pubblico), il trasferimento di dati può essere consentito verso un Paese che non garantisce una tutela adeguata.

Lo Stato deve informare sia la Commissione CE sia gli altri Stati membri sulle autorizzazioni in deroga concesse, e deve uniformarsi alle decisioni che la Commissione può assumere.

Per tale ultimo aspetto, è stata segnalata l'esigenza di perfezionare il modello procedimentale necessario agli Stati membri per conformarsi alle decisioni demandate alla Commissione.

Le disposizioni comunitarie in materia, definite dalla stessa direttiva come inderogabili, sono state recepite nella legge n. 675/1996 all'art. 28, il quale attua il principio dell'adeguatezza ma, al tempo stesso, prevede in termini più garantisti il divieto di trasferimento dei dati "sensibili" e di alcuni dati di carattere giudiziario per il caso in cui il Paese destinatario non assicuri un grado di tutela pari a quello assicurato dalla normativa nazionale.

In tal modo, è stata assicurata una valutazione differenziata in base alla tipologia dei dati da trasferire ed in base al Paese di destinazione.

Il Garante, anche in risposta ad alcuni quesiti formulati da parte di titolari del trattamento, ha fornito indicazioni e suggerimenti allo scopo di semplificare anche in tema di flussi transfrontalieri l'applicazione della legge.

E' stato, anzitutto, evidenziato che la legge (art. 26) non prevede alcuna notificazione qualora il trasferimento di dati all'estero riguarda dati che si riferiscono a persone giuridiche pubbliche o private, enti o associazioni, ovvero nel caso in cui (art. 28, comma 1) il trasferimento di dati personali è diretto unicamente verso Paesi appartenenti all'Unione Europea, purché non si tratti di dati "sensibili" o di carattere giudiziario.

La notificazione è invece necessaria nel caso in cui i dati personali siano trasmessi verso un Paese non appartenente all'Unione Europea; in tal caso, il trasferimento può avvenire dopo 15 giorni dalla data di notifica.

Qualora si intendono trasferire all'estero dati sensibili o relativi a provvedimenti giudiziari a carico dell'interessato, è necessario notificare la circostanza al Garante e attendere 20 giorni prima di effettuare la comunicazione dei dati, indipendentemente dal fatto che lo Stato di destinazione sia appartenente o meno all'Unione Europea.

L'Autorità ha peraltro sottolineato, al pari di quanto indicato nella direttiva europea 95/46/CE, che il trasferimento di dati all'estero è comunque consentito laddove ricorra taluno dei presupposti indicato dall'art. 28, comma 4, (ad esempio, qualora l'interessato abbia espresso il proprio consenso al trasferimento, oppure quando tale operazione sia necessaria per eseguire obblighi derivanti da un contratto di cui sia parte l'interessato).

La notificazione del trasferimento dei dati può essere effettuata utilizzando il modello previsto per la notificazione "generale", ed è possibile dichiarare in un unico contesto l'intero complesso delle attività di trasferimento. La notificazione dovrà essere annotata a cura del Garante in un'apposita sezione del registro dei trattamenti.

Il Garante ha più volte precisato che il trasferimento può essere vietato a seguito di una concreta valutazione che tiene conto delle modalità di trasferimento, dei trattamenti previsti oltre frontiera, delle relative finalità, della natura dei dati e delle misure di sicurezza adottate.

E' opportuno evidenziare che l'attuale disciplina in materia di trasferimento di dati, analogamente a quanto accadrà per molti settori interessati dalla protezione dei dati, subirà importanti integrazioni con l'emanazione dei decreti delegati, in particolare per ciò che riguarda l'individuazione delle modalità di applicazione della disciplina sulla protezione dei dati ai servizi di comunicazione e di informazione offerti per via telematica (art. 1, comma 1, lett. *n)* della legge n. 676/1996).

Il decreto delegato dovrebbe interessare, in qualche modo, anche il complesso flusso di dati in ambito *Internet*.

Avvalendosi dell'indicazione contenuta nella direttiva - quadro (considerando n. 47), l'Italia sarà il primo Paese europeo ad aver emanato una disposizione di legge che prende atto della necessità di dover modulare, anche in rapporto ad *Internet*, la normativa sulla protezione dei dati.

Nell'attesa di un quadro più chiaro sul piano internazionale, il principio che sta maturando è quello di garantire il rispetto della *privacy* nell'ambito delle reti aperte attraverso una strategia diversificata e globale, consistente, tra l'altro, in:

— sviluppo di nuove tecnologie "pulite" che assicurino già sul piano tecnico elevati livelli di sicurezza e di protezione della *privacy;*

— strumenti di "autodifesa" da parte degli utenti, che permettano loro, sulla base di un'idonea informativa, di accertarsi del livello di sicurezza offerto dal fornitore di servizi cui si rivolgono;

— strumenti contrattuali e regole di autodisciplina adottate su impulso dei *provider;*

— cooperazione internazionale ed eventuale creazione di un nucleo circoscritto di regole giuridiche non soggette a rapida obsolescenza;

— diffusione della consapevolezza che *Internet*, per quanto in frenetica evoluzione e con capacità altamente diffusive, è pur sempre un *media* e, pertanto, agli abusi commessi in rete si possono applicare alcune norme riguardanti i comportamenti *off-line*.

Il decreto delegato potrà indicare soluzioni differenziate agli interrogativi esistenti sugli adempimenti, sui compiti e sulle responsabilità dei soggetti che operano quali fornitori di reti, di servizi, di accessi e di contenuti.

In tale ottica il Garante, oltre a partecipare attivamente nelle sedi internazionali competenti, si è attivato per organizzare nel prossimo 8/9 maggio un convegno internazionale da tenersi a Roma sul tema.

4.20. Raccolta di firme per iniziative referendarie.

Nei primi mesi di attività, sono pervenute alcune segnalazioni sulla diffusione di moduli per la raccolta di firme relative ad iniziative referendarie, nei quali è stata prospettata la possibilità di utilizzare e di divulgare i dati acquisiti anche al fine dell'invio di proposte ed informazioni commerciali, scientifiche, campioni gratuiti di prodotti ed omaggi, sondaggi di opinione.

La raccolta e l'utilizzazione di dati personali connesse all'esercizio di un diritto politico fondamentale, come la sottoscrizione di richieste referendarie, devono essere del tutto distinte dai trattamenti delle stesse informazioni per ulteriori finalità di carattere commerciale o pubblicitario.

Mentre nel primo caso non è richiesto alcun particolare adempimento ai sensi della legge n. 675/1996, in quanto sulla base delle disposizioni vigenti i promotori del referendum sono tenuti a raccogliere i dati personali dei sottoscrittori e a darne comunicazione agli organi preposti alla verifica della regolarità delle richieste (non essendo necessario un consenso ulteriore rispetto alla sottoscrizione), nella seconda ipotesi il

Comitato avrebbe dovuto acquisire il consenso dei cittadini elettori, dando ad essi un'ampia informazione sugli specifici aspetti dei successivi trattamenti dei dati non collegati alle procedure referendarie.

Il cittadino non deve sentirsi o essere costretto, per partecipare alla presentazione di un referendum che sente di condividere, ad autorizzare un trattamento "automatico" dei suoi dati personali anche per finalità non strettamente collegate alle attività referendarie.

Sulla base di queste considerazioni, il Garante, a seguito dei chiarimenti forniti dai rappresentanti dei Comitati promotori del referendum, ha adottato a fine luglio un provvedimento con il quale ha invitato i Comitati stessi a separare dalla sottoscrizione necessaria per la richiesta referendaria la parte relativa alla dichiarazione del consenso per l'utilizzazione dei dati a fini diversi da quelli connessi all'iniziativa, oppure ad astenersi da tali richieste.

Inoltre, l'Autorità ha segnalato ai Comitati di astenersi dal compiere qualsiasi operazione di trattamento al di fuori di quanto richiesto dalla legge per le iniziative referendarie, e a fornire ai sottoscrittori un'informativa rispondente ai princìpi dalla legge n. 675/1996 (ad esempio, attraverso la lettura di un foglio disponibile presso gli uffici di raccolta delle firme), nonché un'indicazione sulla circostanza che la manifestazione di consenso riprodotta nel frontespizio dei moduli in distribuzione era da intendersi priva di ogni effetto.

4.21. Accertamenti e ispezioni.

Analogamente a quanto previsto per altre autorità di garanzia, il Garante può, nello svolgimento dei propri compiti, chiedere a chiunque di esibire documenti e di fornire informazioni, ad esempio con una richiesta scritta al titolare o al responsabile del trattamento o a terzi (art. 32, comma 1, legge n. 675).

La richiesta determina una soggezione del destinatario. In caso di inottemperanza, il Garante può applicare una sanzione pecuniaria e può procedere a controlli d'ufficio per appurare le circostanze oggetto della mancata verifica. Al Garante non può essere opposto il segreto professionale o d'ufficio, salvo il segreto professionale del giornalista per ciò che attiene alla fonte della notizia.

Nei casi di necessità, ai fini del controllo delle disposizioni in materia di trattamento dei dati, il Garante può disporre accessi alle banche dati o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento, o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo, avvalendosi, se necessario, della collaborazione di altri organi dello Stato.

L'eventuale accesso da parte del Garante, ovvero le ispezioni e le verifiche *in loco*, sono state delimitate e circoscritte dalle norme contenute nel richiamato articolo 32. In primo luogo, è necessaria un'autorizzazione preventiva concessa dal Presidente del tribunale competente per territorio in relazione al luogo dell'accertamento.

Le modalità di accesso e di verifica sono state precisate nel regolamento di disciplina dell'organizzazione dell'Ufficio del Garante, in corso di pubblicazione. In particolare, nel provvedimento sono stati disciplinati alcuni aspetti fra i quali assume rilievo la garanzia dell'inviolabilità del domicilio, che la legge ha individuato nell'autorizzazione del Presidente del tribunale, e che viene concettualmente meno quando l'accesso

o la verifica avvenga su richiesta o con il pieno consenso del soggetto presso il cui domicilio avviene l'accesso o la verifica. Si è ritenuto che il beneficiario del bene "domicilio", costituzionalmente garantito e tutelato, possa liberamente disporne attraverso un assenso che deve essere scritto ed informato, rendendo così superflua l'acquisizione dell'autorizzazione giudiziaria, tenuto anche conto dei tempi a volte lunghi che essa può richiedere.

Le altre norme contenute nel provvedimento regolamentare, concernenti le modalità di svolgimento degli accertamenti, si caratterizzano per la garanzia della correttezza e, al tempo stesso, dell'efficacia, tenendo conto anche, per ciò che riguarda i limiti temporali, della disciplina delle perquisizioni domiciliari prevista dall'articolo 251 del codice di procedura penale.

L'articolo 32, comma 4, della legge chiarisce che i destinatari degli accertamenti non possono opporre un rifiuto e sono tenuti a prestare quel minimo di attività richiesta affinché l'accesso, l'ispezione o la verifica abbiano luogo.

L'attività del Garante, in questa prima fase di applicazione della disciplina sulla protezione dei dati personali, ha curato gli adempimenti necessari per verificare le eventuali inosservanze di legge, ma ha dedicato, contemporaneamente, particolare attenzione all'informazione e alla divulgazione delle novità introdotte dalla nuova disciplina legislativa, curando, in particolare, il rapporto con i singoli cittadini e fornendo loro chiarimenti e pareri, anche telefonici, in ordine alle problematiche emerse nel corso di questo primo periodo di applicazione della legge.

Non può, tuttavia, non essere evidenziato che questa Autorità ha ritenuto prioritario l'impegno nell'attività di completamento di alcuni importanti adempimenti necessari per l'attuazione della legge e in particolare della procedura per la notificazione e del rilascio delle autorizzazioni per il trattamento dei dati sensibili.

4.22. Schengen: Archivi N. S.I.S. e S.I.RE.N.E.

A seguito della decisione dell'Autorità di controllo comune Schengen del 12 dicembre 1997 di effettuare una verifica sulle misure di sicurezza adottate dagli uffici SIRENE, il Garante ha ricevuto dal Dipartimento di pubblica sicurezza un rapporto scritto sulle misure di sicurezza adottate dal N-SIS e dall'Ufficio SIRENE, e si è recato in visita presso gli uffici il 2 marzo 1998.

L'N-SIS ha segnalato di non aver incontrato particolari difficoltà nel conformarsi ai protocolli e alle procedure stabiliti dalle Parti contraenti ai sensi dell'articolo 92, par. 2, della Convenzione.

In ordine alle misure di sicurezza adottate, il Garante ha attentamente valutato gli aspetti della sicurezza fisica e logica delle strutture N-SIS e SIRENE, anche attraverso un rapporto scritto.

Delle risultanze dell'accesso il Garante ha riferito alla competente commissione parlamentare di controllo nel corso dell'audizione tenutasi il 12 marzo 1998, cui ha preso parte il Presidente del Garante.

Sulla base della verifica effettuata, il Garante ha suggerito all'Autorità di controllo comune di inserire nelle future linee-guida la possibilità di:

— effettuare il tracciamento di tutte le varie operazioni relative alla base dati N-SIS (numero di interrogazioni, frequenza, orario, tipi di dati consultati, ecc.);

— rafforzare le misure di sicurezza volte a garantire che l'accesso sia limitato effettivamente ai dati per i quali i singoli operatori sono abilitati, anche attraverso la modifica periodica delle *password*;

— utilizzare adeguatamente le statistiche dei tracciamenti al fine di individuare eventuali anomalie, specie in riferimento al numero delle interrogazioni;

— invitare gli N-SIS e gli Uffici SIRENE a presentare alle autorità di controllo nazionali un rapporto sulla sicurezza con cadenza periodica, ad esempio annuale.

Peraltro, già il Presidente del Garante era stato sentito dal Comitato parlamentare nel corso dell'audizione svoltasi il 5 giugno 1997. Tale audizione ha riguardato, in particolare, il tema del coordinamento legislativo tra le disposizioni esistenti in materia di protezione dei dati personali nella legge n. 675/1996 e le specifiche norme introdotte dalle leggi n. 121/1981 (recante nuovo ordinamento della Polizia di Stato) e n. 388/1993 (di ratifica della Convenzione di Shengen), nonché del raccordo con le pertinenti disposizioni delle Convenzioni EUROPOL e SID.

4.23. Trattamenti effettuati dal C.E.D del Dipartimento della pubblica sicurezza.

La particolare "sensibilità" dei dati raccolti dalle forze di polizia nello svolgimento dei compiti di tutela della sicurezza pubblica, prevenzione e repressione dei reati, ha indotto a suo tempo il legislatore ad intervenire per disciplinare la materia, con alcune norme che ne regolassero anzitutto le modalità e i limiti di raccolta e di elaborazione da parte del Centro elaborazione dati del Dipartimento della pubblica sicurezza del Ministero dell'interno ove i dati confluivano (legge 1 aprile 1981, n. 121).

Alle prime garanzie introdotte nel 1981, risultate poi superate anche alla luce del contesto internazionale, si aggiungono oggi le elevate misure di protezione previste dalla legge n. 675/1996, anche per ciò che riguarda i poteri di controllo attribuiti al Garante d'ufficio o su segnalazione dell'interessato.

Il sistema degli strumenti di controllo sui "dati di polizia" si presenta quindi articolato. A fianco dei poteri attribuiti al Garante (artt. 31 e 32 della legge n. 675) ed all'autorità giudiziaria, permane anche la facoltà, per il soggetto interessato, di esercitare le consentite verifiche sulla liceità e correttezza dei dati che lo riguardano attraverso una richiesta rivolta direttamente all'ufficio del Dipartimento della pubblica sicurezza responsabile degli archivi, secondo la procedura specificata nell'articolo 10 della legge 121/1981 citata.

Al riguardo, sulla base di diverse segnalazioni pervenute, il Garante è intervenuto presso il predetto ufficio per sottolineare la necessità dell'applicazione del citato articolo 10 nella sua corretta interpretazione, secondo la quale l'"accesso" dell'interessato non è subordinato a particolari situazioni legittimanti, quali la previa pendenza di un procedimento amministrativo o giurisdizionale.

Nella stessa occasione il Garante ha sottolineato la necessità che sia rispettato dall'ufficio competente il termine di venti giorni previsto dall'articolo 10 per il riscontro delle richieste, ovvero per la comunicazione al Garante della sussistenza di motivi ostativi al riscontro stesso.

4.24. Accertamenti presso servizi di informazione e di sicurezza.

Il Garante, sulla base delle richieste pervenute, ha proceduto ad alcuni accertamenti relativi a trattamenti di dati personali effettuati presso il SISDE, il SISMI e il CESIS.

Le verifiche si sono svolte il 25 ed il 26 febbraio 1998 presso le varie strutture interessate, e hanno riguardato otto cittadini richiedenti.

Il controllo si è svolto con la piena collaborazione degli organismi ed è stato preceduto da una nota con la quale il Garante si è pronunciato su alcuni quesiti relativi all'attività di *intelligence*.

Il Garante ha informato i cittadini interessati dell'esito della verifica con modalità rispettose dei criteri stabiliti dall'art. 32 della legge e che tengono conto sia dell'esigenza di rassicurare il cittadino circa l'assenza di violazione di legge sia della necessità di salvaguardare, al tempo stesso, la segretezza dei trattamenti oggetto di verifica.

Il Garante si è peraltro riservato di formulare al Governo alcune ulteriori osservazioni di ordine generale, tenendo conto anche delle disposizioni amministrative di settore che gli organismi di sicurezza hanno reso disponibili nell'ambito della collaborazione prestata.

PAGINA BIANCA

5. ATTIVITÀ COMUNITARIA E INTERNAZIONALE

5.1. Premessa.

A causa del processo di globalizzazione delle economie e delle culture in atto, ai trasferimenti di persone, beni e servizi da un Paese all'altro si affianca un altrettanto imponente flusso di informazioni contenenti dati personali. Per tale ragione, la dimensione internazionale è connaturata al tema della protezione dei dati e la regolamentazione dei trattamenti effettuati deve svilupparsi tenendo conto e cercando di dominare questi fenomeni.

La transnazionalità della materia risulta ancora più evidente se si considera l'enorme mole di transazioni, commerciali e non, fra operatori di diversa provenienza geografica, le quali presuppongono la conoscenza dei dati relativi ai soggetti interessati.

Una sfida di questa portata non può essere lasciata all'iniziativa di un solo Paese e richiede una stretta cooperazione internazionale, in particolare fra gli organismi impegnati nella protezione dei dati personali. È in quest'ottica di progressivo superamento dei confini nazionali che si collocano i principali strumenti elaborati in sede internazionale per fornire una risposta adeguata alle nuove sfide.

Nel corso degli anni Settanta ed Ottanta è emersa nei più importanti organismi internazionali la consapevolezza dell'importanza di intervenire nella materia, approntando un adeguato quadro normativo che vincolasse gli Stati ad uno *standard* comune di garanzie. Si è passati quindi dalle linee guida elaborate dall'OCSE all'adozione della Convenzione n. 108 del 1981 del Consiglio d'Europa e, quindi, alle direttive europee in materia di protezione dei dati personali (nn. 95/46 e 97/66).

Nella piena consapevolezza di tutto ciò, il Garante, fin dalla sua costituzione, ha voluto dedicare particolare impegno ai rapporti con gli organismi internazionali e con le altre autorità di garanzia, contribuendo anche all'elaborazione di diversi provvedimenti normativi internazionali.

5.2. La direttiva-quadro n. 95/46/CE.

La direttiva n. 95/46/CE ha rappresentato un'importante innovazione, sia sotto il profilo contenutistico, sia per il suo stesso porsi come fonte sovraordinata ai legislatori degli Stati membri e, per questo, in grado di delineare una disciplina comune in materia. Essa si fonda sulla considerazione che l'integrazione europea comporta necessariamente un aumento dei flussi di dati personali tra tutti i soggetti degli Stati membri, siano essi privati o pubblici: risulta dunque necessario superare i divari esistenti fra i diversi Paesi nella tutela accordata alle persone rispetto al trattamento dei dati, per evitare il costituirsi di gravi ostacoli alla libera circolazione.

Caratteristica principale della direttiva è quella di garantire una tutela della persona e della vita privata in quanto tali, anche indipendentemente dai rapporti contrattuali all'interno dei quali si trovi ad operare. Il legislatore comunitario ha voluto superare un'impostazione — propria, ad esempio, della normativa dettata a tutela del consumatore — in cui l'individuo è garantito solo relativamente ad una condizione soggettiva temporanea, ed ha inteso assolutizzare, in un certo qual modo, la protezione relativa al trattamento dei dati personali, pur nel rispetto delle esigenze della libera circolazione all'interno dello spazio comunitario.

Questa filosofia particolarmente avanzata è stata in parte all'origine del lungo *iter* di elaborazione della direttiva ed ha costituito un fattore di spinta decisivo per elevare la soglia di protezione accordata dalla legislazione dei diversi Paesi membri.

Il ritardo con cui è stata approvata la legge n. 675/1996 ha consentito all'Italia di recepire gran parte delle norme della direttiva e, per vari profili, anche di arricchire quanto in essa disposto, ponendosi come una delle legislazioni più avanzate nel panorama europeo in materia di protezione dei dati personali.

Inoltre, anche grazie allo strumento flessibile costituito dalle deleghe legislative contenute nella legge n. 676/1996, l'Italia continuerà a garantire agli altri Stati membri una protezione dei dati personali tale da rendere sicuri gli scambi con il nostro Paese, ed insieme potrà esercitare un ruolo di guida rispetto alle altre legislazioni nazionali, nonché alla futura produzione normativa comunitaria.

Il Garante ha operato in questa direzione attraverso un costante lavoro di promozione della conoscenza della nostra normativa negli altri Paesi della Comunità, favorendo lo scambio e il confronto con gli organi dei Paesi membri a vario titolo impegnati nella tutela dei dati personali.

L'Autorità, ai fini del controllo e dell'armonizzazione della normativa comunitaria in materia di tutela dei dati, partecipa ai lavori del Gruppo previsto dall'art. 29 della direttiva ed a quelli del Comitato disciplinato dall'art. 31. Quest'ultimo ha il compito di assistere la Commissione esprimendo pareri sui progetti di misure da adottare sottopostigli dalla Commissione stessa.

"Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" istituito dall'articolo 29 della direttiva, invece, ha carattere consultivo e indipendente, è composto dai rappresentanti di ciascuna delle autorità di controllo nazionale dei 15 Paesi che fanno parte dell'Unione europea e da un rappresentante della Commissione europea.

Il Gruppo è incaricato di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della direttiva, di formulare pareri sia sul livello di tutela nella Comunità e nei Paesi terzi sia sui codici di condotta elaborati a livello comunitario, nonché di consigliare la Commissione in merito ai progetti di modifica della direttiva, alle misure addizionali sul trattamento dei dati e a qualsiasi altro progetto di misure comunitarie che incidano sui diritti e sulle libertà delle persone fisiche con riguardo al trattamento dei dati personali.

Nel corso dei lavori fin qui svolti il Gruppo si è occupato, fra l'altro, dell'elaborazione degli archivi di analisi di Europol, del progetto di convenzione Eurodac e di quello sulla protezione degli interessi finanziari della Comunità.

Il Gruppo può inoltre formulare, di propria iniziativa, raccomandazioni su qualsiasi questione attinente alla materia. Fra quelle adottate si segnalano, per la particolare rilevanza, una raccomandazione recante norme in materia di protezione dei dati e di mezzi di comunicazione e due raccomandazioni concernenti la tutela della riservatezza e dell'anonimato degli utenti di Internet.

Il Garante partecipa a tale Gruppo di lavoro nella persona del prof. Stefano Rodotà (il quale è stato recentemente eletto quale vice presidente del Gruppo stesso), del prof. Ugo De Siervo e del dott. Giovanni Buttarelli.

5.3. La direttiva n. 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni.

La Direttiva 97/66/CE del 15 dicembre 1997" sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni", è stata elaborata a seguito di due risoluzioni con le quali il Parlamento europeo, nel 1986-1988, chiese alla Commissione europea di presentare proposte specifiche nella materia delle telecomunicazioni, tenendo conto della prospettiva dell'apertura dei mercati, al fine di assicurare un livello di riservatezza dei dati personali adeguato alla modernità dei servizi.

La Commissione formulò la sua proposta nel 1990. Successivamente, però, la contestualità dei lavori sulla direttiva n. 95/46/CE ha finito per allungarne i tempi di approfondimento e di discussione.

Nel giugno 1994, dopo il vertice di Edimburgo, la Commissione ha presentato una versione modificata della proposta, semplificandola alla luce del principio di sussidiarietà.

Nel 1995, sotto la presidenza spagnola, il Gruppo ha ipotizzato alcune modifiche alla luce della liberalizzazione dei servizi di telecomunicazione, ed è solo dal 1996 che il Data Protection Working Group ha esaminato la proposta nei dettagli.

La direttiva è apparsa necessaria perché le reti digitali di telecomunicazione permettono la trasmissione della voce, dei dati, delle immagini, dei testi e dei suoni in forma di servizi del tutto nuovi. La digitalizzazione delle reti favorisce lo sviluppo di attività e di funzioni "intelligenti" che incidono in termini nuovi sulla sfera della vita privata e impongono, così, norme più specifiche di quelle contenute nella 95/46/CE, al fine di assicurare un uso corretto dei dati e dei servizi e di garantire, che le reti digitali siano accettate socialmente (basti pensare, ad esempio, al *video-on-demand* e alla *interactive television*).

Ben si può, quindi, definire la direttiva come una direttiva-figlia, visto che essa precisa e integra la direttiva n. 95/46/CE.

Uno dei punti più dibattuti è stato quello riguardante i servizi coinvolti (analogici e/o digitali). La soluzione di compromesso che è stata adottata consente, oggi, di applicare la direttiva a qualunque servizio (via ISDN; reti digitali mobili; reti analogiche ecc.) e questa applicazione non sarà condizionata da valutazioni di economicità. Gli Stati membri potranno unicamente, informando la Commissione, non applicare alle reti analogiche gli articoli riguardanti la presentazione dell'identificazione della linea chiamante e il trasferimento automatico di chiamata,

quando questa applicazione, considerato il minor livello tecnologico delle reti analogiche, non sia tecnicamente possibile o comporti un impegno economico sproporzionato.

Si può affermare che con la direttiva in esame l'impianto comunitario in materia sia stato in grande parte realizzato.

Venendo all'ambito di applicazione, si deve affermare che la direttiva reca una clausola che esclude le attività che ricadono fuori dal diritto comunitario; parimenti, essa non sarà applicabile al *radio-and television broadcasting*, sempreché queste attività siano effettuate nel senso tradizionale del termine.

I nuovi servizi *point-to-point* quali l'*interactive television* e il *video-on-demand* sono disciplinati dalla direttiva. Inoltre essa si occupa di sicurezza e riservatezza delle telecomunicazioni, dati sul traffico e sulla fatturazione, identificazione del numero chiamante, trasferimento automatico della chiamata e chiamate indesiderate, elenchi degli abbonati.

L'aspetto principale della direttiva è relativo al trattamento dei dati inerente il traffico e la fatturazione.

Il delicato argomento concernente la fatturazione dettagliata è stato risolto riconoscendo agli abbonati il diritto di non ricevere questo genere di servizio mentre, per coloro che la ricevono, gli Stati membri devono garantire che gli abbonati e utenti dispongano di sufficienti modalità alternative per le comunicazioni o per i pagamenti (art. 7, par. 1 e 2).

I dati sul traffico dovranno essere cancellati o resi anonimi al termine della chiamata, ferma restando la possibilità di trattare ulteriormente alcuni dati a fini di fatturazione per l'abbonato e dei pagamenti di interconnessione. Sarà anche possibile trattare i medesimi dati per fini di commercializzazione dei servizi del fornitore qualora vi sia il consenso dell'abbonato. Per quest'ultima finalità, quindi, una mera soluzione di *opt-out* quindi, non è stata ritenuta sufficiente.

Quanto alla forma del consenso, varranno le disposizioni attuative della direttiva quadro-generale che richiedono una manifestazione di volontà libera, specifica ed informata.

Sull'argomento occorre però aggiungere che, in deroga a quanto disposto per la commercializzazione dei servizi di telecomunicazione, il consenso non è richiesto per il trattamento già in corso alla data di entrata in vigore delle disposizioni nazionali di attuazione.

Uno degli aspetti più rilevanti concerne il meccanismo da tempo introdotto in altri Stati europei, di identificazione della linea chiamante, reso possibile dalla tecnologia digitale. In base a tale sistema, si è contemperata la scelta di restare anonimi per mezzo della soppressione del loro numero identificativo con il concorrente diritto a non essere disturbati da singole chiamate.

Altre disposizioni significative attengono, infine, all'inclusione dei nominativi degli abbonati negli elenchi, alle chiamate pubblicitarie indesiderate, alle chiamate moleste e alla tutela della vita privata degli utenti chiamanti e degli abbonati chiamati, in caso di fatturazioni dettagliate. La direttiva doveva essere recepita entro il 24 ottobre 1998, e cioè entro lo stesso termine previsto dalla direttiva quadro-generale (art. 16, par. 1). Gli Stati membri possono peraltro conformarsi all'articolo 5 sulla "riservatezza delle comunicazioni" al più tardi e non oltre il 24 ottobre 2000.

L'Italia ha attuato la direttiva con il citato decreto legislativo del 9 aprile 1998 intervenuto durante la stampa della presente relazione.

5.4. La cooperazione europea nei settori giustizia e affari interni.

Nell'ambito della collaborazione fra Paesi europei in materia di giustizia e affari interni (c.d. terzo pilastro del Trattato di Maastricht) sono state elaborate o sono in corso di elaborazione diverse convenzioni.

Si fa riferimento, in particolare, a quelle relative all'istituzione e al funzionamento di un Ufficio europeo di polizia (EUROPOL), al Sistema di informazione doganale (SID), alla rilevazione delle impronte digitali dei richiedenti asilo (EURODAC) nonché alle forme di cooperazione previste dalla convenzione di applicazione dell'Accordo di Schengen.

Ogni Convenzione o progetto di Convenzione — di cui si parlerà più diffusamente avanti — prevede l'istituzione di un sistema automatizzato di elaborazione dei dati, nonché flussi di dati scambiati con altri mezzi automatizzati e cartacei.

Per ciascuno di questi trattamenti di dati svolti per finalità di giustizia o di ordine e sicurezza pubblica vengono definite le misure necessarie per garantire la protezione dei dati, secondo norme spesso collegate alla Convenzione n. 108 citata e alla Raccomandazione N.R. (87)15 del Consiglio d'Europa.

Su proposta italiana, valutata con favore dal Garante, il Consiglio dei ministri europeo giustizia-affari interni discuterà nel mese di maggio un documento volto ad aprire una riflessione sull'incremento degli accordi e delle autorità comuni di controllo previste in materia di dati, anche al fine di ridurre le eventuali incongruenze o duplicazioni e di favorire una maggiore omogeneità della tutela.

Le Convenzioni prevedono inoltre l'attribuzione di competenze in materia di protezione dei dati ad autorità nazionali di controllo; allo stesso tempo individuano un'autorità comune cui sono affidati compiti di controllo su determinati archivi.

5.4.1. Schengen.

In tale contesto assume particolare rilevanza l'Accordo di Schengen, firmato il 14 giugno 1985, nonché la successiva Convenzione di applicazione firmata nel 1990 e resa esecutiva in Italia con la legge n. 388/1993.

Le finalità dell'Accordo, reso operativo in Italia il 26 ottobre 1997, sono quelle di creare uno spazio comune per la libera circolazione delle persone e delle merci, sopprimendo progressivamente i controlli alle frontiere. La Convenzione del 1990 disciplina più specificamente le necessarie forme di cooperazione di polizia, doganale e giudiziaria, e istituisce il Sistema d'informazione Schengen (SIS), attraverso il quale la predetta cooperazione trova un momento applicativo di estrema importanza.

Per un corretto funzionamento del SIS, la Convenzione presuppone che sia garantito un livello di protezione di dati corrispondente almeno a quello previsto dalla Convenzione n. 108 del Consiglio d'Europa e dalla Raccomandazione N/R(87)15. A tal fine è stata istituita un'Autorità di controllo comune (ACC) incaricata di vigilare sulla corretta applicazione delle disposizioni della Convenzione e, più in particolare, sul rispetto delle disposizioni a tutela del trattamento di dati personali.

La Convenzione prevede che, oltre al Sistema d'informazione comune, vengano istituiti archivi nazionali (N-SIS) per la cui vigilanza sono competenti le autorità nazionali di controllo in materia di prote-

zione dei dati. Agli archivi N-SIS si affiancano gli uffici SIRENE, i quali gestiscono informazioni supplementari relative alle segnalazioni da inserire negli archivi N-SIS e nel SIS.

La legge n. 388/1993 citata e la legge n. 675/1996 individuano il Garante quale autorità nazionale di controllo per l'Italia. Ad esso è demandato il compito "di esercitare un controllo indipendente dell'archivio della sezione nazionale del Sistema d'Informazione Schengen e di verificare che l'elaborazione e l'utilizzazione dei dati inseriti non leda i diritti della persona interessata" (art. 114 della Convenzione). In tale veste, la medesima Autorità è chiamata a far parte dell'Autorità comune di controllo (ACC).

Fra le attività di maggior rilievo dell'ACC, alle cui riunioni il Garante ha partecipato attivamente sin dalla sua costituzione e con continuità, rientra sicuramente quella di "elaborare proposte armonizzate allo scopo di trovare soluzioni comuni ai problemi esistenti" (art. 115, comma 4). In tale cornice, vi rientrano i pareri formulati dall'ACC nel corso del 1997, che si riportano per intero in allegato.

Sino al luglio del 1997, l'Italia ha partecipato ai lavori dell'ACC in veste di osservatore, mentre successivamente ha assunto lo *status* di membro a pieno titolo.

Conformemente agli auspici espressi a Bruxelles, il Garante ha convenuto di allegare alla propria relazione annuale il Primo Rapporto (marzo 1995-marzo 1997).

Si differisce invece la pubblicazione dello schema di relazione annuale relativa al periodo marzo 1997-marzo 1998 (nella quale si prende atto dell'entrata in vigore della legge italiana avvenuta rispetto a Schengen, nel gennaio del 1997), non avendo ancora l'ACC formalizzato la sua approvazione.

L'ACC ha deliberato il 12 dicembre 1997 di curare la pubblicazione di un opuscolo esplicativo del diritto di accesso ai dati da parte delle persone segnalate nel SIS. Il testo, al quale verranno allegati gli estremi delle autorità nazionali, verrà distribuito presso i valichi delle frontiere esterne Schengen, per il tramite delle medesime autorità e, quindi, del Garante.

Giova peraltro aggiungere che nel programma di azione approvato per il primo semestre 1998 è stata ribadita l'intenzione di rafforzare il ruolo dell'ACC nella struttura Schengen, in difesa dei princìpi della protezione dei dati. Particolare attenzione verrà dedicata all'attuazione da parte degli organi esecutivi Schengen delle raccomandazioni formulate dall'ACC, in modo specifico per quanto riguarda la sicurezza del C.SIS (vedi allegato).

5.4.2. Europol.

L'istituzione dell'Ufficio europeo di polizia (Europol) — il cui funzionamento è regolato dalla convenzione firmata a Bruxelles nel luglio 1996, la cui legge di ratifica è stata approvata di recente dal Parlamento — mira a favorire la collaborazione fra le forze di polizia nel prevenire e combattere il terrorismo, il traffico illecito di stupefacenti e altre gravi forme di criminalità internazionale.

Il fulcro di questa attività di cooperazione è costituito dallo scambio e dall'elaborazione di informazioni fra gli organi incaricati della tutela della sicurezza e dell'ordine pubblico.

La Convenzione contiene diverse disposizioni a tutela dei dati personali e stabilisce che ciascuno Stato membro istituisca un'autorità di controllo nazionale, incaricata di vigilare sulla liceità delle operazioni di consultazione e trasmissione di dati all'Europol effettuate dallo Stato

stesso (art. 23) nonché un'Autorità di controllo comune, composta dai rappresentanti di tutti i Paesi membri (art. 24), avente il compito di verificare la liceità dei trattamenti effettuati dall'Europol.

Il Garante è intervenuto nella sua qualità di autorità indipendente per il controllo sui trattamenti di dati personali, provvedendo alla realizzazione di tutti gli adempimenti di sua competenza diretti a garantire una pronta applicazione della Convenzione: in particolare, ha partecipato all'elaborazione del regolamento interno dell'autorità di controllo comune — la cui adozione costituisce una precondizione per l'inizio delle attività dell'Europol (art. 45) — e ha preso parte, nel corso del 1997 e dei primi mesi del 1998, all'attività dell'apposito Gruppo di lavoro composto dai rappresentanti degli analoghi organismi della Comunità Europea.

5.4.3. Sistema Informativo Doganale.

Il 26 luglio 1995 è stata firmata la Convenzione fra gli Stati membri dell'Unione Europea relativa all'utilizzazione di tecnologie per scopi doganali (sistema informativo doganale - SID), la cui ratifica è attualmente all'esame del Parlamento. Il SID intende essere uno strumento per la lotta contro le frodi comunitarie e un ausilio alla prevenzione e alla repressione di reati in materia di circolazione delle merci e di traffico di stupefacenti, consentendo maggiore rapidità nello scambio delle informazioni utili al riguardo.

Particolare rilevanza è stata data al rispetto dei princìpi sanciti dalla Convenzione n. 108 di Strasburgo e alla Raccomandazione N. R(87)15 sui dati di polizia.

Come per la Convenzione Europol, le norme nazionali volte a definire il quadro interno di protezione dei dati saranno previste dai decreti delegati di cui dalla legge n. 676/1996, il che dovrebbe favorire un'elaborazione organica anche attraverso l'inclusione in un unico veicolo normativo volto a semplificare la consultazione delle future regole.

5.4.4. Eurodac.

Un recente progetto di Convenzione, basato sull'articolo 15 della Convenzione di Dublino relativa alla determinazione dello Stato competente per l'esame delle richieste d'asilo, è in corso di elaborazione presso l'apposito gruppo di lavoro del Consiglio dell'Unione europea. La Convenzione contempla l'istituzione di un sistema per la raccolta, la memorizzazione, il confronto e lo scambio di dati relativi alle impronte digitali di soggetti che presentino richiesta di asilo in uno degli Stati membri (EURODAC).

Il sistema prevede una banca dati centralizzata contenente tutte le impronte digitali dei richiedenti, con una serie di garanzie relative, ad esempio, alla cancellazione di tali dati una volta trascorso un periodo di 10 anni (o nel momento in cui un soggetto divenga cittadino di uno degli Stati membri), nonché al diritto di accesso da parte degli interessati.

Anche in questo caso si fa riferimento al rispetto dei princìpi sanciti dalla più volte citata Convenzione n. 108, sul quale dovranno vigilare le autorità nazionali competenti per la protezione dei dati personali. Il controllo esercitato da tali autorità si applicherà in modo particolare alla legittimità della memorizzazione e della trasmissione dei dati.

Nell'ambito delle riflessioni avviate dalla citata iniziativa in atto presso il Consiglio GAI (v. par. 5.4.), il Garante si è interrogato circa il rischio che su questo, e sugli altri strumenti sopra ricordati, in corso di

adozione o comunque di applicazione, si creino distinti "corpi normativi" della protezione dei dati, e conseguentemente regole diverse per la tutela sostanziale e procedimentale dei diritti della personalità.

A questo proposito, è stata richiamata l'attenzione — da ultimo nell'audizione svoltasi davanti al Comitato parlamentare di controllo sull'attuazione e il funzionamento di Schengen tenutasi il 12 marzo c.a. — sull'opportunità di assicurare un maggiore coordinamento nelle predette iniziative, come del resto auspicato dal Parlamento europeo nella risoluzione sul funzionamento e sull'avvenire di Schengen n. A4-0014/97 (punto 16).

5.5. Consiglio d'Europa.

Il Consiglio d'Europa è stato uno dei primi organismi internazionali a dedicare specifiche iniziative alla tutela delle persone rispetto al trattamento dei dati personali. Al suo interno, infatti, dopo l'adozione di una serie di provvedimenti di carattere settoriale, nel 1981 si è giunti all'approvazione della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, che costituisce uno dei documenti fondamentali in tema di protezione dati, e la base su cui sono state costruite le successive regolamentazioni in ambito comunitario e nazionale. In seguito all'approvazione della legge n. 675/1996 è stato possibile depositare lo strumento di ratifica il 29 marzo 1997, il che ha permesso di far entrare in vigore la Convenzione per l'Italia lo scorso 1 luglio.

L'attività del Consiglio d'Europa in materia non si è però esaurita con l'approvazione della Convenzione, ed è proseguita in un'intensa attività di elaborazione della normativa di settore nonché nell'aggiornamento di quella preesistente.

Il Garante, sin dalla sua costituzione, ha preso parte alle diverse attività del Consiglio d'Europa, dando un contributo significativo all'elaborazione dei diversi testi attualmente in discussione. In particolare, ha rappresentato l'Italia in seno al Comitato consultivo della convenzione n. 108 (T-PD), al Gruppo di progetto sulla protezione dati (CJ-PD) e al Gruppo di lavoro sulle nuove tecnologie (GT-15).

Il T-PD ha il compito di proporre e discutere eventuali modifiche alla Convenzione n. 108, e di pronunciarsi sui problemi applicativi. Attualmente, al suo interno sono in discussione l'adesione della Comunità europea alla Convenzione n. 108, alcune modifiche della Convenzione concernenti l'estensione dell'applicabilità agli archivi cartacei, alle persone giuridiche nonché la previsione obbligatoria di un'Autorità indipendente di controllo.

Il CJ-PD si occupa dell'elaborazione dei progetti di raccomandazioni in materia di trattamento di dati personali. Durante il 1997, è stato impegnato nella predisposizione di una raccomandazione sui trattamenti di dati personali a fini assicurativi, nell'elaborazione di un codice di condotta per gli utilizzatori di *Internet*, e nella collaborazione con altri comitati costituiti all'interno del Consiglio d'Europa impegnati nell'elaborazione di raccomandazioni che hanno riflessi sul trattamento dei dati personali.

Il GT-15 è, poi, un gruppo di lavoro ristretto costituito all'interno del CJ-PD, che si occupa specificamente della protezione delle persone rispetto al trattamento dei dati personali effettuato attraverso nuove tecnologie, quali ad esempio *Internet*, le carte a microprocessore e la videosorveglianza.

Anche in vista dell'emanazione dei decreti legislativi previsti dalla legge n. 676/1996, è importante ricordare che nel corso del 1997 il Consiglio d'Europa ha approvato due raccomandazioni relative al trattamento dei dati sanitari e di quelli utilizzati a fini statistici.

5.6. Ocse.

L'Organizzazione per la cooperazione e lo sviluppo economico (Ocse) ha avviato un'importante attività per favorire lo sviluppo del commercio elettronico mondiale e per eliminare le barriere esistenti nei diversi settori ed ambiti interessati, che vanno dalla fiscalità alla tutela del consumatore. La protezione della riservatezza è stata identificata come uno dei temi prioritari ai fini della realizzazione di tale obiettivo. La Conferenza tenutasi a Turku (Finlandia) dal 19 al 21 novembre 1997 ha permesso di definire i princìpi generali e l'identificazione delle tipologie d'intervento ritenute più idonee (ad esempio, delle aree dove occorre un intervento governativo, dove è sufficiente una autoregolamentazione degli operatori del settore, dove è necessario un intervento congiunto - come ad esempio - la *privacy*). In preparazione della Conferenza dei Ministri Ocse che si terrà ad Ottawa nel prossimo mese di ottobre, intitolata "Un mondo senza confini - realizzare le potenzialità del commercio elettronico globale", un gruppo di lavoro specializzato ha affrontato il tema della protezione della *privacy*. Nel mese di febbraio il Presidente del Garante ha svolto la relazione che ha tracciato il quadro generale di riferimento dal punto di vista giuridico.

5.7. Collaborazione con altre autorità di garanzia.

Al di là degli obblighi di collaborazione con le altre autorità di controllo nascenti dalla Convenzione n. 108 e da altri atti internazionali e comunitari, il Garante mantiene stretti contatti con tali Autorità al fine di mantenere in vita un proficuo scambio di esigenze che rifluiscono anche nelle conferenze europee e mondiali organizzate con continuità, rispettivamente, nella primavera e nell'autunno di ogni anno.

A parte la partecipazione alle periodiche conferenze organizzate a livello europeo, il Garante ha promosso un seminario per la prima settimana di giugno, al quale ha invitato a partecipare i rappresentanti di tutti i Paesi europei. Il seminario servirà a fare il punto sulle scelte effettuate in ogni Paese rispetto alla direttiva europea, nell'ambito del processo di recepimento della direttiva che registra vari ritardi ma che deve concludersi entro il 29 ottobre 1998.

5.8. Convegni ed incontri internazionali.

Oltre all'attività condotta nelle sedi "istituzionali" prima richiamate, l'Ufficio del Garante ha partecipato a vari convegni e incontri internazionali che, per la loro rilevanza e per la natura dei temi trattati, costituivano occasioni importanti per uno scambio di opinioni ed un aggiornamento puntuale.

In tali sedi il Garante ha avuto modo di portare un proprio contributo alla discussione.

Tra le varie iniziative possono essere citate le seguenti:

- *22nd Meeting of the International Working Group on Data Protection in Telecommunications - Berlin*, 2 September 1997 (*Internet*; crittografia; legislazione in materia di telecomunicazioni).
- *19th International Conference of Privacy Data Protection Commissioners - Brussels*, 17-19 September 1997 (Flussi transfrontalieri; attuazione della Direttiva nei vari paesi membri dell'UE; prospettive USA; Schengen, Europol, Interpol; sviluppi recenti nel campo delle telecomunicazioni; anonimato; protezione della *privacy* e libertà di espressione).
- *International Conference on Privacy - Montreal, 21-26 September 1997.* (Moltissimi i temi affrontati; fra i principali: *privacy*; cifratura; diritto delle telecomunicazioni; *Internet* e nuove tecnologie).
- *The Protection of Personal Data Held by the Administration or in the Police Sector - Prague*, 18-19 December 1997 (protezione di dati e attività di polizia).
- *The Legislation of Personal Data Protection in the European Union and in Hungary - 28-29 January 1998* (Situazione in Ungheria; stato di attuazione della Direttiva negli Stati membri dell'UE; aspetti giuridici).
- *Computers, Freedom and Privacy - Austin, TX, 16-18 February 1998* (Privacy e libertà di espressione; autoregolamentazione e normazione).

6. ALLEGATI

6.1. DATI SULLE PRINCIPALI ATTIVITÀ DEL GARANTE.

DATI

Attività	Norme di riferimento legge n. 675/1996	Numero richieste, atti o documenti
Richieste di informazioni e quesiti telefonici (1)		25.000
Quesiti per iscritto (2)		1.050
Comunicati stampa		67
Bollettini	Art. 31, comma 1 lett. *i)*	3
Notificazioni pervenute (1° gennaio/1° aprile 1998) (3)	Art. 7	250.000
Richieste di autorizzazione al trattamento dei dati sensibili da parte di privati ed enti pubblici economici (4)	Art. 22	8.889
Comunicazioni relative al trattamento di dati sensibili da parte di soggetti pubblici	Artt. 22 comma 3 e 41, comma 5	268
Comunicazioni relative alla divulgazione di dati personali tra soggetti pubblici	Art. 27 comma 2	320
Segnalazioni e reclami di cittadini ed associazioni	Art. 31 comma 1, lett. *d)*	285
Ricorsi	Art. 29	86
Richieste di esonero dall'informativa per i dati raccolti presso terzi	Art. 10 comma 4	265
Lettere-circolari inviate dal Garante		3.300
Autorizzazioni generali rilasciate	Art. 41 comma 7	6
Provvedimenti di richiesta di informazioni e documenti	Artt. 31 e 32 comma 1	810

Attività	Norme di riferimento legge n. 675/1996	Numero richieste, atti e documenti
Segnalazioni e altri provvedimenti adottati	Art. 31	31
Altri provvedimenti relativi a ricorsi	Art. 29	12
Risposte ad istanze e quesiti		95
Notificazioni pervenute nel 1997 (non necessarie o errate o su modelli non conformi)	Art. 7	2.075
Richieste di autorizzazione al trattamento di dati sensibili da parte di soggetti pubblici (5)	Art. 22	224

(1) Stima effettuata sulla base del numero delle telefonate giornaliere ricevute dall'Ufficio.

(2) Vari quesiti trovano già risposta, per la loro portata generale, in alcuni comunicati stampa, nel bollettino, nei pareri forniti ad associazioni di categoria, ordini professionali ed amministrazioni pubbliche, nelle autorizzazioni generali o nel modello di notificazione.

(3) Stima indicata sulla base delle notizie fornite dall'Ente poste italiane, con il quale il Garante ha stipulato una convenzione relativa alla procedura di notificazione.

(4) Alle richieste si è provveduto con le sei autorizzazioni generali pubblicate sulla *Gazzetta ufficiale*.

(5) Richieste non necessarie, in quanto i soggetti pubblici non devono acquisire per il trattamento dei dati sensibili la preventiva autorizzazione del Garante (v. art. 22, comma 3, legge n. 675/1996).

6.2. AUTORIZZAZIONI GENERALI.

6.2.1. Autorizzazione n. 1/1997 al trattamento dei dati sensibili nei rapporti di lavoro.

PROVVEDIMENTO 19 novembre 1997.

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675/1996, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come "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;

Rilevato che tali dati possono essere trattati dai soggetti pubblici solo in presenza di un'apposita disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite, senza necessità, pertanto, di un'autorizzazione di questa Autorità; constatato che i soggetti pubblici possono proseguire fino al 7 maggio 1998 i trattamenti di dati sensibili iniziati prima dell'8 maggio 1997, previa comunicazione a questo Garante;

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati, e che occorre quindi riferire solo a tali soggetti l'ambito di applicazione delle autorizzazioni, fatta eccezione per il trattamento dei dati idonei a rivelare lo stato di salute da parte degli organismi sanitari pubblici, che sarà preso in considerazione con separato provvedimento in applicazione dell'articolo 23 della legge n. 675/1996;

Considerato che il Garante può rilasciare le autorizzazioni, anche d'ufficio, nei confronti di singoli titolari o, con provvedimenti generali, di determinate categorie di titolari o di trattamenti, come precisato dall'articolo 41, comma 7, della legge n. 675/1996, nel testo sostituito dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123;

Ritenuto opportuno rilasciare alcune autorizzazioni generali prima della scadenza del termine del 30 novembre 1997, e ciò al fine di semplificare gli adempimenti che la legge n. 675/1996 pone a carico di determinate categorie di titolari, nonché di assicurare una migliore funzionalità dell'Ufficio del Garante e di armonizzare le prescrizioni da impartire con le autorizzazioni;

Rilevato che sono in fase di predisposizione alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali che, in attuazione della legge 31 dicembre 1996, n. 676, dovranno prevedere entro il 23 luglio 1998 alcune norme integrative in tema di dati sensibili, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Considerata, quindi, l'opportunità che in questa fase transitoria le autorizzazioni non rechino disposizioni particolarmente dettagliate, e ciò allo scopo di evitare che l'attività dei titolari, ferme restando alcune garanzie per gli interessati, sia soggetta a modifiche sostanziali in un breve periodo di tempo;

Ritenuto pertanto opportuno rilasciare, allo stato, alcune autorizzazioni provvisorie, in conformità anche a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che le autorizzazioni prendano in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, 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, specie per quanto riguarda la riservatezza e l'identità personale, princìpi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che un ampio numero di trattamenti di dati sensibili è effettuato ai fini dell'adempimento di obblighi contabili, retributivi, previdenziali, assistenziali e fiscali nell'ambito dei rapporti di lavoro, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

AUTORIZZA

il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, finalizzato alla gestione dei rapporti di lavoro, alle condizioni di seguito indicate.

1) Ambito di applicazione

L'autorizzazione è rilasciata, anche senza richiesta di parte:

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 o parziali o temporanee ai sensi della legge 24 giugno 1997, n. 196, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto *2)*, lett. *b)* e *c)*;

b) ad organismi paritetici e ad altri organismi che gestiscono osservatori in materia di lavoro, previsti da leggi, da regolamenti o da contratti collettivi anche aziendali, ovvero dalla normativa comunitaria.

L'autorizzazione riguarda anche l'attività svolta 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.

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 nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto *1)*.

3) Finalità del trattamento

Il trattamento dei dati sensibili deve essere necessario:

a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, da regolamenti o da contratti collettivi anche aziendali, ovvero dalla normativa comunitaria, in particolare ai fini del rispetto 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, 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 il perseguimento delle finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;

d) per far valere o difendere un diritto in sede giudiziaria anche da parte di un terzo, sempreché, qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere sia di rango pari a quello dell'interessato.

4) Categorie di dati

Il trattamento può avere per oggetto i dati strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto *3)*, 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 (sempreché il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pubbliche iniziative, nonché i dati inerenti alle attività o agli incarichi sindacali, ovvero 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 in riferimento a malattie anche professionali, invalidità, infermità, maternità e puerperio, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psico-fisica a svolgere determinate mansioni o all'appartenenza a categorie protette.

5) Modalità di trattamento

Fermi restando gli obblighi previsti dagli articoli 9, 15 e 17 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza e i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate agli obblighi, ai compiti o alle finalità di cui al punto *3)*.

Restano inoltre fermi gli obblighi di acquisire il consenso scritto dell'interessato e di informare l'interessato medesimo, in conformità a quanto previsto dagli articoli 10 e 22 della legge n. 675/1996.

6) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'articolo 9, comma 1, lett. e) della legge n. 675/1996, 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 verifiche periodiche, deve essere verificata costantemente la stretta pertinenza e la non eccedenza dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati.

7) Comunicazione e diffusione dei dati

Ai sensi dell'articolo 23, comma 4, della legge n. 675/1996, i dati idonei a rivelare lo stato di salute possono essere diffusi solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

I dati idonei a rivelare la vita sessuale non possono essere diffusi.

Gli altri 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, agenzie di intermediazione, associazioni di datori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

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 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'articolo 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'articolo 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.

10) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 30 novembre 1997, fino al 30 settembre 1998.

Qualora alla data del 30 novembre 1997 il trattamento non sia già conforme alle prescrizioni della presente autorizzazione, il titolare può adeguarsi ad esse entro il 31 dicembre 1997, sempreché le caratteristiche del trattamento non permettano un adeguamento entro un termine più breve.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 19 novembre 1997

Il Presidente

6.2.2. Autorizzazione n. 2/1997 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale.

PROVVEDIMENTO 27 novembre 1997.

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675/1996, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della medesima legge, il quale individua come "sensibili" i dati personali idonei a rivelare, tra l'altro, lo stato di salute e la vita sessuale;

Rilevato che tali dati possono essere trattati dai soggetti pubblici solo in presenza di una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite, senza necessità, pertanto, di un'autorizzazione di questa Autorità (articolo 22, comma 3, legge n. 675/1996);

Constatato che i soggetti pubblici possono avvalersi di una disposizione transitoria, in base alla quale i trattamenti di dati sensibili iniziati prima dell'8 maggio 1997 possono essere proseguiti fino al 7 maggio 1998 anche in mancanza di una disposizione di legge avente le caratteristiche predette, purché si effettui una comunicazione a questa Autorità (articolo 41, comma 5, legge n. 675/1996);

Rilevato che gli organismi sanitari pubblici possono avvalersi di tale disposizione transitoria, oppure, a loro scelta, di una disposizione speciale che permette di trattare i dati inerenti alla salute (fatta eccezione, quindi, degli altri dati sensibili) anche in mancanza di una puntuale disposizione di legge e del consenso scritto dell'interessato, qualora perseguano finalità di tutela dell'incolumità fisica e della salute di un terzo o della collettività ed osservino le prescrizioni dell'autorizzazione rilasciata da questa Autorità (articolo 23 legge n. 675/1996);

Considerato che la legge n. 675/1996 prevede che gli esercenti le professioni sanitarie possono trattare: a) i dati idonei a rivelare lo stato di salute, anche senza l'autorizzazione di questa Autorità, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica e la salute degli interessati che abbiano manifestato il proprio consenso per iscritto; *b)* i dati idonei a rivelare lo stato di salute, sulla base di un'autorizzazione, qualora il consenso scritto non sia o non possa essere prestato e i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica e la salute di un terzo o della collettività; *c)* i dati idonei a rivelare la vita sessuale, sulla base del consenso scritto e dell'autorizzazione;

Considerato che gli enti pubblici economici ed ogni altro soggetto privato, inclusi gli organismi sanitari, possono trattare i dati idonei a rivelare lo stato di salute e la vita sessuale solo sulla base del consenso scritto e dell'autorizzazione;

Considerato che il Garante può rilasciare l'autorizzazione anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Ritenuto opportuno rilasciare prima del 30 novembre 1997 una autorizzazione generale volta a semplificare gli adempimenti previsti dalla legge n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Rilevato che sono in fase di predisposizione alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, i quali, in attuazione della legge 31 dicembre 1996, n. 676, dovranno prevedere entro il 23 luglio 1998 alcune norme integrative riguardanti i dati sensibili, anche in attuazione della raccomandazione N.R (97) 5 adottata dal Consiglio d'Europa in materia di dati sanitari;

Constatato che tali decreti dovranno tener conto del principio affermato nella citata raccomandazione, secondo il quale i dati sanitari devono essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza di efficacia pari a quelle previste in tale ambito;

Considerata l'opportunità che in questa fase transitoria le autorizzazioni non rechino disposizioni particolarmente dettagliate, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare, allo stato, un'autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che l'autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, 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, specie per quanto riguarda la riservatezza e l'identità personale, princìpi valutati anche sulla base della citata raccomandazione del Consiglio d'Europa;

Considerato che un numero elevato di trattamenti di dati idonei a rivelare lo stato di salute è effettuato per finalità di prevenzione e di cura, o che riguardano, in particolare, la gestione di servizi socio-sanitari, la ricerca scientifica e la fornitura di prestazioni, beni o servizi all'interessato, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

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 e la salute di un terzo o della collettività, e l'interessato non abbia prestato il proprio consenso per iscritto o non possa prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere;

b) gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, con il consenso scritto dell'interessato;

c) gli organismi sanitari pubblici, 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 scritto (articolo 23, comma 1, ultimo periodo, legge n. 675/1996), in quanto l'interessato non lo ha prestato o non può prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere;

3) il trattamento non sia previsto da una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

1) Ambito di applicazione e finalità del trattamento.

1.1 L'autorizzazione è rilasciata, anche senza richiesta:

a) ai medici-chirurghi, agli odontoiatri 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 al fine di consentire ai destinatari di adempiere o di esigere l'adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, da regolamenti o dalla normativa comunitaria, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie anche professionali e degli infortuni, di cura e di diagnosi, 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 suindicati.

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.

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 (fermo restando quanto previsto dall'arti-

colo 23, comma 1, ultimo periodo, della legge n. 675/1996), 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;

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, ivi comprese le confessioni religiose e le comunità religiose, relativamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, ove esistenti, nelle rispettive norme statutarie;

e) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e ad altri organismi, limitatamente ai dati 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.

1.3 La presente autorizzazione è rilasciata, altresì, per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, quando il trattamento sia necessario:

a) ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni;

b) per far valere o difendere un diritto in sede giudiziaria anche da parte di un terzo, sempreché il diritto sia di rango pari a quello dell'interessato, e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario per il loro perseguimento.

2) Categorie di dati oggetto di trattamento

Il trattamento può avere per oggetto i dati strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto *1)*, e può comprendere le informazioni relative a stati di salute pregressi.

Devono essere considerati sottoposti all'ambito di applicazione della presente autorizzazione, anche i seguenti dati:

a) 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;

b) i dati genetici, limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività, sulla base del consenso scritto ai sensi degli articoli 22 e 23 della legge n. 675/1996. In mancanza del consenso, se il trattamento è volto a tutelare l'incolumità fisica e la salute di un terzo o della collettività, il trattamento può essere iniziato o proseguito solo previa apposita autorizzazione del Garante. I dati genetici non possono essere trattati dai soggetti di cui al punto 1.2, lettere *c)*, *d)*, *e)* ed *f)*. Le informative all'interessato previste dall'art. 10 della legge n. 675/1996 devono porre in particolare evidenza il diritto dell'interessato di opporsi, per motivi legittimi, al trattamento dei dati genetici che lo riguardano. Fino alla data di entrata in vigore del decreto delegato che darà attuazione alla citata raccomandazione in applicazione della legge 31 dicembre 1996, n. 676, i dati genetici trattati per fini di prevenzione, di diagnosi o di terapia nei confronti dell'interessato, ovvero per finalità di ricerca scientifica, possono essere utilizzati unicamente per tali finalità o per consentire all'interessato di prendere una decisione libera e informata, ovvero per finalità probatorie in sede civile o penale, in conformità alla legge.

3) Modalità di trattamento

Fermi restando gli obblighi previsti dagli artt. 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati e il trasferimento all'estero dei dati, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale deve essere effettuato unicamente con logiche e forme di organizzazione dei dati strettamente correlate agli obblighi, ai compiti e alle finalità di cui al punto *1)*.

Restano inoltre fermi gli obblighi di acquisire il consenso scritto dell'interessato e di informare l'interessato medesimo, in conformità a quanto previsto dagli articoli 10, 22 e 23 della legge n. 675/1996. Se l'interessato è minore di età, il consenso può essere prestato disgiuntamente da coloro che esercitano la potestà. Per le informazioni relative ai nascituri, il consenso è prestato dalla gestante.

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lett. *e)* della legge 31 dicembre 1996, n. 675/1996, i dati idonei a rivelare lo stato di salute e la vita sessuale possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto *1)*, ovvero per perseguire le finalità ivi menzionate, verificando anche periodicamente la stretta pertinenza e la non eccedenza dei dati trattati.

5) Comunicazione e diffusione dei dati

Ai sensi dell'art. 23, comma 4, della legge n. 675/1996, i dati idonei a rivelare lo stato di salute possono essere diffusi solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

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.

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.

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 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'articolo 5, comma 2, della legge 5 giugno 1990, n. 135, il quale prevede che la rilevazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona;

b) dall'articolo 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'articolo 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 il 25 giugno 1995 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 30 novembre 1997, fino al 30 settembre 1998.

Qualora alla data del 30 novembre 1997 il trattamento non sia già conforme alle prescrizioni della presente autorizzazione, il titolare può adeguarsi ad esse entro il 31 dicembre 1997, sempreché le caratteristiche del trattamento non permettano un adeguamento entro un termine più breve.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 27 novembre 1997

Il Presidente

6.2.3. Autorizzazione n. 3/1997 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni.

PROVVEDIMENTO 28 novembre 1997.

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675/1996, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come "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;

Rilevato che tali dati possono essere trattati dai soggetti pubblici solo in presenza di una disposizione di legge che specifichi i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite, senza necessità, pertanto, di un'autorizzazione di questa Autorità (articolo 22, comma 3, legge n. 675/1996);

Constatato che i soggetti pubblici possono avvalersi di una disposizione transitoria, in base alla quale i trattamenti di dati sensibili iniziati prima dell'8 maggio 1997 possono essere proseguiti fino al 7 maggio 1998 anche in mancanza di una disposizione di legge avente le caratteristiche predette, purché si effettui una comunicazione a questa Autorità (articolo 41, comma 5, legge n. 675/1996);

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati, e che occorre quindi riferire solo a tali soggetti l'ambito di applicazione delle autorizzazioni, fatta eccezione per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, che forma oggetto dell'autorizzazione n. 2/1997;

Considerato che il Garante può rilasciare le autorizzazioni anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Ritenuto opportuno rilasciare prima del 30 novembre 1997 una autorizzazione generale volta a semplificare gli adempimenti previsti dalla legge n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Rilevato che sono in fase di predisposizione alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, i quali, in attuazione della legge 31 dicembre 1996, n. 676, dovranno prevedere entro il 23 luglio 1998 alcune norme integrative riguardanti i dati sensibili, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Considerata l'opportunità che in questa fase transitoria le autorizzazioni non rechino disposizioni particolarmente dettagliate, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare, allo stato, un'autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che l'autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di questi aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, 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, specie per quanto riguarda la riservatezza e l'identità personale, princìpi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che un numero elevato 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, ove esistenti, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

AUTORIZZA

Il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996 da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, secondo le prescrizioni di seguito indicate.

1) Ambito di applicazione e finalità del trattamento

L'autorizzazione è rilasciata, anche senza richiesta:

a) alle associazioni anche non riconosciute, ivi comprese le confessioni religiose e le comunità religiose, i partiti e i movimenti politici, le associazioni e le organizzazioni sindacali, i patronati, le associazioni di categoria, le 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 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, 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 in sede giudiziaria, anche da parte di terzi, sempreché 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.

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 per perseguire le predette finalità, e in particolare di società editoriali o di centri di assistenza fiscale, la presente autorizzazione è rilasciata anche ai medesimi organismi e persone giuridiche. 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 e le particolari misure di sicurezza adottate. 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 3) e 5) in tema di pertinenza e di non eccedenza dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

2) 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.

3) 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. 2/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 29 novembre 1997, n. 279.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 22, comma 1, della legge 31 dicembre 1996, n. 675/1996, 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, dai regolamenti, dai contratti collettivi o dalla normativa comunitaria.

A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza e la non eccedenza dei dati rispetto ai predetti obblighi e finalità, in particolare per quanto riguarda i dati che rivelano le opinioni e le intime convinzioni.

4) Modalità di trattamento

Fermi restando gli obblighi previsti dagli artt. 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati, il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate alle finalità, agli scopi e agli obblighi di cui al punto *1)*.

Restano inoltre fermi gli obblighi di acquisire il consenso scritto dell'interessato e di informare l'interessato medesimo, in conformità a quanto previsto dagli articoli 10 e 22 della legge n. 675/1996.

5) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lett. *e)*, della legge 31 dicembre 1996, n. 675/1996, 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 *1)*, ovvero per adempiere agli obblighi ivi menzionati.

Le verifiche di cui al punto *3)* devono riguardare anche la pertinenza e la non eccedenza dei dati rispetto all'attività svolta dall'interessato o al rapporto che intercorre tra l'interessato e l'associazione, la fondazione, il comitato o il diverso organismo, tenendo presente il genere di prestazione, di beneficio o di servizio offerto all'interessato e la posizione di quest'ultimo rispetto all'associazione, alla fondazione, al comitato o al diverso organismo.

6) Comunicazione e diffusione dei dati

I dati sensibili possono essere comunicati, e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi di cui al punto *1)* e tenendo presenti le altre prescrizioni sopraindicate.

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 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 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.

9) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia a decorrere dal 30 novembre 1997, fino al 30 settembre 1998.

Qualora alla data del 30 novembre 1997 il trattamento non sia già conforme alle prescrizioni della presente autorizzazione, il titolare può adeguarsi ad esse entro il 31 dicembre 1997, sempreché le caratteristiche del trattamento non permettano un adeguamento entro un termine più breve.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 28 novembre 1997

Il Presidente

6.2.4. Autorizzazione n. 4/1997 al trattamento dei dati sensibili da parte dei liberi professionisti.

PROVVEDIMENTO 29 novembre 1997.

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675/1996, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come "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;

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati (articolo 22, comma 1, legge n. 675/1996);

Considerato che i dati idonei a rivelare lo stato di salute e la vita sessuale possono essere trattati anche ai sensi di una speciale disposizione, in base alla quale, ferma restando l'autorizzazione di questa Autorità, si può prescindere dal consenso degli interessati quando il trattamento è necessario per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato, ovvero è necessario per lo svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione del codice di procedura penale, sempreché i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento (articolo 22, comma 4, della citata legge n. 675/1996);

Considerato che il Garante può rilasciare tali autorizzazioni anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Ritenuto opportuno rilasciare prima del 30 novembre 1997 una autorizzazione generale volta a semplificare gli adempimenti previsti dalla legge n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Rilevato che sono in fase di predisposizione alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, i quali, in attuazione della legge 31 dicembre 1996, n. 676, dovranno prevedere entro il 23 luglio 1998 alcune norme integrative riguardanti i dati sensibili, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Considerata l'opportunità che in questa fase transitoria le autorizzazioni non rechino disposizioni particolarmente dettagliate, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo di tempo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare, allo stato, un'autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che l'autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, 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, specie per quanto riguarda la riservatezza e l'identità personale, princìpi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che un numero elevato di trattamenti di dati sensibili è effettuato da liberi professionisti iscritti in albi o elenchi professionali per l'espletamento delle rispettive attività professionali, e che è pertanto necessario che tali trattamenti formino oggetto di una autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

AUTORIZZA

I liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, secondo le prescrizioni di seguito indicate.

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, o in conformità alle norme di attuazione dell'articolo 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'articolo 34 del regio decreto-legge 27 novembre 1933, n. 1578, recante l'ordinamento delle professioni di avvocato e procuratore.

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'articolo 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 dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 29 novembre 1997, n. 279;

b) per la gestione delle prestazioni di lavoro o di collaborazione di cui si avvale il libero professionista o taluno dei soggetti sopraindicati, alla quale si riferisce l'autorizzazione generale n. 1/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 21 novembre 1997, n. 272;

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 pertinenti e non eccedenti rispetto agli incarichi conferiti.

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. 2/1997.

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) per far valere o difendere un diritto in sede giudiziaria, anche da parte di terzi;

c) ai fini dello svolgimento da parte del difensore nel procedimento penale delle investigazioni di cui all'articolo 38 delle norme di attuazione del codice di procedura penale, anche a mezzo di sostituti e di consulenti tecnici.

4) Modalità di trattamento

Il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate all'incarico conferito dal cliente.

Restano fermi gli obblighi previsti dagli articoli 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati.

Restano inoltre fermi gli obblighi:

a) di informare l'interessato ai sensi dell'articolo 10, commi 1 e 3, della legge n. 675/1996, anche quando i dati sono raccolti presso terzi;

b) di acquisire il consenso scritto.

Se i dati sono raccolti per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive (punto *3*), lettere *b)* e *c)*), l'informativa relativa ai dati raccolti presso terzi, e il consenso scritto, sono necessari anche in riferimento ai dati idonei a rivelare lo stato di salute o la vita sessuale, 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.

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'articolo 9, comma 1, lett. *e)*, della legge n. 675/1996, i dati sensibili possono essere conservati per il periodo di tempo previsto da leggi, regolamenti o dalla normativa comunitaria e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza e la non eccedenza dei dati rispetto agli incarichi.

I dati acquisiti in occasione di precedenti incarichi possono essere mantenuti se pertinenti e non eccedenti 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 diffusi solo se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia (articolo 23, comma 4, della legge n. 675/1996).

I dati relativi 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 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, 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 30 novembre 1997, fino al 30 settembre 1998.

Qualora alla data del 30 novembre 1997 il trattamento non sia già conforme alle prescrizioni della presente autorizzazione, il titolare può adeguarsi ad esse entro il 31 dicembre 1997, sempreché le caratteristiche del trattamento non permettano un adeguamento entro un termine più breve.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 29 novembre 1997

Il Presidente

6.2.5. Autorizzazione n. 5/1997 al trattamento dei dati sensibili da parte di diverse categorie di titolari.

PROVVEDIMENTO 15 dicembre 1997.

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675/1996, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come "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;

Considerato che i soggetti privati e gli enti pubblici economici possono trattare tali dati solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati (art. 22, comma 1, legge n. 675/1996);

Considerato che il Garante può rilasciare l'autorizzazione anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, nei riguardi di determinate categorie di titolari o di trattamenti (articolo 41, comma 7, della legge n. 675/1996, modificato dall'articolo 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Ritenuto opportuno rilasciare un'autorizzazione generale volta a semplificare gli adempimenti previsti dalla legge n. 675/1996, ad armonizzare le prescrizioni da impartire e a favorire la funzionalità dell'Ufficio del Garante;

Rilevato che sono in fase di predisposizione alcuni decreti legislativi per il completamento della disciplina sulla protezione dei dati personali, i quali, in attuazione della legge 31 dicembre 1996, n. 676, dovranno prevedere entro il 23 luglio 1998 alcune norme integrative riguardanti i dati sensibili, anche in attuazione delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Considerata l'opportunità che in questa fase transitoria le autorizzazioni non rechino disposizioni particolarmente dettagliate, e ciò allo scopo di evitare che l'attività dei titolari sia soggetta a modifiche sostanziali nel corso di un breve periodo, ferme restando alcune garanzie per gli interessati;

Ritenuto pertanto opportuno rilasciare, allo stato, un'autorizzazione provvisoria, anche in conformità a quanto previsto dall'emanando regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità;

Ritenuta, tuttavia, la necessità che l'autorizzazione prenda in considerazione le finalità dei trattamenti, le categorie di dati, di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati stessi, in quanto la disciplina di tali aspetti è prevista dalla legge n. 675/1996 ai fini dell'applicazione delle norme sull'esonero dall'obbligo della notificazione e sulla notificazione semplificata (articolo 7, comma 5-*quater*);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni princìpi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i di-

ritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, princìpi valutati anche sulla base delle raccomandazioni del Consiglio d'Europa;

Considerato che numerosi trattamenti di dati sensibili sono effettuati da persone fisiche o giuridiche operanti nei rami assicurativo, previdenziale, assistenziale, bancario, finanziario e di intermediazione finanziaria, nel settore turistico e del trasporto di persone, delle ricerche di mercato, dei sondaggi di opinione o della selezione del personale, nonché della mediazione a fini matrimoniali, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'articolo 41, comma 7, della legge n. 675/1996;

AUTORIZZA

il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, fatta eccezione dei dati idonei a rivelare la vita sessuale, secondo le prescrizioni di seguito indicate.

Capo I
Attività bancarie, assicurative, di gestione di fondi o del settore turistico o del trasporto

1) Soggetti ai quali è rilasciata l'autorizzazione

a) imprese autorizzate all'esercizio dell'attività bancaria o assicurativa ed organismi che le riuniscono;

b) società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;

c) società ed altri organismi 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, ivi comprese le agenzie di viaggio e gli operatori turistici.

2) Finalità del trattamento

L'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, dalla legge, dai regolamenti, dalla normativa comunitaria 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 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'articolo 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 (articolo 13, comma 1, lettera *c)*, n. 4), legge n. 675/1996), 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. 1/1997, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro (pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana n. 272 del 21 novembre 1997), qualora le finalità perseguite siano quelle indicate al punto *3)* di tale autorizzazione;

b) n. 4/1997, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati (pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana n. 281 del 2 dicembre 1997), 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

L'autorizzazione è rilasciata, anche senza richiesta, alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di un'attività svolta anche di propria iniziativa nell'interesse di terzi, ai soli fini della ricerca o della selezione di 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 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 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 non possono essere diffusi.

CAPO V
Mediazione a fini matrimoniali

1) Soggetti ai quali è rilasciata l'autorizzazione

L'autorizzazione è rilasciata, anche senza richiesta, 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, anche senza richiesta, 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 trattamenti

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 (articolo 13, comma 1, lettera *c)*, n. 4), legge n. 675/1996), 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. 2/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 29 novembre 1997, n. 279.

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 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza e i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati, il trattamento dei dati sensibili deve essere effettuato unicamente con logiche e forme di organizzazione dei dati strettamente correlate alle finalità indicate nei capi che precedono.

Resta inoltre fermo l'obbligo di informare l'interessato, ai sensi dell'articolo 10, commi 1 e 3, della legge n. 675/1996, anche quando i dati sono raccolti presso terzi.

3) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'art. 9, comma 1, lett. *e)*, della legge 31 dicembre 1996, n. 675/1996, 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, verificando anche periodicamente la stretta pertinenza e la non eccedenza dei dati trattati.

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 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 o 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 deontologici, nonché 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.

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 30 novembre 1997, fino al 30 settembre 1998.

Qualora alla data odierna il trattamento non sia già conforme alle prescrizioni della presente autorizzazione, il titolare può adeguarsi ad esse entro il 15 gennaio 1998, sempreché le caratteristiche del trattamento non permettano un adeguamento entro un termine più breve.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 15 dicembre 1997

Il Presidente

6.2.6. Autorizzazione n. 6/1997 al trattamento di alcuni dati sensibili da parte degli investigatori privati.

PROVVEDIMENTO 29 dicembre 1997.

IL GARANTE

Vista la legge 31 dicembre 1996, n. 675/1996, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto, in particolare, l'articolo 22, comma 1, della citata legge n. 675/1996, il quale individua come "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;

Considerato che il trattamento di questi dati da parte di privati ed enti pubblici economici è permesso, di regola, solo previa autorizzazione di questa Autorità e con il consenso scritto degli interessati (articolo 22, comma 1, legge n. 675/1996);

Considerato che una speciale disposizione (articolo 22, comma 4, legge n. 675/1996) permette di trattare i dati idonei a rivelare lo stato di salute e la vita sessuale senza il consenso degli interessati, quando il trattamento autorizzato dal Garante è necessario per svolgere una investigazione nell'ambito di un procedimento penale (articoli 190 del codice di procedura penale e 38 delle relative norme di attuazione) o, comunque, per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato;

Considerato che il Garante ha già rilasciato un'autorizzazione di ordine generale relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale (n. 2/1997, emanata il 27 novembre 1997), 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 le prescrizioni dell'autorizzazione n. 2/1997 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;

Ritenuta la necessità di applicare anche al caso di specie le considerazioni già espresse con l'autorizzazione n. 2/1997 per ciò che riguarda la natura provvisoria delle autorizzazioni generali e i criteri direttivi prescelti per la determinazione delle relative prescrizioni;

Considerato che ulteriori misure ed accorgimenti saranno prescritti dal Garante all'atto della sottoscrizione dell'apposito codice di deontologia e di buona condotta che il Garante è in procinto di promuovere (articolo 22, comma 4, legge n. 675/1996):

AUTORIZZA

gli investigatori privati a trattare i dati idonei a rivelare lo stato di salute e la vita sessuale, secondo le prescrizioni di seguito indicate.

1) Ambito di applicazione e finalità del trattamento

L'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 (articolo 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

Il trattamento può essere effettuato unicamente:

a) 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;

b) su incarico di un difensore nell'ambito del procedimento penale, per ricercare e individuare elementi a favore del relativo assistito da utilizzare ai soli fini dell'esercizio del diritto alla prova (articoli 190 del codice di procedura penale e 38 delle relative norme di attuazione).

Restano ferme le altre autorizzazioni generali rilasciate ai fini dello svolgimento delle investigazioni nel procedimento penale o per l'esercizio di un diritto in sede giudiziaria, in particolare:

a) nell'ambito dei rapporti di lavoro (autorizzazione n. 1/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 21 novembre 1997, n. 272);

b) relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione generale n. 2/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 29 novembre 1997, n. 279);

c) da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione generale n. 3/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 29 novembre 1997, n. 279);

d) da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione generale n. 4/1997, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana 2 dicembre 1997, n. 281).

2) Categorie di dati e interessati ai quali i dati si riferiscono

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e la vita sessuale, qualora ciò sia strettamente indispensabile per eseguire specifici incarichi conferiti per scopi determinati e legittimi nell'ambito delle finalità di cui al punto 1).

I dati devono essere pertinenti e non eccedenti rispetto agli incarichi conferiti.

3) Modalità di trattamento

Gli investigatori privati non possono intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta di dati idonei a rivelare lo stato di salute e la vita sessuale. 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 1).

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 fissato per la sua ultimazione.

I dati devono essere registrati ed elaborati mediante logiche e forme di organizzazione strettamente correlate alle finalità di cui al punto 1).

L'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'articolo 10, comma 1, della legge n. 675/1996, 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 (articoli 10, commi 3 e 4 e 22, comma 4, legge n. 675/1996), 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 8 e 19 della legge n. 675/1996, 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 deve essere effettuato nel rispetto delle ulteriori prescrizioni contenute nella citata autorizzazione generale n. 2/1997, in particolare per ciò che riguarda le informazioni relative ai nascituri e ai dati genetici.

Il trattamento dei dati deve inoltre rispettare le prescrizioni di un apposito codice di deontologia e di buona condotta, che il Garante è in procinto di promuovere ai sensi degli articoli 22, comma 4 e 31, comma 1, lett. *h)*, della legge n. 675/1996.

4) Conservazione dei dati

Nel quadro del rispetto dell'obbligo previsto dall'articolo 9, comma 1, lett. e) della legge n. 675/1996, 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 e la non eccedenza 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.

5) 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 diffusi solo se è necessario per finalità di prevenzione, accertamento o repressione dei reati (articolo 23, comma 4, della legge n. 675/1996), con l'osservanza delle norme che regolano la materia.

I dati relativi alla vita sessuale non possono essere diffusi.

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 il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

7) 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:

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;

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'articolo 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 gli obblighi previsti dagli articoli 9, 15, 17 e 28 della legge n. 675/1996, concernenti i requisiti dei dati personali, la sicurezza, i limiti posti ai trattamenti automatizzati volti a definire il profilo o la personalità degli interessati, nonché il trasferimento all'estero dei dati.

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, la legge n. 675/1996 non si applica anche se i

dati sono comunicati occasionalmente ad una autorità giudiziaria o a terzi, sempreché i dati non siano destinati ad una comunicazione sistematica o alla diffusione (art. 3, legge n. 675/1996).

8) Efficacia temporale e disciplina transitoria

La presente autorizzazione ha efficacia fino al 30 settembre 1998.

Qualora alla data odierna il trattamento non sia già conforme alle prescrizioni della presente autorizzazione, il titolare può adeguarsi ad esse entro il 20 gennaio 1998, sempreché le caratteristiche del trattamento non permettano un adeguamento entro un termine più breve.

Resta ferma la data del 31 dicembre 1997 prevista dall'autorizzazione n. 2/1997 per l'adeguamento alle relative prescrizioni.

La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 29 dicembre 1997

Il Presidente

6.3. Autorità di controllo comune Schengen.

6.3.1. Primo rapporto 1995-1997. BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 27 marzo 1997
SCH/Aut-cont (97) 27 riv.
Traduzione: orig. FR

Rapporto sulle attività dell'Autorità di controllo comune di Schengen Marzo 1995 - marzo 1997 (*)

(*) Si riproduce il testo nella traduzione curata dal Segretariato dell'ACC.

PREFAZIONE.

Tra i grandi progetti di cooperazione tra forze di polizia, gli accordi di Schengen e il Sistema d'informazione SIS costituiscono un banco di prova.

Nonostante la Convenzione di applicazione di Schengen contempli disposizioni soddisfacenti in materia di diritti delle persone, di sicurezza dei dati e di controllo del sistema informatico, i successivi rinvii della sua messa in applicazione hanno rischiato che il sistema - che, per ragioni di efficacia, acquisiva maggiore capacità - superasse in velocità l'applicazione dei principi.

Questa situazione era preoccupante in un momento in cui venivano già sviluppati altri progetti di cooperazione europea nell'ambito dei quali gli imperativi di efficacia risultavano prioritari.

Una tale situazione avrebbe potuto pregiudicare il controllo della protezione dei dati se, nel 1992, non fosse stata istituita un'Autorità di controllo comune provvisoria.

Lo scambio di informazioni e la cooperazione di polizia, giudiziaria e doganale, sono chiaramente divenuti, come misure compensative della libera circolazione delle persone, i mezzi necessari per lottare contro il terrorismo, il traffico di stupefacenti e la grande criminalità, per garantire la sicurezza e per controllare i flussi migratori. Ne sono esempio, oltre a Schengen, le Convenzioni di Europol e di Dublino.

E' tuttavia importante che il o i capitali dedicati alla protezione delle informazioni relative alle persone fisiche e agli organi di controllo comuni o nazionali competenti in questo settore non si limitino a pure e semplici clausole stilistiche.

Questa prima relazione verte su due anni di attività ed è in primo luogo la cronistoria incompiuta di un negoziato condotto passo per passo con gli Stati-parti contraenti per consolidare nella prassi, in conformità del disposto della Convenzione, l'indipendenza e l'autorità di un organo di controllo istituito per vigilare al rispetto dei diritti delle persone che costituiscono l'oggetto dello scambio di informazioni.

Più che semplice banco di prova, l'Autorità di controllo comune Schengen, in quanto precursore, è chiamata a svolgere un vero e proprio ruolo di primo piano.

Alex Türk

Marzo 1997

Capitolo 1. Richiami.

1.1. I testi pertinenti

L'Accordo di Schengen è stato firmato il 14 giugno 1985 dai governi degli Stati dell'Unione economica del Benelux, della Repubblica federale di Germania e della Repubblica francese. E' stato provvisoriamente applicato il giorno successivo a quello della firma (articolo 32) ed è entrato in vigore il 2 marzo 1986.

Espressione della volontà di creare uno spazio comune di circolazione delle merci e delle persone per evitare il riprodursi di incidenti come quelli legati, l'anno precedente, allo sciopero bianco dei doganieri italiani (camion stranieri bloccati alle frontiere, sbarramenti di protesta in Francia, perturbazione dell'intera rete stradale europea), l'Accordo di Schengen mirava innanzi tutto a sopprimere gradualmente i controlli alle frontiere comuni degli Stati firmatari. Appena 7 dei 33 articoli dell'Accordo riguardavano la cooperazione tra forze di polizia e la lotta contro l'immigrazione.

La Convenzione di applicazione dell'Accordo di Schengen, firmata dalle stesse Parti contraenti il 19 giugno 1990, ha invece sviluppato, per fini legati ai controlli alle frontiere esterne comuni, la cooperazione di polizia, doganale e giudiziaria, quale contromisura necessaria, considerati i dibattiti nazionali sull'insicurezza e l'immigrazione, all'apertura decisa cinque anni prima.

Una delle misure fondamentali del dispositivo di cooperazione è stata la creazione di un sistema di informazione comune, il Sistema d'informazione Schengen (Titolo IV della Convenzione).

L'istituzione di questo Sistema ha indotto, per effetto dei testi nazionali ed internazionali che obbligano al rispetto di princìpi di protezione dei dati, la creazione, sull'esempio di modelli nazionali di autorità di controllo indipendenti competenti in questo settore, di un'Autorità di controllo comune.

La Convenzione di applicazione, la cui entrata in vigore è soggetta a ratifica, approvazione o accettazione e la cui messa in applicazione è subordinata al fatto che "le condizioni preliminari per la sua applicazione siano soddisfatte e che i controlli alle frontiere esterne siano effettivi", è entrata in vigore il 1 settembre 1993 ed è stata messa in applicazione il 26 marzo 1995. La data inizialmente prevista era il 1 gennaio 1993.

Aperta all'adesione di altri Stati membri delle Comunità europee (articolo 140), la Convenzione ha permesso l'allargamento dello spazio Schengen all'Italia, la Spagna, il Portogallo, la Grecia e l'Austria anche se, al momento, solo la Spagna e il Portogallo soddisfano tutte le condizioni per inserire dati nel SIS, accedere alle informazioni in esso contenute e partecipare a pieno titolo alle riunioni di tutti gli organi Schengen e, in particolare, dell'Autorità di controllo comune.

Più di recente, il 1 maggio 1996, i cinque paesi nordici, legati dall'accordo sull'Unione nordica dei passaporti che ha istituito la libera circolazione delle persone tra i rispettivi territori e le isole Far Oer, hanno ottenuto lo status di osservatori.

Il 19 dicembre 1996, la Danimarca, la Finlandia e la Svezia, stati membri dell'Unione europea, hanno firmato l'Accordo di adesione a Schengen.

Islanda e Norvegia, non essendo membri dell'Unione europea, hanno beneficiato, grazie ad un Accordo di cooperazione firmato lo stesso giorno, dello status di membri associati. Ai sensi di detto Accordo, la Convenzione di Schengen viene applicata nel territorio di questi due paesi, ad eccezione delle disposizioni relative al controllo delle merci. Islanda e Norvegia non possono tuttavia prendere formalmente parte alle decisioni. Questi due Stati partecipano quindi pienamente al funzionamento del Sistema d'informazione Schengen.

1.2. Organi comuni preposti all'applicazione della Convenzione

Ai fini dell'applicazione della Convenzione, le Parti contraenti hanno istituito due organi:

— Il Comitato esecutivo, composto dei ministri competenti per l'attuazione della Convenzione in ogni Stato parte, ha per compito generale di vigilare alla corretta applicazione della Convenzione e dispone di una serie di competenze specifiche (articolo 131).

— L'Autorità di controllo comune (ACC), composta di due rappresentanti di ogni autorità nazionale di controllo, ha il compito di verificare la corretta esecuzione delle disposizioni della Convenzione per quanto riguarda l'unità di supporto tecnico del SIS (articolo 115). Dispone inoltre di competenze più generali in materia di protezione dei dati.

Oltre a questi due organi, il sistema Schengen gravita attorno al Gruppo centrale, dal quale dipendono un Comitato di orientamento SIS nonché diversi gruppi di lavoro, alcuni dei quali istituiti dalla stessa Convenzione.

Gli organi Schengen sono assistiti da un Segretariato. Questo compito è svolto dal Segretariato generale dell'Unione economica del Benelux, la cui sede è a Bruxelles.

L'organigramma figura in allegato.

1.3. Obiettivo ed architettura del Sistema d'informazione Schengen

Il Titolo IV della Convenzione è interamente dedicato al Sistema d'informazione Schengen (SIS).

L'articolo 93 della Convenzione precisa che il SIS "avvalendosi delle informazioni trasmesse per il suo tramite, ha lo scopo di preservare l'ordine pubblico e la sicurezza pubblica, compresa la sicurezza dello Stato, e di assicurare l'applicazione delle disposizioni sulla circolazione delle persone stabilite nella presente Convenzione".

Le informazioni registrate nel sistema

L'articolo 94 elenca limitativamente le categorie di dati che possono essere registrati nel sistema. Gli articoli da 95 a 100 precisano i motivi che giustificano l'inserimento delle segnalazioni.

La categorie di dati riguardano le persone, gli oggetti e i veicoli.

Per quanto riguarda le persone, nel sistema possono essere inseriti cognome e nome, alias, segni fisici particolari, oggettivi ed inalterabili, indicazione eventuale del fatto che la persona è armata o violenta e linea di condotta da eseguire in caso di individuazione della persona in questione.

E' vietato menzionare informazioni dette "sensibili" quali la razza, le opinioni politiche, la confessione religiosa o altre convinzioni nonché informazioni relative allo stato di salute o la vita sessuale. Le finalità che giustificano l'inserimento di una segnalazione nel SIS sono le seguenti:

a) A prescindere dalla cittadinanza della persona:
arresto per fini di estradizione
ricerca in caso di scomparsa, ricerca di minori o di persone che devono essere internate per decisione di un'autorità competente (articolo 97);
arresto ai fini di comparizione dinanzi all'autorità giudiziaria, anche in qualità di testimone, nell'ambito di un procedimento penale o dell'esecuzione di una pena privativa della libertà (articolo 98);
sorveglianza discreta e controllo specifico ai fini della repressione di reati penali o della prevenzione di minacce gravi per la sicurezza dello Stato (articolo 99).

b) Per gli stranieri, ossia chiunque non sia cittadino di uno Stato membro delle Comunità europee (v. definizione all'articolo 1, 6° capoverso):
non ammissione nel territorio a seguito di un provvedimento amministrativo o giudiziario adottato nel rispetto delle regole procedurali nazionali o fondato su un rischio per l'ordine pubblico e la sicurezza pubblica o la sicurezza nazionale o sul fatto che lo straniero in questione abbia violato la normativa nazionale relativa all'ingresso e al soggiorno degli stranieri (articolo 96).

Per quanto riguarda gli oggetti, nel sistema possono essere inseriti solo dati relativi al nome del proprietario di veicoli, armi da fuoco, documenti e banconote rubati, sottratti o smarriti, ricercati per fini di sequestro o di prova nell'ambito di un procedimento penale (articolo 100).

Per quanto riguarda i veicoli, possono essere registrati dati relativi a quei veicoli ricercati per fini di sorveglianza discreta o di controllo specifico (articolo 99 già citato). Questa categoria permette di registrare informazioni relative al conducente e ai passeggeri del veicolo sorvegliato.

Destinatari delle informazioni

Gli articoli 92 e 101 della Convenzione precisano che le autorità designate dalle Parti contraenti possono accedere, mediante consultazione automatizzata o non automatizzata:

— all'insieme dei dati inseriti nel SIS in occasione dei controlli di frontiera e degli accertamenti e di altri controlli di polizia e di dogana effettuati all'interno del territorio in conformità del diritto nazionale;

— alla sola categoria di segnalazioni per fini di non ammissione in caso di rilascio di visti e permessi di soggiorno e di amministrazione degli stranieri nel quadro delle disposizioni della Convenzione relative alla circolazione degli stranieri.

L'elenco delle autorità abilitate a consultare direttamente i dati inseriti nel SIS deve essere comunicato al Comitato esecutivo (articolo 101, 4° comma).

Architettura del Sistema d'informazione Schengen

Diversi articoli del Titolo IV prescrivono il rispetto di diverse misure di ordine tecnico, ma la descrizione generale del sistema figura all'articolo 92.

Il Sistema d'informazione Schengen (SIS) si compone di una sezione nazionale (N.SIS) presso ogni Parte contraente e di un'unità di supporto tecnico (C.SIS) istituita e mantenuta in comune, la cui responsabilità incombe alla Repubblica francese.

L'unità di supporto tecnico ha sede a Strasburgo ed ha il compito di rendere materialmente identici tutti gli N.SIS. A tal fine, il C.SIS contiene un archivio di dati che garantisce l'identità degli archivi nazionali mediante la trasmissione di informazioni on line.

La trasmissione dei dati avviene nel rispetto dei protocolli e delle procedure definiti in comune dalle Parti contraenti per l'unità di supporto tecnico.

L'articolo 118, 4° comma prevede le misure di sicurezza necessarie per l'unità di supporto tecnico. Tali misure sono identiche a quelle richieste per ogni N.SIS (articolo 118, 1°, 2° e 3° comma).

1.4. Gli uffici SIRENE

Gli uffici SIRENE (Supplementi d'informazione richiesti per l'ingresso nazionale) sono una creazione degli Stati-parte non esplicitamente prevista dalla Convenzione.

In ogni Stato Schengen, gli uffici SIRENE sono incaricati di procedere, sulla base del SIS, allo scambio di informazioni supplementari e fungono da intermediari nelle consultazioni tra i vari Stati sulla condotta da adottare in caso di esecuzione di una segnalazione.

Compiti e attività degli uffici SIRENE sono concretamente definiti in un manuale comune detto "Manuale SIRENE". Il loro ruolo consiste essenzialmente nel procedere a consultazioni preliminari alla creazione di segnalazioni, a scambi di informazioni, al controllo delle segnalazioni multiple e alla definizione di ordini di priorità.

CAPITOLO 2. PROTEZIONE DEI DATI PERSONALI.

2.1. Una legge ed un'autorità di controllo nazionale: condizioni preliminari all'applicazione della Convenzione

Gli Stati-parti hanno posto diverse condizioni preliminari all'applicazione della Convenzione nei rispettivi territori. L'Atto finale richiama il carattere imperativo di queste condizioni.

Tra di esse figura l'obbligo, per ogni Stato-parte, di dotarsi, prima di procedere alla trasmissione di dati personali, di un'autorità nazionale di controllo indipendente (articoli 114 e 128) e di una legge sulla protezione dei dati.

Per quanto riguarda il trattamento automatizzato o meno dei dati trasmessi, la Convenzione prevede le seguenti disposizioni:

a) Trattamento automatizzato di dati trasmessi in applicazione del Titolo IV relativo al SIS:

Articolo 117

Ciascuna Parte contraente prenderà, al più tardi al momento dell'entrata in vigore della Convenzione, le disposizioni nazionali necessarie per raggiungere un livello di protezione dei dati di natura personale almeno pari a quello derivante dai princìpi della Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone nei riguardi del trattamento automatizzato dei dati di natura personale, nel rispetto della Raccomandazione R 15 (87) del 17 settembre 1987 del Comitato dei Ministri del Consiglio d'Europa tendente a regolare l'uso dei dati di natura personale nel settore della polizia.

La trasmissione di dati di natura personale potrà avvenire soltanto quando le disposizioni di protezione dei dati personali saranno entrate in vigore nel territorio delle Parti contraenti interessate dalla trasmissione.

b) Trattamento automatizzato di altri dati trasmessi in applicazione della Convenzione, ad eccezione di quelli relativi alle domande di asilo:

Articolo 126

Esigenza, al momento dell'entrata in vigore della Convenzione, di un livello di protezione dei dati di natura personale almeno pari a quello derivante dai princìpi della già citata Convenzione del Consiglio d'Europa e trasmissione dei dati subordinata all'efficacia di tale protezione nel territorio delle Parti contraenti interessate dalla trasmissione.

Articolo 129

Per quanto riguarda la trasmissione dei soli dati relativi alla cooperazione di polizia, le Parti contraenti debbono raggiungere un livello di protezione dei dati di natura personale che rispetti i princìpi della già citata Raccomandazione R (87) 15 del 17 settembre 1987 del Comitato dei Ministri del Consiglio d'Europa.

c) Dati trasmessi in applicazione della Convenzione provenienti da un archivio o registrati in un archivio, ad eccezione di quelli relativi alle domande di asilo, al SIS o all'assistenza giudiziaria in materia penale:

Articolo 127

Applicazione del disposto dell'articolo 126 e, per quanto riguarda la trasmissione di dati relativi alla cooperazione di polizia, livello di protezione dei dati che rispetti i princìpi della già citata Raccomandazione R (87) 15.

d) Infine, ai dati che figurano nei dossier si applicano esclusivamente, salvo un'unica eccezione, le disposizioni specifiche di protezione dei dati di cui all'articolo 126, 3° comma, sotto il controllo, se del caso, dell'autorità nazionale competente (articolo 128, 2° comma).

2.2. Sfere d'applicazione rispettive della Convenzione e del diritto nazionale

La Convenzione opera, in materia di protezione dei dati di natura personale, una complessa suddivisione tra la sfera di applicazione delle proprie disposizioni e la sfera di applicazione del diritto nazionale degli Stati-parti.

Diritti delle persone rispetto al SIS

La norma può essere illustrata in questi termini: laddove la Convenzione non prevede disposizioni particolari, è di applicazione il diritto di ogni Parte contraente.

La Convenzione precisa i diritti riconosciuti alle persone e i loro eventuali limiti. Fermo restando il rispetto di tali disposizioni, le persone esercitano i loro diritti in conformità della legislazione di ogni Stato-parte.

a) Diritto di accesso e di comunicazione (articolo 109)

Chiunque può avere accesso alle informazioni contenute nel SIS che lo riguardano. A tal fine, la persona può presentare una richiesta presso le autorità competenti di ogni Stato parte.

Se il diritto nazionale lo prevede, l'autore della domanda può ricevere le informazioni che lo riguardano. Tuttavia, in applicazione del principio della "proprietà dei dati", la comunicazione di queste informazioni è subordinata al fatto che lo Stato in cui è stata presentata la domanda ma che non è l'autore dell'inserimento della segnalazione dia preliminarmente allo Stato autore della segnalazione l'occasione di prendere posizione in merito.

La comunicazione delle informazioni può essere rifiutata se può nuocere all'esecuzione della segnalazione o se ciò risulta necessario ai fini della tutela dei diritti e delle libertà altrui. La comunicazione viene in ogni caso respinta se la persona è segnalata ai fini di sorveglianza discreta.

In allegato sono illustrate le principali caratteristiche della legislazione nazionale di diversi Stati Schengen in materia di esercizio del diritto di accesso alle informazioni oggetto di un trattamento automatizzato.

b) Diritto di rettifica (articolo 110)

Ogni persona può far rettificare dati contenenti errori di fatto che la riguardano o far cancellare dati contenenti errori di diritto che la riguardano. Nella prassi, l'esercizio di questo diritto è ampiamente facilitato dalla comunicazione delle informazioni contenute nel sistema.

c) Diritto di avviare un'azione di rettifica, cancellazione, informazione o indennizzo (articolo 111)

Qualunque persona deve poter adire, nel territorio di ciascuna Parte contraente, la giurisdizione o l'autorità competente relativamente ad una segnalazione che la riguarda. L'esecuzione delle decisioni definitive avviene ad opera dello Stato-parte interessato.

d) Diritto di chiedere una verifica dei dati (articolo 114, 2° comma)

Ogni persona ha il diritto di chiedere alle autorità di controllo nazionali di verificare i dati inseriti nel Sistema d'informazione Schengen che la riguardano nonché l'utilizzazione che ne viene fatta. Se i dati sono stati inseriti da uno Stato diverso da quello

nel quale viene presentata la domanda, il controllo è effettuato in stretto coordinamento con l'Autorità di controllo dello Stato autore della segnalazione.

Se un elenco delle domande presentate negli Stati Schengen relative all'esercizio dei diritti summenzionati non è ancora stato elaborato, dagli elementi d'informazione di cui dispone l'ACC emerge che, per ogni Stato, il numero di tali richieste varia da uno a quaranta per i due anni trascorsi.

Controllo del Sistema d'informazione Schengen

La Convenzione stabilisce i princìpi della protezione dei dati che, fatto salvo il diritto interno di ogni Parte contraente, sono applicabili in caso di trattamento dei dati inseriti nel SIS (articolo 104). Per quanto riguarda il controllo del rispetto di tali principi, la Convenzione opera una ripartizione di competenze tra l'Autorità di controllo comune e le autorità di controllo nazionali (articoli 114 e 115).

La Convenzione elenca i seguenti principi:

a) Principio della finalità della registrazione dei dati e, salvo eccezioni limitativamente elencate, del loro utilizzo:
estradizione, non ammissione, persone scomparse, testimoni, persone citate o condannate, oggetti rubati, persone e veicoli oggetto di sorveglianza discreta o controllo specifico (articoli da 94 a 100 e 102 già citati).

b) Divieto di trattare dati sensibili ed enumerazione limitativa dei dati registrati (articolo 94 già citato).

c) Definizione dei destinatari: accesso limitato alle autorità nazionali competenti in determinati settori e solo per l'adempimento delle loro missioni (articolo 101 già citato).

d) Divieto di copiare le segnalazioni di un'altra Parte contraente in un archivio nazionale e limitazione delle duplicazioni per scopi tecnici (articolo 102).

e) Obbligo di registrazione di ogni decima trasmissione di dati per fini di controllo dell'ammissibilità (articolo 103).

f) Determinazione di una durata di conservazione dei dati (articoli 112 e 113)

g) Obbligo di conservare i dati cancellati per un anno presso l'unità di supporto tecnico per fini di controllo a posteriori della loro esattezza e della liceità del loro inserimento (articolo 113, 2° comma).

Per quanto riguarda il controllo del sistema, la Convenzione stabilisce che ogni Stato-parte debba incaricare un'autorità nazionale di procedere al controllo, in modo indipendente e nel rispetto della legislazione nazionale (articolo 114), dell'archivio della sezione nazionale del Sistema d'informazione Schengen (N.SIS). È compito di tali autorità accertare il rispetto delle disposizioni sulla protezione dei dati della Convenzione e, se del caso, delle disposizioni aggiuntive del diritto nazionale.

Il controllo dell'unità di supporto tecnico (C.SIS) è invece affidato all'Autorità di controllo comune. Questa deve operare nell'osservanza della Convenzione di Schengen, della Convenzione del Consiglio d'Europa sulla protezione dei dati, della Raccomandazione del Consiglio d'Europa sui dati di polizia e del diritto francese.

Scambi di informazioni al di fuori del SIS

Il Titolo VI della Convenzione (articolo 126 e successivi), intitolato "Protezione dei dati di natura personale", è dedicato alle regole applicabili agli scambi di informazioni che non danno luogo ad una segnalazione nel SIS ma avvengono nel quadro dell'applicazione della Convenzione (v. punti 2.1.b e 2.1.c).

I princìpi definiti (finalità, limitazione dei destinatari, esattezza dei dati, ...) sono applicabili ferme restando le disposizioni della legislazione nazionale in materia di protezione dei dati, legislazione che disciplina in particolare l'esercizio dei diritti delle persone interessate.

Il controllo del rispetto delle regole enunciate dalla Convenzione è di competenza delle autorità nazionali.

Il ruolo dell'ACC è complementare: l'Autorità di controllo comune può, su richiesta delle Parti contraenti, formulare un parere sulle difficoltà di applicazione e di interpretazione poste da queste regole.

CAPITOLO 3. L'AUTORITÀ DI CONTROLLO COMUNE E LE CONDIZIONI DELLA SUA INDIPENDENZA.

3.1. Composizione dell'Autorità di controllo comune

L'articolo 115, 1° comma della Convenzione stabilisce che l'Autorità di controllo comune (ACC) si compone di due rappresentanti di ogni autorità di controllo nazionale.

La scelta dei rappresentanti in seno all'ACC spetta ad ogni autorità nazionale che, nella persona del suo presidente o del suo direttore, notifica la designazione dei due membri al segretariato dell'ACC e al suo presidente. L'ACC prende atto di tali designazioni.

Poiché le autorità di controllo nazionali non sono strutturate secondo un unico modello (alcune sono organi collegiali, altre no), i loro rappresentanti sono, a seconda dei casi, membri del collegio, commissari o direttori, responsabili o agenti di un servizio o esponenti esterni.

La Convenzione non prescrive la durata del mandato dei membri dell'ACC; sono pertanto le singole autorità nazionali a determinarlo.

L'Autorità di controllo comune è stata ufficialmente insediata dopo la messa in applicazione della Convenzione il 26 marzo 1995. La sua composizione figura in allegato.

Tuttavia, su iniziativa del sig. Faber, commissario per la protezione dei dati del Lussemburgo e suo primo presidente, già nel mese di giugno 1992 è stata insediata, con l'assenso dei ministri Schengen, un'Autorità di controllo comune provvisoria (ACCP). La sua composizione figura in allegato.

In quel momento, diversi Stati-parte, dopo i test tecnici realizzati con dati fittizi, prevedevano di inserire progressivamente nel SIS dati personali reali. Risultava pertanto indiscutibile l'utilità di una concertazione con l'organo comune incaricato di controllare l'osservanza delle regole in materia di protezione dei dati.

L'ACCP, composta di uno o due rappresentanti delle autorità di controllo nazionali dei cinque Stati all'origine degli accordi e di uno o due esperti indipendenti designati dagli Stati aderenti nel territorio dei quali la Convenzione non veniva ancora applicata, ha adottato un regolamento interno provvisorio fondato sulla regola dell'unanimità. L'Auto-

rità provvisoria ha preparato un questionario sulla natura delle regole di protezione dei dati applicabili in ogni Stato Schengen rispetto alla Convenzione e in particolare al SIS ed ha proceduto ad una prima visita dell'unità di supporto tecnico a Strasburgo.

L'ACCP si è riunita 12 volte, tra il 29 giugno 1992 e il 22 febbraio 1995, nei locali del Segretariato Schengen a Bruxelles ed una volta a Strasburgo, il 15 e il 16 marzo 1994.

L'Autorità di controllo provvisoria ha svolto un ruolo di pioniere ed ha facilitato il compito dell'ACC una volta questa ufficialmente insediata. Come indicato nella presentazione dei lavori, le attività dell'ACC costituiscono il completamento dell'opera avviata dall'ACCP.

Poco dopo la sua costituzione L'Autorità di controllo comune si è riunita cinque volte, dal 17 maggio al 15 dicembre 1995, sotto la presidenza del sig. Von Pommer Esche (Germania) per elaborare, in particolare, la versione definitiva del regolamento interno. Il 14 dicembre 1995 l'ACC ha eletto, per un mandato rinnovabile un anno, il suo nuovo presidente (senatore Türk, Francia, membro della CNIL-Commission nationale de l'Informatique et des libertés) e il vicepresidente (sig. Labescat, Portogallo, avvocato, membro della Commissione nazionale per la protezione dei dati).

Il 5 dicembre 1996 il presidente e il vicepresidente sono stati rieletti per un nuovo mandato di un anno.

L'ACC si è riunita 9 volte nel 1996 e 3 volte dall'inizio del 1997. La prima sessione ufficiale si è tenuta a Strasburgo il 10 e l'11 febbraio 1997.

L'ACC ha istituito due gruppi di lavoro. Il primo si è riunito due volte all'Aja e a Parigi, e il secondo quattro volte a Bruxelles e a Madrid.

3.2. Attività dell'ACC

Sebbene il suo compito principale consista nel controllo dell'unità di supporto tecnico del SIS, compito che è la sola a poter esercitare (articolo 115, 2° comma), all'ACC è altresì attribuito un ruolo di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

La Convenzione di applicazione dell'Accordo di Schengen ne precisa i compiti nei seguenti articoli.

Articolo 106, 3° comma: l'ACC formula un parere in caso di disaccordo tra due Parti contraenti in merito all'esistenza di un errore di diritto o di fatto in una segnalazione. In tal caso, l'ACC deve essere obbligatoriamente adita dalla Parte contraente che non è all'origine della segnalazione.

Articolo 115, 3° comma:

- l'ACC analizza le difficoltà di applicazione o di interpretazione che possono sorgere nell'utilizzo del SIS;
- l'ACC esamina i problemi che possono sorgere durante il controllo indipendente effettuato dalle autorità di controllo nazionali delle Parti contraenti;
- l'ACC esamina i problemi che possono porsi nell'esercizio del diritto di accesso al sistema;
- su un piano più generale, l'ACC elabora proposte armonizzate allo scopo di trovare soluzioni ai problemi esistenti.

Articolo 115, 4° comma: l'ACC elabora relazioni che vengono trasmesse alle autorità alle quali pervengono le relazioni delle autorità di controllo nazionali.

Articolo 118, 2° comma: l'ACC viene informata delle misure particolari adottate da ogni Parte contraente per assicurare la protezione dei dati in occasione della loro trasmissione a servizi situati al di fuori del territorio delle Parti contraenti.

Per quanto riguarda gli scambi di informazioni al di fuori del SIS:

Articolo 126, 3° comma, lettera f): l'ACC può, su richiesta delle Parti contraenti, formulare un parere sulle difficoltà di applicazione e di interpretazione dell'articolo 126 relativo al trattamento dei dati trasmessi, al di fuori del SIS, in applicazione della Convenzione.

In realtà, tra il mese di dicembre 1995 e il mese di marzo 1997, l'ACC ha incentrato i propri sforzi su come ottenere garanzie sulla propria indipendenza e su due compiti ritenuti prioritari (cooperazione tra autorità di controllo nazionali ai fini dell'esercizio del diritto di accesso delle persone al SIS e controllo dell'unità di supporto tecnico).

3.3. Le condizioni dell'indipendenza

Nonostante l'articolo 115 non preveda esplicitamente l'indipendenza dell'ACC, i suoi membri sono i rappresentanti di autorità nazionali incaricate di esercitare, in ogni Stato parte, un controllo indipendente dell'N.SIS. Va inoltre richiamato che la raccomandazione R (87) 15 del 17 settembre 1987 volta a regolamentare l'utilizzo di dati di natura personale nel settore della polizia, esplicitamente citata all'articolo 115 della Convenzione di Schengen, indica (punto 1.1) che l'Autorità di controllo incaricata di vigilare al rispetto dei princìpi enunciati deve essere indipendente.

L'indipendenza è risultata immediatamente necessaria all'ACC, tanto più che, al momento dell'istituzione dell'ACCP, alcune scelte, come quella di eleggere un presidente piuttosto di adottare, come gli Stati-parti, la regola dei turni di presidenza semestrali, sono state poste in discussione dagli Stati Schengen.

L'ACC ha quindi chiaramente espresso, sin dal suo insediamento, le condizioni della sua indipendenza e, di conseguenza, della sua credibilità e della credibilità degli Stati Schengen.

Tra tali condizioni rivestono particolare importanza l'adozione di un regolamento interno e l'ottenimento di una linea di bilancio propria, subordinato all'elaborazione di un rapporto di attività.

L'adozione del regolamento interno

In occasione dell'elaborazione del proprio regolamento interno, l'ACC ha consacrato la regola dell'elezione del presidente e del vicepresidente, instaurato le regole del quorum e dell'adozione di atti a maggioranza e precisato che i propri membri, gli osservatori, gli esperti e i membri del Segretariato sono tenuti alla riservatezza.

L'ACC ha già chiarito diverse questioni relative alle proprie attribuzioni, alle condizioni necessarie per essere membro o osservatore, alla pubblicità dei propri atti e al ricorso ad esperti quando necessario per l'esercizio delle proprie funzioni.

In un secondo tempo è risultato fondamentale definire alcuni elementi di carattere dottrinale.

Per quanto riguarda i propri compiti, l'ACC ha precisato che era in grado di assolvere, oltre a quelle previste dalla Convenzione, altre missioni relative alla protezione dei dati di natura personale legate all'applicazione della Convenzione.

Ha ricordato che, in conformità del disposto della Convenzione, poteva intervenire d'ufficio o a richiesta di un'autorità di controllo nazionale, di una Parte contraente o di un organo del sistema Schengen.

Dopo un'analisi giuridica della Convenzione, l'ACC ha in seguito precisato che possono essere considerati membri a pieno titolo dell'autorità solo i rappresentanti delle autorità di controllo nazionali degli Stati parte che applicano la Convenzione, che hanno ratificato e che hanno soddisfatto le condizioni preliminari.

L'Autorità di controllo comune ha invece deciso di accogliere, con lo status di osservatori senza voto deliberante, i rappresentanti delle autorità di controllo nazionali o gli esperti indipendenti delle Parti contraenti nel territorio delle quali la Convenzione non è ancora stata messa in applicazione.

Sono membri a pieno titolo dell'ACC dal momento del suo insediamento i rappresentanti delle autorità di controllo nazionali della Germania, del Belgio, della Spagna, della Francia, del Lussemburgo, dei Paesi Bassi e del Portogallo.

Hanno lo status di osservatori:

— i rappresentanti dell'Italia, paese che aveva depositato gli strumenti di ratifica, salvo due eccezioni, ma che non disponeva di una legge sulla protezione dei dati e di un'autorità di controllo nazionale. La situazione è cambiata dopo l'entrata in vigore il 9 gennaio 1997 della legge 675 del 31 dicembre 1996 relativa alla protezione delle persone e degli altri soggetti riguardo al trattamento di dati di natura personale e dopo l'istituzione il 5 marzo 1997 dell'Autorità nazionale di controllo;

— i rappresentanti dell'Autorità di controllo nazionale austriaca, paese nel quale il deposito degli strumenti di ratifica da parte di tutti gli Stati-parte non è ancora stato effettuato. La situazione dovrebbe cambiare tra breve;

— i rappresentanti della Grecia, paese che, dato che la procedura di ratifica non era ancora ultimata, non disponeva di una legge sulla protezione dei dati. La situazione è cambiata dopo il voto della legge sulla protezione dell'individuo riguardo al trattamento dei dati personali del 20 marzo 1997.

Dal mese di marzo 1997 partecipano ai lavori, nella qualità di osservatori, i rappresentanti delle autorità di controllo nazionali della Danimarca, della Finlandia e della Svezia.

Otterranno presto lo status di osservatori anche i rappresentanti della Norvegia e dell'Islanda.

L'ACC ha infatti deciso di emendare, entro la fine del primo semestre 1997, il proprio regolamento interno allo scopo di modificare le condizioni necessarie per ottenere lo status di osservatore.

Per quanto riguarda la pubblicità degli atti, l'ACC ha considerato che le riunioni dovrebbero tenersi a porte chiuse ma ha deciso di determinare di volta in volta i destinatari dei propri atti e di pronunciarsi sulla loro eventuale pubblicità, facendo tuttavia salvo l'articolo 115, 4° comma ai sensi del quale le relazioni dell'ACC vengono trasmesse agli organi ai quali riferiscono le autorità di controllo nazionali. Una tale decisione permette all'ACC di comunicare i propri atti ai vari organi Schengen.

L'ACC ha infine affermato la propria facoltà di istituire gruppi di lavoro e di ricorrere ad esperti. Questa disposizione è stata applicata in occasione del controllo presso il C.SIS nel mese di ottobre 1996.

L'ultima versione del regolamento interno, adottato il 19 ottobre 1995, figura in allegato.

Ottenimento di una linea di bilancio propria

Già il 18 ottobre 1995 l'ACC ha chiesto di ottenere una linea di bilancio per il 1996 che permettesse di svolgere in piena indipendenza le attività di sua competenza. Questa richiesta, esaminata dal Gruppo centrale il mese successivo, non è stata accolta. La stessa domanda è stata reiterata con fermezza il 14 dicembre al Gruppo centrale e in seguito al Comitato esecutivo.

La messa a disposizione di una linea di bilancio si è rapidamente rivelata una questione di principio attorno alla quale le posizioni dell'ACC e degli Stati Schengen, in particolare Francia e Germania, si sono irrigidite per tutto il 1996.

In una nota del 4 aprile 1996 relativa ai suoi compiti e al suo programma d'azione, l'ACC ha elaborato un progetto di bilancio all'attenzione del Comitato esecutivo e del Gruppo centrale.

In questo documento l'ACC ricorda che le spese di viaggio dei propri membri per le riunioni di lavoro a Bruxelles continueranno ad essere coperte dalle rispettive autorità di controllo nazionali e chiede:

— la messa a disposizione di un segretariato, in particolare per conservare il registro di tutti gli atti dell'ACC, di sale riunioni e di un servizio di interpretariato e traduzione in tutte le lingue Schengen;

— stanziamenti sufficienti che permettano di ricorrere ad esperti qualora ciò risulti necessario ai fini dell'espletamento dei suoi compiti, in particolare nel caso di una richiesta di parere o di un controllo;

— stanziamenti sufficienti per l'elaborazione di una relazione di attività annuale che illustri l'utilizzo delle risorse;

— il rimborso delle spese di viaggio dei propri membri in occasione della sessione annuale a Strasburgo e, se del caso, di altre missioni specifiche.

Il bilancio complessivo richiesto ammontava a 4.250.000 FB.

Esaminato dai vari organi Schengen tra il 3 luglio 1996 e il 28 gennaio 1997, il progetto di bilancio dell'ACC, dopo ripetuti scambi di lettere, discussioni, riunioni bilaterali informali ed incontri ufficiali, è stato finalmente accettato e, in pratica, adottato dal Gruppo centrale con alcune modifiche, alcune delle quali concordate con l'ACC (soppressione della voce relativa al Segretariato). Va notato che l'ACC ha ricevuto la garanzia, prima di dare il proprio accordo, che i documenti necessari per l'esercizio delle sue funzioni saranno tradotti in tempi soddisfacenti.

Questa decisione è stata annunciata all'ACC il 10 febbraio 1997, vigilia della prima sessione ufficiale a Strasburgo. L'Autorità ha inoltre ricevuto il progetto di bilancio rettificato per un importo di 2.839.950 FB, sottoposto all'approvazione del Comitato esecutivo mediante procedura scritta in marzo 1996.

Il 17 febbraio 1997, il presidente dell'ACC ha informato il Gruppo centrale della viva sorpresa dei membri dell'Autorità nel constatare la soppressione della voce di bilancio relativa alla sessione annuale a Strasburgo ed indicato che l'ACC considerava che il fatto rischiava di pregiudicare lo svolgimento delle sue missioni e il principio stesso della sua indipendenza. Ha tuttavia precisato che l'ACC avrebbe provvisoriamente accettato questo bilancio, fermo restando che questo sarebbe stato oggetto di una valutazione al termine dell'esercizio al fine di esaminare, in particolare, le possibilità di adattamento dei bilanci delle autorità di

controllo nazionali nella prospettiva di coprire, oltre alle spese di viaggio dei rispettivi rappresentanti per le riunioni a Bruxelles, le spese legate a missioni specifiche decise dall'ACC. E' stato inoltre indicato che il bilancio dovrà essere rettificato per tener conto del fatto che cinque nuove delegazioni partecipano ormai ai lavori dell'Autorità di controllo comune.

Il progetto di bilancio richiesto per il 1997 e il progetto rettificato figurano in allegato.

Elaborazione di un rapporto di attività

Nonostante la Convenzione non preveda un tale obbligo, nel mese di aprile 1996 l'ACC ha deciso di elaborare un rapporto di attività annuale. Tale rapporto mira ad illustrare, in modo trasparente, lo svolgimento delle attività e l'esecuzione del bilancio.

Il primo rapporto è in realtà un rapporto biennale a causa delle difficoltà di diverso tipo, ma in particolare finanziarie, incontrate dall'ACC dal momento del suo ufficiale insediamento. In futuro il rapporto sarà annuale.

I primi destinatari di questo rapporto sono il Comitato esecutivo e il Gruppo centrale nonché, ai sensi dell'articolo 115, 4° comma, le autorità di controllo nazionali. Queste sono in seguito incaricate di trasmetterlo alle autorità nazionali e di renderlo pubblico secondo le procedure vigenti per i loro propri rapporti di informazione sul funzionamento del SIS e della Convenzione.

Informazione sul funzionamento della Convenzione

Sin dal 1995 e con maggiore insistenza prima della preparazione della visita di controllo del C.SIS, l'ACC ha ripetutamente chiesto che venissero messi a sua disposizione, per l'esercizio delle sue funzioni, diversi documenti indispensabili per prendere conoscenza dell'applicazione della Convenzione e del funzionamento del SIS. L'ACC ha spesso avuto difficoltà per ottenere tali documenti in tempo utile e, malgrado i ripetuti reclami, alcuni di questi non le sono ancora stati comunicati man mano che venivano elaborati, in particolare quelli del Comitato di orientamento e del Gruppo di lavoro permanente (GLP).

Capitolo 4. Attività realizzate dall'ACC.

La Convenzione prevede che l'ACC formuli pareri o elabori relazioni. Dalla data di messa in applicazione della Convenzione, l'Autorità ha esaminato 180 note e adottato 6 pareri ed un rapporto, salvo il rapporto annuale di attività.

4.1. Attività realizzate

4.1.1. Raffronto tra le regole di protezione dei dati applicabili negli Stati Schengen

Nel 1993, l'ACCP ha deciso di elaborare un questionario destinato a raccogliere informazioni precise in merito alla situazione di ogni Stato Schengen rispetto alle disposizioni della Convenzione in materia di protezione dei dati (questionario SCH/Aut-cont (94) 16 e documento di sintesi SCH/Aut-cont (96) 19).

L'ACC ha completato il documento in alcuni dei suoi punti, in particolare per quanto riguarda le condizioni di esercizio del diritto di accesso in ogni Stato-parte (v. estratto in allegato).

Strumento pratico di diritto comparato, il questionario verte sui testi internazionali e nazionali applicabili in materia di protezione dei dati e, su un piano più generale, di diritti e di libertà delle persone. Il documento è articolato attorno ai seguenti temi specifici: trasparenza (dichiarazione di istituzione dell'N.SIS, pubblicità), fondamento giuridico degli uffici SIRENE e organo centrale competente per l'N.SIS, meccanismi di controllo (composizione e competenze dell'autorità di controllo nazionale), diritti delle persone rispetto al trattamento dei dati che le riguardano (diritto di accesso, di rettifica, di cancellazione, di indennizzo, mezzi di ricorso), misure di sicurezza adottate per gli N.SIS, archivi nazionali utilizzati per alimentare il SIS e autorità abilitate a consultare direttamente il sistema.

Il questionario è destinato ad essere completato da ogni membro a pieno titolo o osservatore. L'Italia e i paesi nordici saranno tenuti a rispondere alle domande nel corso del 1997, nonché la Grecia dovrà rispondere in un secondo tempo, sulla base della recente legge sulla protezione dei dati.

4.1.2. Esame del fondamento giuridico degli uffici SIRENE e del contenuto del Manuale SIRENE

Fondamento giuridico degli uffici SIRENE

Il fatto che la Convenzione non offra uno specifico fondamento giuridico all'esistenza degli uffici SIRENE ha spinto l'ACCP ad invitare le varie delegazioni a precisare se i rispettivi SIRENE erano stati designati, ai sensi dell'articolo 108, per esercitare la competenza centrale per l'N.SIS o se erano il frutto di testi nazionali autonomi e, in tal caso, quale legame li univa all'Autorità centrale.

L'ACCP ha preso atto del fatto che, fatta eccezione per il Belgio, gli Stati che applicano la Convenzione (Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Portogallo) non avevano attribuito ai rispettivi uffici SIRENE, sulla base dell'articolo 108, la competenza centrale per l'N.SIS ma avevano creato questi organi sul fondamento di testi nazionali (Francia, Paesi Bassi, Portogallo) o consideravano che i vari testi nazionali relativi alla polizia o relativi alla Convenzione di Schengen costituissero una sufficiente base giuridica per la loro esistenza (Germania, Spagna, Lussemburgo).

L'Autorità di controllo provvisoria ha inoltre constatato che, ad eccezione del Belgio (dipendenza del SIRENE, organo avente competenza centrale per l'N.SIS, dal Ministero della Giustizia) e del Portogallo (dipendenza dell'Autorità centrale, distinta dal SIRENE, dal servizio "Stranieri e frontiere" del Ministero dell'interno), gli Stati Schengen avevano affidato la competenza centrale per l'N.SIS ai servizi di polizia o di gendarmeria e subordinato i rispettivi SIRENE a questi servizi.

L'ACCP ha fatto presente agli Stati parte della Convenzione di Schengen l'importanza, per ragioni di trasparenza, di prevedere la creazione e le attribuzioni degli uffici SIRENE nel testo stesso della Convenzione.

Contenuto del Manuale SIRENE

Tra il 1993 e il 1994 l'ACCP ha avuto modo di esaminare diverse volte il contenuto del Manuale SIRENE.

Si tratta di un Manuale comune agli Stati Schengen che descrive la procedura che deve permettere di trasmettere a un utente che ha avuto una segnalazione positiva ad una consultazione del SIS le informazioni complementari necessarie alla sua azione.

4.1.3. Cooperazione tra le autorità di controllo nazionali

Parere sull'esercizio del diritto di accesso e sulla cooperazione ai fini della verifica dei dati

In forza dell'articolo 115, 3° comma, l'ACC ha adottato un parere sui princìpi della cooperazione tra autorità di controllo nazionali fondata sull'articolo 114, 2° comma.

La formulazione di tale parere ha permesso di valutare il coordinamento tra le disposizioni relative all'esercizio del diritto di verifica dei dati inseriti nel SIS e l'uso che ne viene fatto e le disposizioni dell'articolo 109 relativo al diritto di accesso.

Il parere è stato comunicato al Comitato esecutivo e al Gruppo centrale nonché alle autorità di controllo nazionali. Queste ultime sono state invitate a costituire un repertorio con gli estremi dei corrispondenti destinato a facilitare la cooperazione.

Prima autorità a cui è stata presentata, il giorno stesso della messa in applicazione della Convenzione, una domanda di diritto di accesso al SIS, domanda seguita da numerose altre domande, la CNIL francese aveva richiamato l'attenzione dell'ACC sulle difficoltà che si pongono per verificare in modo efficace, come previsto nella Convenzione, la pertinenza dell'inserimento dei dati nell'N.SIS da parte di uno Stato-parte.

L'ACC ha in seguito istituito un gruppo di lavoro composto dei rappresentanti tedesco, francese, olandese e belga incaricandolo di esaminare i problemi posti e di proporre una soluzione armonizzata. Il gruppo di lavoro si è riunito due volte in modo informale e il 21 giugno 1996 ha proposto un progetto di parere all'ACC.

Adottato il 26 novembre 1996, questo parere richiama nel suo preambolo il fatto che la Convenzione, nei suoi articoli 109 e 114, opera una distinzione tra il diritto di accesso e di comunicazione e il diritto di chiedere una verifica dei dati e del loro utilizzo.

Il diritto applicabile è il diritto nazionale della Parte contraente nella quale viene presentata la domanda, mentre l'autorità competente per esaminare tali domande è:

— per il diritto di accesso e di comunicazione, il responsabile dell'archivio dei paesi in cui il diritto di accesso è diretto e l'autorità di controllo nei paesi in cui il diritto di accesso è indiretto;

— per il diritto di verifica dei dati e del loro utilizzo, in entrambi i casi l'autorità di controllo.

Quando i dati sono stati inseriti da una Parte contraente diversa da quella nella quale viene presentata la domanda, l'articolo 109 subordina la comunicazione al fatto che la Parte contraente autrice della segnalazione sia stata messa in grado di prendere posizione. L'articolo 114 prevede, dal canto suo, che la verifica avvenga in stretta collaborazione con l'autorità di controllo della Parte contraente autrice della segnalazione.

La cooperazione tra autorità di controllo nazionali è quindi esplicitamente contemplata solo nel caso di una domanda di verifica e l'articolo 114, 2° comma, non prevede una comunicazione all'interessato.

Fatti questi richiami, il parere dell'ACC comporta le seguenti considerazioni.

L'Autorità di controllo nazionale alla quale viene presentata una domanda di diritto di accesso e di comunicazione che comporta una serie di verifiche (diritto francese, belga ...) o alla quale viene direttamente presentata una domanda di verifica può, qualora i dati siano stati inseriti da un'altra Parte contraente, chiedere all'Autorità di controllo di quest'ultima di procedere, in stretta collaborazione, al controllo dei dati. Una tale richiesta non libera l'Autorità di controllo richiedente dalla propria competenza né modifica il diritto applicabile all'esame della domanda.

L'Autorità di controllo nazionale richiesta procede alle verifiche sollecitate dall'Autorità richiedente. Quest'ultima fornisce all'Autorità richiesta tutti gli elementi in suo possesso utili ai fini della verifica.

In esito a tali verifiche, l'Autorità di controllo richiesta trasmette all'Autorità di controllo richiedente tutte le informazioni raccolte.

Qualora nella sua domanda di cooperazione fondata sull'articolo 114, 2° comma, l'Autorità di controllo richiedente abbia citato l'articolo 109, che prevede che le informazioni inserite nel SIS vengano eventualmente comunicate a colui che le ha richieste, L'Autorità di controllo richiesta allega, nella misura del possibile, il parere del proprio governo in merito alla comunicabilità di tali informazioni.

4.1.4. Controllo del C.SIS

Visita dell'ACCP e parere del 18 maggio 1994

Il 16 marzo 1994, l'ACCP ha effettuato una visita presso il sito del C.SIS a Strasburgo. In quel momento il Sistema d'informazione Schengen non era ancora operativo e non ne è stato quindi controllato il funzionamento. La verifica verteva unicamente sugli impianti, l'edificio e i computer.

In esito alla visita, le delegazioni olandese e francese hanno elaborato due rapporti relativi:

- alla protezione fisica (edificio e sito, impianti, protezione fisica degli accessi, protezione contro incendi, inondazioni, furti e vandalismo, organizzazione, procedure ed istruzioni);
- alla protezione operativa (misure e procedure destinate a garantire l'integrità dei dati e a controllare l'accesso agli archivi e alle reti);
- alla protezione organizzativa (gestione, separazione delle funzioni, procedure, responsabilità e competenze);
- alla protezione della continuità del trattamento dei dati (misure e procedure volte a garantire un corretto svolgimento dei processi di trattamento e prevenzione dei danni che potrebbero risultare da un errato svolgimento dei processi).

Una volta esaminati i rapporti, l'ACCP ha considerato che, tutto sommato, le misure e le procedure adottate, soprattutto per quanto riguarda la protezione fisica, erano soddisfacenti alla luce delle prescrizioni dell'articolo 118, 1° comma della Convenzione.

Il 18 maggio 1994 l'ACCP ha tuttavia adottato tre raccomandazioni all'attenzione del Gruppo centrale, affinché questo vigilasse al momento della messa in applicazione della Convenzione:

— alla creazione di una separazione fisica tra gli impianti del C.SIS e quelli del Ministero dell'interno francese collocati nello stesso sito;

— alla conservazione e al trasporto sicuro dei backup di tutti i dati;

— al miglioramento dell'affidabilità dei collegamenti tra il C.SIS e gli N.SIS al fine di escludere o di ridurre sensibilmente i rischi di caduta delle linee.

Il parere dell'ACCP all'attenzione del Gruppo centrale è stato in seguito oggetto di un esame approfondito da parte del Comitato di orientamento le cui conclusioni, adottate dal Gruppo centrale, sono state successivamente portate a conoscenza dell'ACCP il 13 settembre 1994.

Tali conclusioni affermano che le esigenze dell'ACCP vengono soddisfatte grazie ad apposite misure già adottate e che gli sviluppi tecnici attuali e futuri terranno maggiormente conto di tali esigenze.

Controllo dell'ACC, visita dell'11 febbraio 1997 e parere del 27 marzo 1997

Il 26 marzo 1996 l'ACC ha deciso di effettuare, in conformità dell'articolo 115, 2° comma, della Convenzione, una visita di controllo presso il C.SIS.

Il 21 giugno, l'ACC ha istituito a tal fine un gruppo di lavoro, incaricato di effettuare la visita e, preliminarmente:

— di studiare la documentazione tecnica pertinente relativa al C.SIS;

— di definire il tipo di controllo da effettuare;

— di determinare le competenze tecniche degli esperti;

Il gruppo, presieduto dal sig Faber (Lussemburgo) e composto di altri tre membri dell'ACC (sig Von Pommer Esche, Germania, sig. Cueva, Spagna, e sig.ra Carblanc, Francia) e di tre esperti delle autorità di controllo nazionali (sig. Lopez e sig. Perez, Spagna, e sig. Ngo, Francia), si è riunito il 6 settembre presso il Segretariato generale Schengen ed ha sottoposto un progetto di piano di controllo adottato dall'ACC il 12 settembre. Il gruppo di lavoro si è riunito una seconda volta presso il Segretariato Schengen il 2 ottobre per procedere alla ripartizione dei compiti legati alla missione di controllo tra gli esperti e gli altri componenti del gruppo.

Il responsabile del C.SIS e il Gruppo centrale sono stati informati della composizione definitiva del gruppo di controllo il 3 ottobre e lo stesso giorno è stato loro inviato un questionario relativo al C.SIS.

La visita si è svolta durante la settimana del 7 ottobre. La missione di controllo ha avuto termine il 10 ottobre su richiesta delle autorità francesi che hanno chiesto agli esperti del gruppo di cessare le attività in quanto, a loro parere, solo i membri dell'ACC erano abilitati ad effettuare il controllo. Tale decisione ha suscitato l'immediata reazione del presidente dell'ACC e di tutti i suoi membri. Questo incidente è stato all'origine di numerosi incontri tra il Gruppo centrale e l'Autorità di controllo allo scopo di evitare che situazioni di questo tipo si ripetano e, più in generale, di evocare le difficoltà incontrate dall'ACC per ottenere una linea di bilancio propria e per esercitare i propri compiti in condizioni soddisfacenti (v. punto 5.1).

La metodologia seguita dai gruppo di lavoro nell'impostare la visita di controllo è stata la seguente:

— definizione di elenchi di verifica provvisori;

— elaborazione di un questionario destinato ad ottenere informazioni generali sul sistema e i suoi componenti, sulla documentazione, l'organizzazione e la composizione del team di supporto tecnico (exploitation team del C.SIS);

— adattamento degli elenchi di verifica alle caratteristiche specifiche del C.SIS sulla base delle risposte al questionario e della documentazione messa a disposizione sul posto.

La valutazione effettuata dal gruppo di lavoro è stata necessariamente incompleta a causa del gran numero di documenti da analizzare in brevissimo tempo, dell'impossibilità di trasportare ed esaminare copia dei documenti fuori dal centro C.SIS e dal termine prematuro della visita. Di conseguenza, il rapporto del gruppo di lavoro verte unicamente sugli aspetti oggetto di un controllo sufficiente durante la visita tale da permettere, ai sensi della Convenzione ed in particolare del suo articolo 118, una valutazione fondata.

I controlli hanno riguardato i seguenti aspetti.

a) Controlli generali volti a determinare se l'unità di supporto tecnico del C.SIS ha adottato, utilizza e segue metodi e procedure adeguati perché le sue risorse in materia di tecnologie dell'informazione offrano garanzie ragionevoli sul piano della sicurezza

— Gestione e organizzazione

— Struttura organizzativa e separazione delle funzioni

— Norme, regole e procedure

— Software dei sistemi

— Uso delle apparecchiature

— Sicurezza logica del sistema operativo, del sistema di comunicazione, del sistema di gestione della base dati (SGBD)

— Sistema di audit del sistema operativo, del sistema di comunicazione e dell'SGBD

— Sicurezza fisica (sicurezza dell'area e controllo dell'accesso al sito e agli uffici, controllo dell'accesso fisico alle apparecchiature informatiche e alle apparecchiature di comunicazione).

b) Controlli specifici destinati a verificare che l'archivio C.SIS e le modalità di funzionamento dell'unità di supporto tecnico che ne assicura la gestione siano conformi alle disposizioni della Convenzione.

— Integrità degli archivi C.SIS e N.SIS (articolo 92, 2° comma)

— Contenuto (dati inseriti nella base dati, autorità che li inseriscono, identificazione univoca, indicatori di validità, date esistenti)

— Cancellazione automatica di dati di natura personale (articolo 112, 3° comma)

— Stati collegati (articoli 117 e 118, 1° comma, lettera f)

— Supporti informatici amovibili (archiviazione, etichettatura, inventario, trasferimento verso la sede di archiviazione fuori dell'area controllata, cancellazione dei supporti riutilizzabili, distruzione dei supporti non riutilizzabili)

— Inserimento dei dati (articolo 118, 1° comma, lettere c) e g)

— Trasporto (articolo 118, 1° comma, lettera h)

La valutazione di questi controlli generali e specifici ha motivato una serie di raccomandazioni del gruppo di lavoro.

Il rapporto del gruppo di lavoro è stato esaminato dall'ACC l'8 novembre ed adottato il 5 dicembre 1996; in seguito è stato trasmesso al Gruppo centrale e alle autorità francesi responsabili dell'unità di supporto tecnico invitandoli a comunicare eventuali osservazioni.

L'11 febbraio 1997 l'ACC ha tenuto la sua riunione annuale a Strasburgo e si è recata sul sito del C.SIS al fine in particolare di permettere a tutti i suoi membri di prendere conoscenza delle modalità di funzionamento del C.SIS e di procedere ad uno scambio di informazioni con i rappresentanti del Gruppo centrale e i responsabili dell'unità di supporto tecnico.

Considerate le varie constatazioni fatte e dopo aver preso atto delle osservazioni degli Stati Schengen, l'ACC ha adottato il 27 marzo 1997 il rapporto definitivo di controllo.

Ha considerato che la Convenzione è rispettata su vari punti, in particolare:

— le misure di sicurezza prese per proteggere gli edifici dove si trova il C. SIS sono soddisfacenti;

— la base di dati contiene solo dati inseriti dalla Parti contraenti in virtù degli articoli 92.3 e 113.2;

— la base di dati contiene solo i dati personali previsti dall'articolo 94.3 della Convenzione;

— l'utilizzazione degli indicatori di validità è conforme all'articolo 94.4.

Ha invece ritenuto che i seguenti cinque punti meritano di essere evidenziati e accompagnati da proposte di raccomandazioni.

1. Gli archivi delle Parti contraenti della Convenzione non sono identici. Gli archivi di Francia e Lussemburgo presentano un numero sostanziale di differenze rispetto agli archivi degli altri paesi; tali differenze sono state evidenziate nel mese di aprile 1996 e, a distanza di sei mesi, non sono ancora state corrette.

La procedura attualmente applicata per individuare le differenze tra gli archivi risulta inadatta: la sua frequenza (semestrale) e la sua durata di realizzazione (diversi mesi) non permettono di rilevare e rettificare rapidamente le differenze osservate.

Le spiegazioni addotte per giustificare le differenze evidenziate tra gli archivi grazie alle procedure di raffronto tra le basi dati (differenze in termini di concezione delle basi dati) hanno come conseguenza una sistematica violazione (a causa della concezione stessa di tali basi) del disposto dell'articolo 92, 2° comma. A differenza di quanto previsto da questo articolo, infatti, gli archivi delle Parti contraenti non possono mai essere "materialmente identici".

2. E' stato constatato che, in assenza di un audit esterno che valuta il livello richiesto di sicurezza per il sistema informatico, i responsabili dell'unità di supporto tecnico hanno deciso di adottare un certo li-

vello di sicurezza; che tuttavia le misure tecniche richieste per garantire questo livello di sicurezza non erano sempre attuate e che le regole prestabilite erano insufficientemente precise e insufficientemente diffuse.

3. Troppe persone beneficiano di un profilo massimo (super utente) che permette loro di accedere e di modificare il contenuto di qualunque file del sistema informatico (sistema di gestione, base di dati e rete) e d'inibire ogni traccia della loro azione.

4. Le funzioni di tracciatura che permettono di verificare a posteriori le azioni effettuate da vari utenti, indipendentemente dal loro profilo (data, ora, terminale, identificatore dell'utente, tipo di azione) non sono realizzate in modo soddisfacente.

5. E' stata rilevata una sicurezza insufficiente nella gestione e nel trasporto dei supporti magnetici in cui sono conservati i dati del SIS.

L'ACC ha così fatto le seguenti raccomandazioni.

1. Procedere ad un'analisi completa delle differenze individuate tra i file degli N.SIS e il C.SIS e proporre azioni che permettono di eliminare rapidamente tali differenze al fine di evitare che non si riverifichino in futuro.

Modificare la procedura di raffronto dei file in modo che le eventuali differenze presentate dal contenuto dei file nazionali possano essere individuate e corrette rapidamente.

2. Fare procedere ad una certificazione ITSEM/ITSEC e applicare le misure di sicurezza raccomandate; per lo meno garantire al minimo il livello di sicurezza previsto.

3. Limitare l'accesso privilegiato al sistema al minimo possibile; un conto "super utente" permette di effettuare ogni tipo di operazioni sui dati della base, senza alcuna restrizione.

4. Attivare sistematicamente le funzioni di tracciatura che permettono di verificare a posteriori tutte le operazioni effettuate sul C.SIS.

5. Ricorrere in modo sistematico a metodi di crittaggio qualora i dati debbano essere conservati su supporti magnetici.

Considerato che l'articolo 118 è applicabile ad ogni N.SIS e al C.SIS presi separatamente, l'ACC ha infine insistito sulla necessità di completare il controllo del C.SIS con un controllo di ogni N.SIS realizzato su basi tecniche identiche, al fine di dare una valutazione globale pertinente del rispetto da parte di tutti gli Stati Schengen delle disposizioni della Convenzione relative al SIS.

4.1.5. Parere sul progetto pilota relativo ai veicoli rubati

Il 10 febbraio 1997, il Gruppo centrale ha trasmesso all'ACC una domanda di parere proveniente dal Gruppo I "Polizia e sicurezza", relativa alla partecipazione dei Paesi non integrati nel SIS ad un progetto pilota sui veicoli rubati.

Dopo aver preso conoscenza del fatto che il progetto in questione mirava a permettere ai paesi non integrati nel SIS di consultare il sistema per il tramite dei rispettivi funzionari di collegamento, l'ACC ha chiesto informazioni supplementari in merito al tipo di informazioni scambiate e alle modalità di trasmissione.

Una volta ricevute le informazione supplementari, il 7 marzo 1997 l'ACC ha formulato un parere nel quale ribadisce che:

— le informazioni relative alla marca, al tipo, al colore e alle caratteristiche tecniche del veicolo non costituiscono dati di natura personale se non sono riconducibili al numero di targa, al proprietario o al conducente del veicolo;

— gli scambi di informazioni di polizia provenienti da archivi nazionali tra Stati Schengen integrati nel SIS e Stati Schengen nei quali la Convenzione non è stata messa in applicazione sono disciplinati, tramite i meccanismi di cooperazione bilaterale o multilaterale, dalle legislazioni nazionali di protezione dei dati di natura personale e il loro controllo incombe alle autorità di controllo nazionali.

L'ACC ha ritenuto che, in conformità degli articoli 101 e 126, 1° comma, della Convenzione, le informazioni direttamente o indirettamente nominative registrate nel SIS non sono accessibili e non possono essere consultate direttamente dalle autorità delle Parti contraenti nel territorio delle quali la Convenzione non è stata messa in applicazione.

4.1.6. Parere sull'accordo di cooperazione relativo alla contestazione delle infrazioni stradali e all'esecuzione delle relative sanzioni pecuniarie

Il 10 febbraio 1997 il Gruppo centrale ha sottoposto all'ACC una domanda di parere proveniente dal Gruppo III "Cooperazione giudiziaria" relativo ad un progetto di accordo sulle infrazioni al codice della strada.

Il testo prevede, da un lato, l'accesso alle informazioni e ai dati che figurano nei registri della motorizzazione delle Parti contraenti e, d'altro lato, un sistema di notifica diretta e di cooperazione ed un'esecuzione effettiva ad opera di ogni Stato parte delle decisioni dell'Autorità di un'altra Parte contraente, salvo in determinati casi nei quali l'applicazione di una sanzione pecuniaria è limitata od esclusa.

Il progetto si fonda sulla dichiarazione comune dei Ministri e Segretari di Stato del 19 giugno 1990 ai sensi della quale le Parti contraenti si impegnano ad avviare o proseguire discussioni in vari settori, tra cui quello della contestazione delle infrazioni al codice della strada e della reciproca esecuzione delle sanzioni pecuniarie.

Il progetto di accordo costituisce uno strumento di diritto internazionale, distinto ma complementare alla Convenzione di Schengen, in cui si fa esplicito riferimento al capitolo VI relativo alle norme di protezione dei dati applicabili in caso di trasmissione di informazioni non inserite nel SIS.

Dopo aver esaminato le disposizioni relative alla protezione dei dati previste nel progetto di accordo, nel marzo 1997 l'ACC ha formulato un parere nel quale chiede di integrare o esplicitare i seguenti principi:

— il diritto di qualsiasi persona di esigere la rettifica o la cancellazione di dati che la riguardano contenenti errori di fatto o di diritto;

— il principio della cooperazione tra autorità di controllo nazionali di cui all'articolo 128, 1° comma, della Convenzione, ai fine di garantire i diritti di accesso, rettifica e cancellazione;

— la competenza dell'ACC a formulare pareri sugli aspetti generati relativi alla protezione dei dati di natura personale derivanti dall'applicazione dell'accordo.

4.2. Attività in corso

Le principali attività avviate dall'ACC e ancora in corso sono le seguenti.

4.2.1. Guida sui diritti delle persone nei confronti del SIS

Avendo constatato che le disposizioni della Convenzione di Schengen relative alla protezione dei dati di natura personale e, in particolare, al diritto di accesso al SIS sono poco conosciute, l'ACC ha deciso di far elaborare un opuscolo destinato al pubblico per informare le persone dei loro diritti e per dar loro le informazioni pratiche necessarie.

L'ACC ha deciso di dedicare parte del proprio bilancio, nel 1997, alla realizzazione e alla diffusione di questa guida in tutte le lingue Schengen presso le sedi consolari, gli aeroporti e le amministrazioni nazionali.

4.2.2. Interpretazione dell'articolo 102, 2° comma relativo alla duplicazione dei dati SIS per fini tecnici

L'articolo 102, 2° comma, prevede che i dati inseriti nel SIS "possono essere duplicati soltanto per fini tecnici, sempreché l'operazione sia necessaria per la consultazione diretta da parte delle autorità nazionali (...)".

Su richiesta della Commissione per la tutela della vita privata belga, l'ACC ha aperto, sulla base di questo articolo, una riflessione sull'interpretazione dei concetti di "duplicazione per fini tecnici" e di "interrogazione diretta", in particolare in riferimento alle modalità di interrogazione automatizzata di cui all'articolo 92. L'ACC ha inoltre iniziato una valutazione delle conseguenze della duplicazione di tutto o di parte di un N.SIS su CD-ROM per permettere la consultazione da parte delle rappresentanze diplomatiche e consolari.

L'esame delle condizioni di applicazione dell'articolo 102, 2° comma, suscita dubbi per quanto riguarda l'aggiornamento dei dati duplicati e la sicurezza delle trasmissioni effettuate verso servizi situati al di fuori del territorio delle Parti contraenti.

Contrariamente al disposto dell'articolo 118, 2° comma, l'ACC non è stata informata delle misure specifiche adottate per garantire la sicurezza dei dati in questo caso e, nel corso del 1997, formulerà un parere sull'applicazione dell'articolo 102, 2° comma, da parte degli Stati Schengen e proporrà una soluzione armonizzata compatibile con le regole di tutela dei dati previste dalla Convenzione.

4.2.3. Interpretazione dell'articolo 103 relativo al controllo dell'ammissibilità della consultazione del SIS

La delegazione tedesca ha richiamato l'attenzione dell'ACC sulle difficoltà riscontrate nell'applicazione dell'articolo 103 della Convenzione relativo alla registrazione, in tutti gli N.SIS, ad opera dell'Autorità competente per la gestione dell'archivio, di ogni decima trasmissione di dati di natura personale.

Poiché l'articolo 103 non distingue tra le categorie di segnalazioni, il controllo dell'ammissibilità della consultazione del sistema deve vertere su tutte le categorie di segnalazioni (articoli da 95 a 100).

L'ACC ha avviato uno studio sulle soluzioni tecniche adottate dai vari Stati parte per dare esecuzione all'articolo 103 e, nel corso del 1997, formulerà un parere sull'interpretazione di questo articolo e raccomanderà l'adozione di una procedura armonizzata.

4.2.4. Interpretazione dell'articolo 102, 1° comma, relativo al principio della finalità dell'uso dei dati inseriti nel SIS

La delegazione tedesca ha inoltre richiamato l'attenzione dell'ACC sulle difficoltà poste, ai sensi dell'articolo 102, 1° comma, dalla conservazione dei dossier relativi ad una segnalazione dopo la cancellazione della stessa.

L'articolo 102, 1° comma, vieta infatti alle Parti contraenti di far uso dei dati registrati ai sensi degli articoli da 95 a 100 per fini diversi dai fini enunciati per ciascuna delle segnalazioni di cui ai detti articoli.

L'Autorità centrale responsabile della sezione tedesca del SIS conserva tuttavia nel sistema nazionale della polizia giudiziaria, dopo l'esecuzione della segnalazione, le segnalazioni SIS che ritiene riguardino criminali che operano su scala internazionale.

Entro la fine del 1997, l'ACC formulerà un parere su questo importante aspetto relativo alla finalità dei dati.

CAPITOLO 5. IL FUTURO.

L'esperienza acquisita e in particolare le difficoltà conosciute per consolidare la propria autorità e la propria indipendenza e per esercitare i propri compiti in condizioni materiali soddisfacenti permettono all'ACC di constatare che è indispensabile una reale trasparenza tra tutti gli organi Schengen perché la Convenzione possa essere applicata in modo effettivo ed efficace.

L'ACC considera inoltre che gli obiettivi della Convenzione, l'allargamento dello spazio Schengen tramite la conclusione di nuovi accordi e la complessità dei meccanismi di controllo delle norme relative alla protezione dei dati giustifichino uno sforzo di informazione nei confronti del cittadino.

5.1. Trasparenza nelle relazioni tra organi Schengen

Talune delle difficoltà evocate nella presente relazione avrebbero potuto essere evitate se la Convenzione fosse stata più esplicita in merito alle attribuzioni dell'ACC e alla sua indipendenza budgetaria.

L'ACC desidera quindi che il Comitato esecutivo adotti tre misure semplici destinate a regolare una volta per tutte le difficoltà da essa incontrate nell'esercitare i propri compiti in condizioni soddisfacenti.

Informazione dell'ACC in merito al funzionamento della Convenzione

Per poter esercitare in modo effettivo i propri compiti l'ACC deve poter disporre di informazioni regolari e sistematiche in merito agli obiettivi degli Stati Schengen, in particolare nel concludere accordi complementari, nonché ai funzionamento del SIS e alle sue modifiche tecniche prevedibili, quali il progetto SIRENE fase II. l'ACC deve inoltre essere destinataria delle relazioni mensili relative al funzionamento del C.SIS per poter svolgere nel modo più efficace possibile la propria missione di controllo.

Poiché le ripetute richieste di questo tipo sono state esaudite solo sporadicamente e dopo lunghi tempi di attesa, l'ACC insiste perché vengano sistematicamente messe a sua disposizione le informazioni e la documentazione necessarie.

Completamento del protocollo relativo alla realizzazione dei controlli presso il C.SIS

Ai sensi dell'articolo 115 della Convenzione, il controllo del C.SIS viene effettuato dall'ACC nel rispetto delle disposizioni della Convenzione di Schengen e delle disposizioni della Convenzione del Consiglio d'Europa del 28 gennaio 1981, tenendo conto delle disposizioni della Raccomandazione R (87) 15 del 17 settembre 1987 del Comitato dei Ministri del Consiglio d'Europa e in osservanza della legislazione della Parte contraente responsabile dell'unità di supporto tecnico.

In occasione del controllo del C.SIS avvenuto nel mese di ottobre 1996, sono emerse le difficoltà già illustrate. L'ACC si rallegra nel constatare la reale volontà di cooperazione di cui hanno dato prova il Gruppo centrale e le autorità francesi ai fini dell'elaborazione di un protocollo sulla realizzazione dei controlli presso il C.SIS.

Tale protocollo, la cui elaborazione è stata avviata prima della fine del 1996, verte sulla procedura da seguire per informare gli Stati Schengen e i responsabili francesi in merito alla realizzazione di un controllo, sulla qualità delle persone che possono procedere ad un tale controllo, sul livello di abilitazione richiesto per avere accesso ai documenti classificati, in particolare "secret défense", sulla duplicazione di documenti classificati e sulle modifiche tecniche da apportare al C.SIS per permettere un controllo ad opera degli esperti dell'ACC.

L'ACC auspica che il protocollo possa essere approvato quanto prima e che venga presa in debita considerazione la sua domanda di poter usufruire di un "conto utente" che le permetta di avere accesso diretto, senza possibilità di modifica, al sistema operativo e alle basi dati.

Consacrazione definitiva del principio dell'autonomia budgetaria dell'ACC

Pur rallegrandosi, malgrado le riserve già note, del fatto che il principio della creazione di una linea di bilancio sia stata approvata dal Gruppo centrale e dal Comitato esecutivo in marzo 1997 per consentirle di svolgere le proprie missioni, l'ACC desidera che tale bilancio venga incrementato per tener conto dell'aumento del numero dei suoi membri.

L'ACC auspica inoltre che le difficoltà legate alla traduzione in tempo utile dei suoi documenti da parte del Segretariato Schengen possano trovare una soluzione accettabile che non costringa l'Autorità di controllo ad utilizzare le somme riservate alle spese eccezionali di traduzione ad opera di collaboratori esterni.

5.2. Trasparenza nei confronti del cittadino

Gli obiettivi

Trattati internazionali classici conclusi tra Stati membri della Comunità europea, l'Accordo e la Convenzione di applicazione Schengen hanno abolito, pur prevedendo misure di accompagnamento, i controlli alle frontiere interne prima dell'entrata in vigore, inizialmente prevista il 1 gennaio 1993, dell'articolo 7A del Trattato sulle Comunità europee che istituisce uno spazio senza frontiere interne nel quale le persone circolano liberamente.

L'obiettivo delle Parti contraenti, secondo i "considerando" e l'articolo 134 della Convenzione di applicazione, coincide con quello del Trattato sulle Comunità europee completato dall'Atto unico europeo. A lungo termine, una normativa comunitaria ed un nuovo sistema (Si-

stema d'informazione europeo - SIE) dovevano sostituirsi agli Accordi di Schengen ed applicarsi nel territorio di tutti gli Stati membri dell'Unione europea.

Il contesto intergovernativo che è sempre prevalso nelle relazioni tra le Parti contraenti e le istituzioni europee viene consolidato dall'allargamento dei limiti iniziali della Convenzione oltre i confini degli Stati membri dell'Unione europea oppure l'allargamento va visto come una tappa dell'integrazione di nuovi Stati?

Si tratta comunque indiscutibilmente della prova del successo dello "spazio libero Schengen" e delle sue misure compensative di controllo come il SIS.

Detto questo, l'allargamento effettuato nonché i nuovi progetti di accordo prevedono scambi supplementari di informazioni le cui conseguenze non sono al momento trasparenti per il cittadino.

Allargamento della Convenzione di Schengen e complessità dei meccanismi di controllo delle regole relative alla protezione dei dati

Sulla base della dichiarazione comune dei Ministri e Segretari di Stato del 19 giugno 1990, nuovi accordi complementari ma distinti dalla Convenzione di Schengen mirano in effetti ad accrescere i settori della cooperazione tra le Parti contraenti (veicoli rubati, infrazioni stradali).

Quando questi scambi di informazioni non danno luogo a segnalazioni nel SIS le regole applicabili in materia di protezione dei dati vengono definite in modo più o meno preciso e, nella maggior parte dei casi, in particolare quelle relative ai diritti delle persone, prevedono un rinvio al diritto interno di ogni Stato-parte.

Ne conseguono una maggiore complessità dei meccanismi di controllo del rispetto di queste regole ed un rischio di non armonizzazione della loro interpretazione ed applicazione.

L'ACC, tuttavia, non è in grado di limitare efficacemente questo rischio in quanto, fatta eccezione per il SIS, il suo ruolo è secondario e il suo intervento, in linea di principio, subordinato ad una richiesta delle Parti contraenti.

Se i governi sono liberi di definire gli obiettivi della loro cooperazione nel settore della polizia e della giustizia e di determinare i meccanismi di controllo destinati a vigilare all'osservanza dei loro impegni, è altresì loro compito informare il cittadino in merito ai diritti che gli vengono riconosciuti per garantire il rispetto delle libertà pubbliche ed individuali.

Mentre nella sfera del diritto comunitario una direttiva ha armonizzato le leggi nazionali in materia di protezione dei dati, nessuna iniziativa dello stesso tipo è stata promossa dai governi nel settore della cooperazione di polizia e giudiziaria.

Strumenti internazionali distinti senza legame giuridico che li unisca, le convenzioni di cooperazione, quali Schengen ed Europol, prevedono regole di protezione dei dati elaborate ad hoc e alle persone non rimane altra scelta, per esercitare i diritti loro riconosciuti, che avventurarsi in labirinti giuridici.

In tale contesto, l'ACC desidera stringere contatti con L'Autorità di controllo comune Europol, non appena questa verrà istituita, e promuovere con questa azioni di informazione comuni.

Contatti di questo tipo potrebbero presumibilmente risultare da un accordo distinto ma complementare alle due convenzioni.

Ciò consentirebbe a tali autorità di controllo di condividere le loro esperienze in materia di controllo del rispetto delle regole di protezione dei dati e di trasmettere al cittadino una visione più globale dei diritti che gli vengono garantiti nell'ambito degli obiettivi di ogni convenzione.

In un'epoca in cui la cooperazione di polizia e giudiziaria è rafforzata, in cui la creazione di sistemi d'informazione comuni favorisce la trasmissione rapida d'informazioni e di nuovi metodi di lavoro quali il controllo a distanza e l'anticipazione grazie all'analisi delle informazioni, la volontà legittima di garantire la trasparenza agli occhi del cittadino deve essere una preoccupazione prioritaria non solo dell'ACC e delle altre autorità di controllo comuni e nazionali ma anche dei governi.

6.3.2. ALLEGATI (Sintesi).

— Composizione dell'ACCP
— Composizione dell'ACC
— Regolamento interno
— Progetto di bilancio iniziale e progetto rettificato

Composizione dell'Autorità di controllo comune provvisoria - ACCP

Spagna : Perez Tremps
Belgio : P. Lemmens
Paesi Bassi : P. Michael
Lussemburgo : R. Faber; S. Wagner
Francia : J.P. Michel; F. Fourets
Germania : W. Pommer Esche
Italia : A. Galasso
Portogallo : Montalvão Machado
Grecia : Marinos Plexidas

LL/CG SCHENGEN

Autorité commune de contrôle Bruxelles, le 4 mars 1997

SCH/Aut-cont (95) 19 rev 3

NOTE DE COMPILATION
COMPOSITION DES DÉLÉGATIONS
DE L'AUTORITÉ COMMUNE DE CONTRÔLE
(COMPOSIZIONE DELLE DELEGAZIONI DELL'AUTORITÀ DI CONTROLLO COMUNE)

La Belgique a communiqué officiellement les noms de ses délégués:

M. P. Thomas
Ministère de la Justice - Commission Vie privée
Bld de Waterloo 115 - 1000 Bruxelles
Tél : 542 72 20
fax : 542 72 12
M. B. De Schutter
Commissie bescherming persoonlijke levensfeer - V.U.B.
Pleineaan 2
1050 Brussel
Tel : 629 21 11
Fax : 629 36 33

Les Pays-Bas ont communiqué officiellement le nom de leurs délégués:

MM. P.J. Hustinx & P.A. Michael
Registratiekamer
Prins Clauslaan 20
Postbus 93374
25090AJ' s-Gravenhage
tel: 00 31 70 381 13 00
fax: 00 31 70 381 13 01

L'Espagne a communiqué officiellement les noms de ses délégués:

M. D. Juan Maria Bandres Molet
San martin 13 4
20005 San Sebastian
Tél: 00 34 43 42 24 70
Fax: 00 34 43 43 10 61
M. Miguel Angel Lopez Herrero
Agence de Protection des Données
Paseo de la Castellana 41
28046 Madrid
Tél: 00 341 308 47 02
Fax: 00 341 308 46 92

L'Allemagne a communiqué officiellement les noms de ses délégués:

Dr. J. Jacob, commissaire fédéral à la protection des données
représenté par:
Dr. W. von Pommer Esche
Chef de département auprès du commissaire fédéral à la protection des donnéss
Riemenschnelderstrasse, 11
53175 Bonn (Bad Godesberg)
Tél: 00 49 228 81 99 50
Fax: 00 49 228 81 99 550

Prof.Dr. R. Hamm, commissaire du Land de Hessen à la protection des données représenté par:

Mme A. Schriever-Steinberg, chef du département auprès du commissaire hessois à la protection des données
Uhlandstr, 4
65189 Wiesbaden
Tél: 0049 611 1408 0
fax: 00 49 611 37 85 79

La France a communiqué officiellement les noms de ses délégués:

M.A. Türk et Melle F. Fourets
C.N.I.L.
rue Saint Guillaume, 21
75340 Paris Cédex 07
Tél : 00 33 1 53 73 22 22
fax : 00 33 1 53 73 22 00

Le Portugal a communiqué officiellement les noms de ses délégués:

Dr. J.A. M. Labescat da Silva
Dr. Nuno Albuquerque Morais Sarmento
Rua de S. Bento, 148 3° Andar
1200 Lisbonne
Tl :00 351 1 39 601 41
Fax :00 351 1 39 76 832

Le Luxembourg a communiqué officiellement les noms de ses délégués:

M. R. Faber et M. S. Wagner, représentants effectifs
Secrétariat de la Commission
Ministère de la Justice
2934 Luxembourg
Tél: 00 352 478 45 46
Fax :00 352 227 661

M. Cl. Nicolay et M. Jean Wagner, représentants suppléants

L'Autriche a communiqué officiellement les noms de ses délégués en tant qu'observateurs:

Mme E. Souhrada
Ballhausplatz 1
A-1014 Wien
Österreich
tel: 00 43 1 1531 15/2679
fax: 00 43 1 53 115/2690

Italie: en tant qu'observateurs

M.S. Neri
tel. 00 39 6 67 60 46 93
fax 00 39 95 62 12 20
fax 00 39 6 676 096 78

M. G. Buttarelli
tel 00 39 6 68 18.637
fax 00 39 6 68 18.669

Grèce: en tant qu'observateur

M.I. Papageorgiou
tel: 00 301 322 9127
fax 00 301 323 11 54

Islande: en tant qu'observateur

Mr. S. Johannesdóttir
Mr. T. Orlygsson

Data Protection Commission
Ministry of Justice
Armarhvoll
150 Reykjavik - Islande
tel. 00 354 560 90 10
fax O0354 552 73 40

Danemark: en tant qu'observateur

Ms. Lotte N. Jørgensen

Registertilsynet
Christians Brygge 28 - 1559 København V
Danemark
tel. 00 45 33 14 38 44
fax 00 45 33 13 38 43

Suède: en tant qu'observateur

Ms. A. Bondestam
General-Director

Ms. B-M. Wester
Admnistrative Officer

Datainspektionen
box 8114
S-104 20 Stockholm - Sweden
tel. 00 46 8 657 61 00
fax 00 46 8 650 86 13

Norvège: en tant qu'observateur

Ms G. Slettemark
Datatilsynet
Postboks 8177 Dep. 0034 Oslo
tel. 00 47 22 42 19 10
fax 00 47 22 42 23 50

Finlande: en tant qu'observateur

Ms. J. Meklin
Office of the Data Protection Ombudsman
P.O.Box 170 - Fin-00131 Helsinki
tel. 00 358 9 18 251
fax 00 358 9 18 25 7835

BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 14 dicembre 1995
SCH/Aut-contr (95) 25 rev 4
Traduzione: orig./FR

REGOLAMENTO INTERNO DELL'AUTORITA' DI CONTROLLO COMUNE

approvato dall'ACC il 2 febbraio 1996

L'Autorità di controllo comune,

visto l'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 relativo alla eliminazione graduale dei controlli alle frontiere comuni, firmato il 19 giugno 1990, denominata in appresso "la Convenzione", adotta il 19 ottobre 1995 il seguente regolamento interno:

Articolo 1 - Compiti

1) L'Autorità di controllo comune assolve, conformemente al presente regolamento interno, i compiti previsti dalla Convenzione e qualsiasi altro compito relativo alla protezione dei dati di natura personale che essa ritenga connesso con l'applicazione della Convenzione.

2) Nell'esercizio dei suoi compiti, l'Autorità di controllo comune può intervenire d'ufficio, o su richiesta di un'Autorità di controllo nazionale di uno Stato Schengen o di una Parte contraente o di un organo del Sistema Schengen, secondo le disposizioni della Convenzione.

Articolo 2 - Composizione

1) L'Autorità di controllo comune si compone, conformemente all'articolo 115 della Convenzione, di due rappresentanti dell'Autorità di controllo nazionale di ogni Parte contraente di cui all'articolo 114 della Convenzione. Ciascuna delegazione dispone di un voto deliberante.

2) L'Autorità di controllo comune può, su decisione presa all'unanimità, concedere lo status di osservatore senza voto deliberante ai rappresentanti o agli esperti indipendenti delle Parti contraenti sul cui territorio la Convenzione non è ancora entrata in vigore.

3) I membri dell'Autorità di controllo comune, nonché gli osservatori, non possono essere membri di un gruppo di lavoro o di un'autorità - che non sia l'Autorità di controllo nazionale per la protezione dei dati di natura personale - istituiti in virtù della Convenzione. Possono tuttavia aggregarsi alle delegazioni nazionali in qualità di esperti.

4) Un membro dell'Autorità di controllo comune che si trovi nell'impossibilità di partecipare ad una riunione può farsi sostituire da una persona designata dall'Autorità di controllo nazionale in conformità del presente articolo.

5) I membri dell'Autorità di controllo comune possono farsi accompagnare da un esperto che li assiste.

Articolo 3 - Presidenza

1) L'Autorità di controllo comune elegge il presidente e il vicepresidente tra i suoi membri. Essi sono eletti a maggioranza dei due terzi delle delegazioni di cui all'articolo 2, par. 1. Il loro mandato ha una durata di un anno, rinnovabile una volta.

2) Il vicepresidente fa parte di una delegazione che non è quella del presidente; sostituisce il presidente in caso di assenza o di impedimento.

3) In caso di vacanza prima dello scadere del mandato del presidente o del vicepresidente, si provvederà alla sua sostituzione. Il membro eletto per sostituire il presidente o il vicepresidente assicura le sue funzioni per la restante durata del mandato.

Articolo 4 - Ruolo del Presidente

1) Il presidente rappresenta l'Autorità di controllo comune. Vigila sul suo buon funzionamento. Convoca l'Autorità di controllo comune e stabilisce il luogo, il giorno e l'ora delle riunioni. Apre e chiude le riunioni. Dirige le discussioni. Il presidente stabilisce l'ordine del giorno provvisorio.

2) Al fine di preparare le deliberazioni dell'Autorità di controllo comune, il presidente può designare, per un determinato tema, uno o più relatori tra i membri.

Articolo 5 - Funzionamento

1) L'Autorità di controllo comune si riunirà non meno di due volte l'anno. Si riunisce anche su iniziativa del presidente, in caso di richiesta motivata, scritta o orale, fatta in sede di riunione di almeno tre delegazioni di cui all'articolo 2, par. 1. Si riunisce inoltre nei casi previsti dalla Convenzione.

2) Tranne nei casi ritenuti urgenti dal presidente, le convocazioni sono inviate almeno 14 giorni prima della riunione. La convocazione comprende l'ordine del giorno provvisorio della riunione e, eventualmente, la relativa documentazione.

3) L'Autorità di controllo comune adotta l'ordine del giorno definitivo all'inizio di ogni riunione.

Articolo 6 - *Quorum* e regole di maggioranza

1) L'Autorità di controllo comune può tenere una riunione valida solo se sono presenti almeno due terzi delle delegazioni di cui all'articolo 2, par. 1.

2) Fatte salve le disposizioni dell'articolo 13, le deliberazioni dell'Autorità di controllo comune sono adottate allorché la metà più uno delle delegazioni presenti di cui all'articolo 2, par. 1 si esprimono favorevolmente.

3) Ogni delegazione dispone della possibilità di depositare una nota esplicativa del voto.

4) L'Autorità di controllo comune delibera in base a documenti e progetti redatti nelle lingue nazionali degli Stati Schengen.

Articolo 7 - Pubblicità e destinatari delle deliberazioni

1) Le riunioni dell'Autorità di controllo comune non sono pubbliche, salvo decisione contraria dell'Autorità di controllo comune.

2) L'Autorità di controllo comune stabilisce a chi trasmettere le sue deliberazioni nonché le modalità di una loro eventuale pubblicazione, fatto salvo il disposto dell'articolo 115, paragrafo 4 della Convenzione.

Articolo 8 - Procedura scritta

1) Le deliberazioni dell'Autorità di controllo comune possono essere adottate mediante una procedura scritta, a condizione che tutte le delegazioni ne abbiano accettato il principio nel corso di una riunione.

2) Il presidente puo' ricorrere d'ufficio alla procedura scritta in caso di urgenza.

3) In entrambi i casi, il presidente invia il progetto a tutti i membri dell'Autorità di controllo comune. Qualora le delegazioni non si oppongano a tale progetto entro un termine fissato dal presidente di almeno quattordici giorni, a decorrere dalla ricezione del progetto di deliberazione, esso verrà considerato approvato.

4) La procedura scritta nel caso di cui al paragrafo 2 del presente articolo cessa qualora una delegazione chieda, entro un termine di cinque giorni lavorativi, a decorrere dalla data di ricezione del progetto, di poterne discutere in seno all'Autorità di controllo comune.

Articolo 9 - Gruppi di lavoro, esperti, verifiche in loco

1) L'Autorità di controllo comune può istituire gruppi di lavoro definendone i compiti.

2) L'Autorità di controllo comune può far ricorso a esperti. Può elaborare un elenco di esperti ai quali si fa ricorso in via prioritaria.

3) Per quanto concerne il controllo della funzione di supporto tecnico, l'Autorità di controllo comune può designare uno o più dei suoi membri al fine di procedere a verifiche in loco. Se lo ritiene urgente, il presidente puo' procedere d'ufficio a tale designazione. In tal caso, ne informa senza indugio i membri dell'Autorità di controllo comune. I membri incaricati di effettuare verifiche possono farsi assistere da esperti che figurano nel summenzionato elenco.

4) I gruppi di lavoro, gli esperti e i membri dell'Autorità incaricati di procedere a verifiche riferiscono sull'esito delle stesse all'Autorità di controllo comune.

Articolo 10 - Segretariato

1) Il Segretariato dell'Autorità di controllo comune è assicurato sotto la responsabilità del presidente dalle persone e dai servizi messi a disposizione dall'autorità competente della cooperazione Schengen.

2) Il Segretario tiene un registro delle deliberazioni adottate dall'Autorità di controllo comune.

3) La corrispondenza destinata all'Autorità di controllo comune è indirizzata al Segretariato, all'attenzione del presidente.

Articolo 11 - Verbali

1) E' redatto un verbale di ogni riunione dell'Autorità di controllo comune.

2) Sotto la responsabilità della presidenza, il Segretariato elabora il progetto di verbale. Tale progetto è sottoposto all'Autorità di controllo comune per approvazione nel corso della riunione successiva.

3) I membri e gli osservatori possono fare rettificare il verbale in un secondo tempo secondo le osservazioni da loro formulate nella relativa riunione.

Articolo 12 - Riservatezza

Fatta salva l'applicazione dell'articolo 7, paragrafo 2, i membri dell'Autorità di controllo comune, gli osservatori, gli esperti e i membri del Segretariato hanno l'obbligo della riservatezza. Tale obbligo non vige nei confronti delle autorità di controllo nazionali, né delle Autorità nazionali cui i membri e gli osservatori debbono riferire sulle loro attività secondo il diritto nazionale.

Articolo 13 - Modifica del regolamento

Le modifiche del presente regolamento sono adottate all'unanimità dall'Autorità di controllo comune. Tali modifiche entrano in vigore una settimana dopo la loro adozione, salvo disposizioni contrarie.

BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 19 aprile 1996
SCH/Aut-contr (96) 11
Traduzione: orig./FR

Progetto di bilancio annuale dell'ACC in base al programma di azione proposto dal presidente, M. A. Türk (SCH/Aut.Contr. (96) 10).

1) La gestione del segretariato e l'organizzazione delle riunioni plenarie dell'ACC, sulla base di 4 riunioni l'anno (2 riunioni ordinarie previste dal regolamento (art. 5 e due riunioni supplementari)

A) *personale:*	
– 1/6 amministratore, livello A6-5	360.000
– 1/6 segretaria, livello B2-6	260.000
B) *spese generali:*	
– materiale (ammortamento)	15.000
– telefono-fax-spedizione	100.000
– locali	100.000
– traduzione/interpret.	800.000
– fotocopie	20.000
	1.035.000
C) *colazione:*	50.000
TOTALE . . .	**1.705.000**
2) *Una riunione l'anno dell'ACC a Strasburgo*	
– spese di viaggio delle delegazioni (10 delegazioni di 2 persone)	400.000
– spese di viaggio del Segretariato (2 persone) spese di viaggio e prestazioni dell'équipe di interpreti (15 persone)	340.000
– spese di soggiorno (2 pernottamenti colazioni) somma forfetaria: 15.000 FB per persona .	555.000
TOTALE . . .	**1.295.000**
3) *Ricorso ad esperti*	
– somma forfetaria per coprire perizia e spese di viaggio	900.000
4. *Elaborazione e pubblicazione della relazione annuale dell'ACC* (50 pagine, 3.000 es.) (fotocopie, traduzione, spedizione)	350.000
TOTALE BILANCIO ANNUALE DELL'ACC . . .	**4.250.000 FB**

P.S. Per l'anno 1996: le spese di segretariato e dell'organizzazione di 4 riunioni sono previste nel bilancio di funzionamento del Segretariato Schengen
(punto 1 - 1.705.000 FB).
Per il 1996 rimane pertanto da prevedere un bilancio di 2.545.000.

BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1997
SCH/Aut-contr (96) 11, Sa rev.
Traduzione: orig./FR

Progetto di bilancio annuale dell'ACC in base al programma di azione (SCH/Autcont (96) 10).

Il costo delle riunioni ordinarie dell'ACC presso il Segretariato generale (circa 8 riunioni l'anno) è imputato al bilancio Schengen destinato a coprire tutte le riunioni che si svolgono in ambito Schengen.

Per quanto riguarda i compiti particolari di cui l'ha investita la Convenzione, che necessitano per esempio il ricorso ad un esperto, l'ACC ritiene di essere in grado di assolverli in modo indipendente solo se dotata, nel quadro del bilancio Schengen, di una linea di bilancio propria e se può disporre di questi fondi senza dover ottenere l'autorizzazione del Comitato esecutivo.

Per tale motivo, l'ACC ha elaborato il presente progetto di bilancio che copre solo le seguenti voci:

1) *Una riunione l'anno dell'ACC a Strasburgo*	
spese di viaggio delle delegazioni (10 delegazioni di 2 persone)	0[1]
spese di viaggio del Segretariato (2 persone) spese di viaggio e prestazioni dell'équipe di interpreti (15 persone)	340.000
spese di soggiorno (2 pernottamenti - colazioni) somma forfetaria: 15.000 FB per persona	555.000
TOTALE	**895.000**
2) *Missioni di controllo e di perizia*	
somma forfetaria per coprire tali missioni, nonché le spese di viaggio e le spese connesse	900.000
3) *Elaborazione e pubblicazione della relazione annuale dell'ACC*	
(50 pagine, 1.000 es.[2]	
(fotocopie, spedizione)	116.633
traduzione ad opera di un servizio esterno, se necessario	700.000
	816.633
TOTALE BILANCIO ANNUALE DELL'ACC	**2.611.633 FB**

Nota: Questi importi dovranno essere rivisti in caso di partecipazione di nuovi paesi ai lavori dell'ACC.

1) In occasione della sua riunione del 28 gennaio 1997, il Gruppo centrale ha ritenuto che queste spese di viaggio possono essere imputate sui bilanci nazionali.

2) Di concerto con il presidente dell'ACC, in occasione della sua riunione del 28 gennaio 1997, il Gruppo centrale ha ridotto il numero di esemplari da 3.000 a 1.000

6.3.3. Pareri adottati.

SCHENGEN IT

Autorità di controllo comune

Bruxelles, 26 maggio 1997
SCH/Aut-cont (97)-38 riv.
Traduzione: orig./FR

Parere n. 01/97 all'attenzione del comitato esecutivo di Schengen

Oggetto: utilizzazione di supporti tecnici di duplicazione ai fini della consultazione delle segnalazioni ex articolo 96 della Convenzione di applicazione degli Accordi di Schengen da parte delle Rappresentanze diplomatiche consolari di alcuni Stati Schengen all'estero.

Nel corso della riunione del 22 maggio 1997, l'Autorità di controllo comune (in seguito denominata ACC) ha deciso, ai sensi degli articoli 115, 3° comma, e 126, lett. *f)* della Convenzione di applicazione degli Accordi di Schengen (in seguito denominata CSCH), di rivolgere il seguente parere al Gruppo centrale in merito al problema in oggetto:

— constatando che le Rappresentanze diplomatiche e consolari di alcune Parti contraenti (Belgio, Spagna, Paesi Bassi e Francia) utilizzano vari mezzi tecnici al fine di facilitare la consultazione sul posto delle segnalazioni ex articolo 96 CSCH,

— che tali consultazioni sono effettuate ai fini del rilascio di un visto d'ingresso nel territorio Schengen in conformità degli articoli 82, 1° comma in fine, CSCH e 101, 2° comma CSCH,

— che un sistema d'interrogazione diretta del SIS non è sempre disponibile presso le Rappresentanze diplomatiche e consolari di alcune Parti contraenti e questo per molteplici motivi,

L'ACC ha proceduto alla verifica della loro compatibilità con il modello iniziale del SIS come sviluppato nella CSCH.

Infatti, varie disposizioni della CSCH impongono condizioni rigorose per quanto riguarda le procedure di utilizzazione del SIS:

a) vari passaggi dell'articolo 92 CSCH sviluppano "una procedura d'interrogazione diretta" (art. 92, 1° comma, CSCH) basata su una "trasmissione rapida ed efficace" dei dati (art. 92, 2° comma, CSCH).

L'articolo 92, 3° comma, CSCH precisa del resto che l'unità di supporto tecnico, denominata più comunemente C.SIS, comprende un archivio di dati che garantisce l'identità degli archivi dei vari N.SIS "mediante la trasmissione in linea delle informazioni".

Inoltre, anche l'articolo 101, 2° comma, CSCH che autorizza varie autorità ad accedere alle segnalazioni ex articolo 96 evoca il modo "di interrogazione diretta" esercitato proprio dalle autorità competenti per il rilascio di visti e dalle autorità centrali competenti per l'esame delle domande dei visti.

Infine, la procedura d'interrogazione diretta è altresì menzionata all'articolo 101, 4° comma CSCH nonché all'articolo 102, 2° comma, e l'articolo 106, 2° comma CSCH evoca l'eventualità di correzioni o di cancellazioni, vale a dire di modifiche o di aggiornamenti dei dati senza indugio obbligatoriamente a carico di ciascuna Parte contraente.

Dai vari passaggi del Titolo IV della CSCH risulta che il modo di trattamento dell'informazione che gli autori della CSCH hanno voluto sviluppare fa riferimento a un sistema d'interrogazione automatizzata di dati che permette trattamenti di dati in tempo reale.

b) La CSCH prevede un certo numero di disposizioni in materia di sicurezza.

L'articolo 118, 1° comma, CSCH esige da ogni Parte contraente un insieme di garanzie volte a proteggere i dati di natura personale inseriti nel SIS.

Tra queste, l'ACC rileva in particolare:

— le misure atte "ad impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate (controllo dei supporti di dati)" (art. 118, 1° comma, lettera *b)*, CSCH;

— le misure atte "a garantire la possibilità di verificare ed accertare a quali Autorità possono essere trasmessi dati di natura personale mediante apparecchiature di trasmissione di dati controllo della trasmissione)" (art. 118, 1° comma, lettera *f)*, CSCH)

— le misure atte "ad impedire che, all'atto della trasmissione di dati di natura personale nonché del trasporto di supporti di dati, essi possano essere letti, copiati, modificati o cancellati senza autorizzazione (controllo del trasporto)" (articolo 118, 1° comma, lettera *h)*, CSCH).

c) Sono inoltre previste esigenze di registrazione ai fini del controllo.

L'articolo 103 CSCH raccomanda ad ogni Parte contraente di registrare una trasmissione in media su dieci di dati personali ai fini del controllo dell'ammissibilità dell'interrogazione.

In seguito ad una domanda dell'Autorità di controllo comune provvisoria nel gennaio 1994 (vedasi nota SCH/Aut-cont (94) 33 del 10 gennaio 1994), il rappresentante del Comitato di orientamento ha precisato che l'interpretazione data a questo articolo va nel senso di una registrazione minima di una segnalazione positiva su dieci (vedasi nota SCH/OR.SIS (95) 116 del 16 giugno 1995).

PER QUESTO MOTIVO, l'ACC ritiene che l'utilizzazione di mezzi di duplicazione, qualunque sia la loro forma (CD-ROM, dischetto, ...) ai fini della consultazione delle segnalazioni ex articolo 96 della CSCH da parte delle Rappresentanze diplomatiche e consolari di taluni Stati Schengen all'estero sia subordinata a tre condizioni essenziali:

1) le tecniche e i mezzi di duplicazione devono garantire l'identità di dati in tempo reale rispetto al trattamento centrale SIS. Qualsiasi spostamento nel tempo, pur minimo che sia, deve conformarsi alle condizioni previste al punto 4.

2) devono garantire un minimo di protezione nel senso richiesto dall'articolo 118, 1° comma e più in particolare alle lettere *b)*, *d)*, *f)* a *h)* di tale articolo; nonché conformarsi al disposto dell'articolo 118, 3° comma, CSCH.

3) il programma che permette la loro utilizzazione deve permettere una registrazione che soddisfa il disposto dell'articolo 103 CSCH,

tali registrazioni devono essere rimpatriate ogni sei mesi ed essere tenute a disposizione dell'Autorità di controllo nazionale di cui all'articolo 114 CSCH presso l'Autorità che ha la competenza centrale per la sezione nazionale del SIS di cui all'articolo 108, 1° comma, CSCH.

4) in caso di utilizzazione dei mezzi di duplicazione che presentano un rischio di mancanza d'identità di dati, l'ACC raccomanda insistentemente che la Parte contraente che assume in tal modo la sua responsabilità, come prevista dagli articoli 92, 2° comma, e 116 della CSCH, si obbliga:

— in caso di segnalazione della persona nel supporto di duplicazione utilizzato, a fare una verifica in tempo reale (rete, telefono, fax) per accertarsi della conferma di tale informazione;

— in caso di non segnalazione della persona nel supporto di duplicazione utilizzato, ad accettare la sua responsabilità in caso di segnalazione di questa stessa persona intervenuta nel lasso di tempo tra la fissazione dei dati sul duplicatore e il tempo reale. Questa responsabilità può venir meno solo mediante la prova di una verifica in tempo reale al momento della domanda di ottenimento del visto.

BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 55, 2a rev.
Traduzione: orig./DE

Parere n. 98/1 dell'Autorità di controllo comune destinato al Comitato esecutivo.

Oggetto: Conservazione dei dossier ad avvenuta cancellazione di una segnalazione.

In occasione della riunione del 3 febbraio 1998, l'Autorità di Controllo comune (di seguito denominata ACC) ha adottato, sulla base dell'articolo 115, 3° comma della Convenzione di Schengen (di seguito denominata CSCH), il seguente parere:

Consapevole del fatto che servizi di polizia nazionali di determinate Parti contraenti continuano a conservare dossier anche ad avvenuta cancellazione di segnalazioni ex art. 95 e segg. CSCH e che ne fanno l'oggetto di fascicoli penali,

che le Autorità di polizia interessate si basano, in tale contesto, sulle disposizioni previste dal diritto nazionale in materia di protezione dei dati cfr. punto 2.1.3, lett. *b)*, del Manuale SIRENE) e che si applicano anche le disposizioni di cui al Titolo VI della Convenzione di Schengen,

l'ACC ha esaminato questa prassi e al riguardo rinvia soprattutto alle seguenti esigenze attinenti al diritto in materia di protezione dei dati.

L'Autorità di controllo comune conferma i princìpi ed i diritti fondamentali in materia di protezione dei dati di cui alla Convenzione di Schengen, in particolare:

a) i dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (artt. 102, 1° comma, e 94, 1° comma, CSCH). Una deroga a tale principio generale è ammessa soltanto se giustificata dalla necessità di prevenire una minaccia grave imminente per l'ordine pubblico e la sicurezza pubblica dello Stato, per gravi ragioni di sicurezza dello Stato o ai fini della prevenzione di un fatto punibile grave (art. 10, 3° comma, CSCH);

b) qualsiasi utilizzo dei dati non conforme ai commi da 1 a 4 dell'art. 102 sarà considerato uno sviamento di finalità (art. 102, 5° comma);

c) in conformità dell'articolo 112 CSCH, i dati personali inseriti nel Sistema d'Informazione Schengen ai fini della ricerca di persone sono conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti;

d) questi princìpi si applicano, nel quadro di un'interpretazione integrativa della Convenzione, a ogni tipo di trattamento dell'informazione relativo a segnalazioni contenute nel Sistema d'informazione Schengen o basato sulle stesse.

L'Autorità di controllo comune considera pertanto che si debbano adottare le seguenti misure:

a) in caso di soppressione di una segnalazione ai fini della ricerca di persone, ciascuna Parte contraente Schengen, in conformità dell'art. 112 CSCH, è tenuta a cancellare tale segnalazione e a distruggere senza indugio la corrispondente documentazione,

b) le Autorità Schengen devono procedere ad una revisione del Manuale SIRENE allo scopo di cancellare le disposizioni contrarie di cui al suo punto 2.1.3 lett. *b)*.

BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont(97) 42, 2ª rev.
Traduzione: orig./PT

Parere n. 98/2 dell'Autorità di controllo comune destinato al Comitato esecutivo.

Oggetto: Segnalazione nel Sistema d'informazione Schengen di persone la cui identità è stata usurpata.

L'ACC ha esaminato i problemi posti dall'utilizzazione abusiva di alias di persone segnalate nel SIS (vedasi le note SCH/Aut-cont (95) 46, SCH/Aut-cont (97) 41 e SCH/Aut-cont (97) 42), alla luce dei princìpi di protezione dei dati di natura personale previsti dalla Convenzione di Schengen.

La segnalazione del titolare legittimo la cui identità è stata usurpata viene conservata nel SIS dalla maggioranza degli Stati. Attualmente non sembra possibile precisare nel SIS, quanto meno in testo libero, che si tratta di un caso d'identità usurpata.

L'ACC riafferma, in particolare, i seguenti princìpi e diritti fondamentali in materia di protezione dei dati:

a) I dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (articolo 102, primo comma e articolo 94, primo comma). Si tratta di un principio generale a cui si può derogate in via eccezionale se necessario per prevenire una minaccia grave o un reato grave (articolo 102, terzo comma).

b) Qualunque utilizzazione dei dati non conforme ai commi da 1 a 4 dell'articolo 102 sarà considerata uno sviamento di finalità (articolo 102, quinto comma).

c) Chiunque ha diritto di esigere la rettifica o la cancellazione dei dati che lo riguardano contenenti errori di fatto o di diritto (articolo 10).

d) Chiunque ha il diritto di promuovere un'azione dinanzi alla giurisdizione o all'autorità competente in base alla legislazione nazionale, finalizzata ad assicurare il diritto di rettifica o di cancellazione (articolo 111, primo comma).

e) Chiunque ha il diritto di verifica dei dati, esercitato presso l'autorità di controllo nazionale (articolo 114, secondo comma).

L'ACC, tenendo conto in modo proporzionale ed equilibrato dei diritti della persona la cui identità è stata usurpata, previsti dalla Convenzione di Schengen, nonché della necessità di individuare l'usurpatore, formula il seguente parere:

1) Alle segnalazioni nel SIS relative a persone la cui identità è stata usurpata si applica il diritto nazionale, fatte salve norme più rigorose previste dalla Convenzione (articolo 104, primo comma).

2) Spetta alla Parte contraente autrice della segnalazione garantire che i dati siano registrati per gli scopi enunciati e mantenerli attuali ed esatti (articolo 102, primo comma; articolo 106, primo comma; articolo 110; disposizioni in materia di protezione dei dati della Convenzione 108 del Consiglio d'Europa vincolanti per gli Stati Schengen, in particolare quelle dell'articolo 5).

3) In conformità della procedura prevista dall'articolo 106 della Convenzione, spetta alla Parte contraente autrice della segnalazione garantire l'esercizio del diritto di rettifica e di cancellazione dei dati registrati.

4) La conservazione nel SIS della segnalazione di una persona la cui identità è stata usurpata deve essere valutata secondo il principio della proporzionalità, tenuto conto, da un lato, dei diritti della persona la cui identità è stata usurpata e, dall'altro, della necessità di individuare l'usurpatore.

5) Nell'attesa che il SIS II sia messo in funzione, occorre studiare e adottare una soluzione adeguata e se possibile comune che consenta di indicare che si tratta di una segnalazione con identità usurpata. L'ACC esprime la sua volontà di collaborare per trovare tale soluzione.

BPH/CP SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 dicembre 1997
SCh/Aut-cont (97) 50, 2ª rev.
Traduzione: orig. FR

Parere n. 98/3 dell'autorità dl controllo comune all'attenzione del comitato esecutivo

Relativo alle eventuali relazioni tra il Sistema d'informazione Schengen e il progetto ASF - veicoli rubati (Automated Search Facility) di Interpol (97) 81.

L'ACC è stata invitata ad esaminare una nota della delegazione tedesca del Comitato di orientamento SIS (doc. SCH/OR.SIS (97) 81) del 30 aprile 1997 nella quale si presenta il progetto "ASF - veicoli rubati (Automated Search Facility)" in vista di una presa di posizione in ambito Schengen nei confronti di Interpol. Il progetto in questione spinge l'ACC a chiedersi se i dati SIS relativi alle persone e ai veicoli rubati possano essere trasmessi a Interpol.

La nota in oggetto descrive sommariamente il progetto: "Stando alle informazioni di cui dispone la delegazione tedesca, solo quattro Stati (Svezia, Lussemburgo, Russia e Slovacchia) partecipano attualmente alla parte del progetto relativa ai veicoli rubati. Sono disponibili attualmente record relativi a circa 80.000 veicoli rubati. (...) non solo per quanto riguarda in particolare le parti del progetto già in funzione relative alle persone e ai veicoli rubati, ma anche (...)".

E' inoltre prevista l'estensione del progetto ad altre categorie di dati (opere d'arte, carte di credito, documenti e passaporti falsificati, navi/aerei rubati). Considerata l'importanza che possono assumere in futuro progetti di questo tipo, l'ACC ha deciso di formulare un parere in merito a questo progetto e di rispondere al quesito relativo alla possibilità di trasmettere a Interpol nell'ambito del progetto ASF i dati del SIS relativi alle persone e ai veicoli rubati.

Limitandosi ai soli aspetti relativi alla protezione dei dati di natura personale, l'ACC

considerando che:

a) in virtù dell'articolo 101, quarto comma della Convenzione, solo le autorità competenti sono autorizzate a consultare direttamente i dati inseriti nel SIS. A tal fine, ciascuna Parte contraente comunica al Comitato esecutivo l'elenco delle autorità competenti autorizzate a consultare direttamente i dati inseriti nel Sistema d'Informazione Schengen. L'elenco indica per ciascuna autorità i dati che essa può consultare e per quali missioni;

b) in virtù dell'articolo 102, primo comma della Convenzione, le Parti contraenti possono utilizzare i dati soltanto ai fini enunciati per ciascuna categoria di segnalazioni;

— *in virtù dell'articolo 102,* secondo comma, della Convenzione, la duplicazione dei dati è vietata (salvo per motivi tecnici necessari per l'interrogazione diretta da parte delle autorità competenti);

— *in virtù dell'articolo 102,* quarto comma, della Convenzione, i dati non possono essere utilizzati per fini amministrativi;

— *infine, in virtù dell'articolo 102,* quinto comma, della Convenzione, qualsiasi utilizzazione dei dati non conforme ai summenzionati commi di tale articolo sarà considerata uno sviamento di finalità;

c) in virtù dell'articolo 104, primo comma, della Convenzione, fatte salve condizioni più rigorose previste dalla Convenzione, ai dati inseriti nella sezione nazionale de SIS si applica la legislazione nazionale;

d) in virtù dell'articolo 126, primo e secondo comma, della Convenzione, le trasmissioni di dati di natura personale potranno avvenire solo verso le Parti contraenti che hanno adottato le disposizioni nazionali necessarie per ottenere un livello di protezione dei dati personali almeno pari a quello derivante dai princìpi della Convenzione del Consiglio d'Europa del 28 gennaio 1981;

e) in virtù dell'articolo 118, lettera d), della Convenzione, ogni Parte contraente si impegna ad impedire che persone non autorizzate utilizzino i sistemi di elaborazione automatizzata di dati mediante apparecchiature per la trasmissione di dati;

f) i dati relativi alla marca, al tipo, al colore e alle caratteristiche tecniche dei veicoli non sono dati di natura personale a condizione che non sia possibile stabilire un collegamento con un dato che consenta di identificare una persona in relazione con il veicolo come, ad esempio, il numero di targa o di telaio, e di risalire all'identità del proprietario o del conducente del veicolo;

g) le autorità di polizia di ogni paese partecipante al sistema ASF possono scambiare informazioni (nella fattispecie dati di natura personale) provenienti da basi dati nazionali, nella misura in cui, mediante meccanismi di cooperazione di polizia bilaterale o multilaterale, questo scambio di informazioni sia autorizzato o non sia vietato dalla legislazione nazionale in materia di protezione dei dati;

h) si deve tener conto del parere dell'ACC del 7 marzo 1997 relativo al progetto pilota sui veicoli rubati (v. doc. SCH/Aut-cont (97) 2 riv.). In tale parere si trattava di determinare se i paesi non ancora integrati nel Sistema di Informazione Schengen possono avere accesso ai dati del SIS riguardanti i veicoli rubati;

BPH/div. SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 70 riv.
Traduzione: orig.\DE

Parere n. 98/4 dell'Autorità di controllo comune destinato al Comitato esecutivo

Oggetto: Registrazione delle consultazioni di cui all'articolo 103 della Convenzione

L'Autorità di controllo comune,

visto l'articolo 115 della Convenzione di applicazione dell'accordo di Schengen,

consapevole del fatto che il Sistema d'informazione Schengen (SIS) è un sistema di ricerca automatizzato che richiede un'efficace protezione contro l'accesso non autorizzato da parte di terzi,

che la registrazione di una media rappresentativa delle consultazioni del sistema effettuate costituisce un mezzo di protezione adeguato contro l'accesso non autorizzato,

che l'articolo 103 CSCH impone a ciascuna Parte contraente di provvedere affinché una trasmissione in media su dieci di dati personali sia registrata nella sezione nazionale del Sistema d'informazione Schengen dall'organo di gestione dell'archivio, ai fini del controllo dell'ammissibilità dell'interrogazione,

ritiene necessarie le seguenti esigenze minime per quanto concerne una regolare registrazione ai sensi dell'art. 103 CSCH:

1) Deve essere registrata una media sufficientemente rappresentativa di tutte le consultazioni, a prescindere dal fatto che alla relativa interrogazione venga data una risposta positiva o negativa. L'esigenza minima della registrazione del 10% può essere rispettata anche mediante una registrazione ad intervalli regolari.

2) Fanno parte degli elementi essenziali di un'adeguata registrazione:

a) generalità trasmesse dalla persona oggetto della consultazione,

b) identificazione del terminale utilizzato o dell'Autorità che ha proceduto all'interrogazione, badando a che siano adottate tutte le misure utili per consentire l'identificazione dell'utente,

c) luogo, data e ora della consultazione,

d) motivo della consultazione, per es. indicazione del fondamento giuridico di una segnalazione.

3) Ai fini di un controllo, in singoli casi, dell'ammissibilità della consultazione sarebbe inoltre auspicabile indicare il riferimento del dossier o il numero di protocollo della polizia per poter risalire al dossier di base, se disponibile.

4) I dati sono utilizzati esclusivamente ai fini previsti dall'art. 103.

5) I dati registrati vanno cancellati entro 6 mesi.

L'ACC insiste affinché si tenga conto dell'obbligo previsto dall'art. 103 in conformità del presente parere.

6.4. Unione Europea - Gruppo per la tutela delle persone in relazione al trattamento dei dati personali.

6.4.1. Raccomandazioni.

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV

Mercato interno e servizi finanziari
Libera circolazione delle informazioni, diritto delle società e informazione finanziaria
Libera circolazione delle informazioni, protezione dei dati e relativi aspetti finanziari

XV/5012/97-IT

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

RACCOMANDAZIONE 1/97

Norme in materia di protezione dei dati e mezzi di comunicazione

Adottata dal gruppo il 25 febbraio 1997.

SOMMARIO

IL GRUPPO PER LA TUTELA DELLE PERSONE
CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995.[1]

Visti gli articoli 29 e 30, paragrafo 3 della direttiva,

Visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato la presente raccomandazione:

1. INTRODUZIONE

L'articolo 9 della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("la direttiva"), dispone che:

"Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica e letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà di espressione".

Il gruppo, conformemente al mandato disposto dall'articolo 30 paragrafo 1, lettera a) della direttiva, nel corso della prima riunione ha iniziato a discutere la possibile attuazione dell'articolo 9. Le delegazioni britannica e tedesca hanno presentato dei documenti di lavoro. Il dibat-

1) GU n. L 281 del 23 novembre 1995, pag. 31.

tito ha evidenziato le differenze attualmente esistenti nelle legislazioni nazionali per quanto riguarda l'applicazione ai media[2] delle disposizioni sulla protezione dei dati.

Si è riconosciuto che il gruppo potrebbe dare utili orientamenti sull'interpretazione dell'articolo 9 della direttiva. Come prima iniziativa è stato deciso che il segretario raccolga informazioni sull'attuale situazione giuridica ed elabori una relazione tenendo conto del rapporto pubblicato dal Consiglio d'Europa nel 1991 "Data Protection and the Media" (La protezione dei dati e i media).[3]

Il 21 febbraio 1996 è stato distribuito un questionario elaborato dal gruppo.

Nel corso della terza riunione il gruppo ha esaminato un documento di lavoro e ha tratto alcune conclusioni che sono state discusse in dettaglio nel corso della quarta riunione. Alla luce di dette conclusioni è emerso un consenso a favore dell'adozione del documento in forma di raccomandazione ai sensi dell'articolo 30, paragrafo 3, della direttiva. La raccomandazione è stata adottata dal gruppo il 25 febbraio 1997.

La parte che segue sottolinea alcuni aspetti generali dell'applicazione ai media delle norme sulla protezione dei dati compreso il contesto legislativo in cui s'inquadra l'articolo 9 della direttiva. La parte terza riassume alcune delle principali caratteristiche dell'attuale situazione normativa a livello nazionale.[4] La parte quarta contiene le conclusioni della discussione del gruppo sull'applicazione ai media delle norme sulla protezione dei dati.

L'articolo 9 prevede esenzioni e deroghe all'applicazione di alcune disposizioni della direttiva al trattamento di dati personali a scopi giornalistici o di espressione artistica e letteraria. Il dibattito del gruppo si è concentrato sul trattamento dei dati da parte dei media a scopi giornalistici. La presente raccomandazione riguarda quindi le esenzioni e deroghe in relazione a tale trattamento dei dati[5]

2. ASPETTI GENERALI

2.1 Libertà di espressione e tutela della vita privata

L'articolo 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) stabilisce che:

"Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o comunicare informazioni o idee senza ingerenza alcuna da parte delle Autorità pubbliche e senza considerazioni di frontiera .[..]".

Si tratta di uno dei diritti umani fondamentali derivante dalle tradizioni costituzionali comuni a tutti gli Stati membri e di uno degli elementi peculiari del patrimonio giuridico delle società democratiche. Storicamente è stato questo uno dei primi diritti dell'uomo ad essere riven-

---

2) Salvo diversamente indicato, il termine "media" è riferito a tutti i diversi mezzi di comunicazione di massa come la stampa, l'emissione radiofonica e televisiva, ecc.
3) Data protection and the media, studio elaborato dal comitato di esperti sulla protezione dei dati (CJ-PD) sotto l'autorità del Comitato europeo per la cooperazione giuridica (CDCJ), Consiglio d'Europa, Strasburgo 1991.
4) Ulteriori dettagli sulla situazione nazionale in ogni Stato membro figurano nel documento XV D 502/96.
5) La delegazione svedese precisa che la presente raccomandazione non pregiudica la libertà costituzionale garantita in Svezia ad ogni persona di esprimere le proprie opinioni attraverso i media.

dicato e di fatto garantito dalla legge. La stampa soprattutto ha ottenuto garanzie giuridiche e costituzionali specifiche, in particolare contro la censura preventiva.

Il diritto al rispetto della vita privata è ugualmente garantito dall'articolo 8 della CEDU. La protezione dei dati rientra nel rispetto della vita privata garantito da tale articolo. Le deroghe ai princìpi della protezione dei dati e all'articolo 8 della CEDU devono essere conformi alla legge e rispettare il principio di proporzionalità.[6] Ugualmente i limiti alla libertà di espressione, quali potrebbero derivare dall'applicazione dei princìpi in materia di protezione dei dati, devono essere conformi alla legge e rispettare il principio di proporzionalità.[7]

I due diritti fondamentali non devono tuttavia essere considerati in sé contraddittori. In assenza di sufficienti garanzie di tutela della vita privata le persone possono essere restie ad esprimere liberamente le proprie idee. Analogamente il fatto di identificare lettori ed utenti dei servizi di informazione e di tracciarne il profilo rischia di disincentivare le persone a ricevere e dare informazioni.

2.2 Genesi legislativa dell'articolo 9 della direttiva

Conformemente all'articolo K, paragrafo 2 del trattato sull'Unione europea, l'Unione rispetta i diritti fondamentali quali sono garantiti dalla CEDU e quali risultano dalle tradizioni costituzionali comuni degli Stati membri.

Il legislatore comunitario ha riconosciuto il caso particolare dei media e la necessità di conciliare il rispetto della vita privata con la tutela della libertà d'espressione.[8]

L'articolo 19 della proposta originaria della Commissione[9] prevedeva che gli Stati membri potessero accordare deroghe alle disposizioni della direttiva a favore degli organismi di stampa e audiovisivi. La relazione precisava che la principale caratteristica dell'articolo consisteva nell'esigenza di conciliare gli interessi in gioco e che a tal fine si poteva tener conto della possibilità di altri mezzi di ricorso o di un diritto di replica, dell'esistenza di un codice deontologico, dei limiti fissati dalla CEDU e dei princìpi generali del diritto.

L'articolo 9 della proposta modificata dalla Commissione[10] ha reso obbligatoria la concessione di deroghe a favore dei media. Il testo è stato inoltre modificato per includervi i giornalisti e limitare le deroghe alle attività giornalistiche.

L'articolo è stato ulteriormente modificato affinché le deroghe non possano applicarsi indiscriminatamente a tutte le disposizioni sulla tutela dei dati: nel testo attuale le deroghe sono sì obbligatorie, ma "soltanto se necessarie", nel senso che le deroghe ad ogni principio specifico della direttiva devono essere concesse soltanto laddove (in francese

---

6) P. es. European Court of Human Rights (CHR) Sunday Times, Series A, N. 30.
7) Vedere da ultimo CHR Goodwin c. Regno Unito, 27 marzo 1996, non ancora pubblicata.
8) La necessità di conciliare gli interessi tutelati da queste norme è stata riconosciuta anche dalla Convenzione 108/81 ("la Convenzione"). Nella relazione (rapporto esplicativo sulla convenzione relativa alla tutela delle persone fisiche con riguardo al trattamento automatico dei dati personali, Consiglio d'Europa, Strasburgo 1991) la libertà d'espressione è considerata come uno dei "diritti e libertà di altri" per la cui tutela i legislatori nazionali, conformemente all'articolo 9, paragrafo 2, lettera b) della Convenzione, possono derogare ai princìpi fondamentali della protezione dei dati.
9) COM(90) 314 def.-SYN 287.
10) COM(92) 422 def.-SYN 287.

"dans la seule mesure où", in tedesco "nur insofern vor, als sich dies als notwendig erweist") risultino necessarie per conciliare tutela della vita privata e libertà d'espressione.

Inoltre queste deroghe possono riguardare soltanto le disposizioni generali sulla legalità del trattamento dei dati a carattere personale, quelle sul trasferimento dei dati a paesi terzi e quelle sull'Autorità di vigilanza. Conformemente al "considerando" 37 non sarà possibile accordare nessuna deroga alle disposizioni in materia di sicurezza e le Autorità di vigilanza competenti in tale materia dovrebbero essere dotate almeno di alcuni poteri ex-post facto, quali il potere di pubblicare regolari relazioni o di adire le Autorità giudiziarie.

2.3 Sintesi dell'attuale situazione in diritto nazionale

Le varie normative nazionali attualmente affrontano il problema in uno dei modi seguenti:

a) In alcuni casi le norme sulla tutela dei dati non prevedono espressamente esenzioni dall'applicazione ai media di tali disposizioni. È il caso di Belgio, Spagna, Portogallo, Svezia e Regno Unito.

b) In altri casi i media sono esentati dall'applicazione di varie disposizioni sulla protezione dei dati. Si tratta attualmente di Germania[11] Francia, Paesi Bassi, Austria e Finlandia. Deroghe analoghe sono previste anche dai disegni di legge italiani.

c) In altri ancora i media sono esentati dalla normativa generale sulla protezione dei dati e disciplinati da specifiche disposizioni in materia. È il caso della Danimarca per tutti i media e della Germania per le emittenti pubbliche, che non sono soggette alle leggi federali o dei Länder sulla tutela dei dati, ma sottostanno a specifiche disposizioni in materia contenute negli accordi inter-Länder che le regolamentano.

Le differenze tra questi tre tipi di approccio non andrebbero, tuttavia, sopravvalutate. In molti casi, indipendentemente dall'esistenza o meno di una deroga espressa, la normativa sulla tutela dei dati non si applica integralmente ai media a motivo dello status costituzionale particolare delle norme sulla libertà di espressione e di stampa. Tali norme limitano de facto l'applicazione di disposizioni fondamentali per la tutela dei dati o quanto meno il loro effettivo rispetto.

D'altro canto il regime ordinario di tutela dei dati generalmente si applica alle attività non editoriali svolte dai media.

Le autorità garanti della tutela dei dati riconoscono, nell'applicare le norme in materia, la particolarità dei media a prescindere dall'eventuale esistenza di un regime giuridico speciale.

La portata effettiva delle deroghe, inoltre, non può essere valutata in astratto ma dipende dalla struttura generale della normativa sulla tutela dei dati in ogni singolo paese. Chiaramente la portata delle deroghe necessarie dipende da quanto effettivamente le norme sostanziali incidono sulle attività dei media.

Le differenze per quanto riguarda l'applicazione ai media delle norme sulla tutela dei dati possono altresì spiegarsi col mutare delle prospettive sia quanto al ruolo di tali norme, sia quanto all'utilizzazione delle tecnologie dell'informazione da parte dei media. Ai primordi dell'applicazione

---

11) Con un'importante eccezione, per la quale vedere lettera c).

della tutela dei dati l'attenzione, si è concentrata essenzialmente sulle banche dati dotate di una grande unità centrale. Allora tali norme sembravano avere scarsi effetti sui media e non sembrava quindi necessaria nessuna deroga. Il maggior rilievo assunto dalla nozione di trattamento dei dati rispetto alla normativa sulla tutela dei medesimi e l'uso diffuso delle tecnologie dell'informazione da parte dei media hanno sostanzialmente mutato la situazione.

Un importante elemento che emerge dallo stato attuale delle normative negli Stati membri è che i media, o quanto meno la stampa, sono obbligati a rispettare determinate norme che pur non appartenendo alla legislazione sulla tutela dei dati *stricto sensu*, contribuiscono al rispetto della vita privata delle persone. Tale legislazione e la giurisprudenza spesso abbondante in materia accordano forme specifiche di riparazione che sono talvolta considerate un surrogato alla mancanza di mezzi correttivi preventivi in base alla legge sulla tutela dei dati.

Il diritto di replica e la possibilità di ottenere la rettifica delle false informazioni, gli obblighi professionali dei giornalisti e le relative procedure specifiche di autoregolamentazione, insieme alle norme per la tutela dell'onore (disposizioni di diritto civile e penale concernenti la diffamazione), devono esser presi in considerazione nel valutare come sia tutelata la vita privata in relazione ai media.[12)]

L'evoluzione dei media tradizionali verso la pubblicazione elettronica e la prestazione di servizi on-line sembra aggiungere ulteriori elementi di riflessione. La distinzione tra attività editoriali e non editoriali assume nuove dimensioni per i servizi on-line che, diversamente da tutti i media tradizionali, consentono di identificare le persone che li ricevono.

3. Conclusioni

Quanto precede sembra confermare che in ogni Stato membro è necessario riconsiderare il quadro legislativo per l'applicazione ai media delle norme sulla tutela dei dati In proposito è necessario valutare fino a che punto l'applicazione di ciascuna delle disposizioni dei capitoli II, IV e VI della direttiva debba essere limitata per tutelare la libertà di espressione.

A tal fine occorre tener presenti vari elementi:

- Le norme sulla tutela dei dati si applicano normalmente ai media. Deroghe ed esenzioni possono essere accordate unicamente in relazione al capo II (condizioni generali di liceità dei trattamenti di dati personali), al capo IV (trasferimento di dati personali verso paesi terzi) e al capo VI (poteri delle Autorità di controllo). Non è possibile accordare deroghe o esenzioni con riferimento alle disposizioni di sicurezza. Le Autorità garanti responsabili per questo settore devono in tutti i casi conservare alcuni poteri *ex-post facto*.

---

12) Una delle principali conclusioni del lavoro del Consiglio d'Europa in materia è che l'esistenza di correttivi speciali in base alla legge sui media può giustificare deroghe alla normativa sulla tutela dei dati e proprio per questo all'articolo 8 della CEDU, soltanto in determinate circostanze. Il rapporto del Consiglio d'Europa (supra) suggerisce che, per compensare la non applicazione di alcuni princìpi di tutela dei dati, la legislazione sui media si conformi alla risoluzione 428 dell'assemblea parlamentare del Consiglio d'Europa (1970) sui mezzi di comunicazione di massa e sui diritti dell'uomo e alla risoluzione del Comitato dei ministri sul diritto di replica. Il diritto di replica è stato inserito nell'articolo 8 della Convenzione europea sulla televisione transfrontaliera (European Treaty Series, n. 132/89).

- Deroghe ed esenzioni ai sensi dell'articolo 9 devono rispettare il principio di proporzionalità e devono essere accordate soltanto in relazione alle disposizioni che possono ledere la libertà d'espressione e unicamente nella misura necessaria all'effettivo esercizio di tale libertà conciliandola con il diritto al rispetto della vita privata della persona cui si riferiscono i dati.

- Deroghe ed esenzioni ai sensi dell'articolo 9 potrebbero non essere necessarie se la flessibilità delle varie disposizioni della direttiva o le deroghe accordate in base ad altre disposizioni specifiche (che naturalmente vanno interpretate restrittivamente) permettono già di conciliare in modo soddisfacente il rispetto della vita privata con la libertà d'espressione.[13)]

- L'articolo 9 della direttiva rispetta il diritto delle persone alla libertà di espressione. Le deroghe e le esenzioni ai sensi dell'articolo 9 non possono essere accordate ai media o ai giornalisti in quanto tali, ma soltanto a chi effettui il trattamento dei dati personali esclusivamente a scopi giornalistici.

- Deroghe ed esenzioni possono riguardare soltanto il trattamento dati per scopi giornalistici (editoriali) compresa la pubblicazione elettronica. Qualsiasi altra forma di trattamento dati da parte dei giornalisti o dei media è soggetta alle disposizioni ordinarie della direttiva. Tale distinzione è particolarmente importante per la pubblicazione elettronica. Il trattamento di dati degli abbonati a fini di fatturazione o il trattamento a fini di marketing diretto (compreso il trattamento dei dati sull'uso dei media per tracciare il profilo degli utenti) ricade nel regime ordinario di tutela dei dati.

- La direttiva esige che si concilino due libertà fondamentali. Per valutare se le limitazioni dei diritti ed obblighi derivanti dalla direttiva siano proporzionate alla finalità perseguita, consistente nel tutelare la libertà d'espressione, occorrerebbe prestare particolare attenzione alle garanzie specifiche di cui godono le persone in relazione ai media. I limiti al diritto d'accesso e di rettifica preventiva potrebbero essere proporzionati soltanto se le persone godono del diritto di replica o ottengono la rettifica delle informazioni false dopo la pubblicazione.

- Le persone hanno in ogni caso diritto a forme adeguate di riparazione in caso di violazione dei loro diritti.[14)]

Nel valutare se le esenzioni o le deroghe sono proporzionate, occorre prestare attenzione ai vigenti obblighi etici e professionali dei giornalisti e alle forme di autoregolamentazione previste dalla categoria.

Fatto a Bruxelles, addì 25 febbraio 1997

Per il gruppo
Il Presidente
P.J. Hustinx

13) Ad esempio, nel valutare se si debbano accordare esenzioni dall'articolo 11 occorre considerare che l'obbligo di informare le persone cui si riferiscono i dati non si applica quando ciò comporta un onere sproporzionato.

14) Non è possibile nessuna esenzione o deroga al capo III della direttiva.

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV

Mercato interno e servizi finanziari
Libera circolazione delle informazioni - Diritto delle società e informazione finanziaria
Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

XV/5060/97- Final Corr IT
WP2

Gruppo sulla tutela delle persone
in relazione al trattamento dei dati personali

RACCOMANDAZIONE 2/97

Relazione e orientamento del Gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni ("Memorandum di Budapest - Berlino sulla tutela dei dati e della vita privata su Internet")

adottato dal Gruppo il 3 dicembre 1997.

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito con direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1)]

Visti gli articoli 29 e 30, paragrafo 3 di detta direttiva,

Visto il regolamento interno e in particolare gli articoli 12 e 14, ha adottato la seguente raccomandazione:

In occasione della sua 8ª riunione, tenutasi a Bruxelles il 3 dicembre 1997, il Gruppo prende atto della relazione e della guida del Gruppo internazionale sulla tutela dei dati nelle telecomunicazioni ("Memorandum di Budapest - Berlino sulla tutela dei dati e della vita privata su Internet");

Ritiene che tale iniziativa possa contribuire ad una migliore tutela dei diritti fondamentali della persona, in particolare la vita privata, su scala mondiale.

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV

Mercato interno e servizi finanziari
Libera circolazione dell'informazione, diritto delle società e informazione finanziaria
Libera circolazione dell'informazione e protezione dei dati, inclusi gli aspetti internazionali

XV D /5022/97 def.
WP6

1) GU n. L 281 del 23 novembre 1995, p. 31.

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

RACCOMANDAZIONE 3/97

Anonimato su Internet

Adottata dal gruppo di lavoro in data 3 dicembre 1997

IL GRUPPO PER LA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito con la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1]

Visti gli articoli 29 e 30, paragrafo 3 della suddetta direttiva,

Visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato la seguente raccomandazione:

Il gruppo di lavoro nel corso dell'ottava riunione svoltasi a Bruxelles il 3 dicembre 1997 ha adottato il documento di lavoro XV/5022 ("Anonimato su Internet") e ha preso atto della relazione e degli orientamenti espressi dal lavoro internazionale sulla tutela dei dati nelle telecomunicazioni ("Protocollo di Budapest-Berlino relativo alla tutela dei dati e sulla riservatezza su Internet");

Raccomanda che la Commissione europea sviluppi delle proposte sulla base del documento di lavoro allegato ("Anonimato su Internet"; Allegato 1) nonché delle raccomandazioni contenute nel protocollo Budapest-Berlino (Allegato 2) per favorirne l'applicazione in tutte le sedi internazionali appropriate.

DOCUMENTO DI LAVORO - ANONIMATO SU INTERNET

Adottato nel corso dell'ottava riunione

Introduzione

Il rapido sviluppo di Internet e la prolifica crescita dei tipi e del numero di servizi disponibili attraverso questo nuovo strumento sono già stati ben documentati. È chiaro che il fenomeno Internet sta già trasformando le nostre abitudini di vita e di lavoro, apportando enormi cambiamenti alle modalità di acquisto e vendita di beni e servizi e rimodellando il comportamento delle organizzazioni del settore sia pubblico che privato.

Trasformazioni così importanti e complesse comportano inevitabilmente nuovi problemi e nuove sfide per coloro cui spetta il compito di definire, sviluppare e applicare una nuova politica. Inizialmente l'attenzione degli operatori politici si è concentrata sul potenziale di Internet sia come sede per comportamenti penalmente rilevanti o "riprovevoli sulla rete" (come la distribuzione di pornografia infantile) e come "strumento sicuro" di comunicazione per facilitare le attività criminali "fuori della rete".

---

1) GU L.281 del 23 novembre 1995, pag. 31.

A livello europeo queste preoccupazioni hanno costituito la motivazione principale di una serie di iniziative: il Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e d'informazione (COM (36) 483 def.), la Comunicazione della Commissione sul contenuto illegale e nocivo su Internet (COM (96) 487), la risoluzione del Consiglio del 28 novembre 1996 sul contenuto illegale e nocivo e la relazione del gruppo di lavoro sul contenuto illegale e nocivo preparata dal Consiglio informale riunito a Bologna.

Gradualmente, tuttavia, è emerso con chiarezza che vi sono connessi anche altri problemi. La comunicazione della Commissione "Una iniziativa europea in materia di commercio elettronico" (COM (97) 157) cerca di ampliare il dibattito includendo un'ampia serie di altri settori importanti come l'imposizione fiscale (in particolare l'IVA) dell'attività commerciale on-line e la tutela dei diritti di proprietà intellettuale rispetto al contenuto distribuito sulla rete[2)]

In tutti questi settori vengono discusse nuove idee e vengono presentate nuove potenziali soluzioni al fine di assicurare che i valori tradizionali e gli interessi societari sviluppati nel corso di molti decenni possano continuare a essere conservati anche in questa nuova età tecnologica. Un problema che tocca molti di questi ambiti risiede nella difficoltà di individuare il verificarsi di un atto illegale e successivamente identificare il responsabile. Chi è responsabile per l'inserimento di un particolare documento di pornografia infantile su Internet? Chi ha trasmesso un particolare documento protetto da copyright? Chi non ha dichiarato l'IVA rispetto a servizi offerti sulla rete?

Di fronte a questi problemi una reazione comprensibile ha consistito nel suggerire che quanti desiderano accedere a Internet e ai suoi vari servizi in linea debbono essere debitamente identificati e che tutta l'attività in linea possa essere individuabile.

La prospettiva della riservatezza

Lo sviluppo di una politica nei confronti di Internet non avviene in uno spazio vuoto, ma piuttosto sulla base di princìpi e valori ben stabiliti. I critici dei tentativi di limitare o disciplinare l'attività nel ciberspazio citano frequentemente il diritto alla libera espressione, un diritto fondamentale garantito in Europa dall'articolo 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo (ECHR) e incluso come principio generale del diritto comunitario nell'articolo K.2. del trattato sull'Unione europea. Tuttavia, il diritto alla riservatezza (articolo 8 della Convenzione europea dei diritti dell'uomo, analogamente inserito nel diritto comunitario) è altrettanto importante quando si tratta di valutare la politica da adottare nei confronti di Internet.

Nel corso degli ultimi 25 anni è emerso chiaramente che una delle maggiori minacce al diritto fondamentale alla riservatezza è la capacità delle organizzazioni di accumulare un gran numero di informazioni sulle persone, in forma digitale, la quale si presta alla manipolazione, alterazione e comunicazione a terzi ad alta velocità (ed ora a basso costo). Le preoccupazioni in merito a tali sviluppi e al potenziale abuso di questi dati personali ha indotto tutti gli Stati europei (ed ora anche la Comu-

2) Quest'ultimo problema è già stato affrontato nel Libro verde e nella comunicazione della Commissione "Iniziative da prendere a seguito del Libro verde sul diritto d'autore e i diritti connessi nella società dell'informazione".

nità con la direttiva 95/46/CE) ad adottare una legislazione specifica in materia di protezione dei dati, introducendo così un quadro normativo che disciplina il trattamento delle informazioni personali.

Un principio fondamentale in materia di protezione dei dati (vedi articoli 6(l)(c) e 7 della direttiva 95/46/CE) è che i dati personali raccolti in qualsiasi situazione debbano limitarsi a quanto è strettamente necessario e attinente alla finalità in questione. Ogni tipo d'informazione personale costituisce una minaccia potenziale alla riservatezza di una persona ed è quindi necessario fare in modo che, quando tali informazioni vengono raccolte, ciò avvenga per una finalità legittima e che la quantità d'informazioni raccolte sia limitata al minimo indispensabile.

Una caratteristica delle reti di telecomunicazioni e di Internet in particolare è il loro potenziale atto a generare una grande quantità di dati transazionali (i dati generati per assicurare le connessioni corrette). Le possibilità di uso interattivo delle reti (una caratteristica che distingue molti servizi Internet) aumentano ulteriormente il numero di dati transazionali. Quando consulta un giornale sulla rete, l'utilizzatore "interagisce" scegliendo le pagine che desidera leggere. Queste scelte creano un "clickstream" di dati transazionali. Le notizie e i servizi d'informazione più tradizionali, invece vengono consumati in modo molto più passivo (come la televisione, ad esempio), dove la interattività è limitata al mondo off-line delle edicole e delle librerie. Sebbene i dati transazionali in taluni ordinamenti ricevano un certo grado di protezione nel quadro della legislazione che tutela la riservatezza della corrispondenza, la crescita massiccia della quantità di questi dati costituisce tuttavia una fonte di legittime preoccupazioni.

Dato che i servizi sulla rete si sviluppano sia dal punto di vista della loro sofisticazione che della loro popolarità, il problema dei dati transazionali non potrà che aggravarsi. Per ogni dove ci spostiamo su Internet, lasciamo una traccia digitale. Nella misura in cui un sempre maggior numero delle nostre attività quotidiane viene condotto sulla rete, sempre più quello che facciamo, le nostre scelte, le nostre preferenze, diventerà oggetto di registrazione.

Ma i rischi alla nostra riservatezza personale risiedono non solo nell'esistenza di grandi quantitativi di dati personali su Internet, ma anche nello sviluppo del software capace di esplorare la rete e mettere assieme tutti i dati disponibili relativi a una determinata persona. Un articolo apparso recentemente sul Minneapolis Star Tribune ha spiegato come si poteva compilare una biografia dettagliata di una persona scelta a caso, utilizzando tale software e sfruttando le informazioni provenienti da tutti i gruppi di discussione a cui la persona ha partecipato. In tal modo il giornale è stato in grado di scoprire l'indirizzo e il numero di telefono di una persona, il suo luogo di nascita, dove essa ha studiato, la sua professione, il suo attuale posto di lavoro, la sua passione per le recite di attori dilettanti, il tipo di birra che preferisce, i ristoranti e luoghi di vacanza abituali e la sua opinione su argomenti diversi come Bill Gates o lo Stato dell'Indiana considerato "socialmente repressivo". Vi è già una serie di siti negli Stati Uniti che offrono a titolo commerciale questi "servizi di ricerca".

I dati anonimi - un modo per affrontare le preoccupazioni relative alla riservatezza

I dati transazionali costituiscono una minaccia per la riservatezza dell'individuo solo se essi fanno riferimento a una determinata persona. Evidentemente, un modo per venire incontro alle preoccupazioni relative

alla riservatezza consisterebbe nel fare in modo che, quando ciò sia possibile, le tracce create dai dati nell'utilizzo di Internet non consentano l'identificazione dell'utilizzatore. Garantendo l'anonimato, i singoli potrebbero partecipare alla rivoluzione di Internet senza il timore che ogni loro mossa possa essere registrata consentendo di raccogliere informazioni su di loro, che potrebbero essere utilizzate successivamente contro la loro volontà.

La necessità dell'anonimato nelle comunicazioni in rete è già riconosciuta come assolutamente legittima in talune situazioni, ad esempio quando una vittima di un'aggressione sessuale o di una persona che soffre di dipendenza dall'alcol o dalle droghe desidera condividere le sue esperienze con altri, quando una persona che pensa al suicidio desidera consultare uno specialista sulla rete o quando qualcuno desidera denunciare un crimine senza timore di subire ritorsioni. In altre situazioni, l'anonimato garantito serve a proteggere non solo la riservatezza ma anche la libertà di espressione, come nei casi dei dissidenti politici soggetti a un regime politico totalitario che desiderano esprimere la loro opposizione al sistema politico in cui vivono e richiamare l'attenzione sulle violazioni dei diritti umani.

Ma la necessità di anonimato va molto oltre questi casi specifici. Infatti i dati transazionali, identificabili per il solo fatto di esistere, possono costituire uno strumento attraverso il quale il comportamento di una persona può essere seguito e controllato in una misura che non è mai stata possibile prima.

Conciliare la riservatezza con gli altri obiettivi politici

È chiaro quindi che il problema dell'anonimato su Internet è al centro di un dilemma per i governi e le organizzazioni internazionali. Da un lato la possibilità di conservare l'anonimato è essenziale se si vogliono mantenere nel ciberspazio i diritti fondamentali alla riservatezza e alla libertà di espressione. D'altro lato, la capacità di partecipare e comunicare in rete senza rivelare la propria identità contrasta con le iniziative che vengono attualmente sviluppate a sostegno di altri settori importanti come la lotta contro il contenuto illegale e nocivo, le frodi finanziarie o le violazioni al diritto d'autore.

Naturalmente questo apparente conflitto tra diversi obiettivi politici non è nuovo e, come sottolinea il Libro verde della Commissione sulla tutela dei minori e della dignità umana nei servizi audiovisivi e d'informazione, la Convenzione europea per la salvaguardia dei diritti dell'uomo già offre un quadro per la soluzione di tali conflitti: una serie di diritti fondamentali soggetti a talune restrizioni per ragioni specifiche, fra le quali la prevenzione del crimine.

Nell'esaminare tali restrizioni la giurisprudenza della Corte europea per i diritti dell'uomo ha sviluppato il principio di proporzionalità come criterio fondamentale per valutare la conformità di eventuali misure restrittive applicate ai diritti fondamentali garantiti dalla Convenzione.

Il fatto che si sia sviluppata tale giurisprudenza dimostra che è sempre stato necessario trovare un equilibrio fra obiettivi politici contrastanti. Nel contesto degli strumenti di comunicazione più tradizionali "fuori della rete" come lettere e plichi postali, telefono, giornali o trasmissioni radio-televisive, è stato possibile raggiungere un equilibrio fra questi obiettivi. La sfida che debbono affrontare oggi i politici consiste nell'assicurare che questa impostazione equilibrata, che garantisce i diritti fondamentali consentendo restrizioni proporzionate, in circostanze

limitate e specifiche, venga mantenuta nel nuovo contesto del ciberspazio. Un elemento fondamentale ai fini di questo equilibrio sarà costituito dall'ampiezza e dai limiti stabiliti alle possibilità di una persona ad intervenire sulla rete mantenendo l'anonimato.

Imparando dal passato per trovare le soluzioni per il futuro

Sussiste un consenso generale sul fatto che l'attività su Internet non può sottrarsi ai princìpi giuridici fondamentali che vengono normalmente applicati. Internet non può costituire una zona franca dove le regole della società non vengono applicate. D'altronde, le possibilità degli Stati e delle autorità pubbliche di limitare i diritti degli individui e controllare comportamenti potenzialmente illegali non dovrebbero essere più ampie nel quadro di Internet di quanto possano esserlo nel mondo fuori della rete. L'esigenza che le limitazioni ai diritti e alle libertà fondamentali siano debitamente giustificate, necessarie e proporzionate alla luce degli altri pubblici obiettivi, deve valere anche nel ciberspazio.

Il principio di trattare Internet esattamente come le altre tecnologie si rispecchia sia nell'introduzione alla Comunicazione della Commissione sul contenuto illegale e nocivo su Internet che stabilisce "che quello che è illegale fuori della rete rimane illegale anche sulla rete" e nella relazione del gruppo di lavoro sul contenuto illegale e nocivo su Internet che afferma nella sua seconda proposta di azione il principio che "l'informazione su Internet deve avere lo stesso libero flusso consentito all'informazione cartacea".

Sul problema fondamentale dell'anonimato bisogna seguire la stessa impostazione. Come dichiarato correttamente nella "Dichiarazione ministeriale di Bonn"[3], il principio da seguire deve essere che quando l'utilizzatore può scegliere di mantenere l'anonimato fuori della rete, tale possibilità deve sussistere anche sulla rete. I vari servizi e attività disponibili su Internet devono essere esaminati, e dove ciò sia possibile, debbono essere stabilite delle analogie con i servizi esistenti che utilizzano modalità di comunicazione e strumenti di consegna più tradizionali. Tali raffronti forniranno un quadro approfondito di quei settori dove è auspicabile la possibilità di mantenere l'anonimato e di quelli in cui non lo è.

Posta elettronica (corrispondenza da punto a punto attraverso Internet)

La maggior parte delle comunicazioni in posta elettronica identificano correntemente lo speditore sia attraverso il suo indirizzo e-mail o attraverso l'indirizzo IP. Questa informazione è di solito disponibile sia per il destinatario della posta elettronica che per i fornitori di accesso e di servizi che partecipano alla prestazione del servizio posta elettronica. Vi sono tuttavia due tipi di soluzioni alternative che possono offrire un certo grado di anonimato:

1) servizi anonimi di ritrasmissione di posta elettronica - si tratta di un'opzione offerta dal fornitore di accesso o quando una persona si avvale di un servizio specifico "anonimizzante" al quale egli invia la propria posta elettronica. Il ritrasmettitore anonimo invierà il messaggio in forma anonima;

---

3) Dichiarazione della Conferenza ministeriale di Bonn sulle reti d'informazione globali, 6-8 luglio 1997.

2) accesso anonimo alla rete - in questo caso una persona può accedere a Internet mantenendo l'anonimato, ad esempio pagando in anticipo un certo importo di tempo in rete e ricevendo un indirizzo anonimo di posta elettronica o accedendo alla rete attraverso un chiosco pubblico di Internet.

I servizi di ritrasmissione anonima implicano la conservazione di un collegamento fra lo speditore del messaggio e il messaggio stesso che può essere ricostruito in una fase successiva, ad esempio nel quadro di un'indagine di polizia. Quindi esso non garantisce l'anonimato come permette invece la seconda alternativa e vi è la necessità di introdurre delle regole sull'uso fatto dal servizio di ritrasmissione dei dati identificabili che esso conserva. Tuttavia entrambe queste possibilità offrono importanti vantaggi ai fini della riservatezza degli individui e debbono essere salvaguardate e promosse.

L'esistenza di una possibilità di anonimato per la posta elettronica è particolarmente importante se si raffronta il servizio con altre tecnologie delle comunicazioni da punto a punto più tradizionali. Il vecchio servizio postale, ad esempio, è molto più favorevole alla riservatezza, in quanto la spedizione di una lettera normale può avvenire in un totale anonimato. Il servizio postale non è in grado di raccogliere dati transazionali identificabili circa il mittente della comunicazione (a meno che quest'ultimo scelga di rivelarsi sul lato esterno della busta). Il sistema di pagamento più comune (il francobollo postale) è anch'esso totalmente anonimo. È inoltre possibile per il mittente mantenere l'anonimato anche nei confronti del destinatario di una lettera.

I servizi di telefonia tradizionali offrono inoltre un maggior grado di anonimato rispetto alla posta elettronica. L'ampia disponibilità di chioschi pubblici consente un accesso anonimo alla rete e i servizi possono essere pagati con denaro liquido o con carte prepagate anonime. Le chiamate telefoniche eseguite in questo modo non creano dati transazionali identificabili. Quando un abbonato chiama utilizzando il proprio telefono, tuttavia, vengono prodotti dei dati transazionali ed è stato necessario introdurre delle regole sulla produzione di tali dati (attualmente è in atto un processo di armonizzazione a livello comunitario in conseguenza della direttiva "ISDN"[4]) allo scopo di limitare il periodo di conservazione di tali dati e le finalità per le quali essi possono essere utilizzati). Nondimeno, chi chiama resterà sconosciuto per il destinatario di una telefonata finché quest'ultimo non solleva il telefono, a meno che sia funzionante un sistema di identificazione delle chiamate, che consente di indicare il numero dell'apparecchio di chi chiama sull'apparecchio del destinatario prima che questi risponda. L'impatto di tale sistema sulla riservatezza delle parti nelle chiamate telefoniche è tale, tuttavia, che si è ritenuto necessario inserire un articolo specifico nella direttiva citata sopra, che assicuri la possibilità per l'utente di bloccare la trasmissione del proprio numero quando questi desideri farlo. Questa disposizione costituisce un precedente che puo essere preso in considerazione nel campo della corrispondenza sulla rete da punto a punto.

---

4) Direttiva 97/66/CE del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla protezione della riservatezza nel settore delle telecomunicazioni, adottata, ma non ancora pubblicata.

Vi possono essere circostanze nelle quali si giustificano restrizioni alle comunicazioni anonime con la posta elettronica, ad esempio se vi è ragione di sospettare che una particolare comunicazione sia collegata alla preparazione di un atto di terrorismo o di altro grave atto criminale. Tali restrizioni possono comportare che un ritrasmettitore anonimo sia tenuto a fornire alla autorità di polizia la vera identità dei soggetti di una comunicazione. Tuttavia, tali restrizioni dovrebbero rispettare il criterio della proporzionalità ed essere rigidamente applicate in base ai casi individuali.

Newsgroups, Bulletin Boards, e altre sedi di dibattito pubblico

La comunicazione attraverso Internet non assume sempre la forma di corrispondenza privata da punto a punto. Le "newsgroups" e "chat rooms" dedicate ad argomenti particolari o a interessi comuni sono numerose e molto popolari. Qui le persone che contribuiscono con del materiale lo fanno sapendo che esso deve essere accessibile a un vasto pubblico che potrebbe includere bambini o altri soggetti vulnerabili. In tale situazione sussiste un'autentica preoccupazione per la natura dei contenuti che vengono offerti e la necessità di assicurare che contenuti non adeguati non possano essere resi disponibili in queste sedi aperte e/o che sussista una responsabilità qualora ne emerga l'illegalità.

Vi sono varie possibilità con le quali può essere esercitato un certo controllo su questi newsgroups. Un suggerimento è che tutti coloro che contribuiscono con del materiale possano essere identificati, e che venga tenuta traccia dei dati quando viene presentato del materiale. Tuttavia, ci si può chiedere se questa sia una soluzione proporzionata e praticabile al problema. Dopo tutto, nel mondo non virtuale, vi sono numerose bacheche collocate nei posti di lavoro, in scuole e università, sulle quali i singoli sono invitati ad apporre del materiale. Non è concepibile che l'accesso a tali bacheche possa essere rigidamente controllato in maniera analoga.

Tuttavia, esistono anche altre possibilità. Ad esempio, possono essere sviluppate soluzioni contrattuali atte a garantire un certo grado di "qualità del contenuto". Il fornitore del servizio di newsgroup potrebbe assicurare la partecipazione costante di un moderatore ai newsgroups, il cui ruolo sarebbe di controllare i contributi, per individuare un eventuale contenuto illegale e nocivo. Tale moderatore potrebbe assicurare che il contenuto non adeguato possa essere rapidamente eliminato e che le persone responsabili di tale materiale possano essere allontanate dal gruppo. Le chat line e party line telefoniche hanno sempre utilizzato tali meccanismi per controllare il comportamento dei partecipanti. È anche possibile attribuire ai fornitori di servizi un certo grado di responsabilità giuridica per il materiale che viene messo a disposizione, suscitando in tal modo in essi un interesse diretto ad esaminare tutto il materiale che entra e pubblicando solo quello che è considerato legale e accettabile per il consumo del pubblico. In questo scenario è possibile conservare l'anonimato dei contributori, mentre il fornitore di servizi assume un ruolo analogo a quello del direttore per la rubrica della posta di un quotidiano.

Questo potrebbe anche essere un settore dove le soluzioni tecnologiche potrebbero svolgere un ruolo importante. Se l'accesso completamente anonimo ad alcuni centri di discussione dovesse porre dei problemi, gli utilizzatori potrebbero essere autorizzati ad accedere sulla base di una "pseudoidentità" attribuita loro da un fornitore di servizi specializzato analogo ai ritrasmettitori anonimi di cui sopra. In tali

casi, mentre l'anonimato sarebbe normalmente rispettato, in caso di sospetta attività criminale, sarebbe possibile risalire alla vera identità dell'utilizzatore.

È chiaro che contributi interamente anonimi a questi centri di discussione sollevano difficoltà, che non sussistono nel caso della semplice comunicazione da punto a punto, e che debbono essere sviluppati meccanismi adeguati per impedire abusi. Tuttavia, i diritti fondamentali alla riservatezza e alla libertà di espressione non devono essere limitati in maniera sproporzionata da sistemi di identificazione obbligatori, in particolare quando sono disponibili altri strumenti più adeguati di controllo e moderazione del contenuto.

La navigazione passiva per i vari siti su Internet

La maggior parte dei siti di Internet esistono soprattutto per fornire informazioni al grande pubblico e milioni di individui trascorrono il loro tempo sulla rete navigando oziosamente per la miriade di diversi siti disponibili.

La più stretta analogia con questa pratica nel mondo non virtuale potrebbe essere quella del girare in una libreria o in una biblioteca o per i negozi in una città. Come per il navigare in rete, spesso non vi è l'intenzione di acquistare, ma semplicemente si è spinti dalla curiosità a vedere quello che è disponibile. Una differenza chiave, tuttavia, è che mentre il girare in una libreria o per negozi può essere fatto nell'anonimato pressoché completo, la stessa azione fatta sulla rete lascia invariabilmente una traccia digitale permanente e individuabile.

Non vi è una giustificazione dell'interesse generale o di ordine politico perché tali tracce possano essere identificabili, a meno che l'utilizzatore desidera che lo siano. Naturalmente la raccolta dei nomi e indirizzi di posta elettronica dei visitatori di un determinato sito commerciale costituiranno dei dati importanti per il proprietario del sito, che può voler usarlo a fini commerciali. Tuttavia, una simile raccolta di dati di individui che si limitano a navigare dev'essere totalmente trasparente e deve avvenire sulla base dell'autorizzazione dell'utilizzatore. Quanti desiderano navigare sulla rete anonimamente debbono essere liberi e in grado di farlo.

Acquisto di beni e servizi su Internet

Man mano che vengono sviluppati strumenti di pagamento sicuri, assieme a meccanismi relativi all'integrità dei dati e all'autenticazione delle operazioni (ad esempio firma digitale), Internet diventerà sempre di più un'area fondamentale di attività commerciale dove si va non solo per ottenere informazioni, ma anche per acquistare beni e servizi. In questo contesto sorge il problema se una persona per poter fare acquisti attraverso Internet debba poter essere identificabile o se debba sempre essere disponibile l'opzione dell'anonimato.

Nel mondo non virtuale i pagamenti anonimi effettuati con denaro liquido sono comuni e questa è considerata la modalità di pagamento più conveniente ed efficiente per beni e servizi, in particolare nel caso di somme relativamente modeste di denaro. Il venditore del negozietto all'angolo non è interessato tanto all'identità del cliente, quanto al fatto che il denaro che gli viene offerto sia moneta avente corso legale.

Per gli acquisti più importanti è spesso scomodo sia per l'acquirente che per il venditore utilizzare denaro liquido. Le banconote occupano molto spazio in un portafoglio o nella cassa. Tenere molto denaro liquido comporta poi il problema della sicurezza. Per queste ragioni i metodi di pagamento non anonimi come assegni o carte di credito tendono a essere preferiti quando l'importo dell'acquisto è importante.

Naturalmente quando il pagamento viene effettuato utilizzando il credito, l'anonimato non è più un'opzione. Quando si acquista a credito, l'individuo incorre in un debito per il quale è responsabile. E naturalmente ci dev'essere una registrazione che collega l'individuo al debito sorto. Quando viene utilizzata una carta di credito convenzionale la responsabilità della persona è nei confronti dell'emittente della carta piuttosto che direttamente nei confronti del venditore, tuttavia e necessaria una traccia identificabile dell'operazione.

Il commercio elettronico attraverso Internet in linea di principio dovrebbe seguire il modello che è stato stabilito per i pagamenti fuori della rete. I singoli dovrebbero poter scegliere attraverso una varietà di metodi di pagamento sicuri, fra i quali dovrebbe esserci la possibilità di un sistema anonimo. I pagamenti in moneta elettronica dovrebbero offrire decisamente vantaggi rispetto a quelli tradizionali effettuati con denaro liquido, in modo da renderli più attraenti. Anzitutto possono essere conservati importi illimitati, ad esempio, su una piccola carta. In secondo luogo, la carta, senza incidere sull'anonimato, potrebbe prevedere aspetti connessi alla sicurezze come un codice di accesso individuale noto solo all'acquirente, che ridurrebbe notevolmente i rischi nel caso di perdita della carta. Questi aspetti potrebbero fare della moneta elettronica anonima un'opzione attraente anche per i grandi acquisti effettuati sulla rete.

Un requisito fondamentale è che tale moneta elettronica sia "denaro effettivo" verificabile. Ciò implica l'inclusione di tecniche anticontraffazione che garantiscano l'autenticità della moneta elettronica, senza incidere sulla possibilità di utilizzarla in maniera anonima.

Tuttavia vi sono altre considerazioni che devono essere tenute presenti nel valutare la auspicabilità dei metodi di pagamento anonimi sulla rete. Principale fra esse è la lotta contro il riciclaggio del denaro sporco. Il riciclaggio di importanti somme di denaro ottenuto da attività illecite come il traffico di droga, sia in modo anonimo sia utilizzando un'identità fittizia, costituisce un grave problema. Per contribuire a combattere questa attività, nel 1991 è stata adottata una direttiva (91/308/CEE) che cerca di impedire l'uso del sistema finanziario a fini di riciclaggio. Le disposizioni chiave di questa direttiva impongono alle istituzioni finanziarie e creditizie di esigere l'identità dei loro clienti prima di entrare in rapporti d'affari con essi e mantenere delle registrazioni delle operazioni effettuate per almeno un periodo di cinque anni.

La direttiva in se stessa non è tuttavia incompatibile con i pagamenti anonimi. Essa si concentra anzitutto sulle operazioni effettuate con banche o altre istituzioni[5], mentre i sistemi di pagamento elettronico sarebbero utilizzati essenzialmente per operazioni fra soggetti e commercianti che non fanno parte del sistema finanziario. Sarebbe nor-

5) L'articolo 12 comprende una disposizione che nel suo campo di applicazione potrebbe venire estesa a settori come le case da gioco e i commercianti di oggetti di elevato valore (arte, antiquariato, proprietà immobiliare, metalli preziosi).

male per una persona dover dimostrare la propria identità prima di effettuare un prelievo elettronico da una banca, e magari al momento di depositare importanti somme di moneta elettronica. Ma una volta che il denaro gli viene accreditato, non vi è ragione perché esso non sia anonimo come avviene per il denaro tradizionale. Le esigenze delle autorità di polizia nella loro opera di individuazione dei responsabili dei reati di riciclaggio debbono quindi essere vagliate molto attentamente rispetto ai vantaggi per la riservatezza che i pagamenti anonimi offrono. Limiti all'uso del pagamento anonimo possono essere introdotti, ma solo quando vi è la prova evidente che l'anonimato di una operazione può pregiudicare l'individuazione di un fenomeno di riciclaggio. Le operazioni di valore modesto non dovrebbero porre un problema a questo riguardo e anche le operazioni più importanti (ad esempio l'acquisto di un software costoso sulla rete) non significano necessariamente forme di riciclaggio.

RIASSUNTO DELLE PRINCIPALI CONCLUSIONI

- La possibilità di scegliere di restare anonimi è essenziale ai fini della tutela, per i singoli, sulla rete dello stesso grado di riservatezza esistente attualmente fuori della rete.
- L'anonimato non è adatto in tutte le circostanze. Stabilire le circostanze in cui l'opzione dell'anonimato è opportuna o quelle in cui non lo è, comporta un attento confronto fra i diritti fondamentali, non solo nei confronti della riservatezza, ma anche della libertà di espressione, e altri importanti obiettivi politici come la prevenzione del crimine. Le limitazioni di ordine giuridico che possono essere imposte dai governi al diritto di restare anonimi, o sugli strumenti tecnici per farlo (ad esempio disponibilità di prodotti cifrati), dovrebbero essere sempre proporzionate e limitate a quello che è necessario per proteggere uno specifico interesse pubblico in una società democratica.
- Dove possibile, l'equilibrio che è stato raggiunto in relazione alle precedenti tecnologie dovrebbe essere mantenuto per quanto riguarda i servizi offerti attraverso Internet.
- L'invio di posta elettronica, il navigare fra i siti della rete e l'acquisto di merci e servizi attraverso Internet dovrebbero essere tutti possibili in via anonima.
- Alcuni controlli sui soggetti che contribuiscono con del materiale a centri di discussione sulla rete (news-group, ecc.) sono necessari, ma il requisito imposto ai soggetti di identificarsi, nella maggior parte dei casi è sproporzionato e impraticabile. Devono essere preferite altre soluzioni.
- Gli strumenti anonimi per accedere a Internet (ad esempio chioschi pubblici di Internet, carte di accesso prepagate) e gli strumenti anonimi di pagamento sono due elementi essenziali per un vero anonimato sulla rete.

Mettere in pratica le conclusioni - Raccomandazioni operative

Le conclusioni di cui sopra, che sono essenzialmente relative all'estensione del diritto legittimo di una persona all'anonimato nel contesto di Internet, illuminano la situazione che deve essere realizzata se non si

vuole erodere la riservatezza dell'individuo. La situazione attuale è molto diversa. L'accesso dell'utilizzatore e l'attività su Internet solo raramente sono anonime. Gli sforzi per fornire servizi semianonimi (ad esempio ritrasmettitori anonimi) hanno posto regolarmente dei problemi, in quanto la configurazione tecnica sui protocolli Internet non consente facilmente un vero anonimato e gli strumenti di pagamento più diffusi sulla rete restano le carte di credito, mentre esperimenti con la moneta elettronica anonima debbono ancora affermarsi sul mercato elettronico tradizionale.

Perché questa situazione cambi, bisogna trovare il modo di mettere in pratica queste conclusioni. Debbono essere intraprese delle iniziative a una serie di livelli diversi:

1) *Ambiente normativo*

Il principio che la raccolta di dati personali identificabili deve essere limitata al minimo necessario, dov'essere riconosciuto nelle legislazioni nazionali e internazionali che si occupano di Internet. Inoltre esso deve essere incluso nei codici di condotta, nelle linee guida degli altri strumenti di "soft law" che vengono sviluppati. Dove ciò sia appropriato, il principio deve specificare che ci deve sempre essere la possibilità di conservare l'anonimato.

2) *Contesto tecnologico*

Le discussioni nel quadro del consorzio della rete Internet dovrebbero essere intensificate al fine di sviluppare l'infrastruttura e i protocolli Internet che conducono all'attività dell'utilizzatore anonimo.

Il finanziamento della ricerca e dello sviluppo (come quella disponibile nel quadro del 5° programma quadro di ricerca e sviluppo tecnologico) dovrebbero essere mirate specificamente a progetti che cercano di sviluppare strumenti anonimi di pagamento attraverso Internet e strumenti di accesso anonimi (ad esempio, terminali pubblici Internet).

3) *Ambiente economico*

I governi dovrebbero esaminare le modalità per fornire un sostegno economico diretto a promuovere la diffusa adozione sul mercato di tecnologie che migliorano la riservatezza e consentono agli utilizzatori di restare anonimi. Ad esempio, un governo potrebbe utilizzare il proprio potere di mercato come cliente maggiore per prodotti e servizi della tecnologia delle informazioni e includere i requisiti sulla riservatezza e l'anonimato fra i criteri per il proprio appalto pubblico. Bisogna anche prendere in considerazione la necessità di prodotti e servizi che favoriscano la riservatezza attraverso sovvenzioni o agevolazioni fiscali, come avviene nel caso di prodotti ecologici come la benzina senza piombo.

4) *Accrescere la consapevolezza fra gli utilizzatori di Internet, i fornitori di accesso e di servizi e l'industria della tecnologia dell'informazione*

La maggior parte degli utilizzatori di Internet non si rende conto dei rischi che corre la loro riservatezza a causa dell'attività da essi svolta sulla rete. Vi è una necessità urgente di fornire consulenza e orientamenti a questo riguardo. Le autorità per la protezione dei dati in tutto il mondo hanno un importante ruolo da svolgere nel fornire tale consu-

lenza. Gli orientamenti prodotti dalla commissione spagnola per la protezione dei dati indicano la strada da seguire. Bisogna preoccuparsi di assicurare la diffusione più ampia possibile di tale consulenza alla comunità Internet.

Anche quelli che raccolgono ed elaborano i dati attraverso Internet (fornitori di accesso, fornitori di servizi, siti web) debbono essere coscienti che sono già soggetti alle legislazioni esistenti in materia di protezione dei dati che richiedono, fra l'altro, trasparenza e apertura nella raccolta dei dati e che limitano le finalità per cui i dati personali possono essere utilizzati e pubblicati.