SENATO DELLA REPUBBLICA

XIV LEGISLATURA

Doc. CXXXVI
n. 1

RELAZIONE

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

(Anno 2000)

(articolo 31, comma 1, lettera n), *della legge 31 dicembre 1996, n. 675)*

Presentata dal Garante per la protezione dei dati personali

(RODOTÀ)

Comunicata alla Presidenza il 17 luglio 2001

TIPOGRAFIA DEL SENATO (150)

INDICE

INDICE ABBREVIAZIONI

La presente relazione è riferita al 2000 e contiene alcune ulteriori notizie relative a sviluppi significativi intercorsi nei primi mesi del 2001 che si è ritenuto opportuno menzionare.

art.	articolo
Bollettino	Bollettino del Garante per la protezione dei dati personali *«Cittadini e Società dell'Informazione»*
c.c.	codice civile
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cd.	cosiddetto/a
cfr.	confronta
Cost.	Costituzione
d.l.	decreto legge
d.lg.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
Pa	Pubblica amministrazione
Provv.	provvedimento
r.d.	regio decreto
reg.	regolamento
s.r.l.	società a responsabilità limitata
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

STATO DI ATTUAZIONE DELLA LEGGE N. 675/1996

LE PRINCIPALI NOVITÀ SUL PIANO NORMATIVO

1. L'INTEGRAZIONE DELLA LEGGE N. 675/1996

Nel corso del 2000 non sono intervenute novità normative volte a modificare in modo significativo la legge n. 675/1996 in tema di trattamento dei dati personali.

Il complessivo processo di integrazione e di aggiornamento della materia è però proseguito.

La disciplina resta trasversale ed abbraccia molteplici settori. Il suo perfezionamento ha comportato anche un migliore collegamento tra i principi della protezione dei dati personali ed importanti fonti normative primarie, nonché l'introduzione di nuove fonti per certi aspetti atipiche rivolte a specifici settori (si pensi alle autorizzazioni generali rilasciate dal Garante o ai codici di deontologia e di buona condotta per determinati settori).

Particolare rilievo è da attribuire alla recente legge 24 marzo 2001, n. 127 ("*Differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali*", in *G.U.* 19 aprile 2001, n. 91), che ha differito il termine per esercitare la delega legislativa già prevista dalle leggi nn. 676/1996 e 344/1998. La legge consentirà di completare entro il 31 dicembre 2001 il quadro normativo di riferimento in materia di trattamento dei dati, nei settori nei quali è opportuno specificare o integrare i principi generali introdotti nel 1996 e nei quali il Governo non è ancora intervenuto o ha introdotto una disciplina parziale. La medesima legge ha inoltre previsto l'emanazione, entro il 31 dicembre 2002, di un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse, dove dovranno essere riunite le norme vigenti apportandovi le integrazioni e modificazioni necessarie per un più armonico coordinamento o per assicurarne la migliore attuazione.

Prima della legge n. 127/2001, la legge 3 novembre 2000, n. 325 ("*Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste all'articolo 15 della legge 31 dicembre 1996, n. 675*" – *G.U.* n. 262 del 9 novembre 2000) ha consentito ai soggetti che non avevano ancora potuto adottare le c.d. misure minime di sicurezza entro il 29 marzo 2000 di beneficiare di un termine ulteriore, spirato il 31 dicembre 2000, predisponendo un documento avente data certa e indicante: *a)* le particolari esigenze tecniche e organizzative che avevano reso necessario ricorrere ad una scadenza ulteriore di un termine più ampio; *b*) gli accorgimenti da adottare o già adottati e gli elementi che caratterizzavano il programma di adeguamento; *c*) le linee-guida previste per dare piena attuazione alle misure di sicurezza.

Significativo risulta il Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici (v. il *Provv.* del Garante n. 8/P/2001, in *G. U.* 5 aprile 2001, n. 80) la cui emanazione era prevista dal decreto legislativo 30 luglio 1999, n. 281: esso è volto a garantire che l'utilizzazione dei dati di carattere personale acquisiti nell'ambito della ricerca storica, dell'esercizio del diritto allo studio e all'informazione, e nell'attività archivistica si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e all'identità personale.

Appare infine doveroso anticipare in questa prima parte della relazione che il Garante, sulla base di una propria deliberazione del 28 giugno 2000, si è potuto finalmente dotare di una completa ed autonoma disciplina interna, esercitando i poteri previsti dal legislatore nel 1999 (con la modifica dell'art. 33 della legge n. 675/1996) ed approvando tre regolamenti attinenti, rispettivamente, all'organizzazione e al funzionamento dell'Ufficio del Garante, al trattamento giuridico ed economico del personale e alla gestione amministrativa e contabilità (pubblicati nella *G.U.* 13 luglio 2000, n. 162).

2. ALTRI PROVVEDIMENTI SIGNIFICATIVI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Alcuni interventi normativi hanno interessato aspetti di significativo interesse anche per la tematica del trattamento dei dati personali. Tra questi, i più rilevanti riguardano:

a) la *legge 18 agosto 2000, n. 235*, recante nuove norme in materia di cancellazione dagli elenchi dei protesti cambiari. Il relativo art. 2 ha previsto che il debitore che esegue il pagamento della cambiale o del vaglia cambiario protestati entro dodici mesi dalla levata del protesto (o chi dimostri di aver subito levata di protesto illegittimamente o erroneamente) ha il diritto di ottenere la cancellazione del proprio nome dal registro informatico entro cinque giorni dalla pronuncia del presidente della camera di commercio, industria, artigianato e agricoltura. L'art. 4 ha inoltre stabilito che la notizia di ciascun protesto levato è conservata nel registro informatico fino alla sua cancellazione o, in mancanza di tale cancellazione, per cinque anni dalla data della registrazione. Altre disposizioni riguardano il pagamento oltre i termini e la riabilitazione;

b) il *decreto del Presidente della Repubblica 8 settembre 2000, n. 299*, recante il regolamento concernente l'istituzione, le modalità di rilascio, l'aggiornamento e il rinnovo della tessera elettorale personale a carattere permanente, ai sensi dell'art. 13 della legge 30 aprile 1999, n. 120. Nella presente relazione è illustrata la posizione del Garante rispetto all'annotazione della partecipazione al voto. Per altri aspetti, l'art. 5 del regolamento prevede che tutte le operazioni di trattamento dei dati personali debbano avvenire nel rispetto delle disposizioni vigenti in materia di riservatezza e svolgersi sotto la diretta vigilanza del responsabile del trattamento dei dati personali di ogni comune;

c) la *legge 24 novembre 2000, n. 340*, recante disposizioni per la delegificazione di norme e per la semplificazione di procedimenti amministrativi. L'art. 3 considera di rilevante interesse pubblico (*v.*, in proposito, quanto previsto dal decreto legislativo 11 maggio 1999, n. 135, in materia di trattamento di dati particolari da parte di soggetti pubblici) la consultazione diretta, da parte di una pubblica amministrazione o di un gestore di pubblico servizio, degli archivi dell'amministrazione certificante, finalizzata all'accertamento d'ufficio di stati, qualità e fatti, ovvero al controllo sulle dichiarazioni sostitutive presentate dai cittadini. Per l'accesso diretto ai propri archivi, l'amministrazione certificante rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente. L'art. 25 si occupa dell'accesso alle banche dati pubbliche, prevedendo che le pubbliche amministrazioni, titolari di programmi applicativi realizzati su specifiche indicazioni del committente pubblico, hanno facoltà di darli in uso gratuito ad altre amministrazioni pubbliche, che li adattano alle proprie esigenze. Hanno inoltre accesso gratuito ai dati contenuti in pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

d) il *decreto del Presidente del Consiglio dei ministri 6 dicembre 2000*, relativo al Programma statistico nazionale 2001-2003. Il paragrafo 1.3 del preambolo si occupa specificamente del trattamento dei dati personali, fornendo alcuni riferimenti normativi rispetto alla rilevanza delle finalità per cui vengono raccolti i dati e alle garanzie per i diritti fondamentali. In particolare vengono affrontati i temi dell'informativa, del diritto di accesso ai dati personali e delle maggiori cautele necessarie nel trattamento di dati sensibili;

e) la *legge 7 dicembre 2000, n. 397*, recante disposizioni in materia di indagini difensive. L'art. 11 prevede che il difensore, il sostituto, gli investigatori privati autorizzati e i consulenti tecnici, all'atto di conferire con le persone in grado di riferire circostanze utili ai fini dell'attività investigativa, debbano fornire un'informativa – da coordinare con quella prevista dalla legge n. 675/1996 – contenente la propria qualità e lo scopo del colloquio, l'intenzione di conferire ovvero di ricevere dichiarazioni, l'obbligo di dichiarare se le persone sono sottoposte ad indagini o imputate nello stesso procedimento, in un procedimento connesso o per un reato collegato, la facoltà di non rispondere o di non rendere la dichiarazione, il divieto di rivelare le domande eventualmente formulate dalla polizia giudiziaria o dal pubblico ministero e le risposte date;

f) il *decreto legislativo 28 dicembre 2000, n. 443*, recante disposizioni legislative in materia di documentazione amministrativa. Oltre ai numerosi rinvii alle norme sulla protezione dei dati personali si sottolinea, in particolare, l'art. 16, che al comma 1, con riferimento ai dati particolari di cui agli articoli 22 e 24 della legge n. 675/1996, prevede che i documenti trasmessi ad altre pubbliche amministrazioni contengano solo le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per perseguire le finalità per le quali vengono acquisite. Nel comma 2, ai fini

della dichiarazione di nascita, si sostituisce una semplice attestazione contenente i dati richiesti nei registri di nascita al certificato di assistenza al parto previsto in precedenza. L'art. 78 ribadisce che rimangono in vigore le disposizioni in materia di dati personali;

g) il *decreto ministeriale 2 febbraio 2001*, relativo alla descrizione dei tipi e delle caratteristiche nonché alle modalità di installazione ed uso dei mezzi elettronici e degli altri strumenti tecnici destinati al controllo delle persone sottoposte agli arresti domiciliari o alla detenzione domiciliare previsti dagli articoli 275-*bis* c.p.p. e 47-*ter*, comma 4-*bis*, della l. 26 luglio 1975, n. 354 (c.d. "braccialetto elettronico"). L'art. 4 del decreto, relativo al trattamento dei dati personali, prevede che l'applicazione dei mezzi e degli strumenti avvenga nel rispetto della dignità dell'interessato, che sia delimitato il tempo di conservazione dei dati e che siano individuate le persone legittimate a trattarli nel rispetto delle misure di sicurezza ai sensi dell'art. 15 della legge n. 675/1996;

h) la *legge 29 marzo 2001, n. 135*, recante la riforma della legislazione sul turismo, il cui articolo 8 apporta alcune modifiche all'articolo 109 del testo unico delle leggi di pubblica sicurezza (r.d. 18 giugno 1931, n. 773) in materia di "schedine d'albergo". Prima della riforma, il testo in questione era stato modificato altre due volte (dall'articolo 16 della legge n. 388 del 1993, di ratifica dell'Accordo di Schengen e dal decreto-legge n. 97/1995, convertito dalla legge n. 203/1995) al fine di adeguare la disciplina ai principi stabiliti dall'art. 45 della Convenzione di applicazione dell'Accordo di Schengen. Il testo in vigore prima della modifica apportata dalla legge n. 135/2001 prevedeva che le schede fossero conservate, a disposizione degli ufficiali o agenti di pubblica sicurezza, nella struttura ricettiva per dodici mesi e che copia ne fosse trasmessa giornalmente agli uffici di p.s. anche con mezzi telematici. Il testo novellato prevede, invece, che il gestore comunichi all'autorità le generalità degli alloggiati mediante consegna di copia della scheda o, in alternativa, i dati nominativi delle predette schede mediante la loro comunicazione in via informatica o telematica, secondo le modalità che saranno stabilite con decreto del Ministro dell'interno. Il testo non reca disposizioni specifiche sulle modalità e sui limiti del trattamento dei dati personali acquisiti dagli organi di polizia, diversamente da quanto previsto nella versione approvata dal Senato. È da segnalare, inoltre, che il decreto ministeriale sulle modalità di trasmissione dei dati per via telematica è stato adottato (peraltro senza acquisire il previo parere del Garante – sul punto v. par. 4) pochi mesi prima dell'approvazione della riforma dell'articolo 109 (d.m. 11 dicembre 2000) sicché, allo stato, le modalità applicative previste non appaiono perfettamente in linea con la nuova versione della norma.

3. LAVORI PARLAMENTARI

Oltre ai provvedimenti normativi approvati dal Parlamento e dal Governo nel corso della XIII legislatura, il Garante ha seguito nel corso del 2000 i lavori parlamentari relativi ad altre iniziative legislative in vario modo attinenti alla protezione dei dati personali e all'attività del Garante. Tra queste vanno fra l'altro ricordati:

a) il disegno di legge in materia di conflitti di interesse (AS 3236) che prevedeva alcune incompatibilità per i titolari di cariche di Governo estese ai presidenti e componenti delle autorità di controllo e di garanzia (art. 1, co. 3, lett. d));

b) il disegno di legge in materia di notificazioni degli atti giudiziari a mezzo posta (AC 6735) che mirava ad aggiornare la relativa disciplina in considerazione dei principi in materia di riservatezza previsti dalla legge n. 675/1996;

c) la proposta di legge recante modifiche al codice penale e al codice civile in materia di diffamazione col mezzo della stampa o con altro mezzo di diffusione (AC 7292);

d) il disegno di legge in materia di disciplina dell'utilizzazione di nomi per l'identificazione di domini Internet e di servizi in rete (AS 4549);

e) le proposte di legge in materia di discriminazione motivata dall'orientamento sessuale (AC 2551 e AC 5865);

f) il disegno di legge recante modifiche al testo unico in materia di immigrazione e condizione dello straniero (approvato con il d. lg. n. 286/1998), in particolare per quanto riguarda la proposta di modifica dell'articolo 6 sull'acquisizione delle impronte digitali dello straniero (AS 4938).

4. REGOLAMENTI ED ATTI AMMINISTRATIVI EMANATI SENZA IL PARERE DEL GARANTE

In relazione agli atti di competenza governativa è risultato doveroso sottolineare nuovamente il grave problema della mancata consultazione del Garante in numerose occasioni. L'art. 31, comma 2, della legge n. 675/1996 prevede che il Presidente del Consiglio dei ministri e ciascun ministro debbano consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere in materia di protezione dei dati personali.

Nel corso dell'anno, il Garante ha segnalato due volte al Presidente del Consiglio dei ministri il persistere di varie omissioni da parte dei ministeri nel consultare questa Autorità. È stato altresì evidenziato che i provvedimenti mancanti del parere previsto dalla legge n. 675/1996 sono viziati ed annullabili per violazione di legge, nonché del diritto comunitario in materia che impone una consultazione per assicurare il massimo rispetto dei diritti dei cittadini in tema di dati personali, spesso anche di natura sensibile.

In un'ottica di massima trasparenza, l'Autorità ha inoltre deciso di segnalare sul proprio sito Internet i casi più rilevanti di mancata consultazione, al fine di portarli a conoscenza dei cittadini. Vanno tra l'altro menzionati il decreto del Ministro dell'interno dell'11 dicembre 2000 (disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive), il d.P.C.M. 31 ottobre 2000 (in materia di protocollo informatico), il d.P.R. 10 ottobre 2000, n. 333 (in materia di diritto al lavoro dei disabili), il d.P.R. 30 giugno 2000, n. 230 (relativo alle norme sull'ordinamento penitenziario e sulle misure private e limitative della libertà), il d.m. 15 giugno 2000 del Ministero delle finanze (relativo all'accettazione telefonica o telematica delle scommesse ippiche), il d.m. 30 maggio 2000 (concernente il trattamento dei dati sensibili di competenza del Ministero del commercio con l'estero), il d.m. 27 marzo 2000, n. 264 (recante norme per la tenuta dei registri presso gli uffici giudiziari), il d.m. 9 dicembre 1999 del Ministero delle finanze (relativo all'approvazione dei modelli di questionario con i quali determinati uffici di tale Ministero possono chiedere alle banche e a Poste italiane S.p.a. ulteriori dati, notizie e documenti di carattere specifico relativi ai conti intrattenuti con il contribuente).

Il Presidente del Consiglio dei ministri ha risposto al Garante con una nota del 20 gennaio 2001, assicurando il massimo impegno a porre in essere prontamente le azioni necessarie a garantire l'osservanza dell'art. 31, comma 2, e ribadendo che il parere del Garante costituisce una componente fondamentale del processo di predisposizione delle norme regolamentari e degli atti amministrativi che hanno un impatto sulla tutela dei dati personali.

PUBBLICA AMMINISTRAZIONE

5. PROFILI GENERALI

Dopo la controversa vicenda che si è sviluppata nel corso degli anni 1998-1999, relativa al livello di protezione dei dati sensibili nella pubblica amministrazione, trattata ampiamente nella scorsa Relazione, l'attenzione delle amministrazioni si è concentrata nel corso del 2000 sui profili attuativi specie del decreto legislativo n. 135 del 1999.

Dai numerosissimi quesiti pervenuti da innumerevoli amministrazioni locali e centrali è emersa, però, la constatazione che il grado di piena applicazione e di integrale comprensione degli effetti della legge n. 675/1996 negli uffici pubblici non è ancora soddisfacente.

Sebbene siano ormai trascorsi ben quattro anni dall'entrata in vigore della legge, permangono in diversi uffici pubblici ingiustificate incertezze e lacune, in parte derivanti dai tempi obiettivamente necessari per far maturare un ottimale approccio culturale ai principi di garanzia fissati dalla legge, in parte però determinati dalla tendenza ad esaurire l'impegno nell'attuazione – spesso tardiva, inesatta o incompleta – della legge n. 675/1996 assolvendo in modo riduttivo i soli adempimenti di ordine formale. Numerosi ed inutili equivoci permangono rispetto ad aspetti pure oggetto di svariati provvedimenti di chiarimento.

Sintomatico è, ad esempio, l'approccio estremamente burocratico riservato alla problematica dei dati sensibili, che pure dovrebbe rappresentare un nodo importante nella costruzione di una completa tutela per i cittadini. Parimenti insoddisfacente è la metodologia riservato alla problematica della sicurezza e della valutazione dei rischi per l'integrità dei dati e dei sistemi, specie presso le amministrazioni locali.

Al di là dei problemi legati a particolari problematiche, evidenziati nei successivi paragrafi, manca ancora una visione di insieme dei problemi, mentre è maturo e si impone un salto di qualità nello studio delle problematiche e nella costruzione di un rapporto migliore tra l'amministrazione e il cittadino sul piano della tutela dei diritti della personalità.

6. LA GESTIONE DEI DATI SENSIBILI E DEI DATI A CARATTERE GIUDIZIARIO

Successivamente all'emanazione del d.lg. n. 135/1999 sul trattamento di dati sensibili e a carattere giudiziario da parte dei soggetti pubblici, l'attenzione dell'Autorità si è concentrata nel 2000 in modo particolare sul suo corretto completamento da parte delle amministrazioni.

Il decreto n. 135, come si ricorderà, ha introdotto una nuova possibilità attraverso cui i soggetti pubblici possono trattare lecitamente tali tipi di dati. Accanto all'originaria previsione dell'art. 22, comma 3, L. n. 675/1996, secondo cui i trattamenti di dati sensibili sono consentiti solo laddove siano autorizzati da un'"espressa norma di legge nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità d'interesse pubblico perseguite", il decreto del 1999 ha infatti previsto una seconda soluzione che presuppone un intervento diretto delle amministrazioni.

In particolare, si ricorderà che l'art. 5 del d.lg. n. 135, modificando il citato art. 22, ha stabilito che, laddove risultino individuate per legge o, in via transitoria, dal Garante, le rilevanti finalità d'interesse pubblico perseguite da un determinato trattamento, i soggetti pubblici debbano individuare e rendere noti, "secondo i rispettivi ordinamenti", i tipi di dati e di operazioni su questi eseguibili.

Nei mesi successivi all'entrata in vigore di tale modifica si è registrata una diversità di vedute tra il Garante e la Presidenza del Consiglio dei ministri relativamente agli strumenti necessari per dare esecuzione al dettato normativo. Mentre il primo aveva sottolineato la necessità di provvedere a tale adempimento tramite atti di natura regolamentare (in considerazione della generalità ed astrattezza delle regole da introdurre e della loro attitudine a spiegare effetti rilevanti su diritti e libertà fondamentali dei soggetti interessati), la seconda propendeva per una soluzione diversa, considerando detta attività come

meramente ricognitiva. La Presidenza del Consiglio, che pure non risulta aver formalmente mutato l'originario orientamento, ha tuttavia impartito ulteriori direttive con circolare Dagl/643–Pres. 2000 (in *G.U.* del 3 maggio 2000, n. 101) ed ha ricordato alle amministrazioni l'obbligo di fornire la massima diffusione della rilevazione effettuata, attraverso opportune pubblicazioni.

Purtroppo, nonostante i ripetuti richiami del Garante, gli atti adottati dalle amministrazioni risultano ancora in numero assolutamente esiguo e non privi di gravi difetti, lacune ed errori, tanto da giustificare, al momento, la considerazione che varie disposizioni del d.lg. n. 135 restano sostanzialmente inapplicate e che diversi trattamenti di dati personali effettuati in ambito pubblico, su cui verranno proseguite ed intensificate le doverose verifiche anche ispettive, sono proseguiti in modo illegittimo. Tale stato di cose ha indotto l'Autorità ad interessare il Presidente del Consiglio chiedendo un preciso intervento a livello politico (v. nota del 20 ottobre 2000, in *Bollettino,* n. 14-15, pp. 24-25).

Fra i pochi tentativi di dare esecuzione alla citata modifica normativa, deve segnalarsi l'adozione del decreto del Ministro del commercio con l'estero del 30 maggio 2000, che presenta però un'individuazione inidonea di dati e di operazioni, effettuata peraltro violando l'obbligo di consultare preventivamente il Garante con le descritte ripercussioni sulla legittimità e validità del decreto stesso.

Il rispetto del cennato obbligo di consultazione da parte del Dipartimento per la solidarietà sociale, relativamente allo schema di decreto in materia di assegni familiari poi approvato con d.m. 21 dicembre 2000, n. 452 (in *G.U.* 6 aprile 2001, n. 81), ha consentito a questa Autorità, invece, di fornire alcune indicazioni che potrebbero essere utilmente tenute in considerazione anche da altre amministrazioni.

Ribadito l'obbligo di procedere alla rilevazione in questione attraverso atti di natura regolamentare, il Garante ha anzitutto ricordato che l'esistenza del quadro normativo introdotto dal d.lg. n. 135 non deve essere riprodotto nei singoli atti ministeriali, apparendo pacifico che al trattamento dei dati in questione si applichino comunque le disposizioni generali fissate nel decreto in tema di essenzialità, pertinenza, modalità di conservazione dei dati, ecc. (artt. 1–5).

Piuttosto, risulta necessario collegare alle rilevanti finalità perseguite dal trattamento già individuate dal decreto o dal Garante, i tipi di dati sensibili trattati (nel caso specifico si trattava di dati idonei a rivelare l'origine razziale ed etnica e lo stato di salute dei richiedenti e dei minori interessati) e i tipi di operazioni su di essi eseguite (raccolta, registrazione, organizzazione, conservazione, modificazione, estrazione, utilizzo, blocco, cancellazione e distruzione dei dati). Ciò che occorre, in altre parole, è chiarire ai cittadini in un quadro di piena trasparenza, quali categorie di informazioni vengono utilizzate in relazione alle singole finalità e rendere note, nel complesso, le sostanziali forme della loro utilizzazione, evitando la pedissequa quanto inutile menzione di tutte le operazioni che compongono l'ampia definizione legislativa di "trattamento" (art. 1 legge n. 675/1996).

Il Garante ha poi suggerito di precisare che eventuali operazioni di selezione, elaborazione e comunicazione dei dati non previste dal d.lg. n.135 sono consentite solo con l'indicazione scritta dei motivi.

Poiché nel decreto in questione si prevedeva la possibilità di trasferire dati particolari ad altri soggetti, l'Autorità ha poi ribadito che il titolare è tenuto a rendere previamente pubblica con proprio atto la lista dei soggetti ai quali detti tipi di dati possono essere comunicati in base alle leggi e ai regolamenti. Ha infine precisato che i dati raccolti dal titolare possono essere trattati in forma anonima, anche a fini statistici, di studio, di informazione, di ricerca e di diffusione, in relazione alle finalità di interesse pubblico perseguite.

Analoghi problemi e ritardi nell'attuazione delle modifiche introdotte dal d.lg. n. 135 si sono riscontrate in ambito locale. Anche in questo caso il Garante, ad esempio nel rispondere ad una nota dell'Associazione nazionale dei comuni (ANCI) (v. nota del 23 maggio 2000, in *Bollettino* n. 13, p. 21), ha ricordato che gli adempimenti in questione, il cui scopo è quello di garantire l'uso corretto dei dati più delicati semplificando al tempo stesso le procedure, deve avere caratteri di uniformità in modo da evitare diversità di garanzie non giustificabili, nonché difformità nei trattamenti fra comune e comune.

In particolare, relativamente ai modelli di regolamento elaborati e diffusi dall'Associazione tramite Internet ed organi di stampa, l'Autorità, nel sottolineare in linea generale l'utilità dell'iniziativa, ha dovuto però rilevare che essi risultavano per una parte carenti e, per l'altra, non conformi alle norme in materia di protezione dei dati personali. Nel segnalare la necessità di modificarli ha quindi offerto la propria collaborazione alle iniziative che i comuni intendano adottare allo scopo di assicurare il rispetto più puntuale ed armonizzato delle garanzie previste.

Il problema di individuare i tipi di dati e di operazioni si pone in altro modo per i singoli soggetti pubblici in materia sanitaria; l'art. 2, comma 1, d.lg. n. 282/1999, ha infatti affidato tale compito ad un

decreto del Ministro della sanità (da adottarsi sentiti la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano ed il Garante), che dovrebbe permettere una disciplina uniforme del settore.

Tale decreto, nonostante alcune riunioni svoltesi nel corso dell'anno, non è stato ancora emanato costringendo, anche in questo caso, il Garante ad interessare il Presidente del Consiglio (v. nota cit. del 20 ottobre 2000); esso, infatti, è di vitale importanza sia perché interessa l'intero Servizio sanitario nazionale sia perché la sua mancanza comporta gravi problemi a tutti gli operatori sanitari, anche in sede contenziosa, per ciò che riguarda la liceità del proprio operato.

Sempre in materia di dati sanitari è stata nuovamente rilasciata dal Garante, senza modifiche sostanziali rispetto all'anno precedente, l'autorizzazione generale n. 2 relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, che trova parziale applicazione anche in ambito pubblico.

Per quanto riguarda i dati a carattere giudiziario è noto, invece che il loro trattamento è regolato dall'art. 24 della legge n. 675/1996, il quale non prevede una disciplina differenziata fra soggetti pubblici e privati e stabilisce che esso possa aver luogo solo se autorizzato da un'espressa norma di legge o da un provvedimento del Garante dal quale risultino le rilevanti finalità d'interesse pubblico perseguite dal trattamento, i tipi di dati trattati e le precise operazioni autorizzate.

Per i dati a carattere giudiziario, quindi, si configuravano due soluzioni consistenti nella previsione di legge e nell'autorizzazione del Garante.

La prima di queste è stata integrata dalle modifiche introdotte dall'art. 5 del d.lg. n. 135/1999 (così come modificato dall'art. 15 del d.lg. n. 281/1999), il quale ha previsto anche per i trattamenti di tali dati la possibilità per le amministrazioni pubbliche di specificare i tipi di dati e di operazioni eseguibili in relazione alle finalità di rilevante interesse pubblico ivi indicate.

Tali rilevazioni hanno incontrato i medesimi problemi già segnalati con riferimento ai dati sensibili e necessitano pertanto di una rapida emanazione dei regolamenti attuativi da parte di tutte le amministrazioni interessate.

Il Garante ha mantenuto la potestà, che ha esercitato già nel 1999 con l'autorizzazione n. 7 rilasciata a favore di soggetti privati e anche pubblici, di autorizzare detti trattamenti per alcune ulteriori rilevanti finalità di interesse pubblico, autorizzazione rinnovata nel 2000 con scadenza al 31 dicembre 2001.

7. RISERVATEZZA E TRASPARENZA DELL'ATTIVITÀ AMMINISTRATIVA

Nelle relazioni annuali pubblicate negli anni precedenti, è stato più volte evidenziato che la normativa sulla tutela dei dati personali non può essere interpretata nel senso di una riduzione indiscriminata della trasparenza amministrativa e, in particolare, di quella che ne costituisce la sua più frequente forma di applicazione: il diritto di accesso agli atti amministrativi.

Rimandando ad un successivo paragrafo una più attenta disamina dei provvedimenti sul diritto d'accesso, si intende qui dar conto di alcune interpretazioni dell'Autorità che nell'anno preso in considerazione hanno contribuito, in diversi casi, ad offrire una chiave di lettura nel delicato bilanciamento fra esigenze di trasparenza e tutela della riservatezza.

Uno degli elementi che merita evidenziare in questa sede – e che spesso è stato sottovalutato – è l'incidenza che un diverso diritto di accesso, quello introdotto dall'art. 13 della legge n. 675, ha avuto in termini di maggiore trasparenza dell'attività della p.a.

Il Garante ha in varie occasioni messo in evidenza le differenze fra le due forme, quella prevista dalle leggi nn. 142 (ora riprodotta nel d.lg. n. 267/2000) e 241 del 1990 e quella introdotta dal citato art. 13, precisando che quest'ultima consente all'interessato di accedere solo alle informazioni che lo riguardano e che tale accesso non necessariamente deve avvenire attraverso le forme previste per le prime (visione e copia).

Il diritto d'accesso previsto dalla l. n. 675/1996 consente all'interessato di ottenere tali informazioni attraverso l'estrazione delle stesse dagli archivi, atti e documenti in possesso dell'amministrazione e la

loro trasposizione, in forma agevolmente comprensibile, su di un supporto cartaceo od informatico da consegnare all'interessato medesimo (v. art. 17 d.P.R. n. 501/1998). Soltanto laddove l'estrazione dei dati risulti particolarmente difficoltosa l'adempimento della richiesta di accesso può avvenire anche tramite l'esibizione e/o la consegna in copia della documentazione (si vedano, in proposito, le modalità più volte richiamate dal Garante, in particolare nei provvedimenti del 21 giugno e del 13 ottobre 1999, pubblicati nel *Bollettino* n. 11/12, p. 61).

Nonostante tale distinzione, appare indubitabile che l'esercizio di questo nuovo diritto da parte degli interessati ha contribuito ad una maggiore "apertura" e trasparenza della pubblica amministrazione: si pensi, ad esempio, agli effetti che esso ha nei riguardi della conoscenza delle valutazioni operate sui dipendenti (v., anche per questo, il citato provvedimento del 2 giugno 1999, richiamato in molti provvedimenti e note anche nel corso del 2000).

L'utilizzo di tale diritto, che costituisce un vero e proprio elemento di rottura nei confronti di determinate logiche proprietarie delle informazioni personali anche in ambito pubblico, può però presentare talvolta risvolti delicati e in circoscritti casi addirittura pregiudizievoli nei confronti di alcuni soggetti.

Già nel passato era stato ad esempio lamentato da alcuni comuni il timore che, dando riscontro ad una richiesta d'accesso legittimamente presentata da una persona nei confronti dei propri dati (o di quelli di minori sui quali si esercita la potestà parentale), trattati ad esempio dai servizi sociali, si potessero rivelare informazioni delicate a persone che non dovrebbero conoscerle (il riferimento va al caso di nuclei familiari nei quali si realizzano abusi su minori e all'eventuale richiesta del genitore "maltrattante" di accedere alle informazioni).

Al riguardo l'Autorità, interessata formalmente dall'ANCI, nel ricordare che le richieste d'accesso presentate ai sensi dell'art. 13 della legge non danno diritto ad un'integrale visione o conoscenza dei dati e dei documenti, ha evidenziato che le migliori cautele risiedono, da un lato, nel disciplinare accuratamente i casi di riconoscimento dell'accesso ai sensi delle due citate leggi del 1990 e, dall'altro, nell'individuare con attenzione, attraverso i regolamenti previsti dal d.lg. n. 135/1990, le operazioni effettuabili sui dati sensibili, con particolare riferimento alla loro raccolta ed al rispetto degli obblighi di pertinenza, non eccedenza, esattezza ed aggiornamento degli stessi (v. nota del 23 maggio 2000, in *Bollettino* n. 13, p. 21).

Con la medesima nota di risposta all'ANCI è stato poi preso in considerazione un altro importante aspetto collegato al bilanciamento fra le due menzionate esigenze di trasparenza dell'attività pubblica e di tutela della riservatezza degli interessati.

È noto, infatti, che da qualche anno le amministrazioni stanno perseguendo obiettivi di maggior trasparenza e funzionalità rendendo meglio conoscibili le informazioni detenute attraverso reti telematiche. In particolare, in ambito locale, si assiste ad un forte sviluppo delle c.d."reti civiche": al riguardo, il Garante ha messo in evidenza ancora una volta l'importante ruolo dei regolamenti di attuazione della legge n. 142/1990. Nel disciplinare per regolamento la conoscibilità delle informazioni in suo possesso, l'ente locale può infatti contemplarne anche la diretta divulgabilità tramite pubblicazioni, riviste e notiziari telematici curati dall'ente stesso, o attraverso le "reti civiche", qualora ciò sia ritenuto opportuno per lo svolgimento delle proprie funzioni istituzionali.

Tale previsione regolamentare è necessaria sia alla luce di quanto previsto dall'art. 27, comma 3, della legge n. 675, sia relativamente ai dati "sensibili" per completare la disciplina introdotta dal d.lg. n. 135/1999.

Su queste basi, ha affermato l'Autorità, non si rinvengono elementi ostativi alla possibilità che l'ente locale preveda, con proprio regolamento, anche un regime di ampia conoscibilità di determinati elenchi nominativi di coloro che, ad esempio, hanno ottenuto il rilascio di concessioni ed autorizzazioni edilizie, a nulla rilevando il fatto che la normativa in materia urbanistica non preveda una specifica modalità di diffusione di tali elenchi.

Considerazioni diverse, invece, devono essere formulate per quanto riguarda la possibilità per l'ente locale di pubblicare, sui predetti notiziari, dati idonei a rivelare lo stato di salute delle persone (v. divieto sancito dall'art. 23, comma 4, legge n. 675/1996) o notizie estratte dalle anagrafi della popolazione o dai registri dello stato civile, poiché per tali anagrafi e registri esistono specifiche disposizioni che delimitano le forme di conoscibilità dei dati registrati.

L'immissione nel circuito informativo dei dati pubblici accessibili a chiunque non può rendere infatti inefficaci le cautele e le prescrizioni che caratterizzano, caso per caso, il regime di pubblicità e di conoscibilità di ogni singola informazione e che, in rapporto a ciascun atto, documento o informazione, ope-

rano con norme speciali un bilanciamento degli interessi coinvolti (tra cui, appunto, la disciplina degli atti anagrafici e degli atti dello stato civile compresa quella concernente le pubblicazioni matrimoniali).

Con la medesima pronuncia il Garante ha avuto modo di precisare che la pubblicazione dei notiziari telematici ricade anche nell'ampia nozione di trattamento finalizzato *"alla pubblicazione o diffusione occasionale di articoli, saggi o altre manifestazioni del pensiero"*, la cui disciplina, prevista in termini generali dall'art. 25 della legge n. 675, è stata dettagliata dal codice di deontologia per l'attività giornalistica, che, tra l'altro, consente all'ente di rendere un'informativa semplificata da inserirsi nel notiziario.

L'Autorità è pervenuta alle medesime conclusioni in tema di divulgabilità tramite notiziari ed organi di diffusione, in occasione della decisione su un ricorso presentato da un avvocato che si opponeva alla pubblicazione su una rivista – curata dal locale Consiglio dell'ordine di appartenenza – della notizia concernente un provvedimento di temporanea sospensione che lo riguardava (v. decisione del 29 marzo 2001, in *Bollettino* n. 18, p. 20).

Più volte, nel passato, il Garante aveva affrontato la questione della pubblicità degli albi professionali, giungendo alla conclusione che, nonostante una variegata e spesso datata base normativa, tali albi sono destinati 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 i relativi iscritti.

Nel caso del cennato ricorso, l'Autorità ha preliminarmente rilevato che la *ratio* sottesa alla pubblicità degli albi e dei periodici aggiornamenti relativi a nuove iscrizioni e cancellazioni ricorre anche, con evidenza, per i provvedimenti che comportano una sospensione o l'interruzione dell'esercizio della professione, i quali, per loro stessa natura, devono considerarsi soggetti anch'essi ad un regime di ampia conoscibilità.

I provvedimenti disciplinari dei consigli dell'ordine e del Consiglio nazionale forense si configurano peraltro quali atti pubblici soggetti ad un regime di conoscibilità da parte di altri professionisti e di terzi, che si fonda su rilevanti motivi di interesse pubblico connessi anche a ragioni di giustizia ed al regolare svolgimento dei procedimenti in ambito giudiziario. L'Autorità ha pertanto affermato che in tali casi non può ritenersi prevalente l'interesse alla riservatezza del singolo professionista destinatario di una misura disciplinare, ferma restando la necessità che la menzione del provvedimento che applica la misura avvenga in modo corretto nonché con informazioni esatte e complete.

La conoscibilità delle informazioni relative ai suddetti provvedimenti disciplinari rende quindi lecita la loro divulgabilità tramite riviste, notiziari o altre pubblicazioni curati dai consigli dell'ordine.

8. L'ACCESSO AI DOCUMENTI AMMINISTRATIVI

Il rapporto tra il diritto di accesso ai documenti amministrativi e il diritto alla riservatezza dei dati personali è rimasto al centro di un intenso dibattito dottrinale e giurisprudenziale e su di esso il Garante è tornato ripetutamente come già avvenuto sin dai primi mesi della sua attività.

L'Autorità ha costantemente ritenuto che la legge n. 675/1996 non ha ridotto il regime giuridico sulla trasparenza e l'accesso agli atti della pubblica amministrazione, anche in ragione della clausola di salvezza espressamente prevista dal legislatore (art. 43, comma 2, della legge n. 675/1996).

Nei numerosi atti adottati anche nel corso del 2000 il Garante ha ulteriormente ribadito che l'esistenza di una specifica normativa sulla protezione dei dati personali non può essere invocata di per sé per negare o limitare il diritto di accesso e che spetta all'amministrazione destinataria della richiesta valutare anzitutto la sussistenza dell'interesse giuridicamente rilevante e delle altre condizioni per accedere ai documenti amministrativi (art. 22 della legge n. 241/1990; art. 2 d.P.R. n. 352/1992).

Come si ricorderà, una parte della giurisprudenza amministrativa aveva in passato sostenuto, analogamente a quanto affermato dal Garante, che l'emanazione della legge sulla protezione dei dati personali non ha modificato l'impianto normativo sulla trasparenza amministrativa, anche con riferimento all'accesso ai dati sensibili (cfr. C.d.S., ad. plen., n. 5/1997; T.A.R. Abruzzo, sez. Pescara, n. 681/1997; C.d.S., sez. IV, n. 14/1998, sez. IV, n. 1137/1998, sez. VI, n. 65/1999).

Altra parte aveva invece evocato una "portata dirompente della legge n. 675 del 1996", ritenendo possibile l'accesso unicamente a condizione che ricorressero i presupposti previsti dalla legge del 1996, soprattutto con riguardo ai dati sensibili.

Secondo tale orientamento, anteriore al decreto legislativo n. 135 del 1999 sul trattamento dei dati sensibili da parte dei soggetti pubblici, l'accesso ai dati ordinari era consentito in base al combinato disposto degli articoli 27 della legge n. 675 del 1996 e 24 della legge 241 del 1990, mentre l'accesso ai dati sensibili, in applicazione dell'articolo 22, comma 3, della legge del 1996 – allora non ancora riformulato-, trovava un ostacolo nell'assenza di un'espressa previsione legislativa e quindi nella prevalenza del diritto alla riservatezza su quello alla trasparenza (C.d.S., sez. VI, n. 59/1999).

L'emanazione del citato decreto legislativo n. 135 del 1999 ha permesso di superare in gran parte tali contrasti.

Il decreto n. 135 del 1999, nell'integrare la normativa sul trattamento dei dati sensibili da parte dei soggetti pubblici, ha infatti individuato alcune rilevanti finalità d'interesse pubblico per il cui perseguimento è consentito il trattamento di tali dati. In particolare il relativo articolo 16, comma 1, lettere b) e c) ha stabilito che si considerano di rilevante interesse pubblico i trattamenti effettuati per far valere il diritto di difesa in sede amministrativa o giudiziaria e per applicare la disciplina sull'accesso ai documenti amministrativi.

Il Consiglio di Stato ha recentemente sostenuto, sulla base di un'interpretazione dei commi 1 e 2 del citato articolo 16 del d.lg. n. 135 del 1999, la sussistenza di un'autonoma previsione normativa in materia di accesso ai dati sulla salute e sulla vita sessuale (C.d.S., sez. VI, n. 1882/2001). Secondo tale impostazione, il legislatore del 1999 avrebbe consentito il trattamento dei dati sensibili diversi da quelli sulla salute e sulla vita sessuale, mentre avrebbe condizionato l'accesso ai documenti amministrativi contenenti dati sulla salute e sulla vita sessuale ad un giudizio comparativo tra il diritto da far valere e il diritto alla riservatezza dell'interessato. Il Consiglio di Stato ha inoltre sostenuto che tale valutazione deve essere fatta in concreto "in modo da evitare il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica dei diritti in contesa".

Come già accennato, nel corso dell'anno l'Autorità ha inoltre confermato il proprio positivo orientamento sulla questione relativa alla compatibilità tra la normativa sul trattamento dei dati personali e il diritto di accesso riconosciuto ai consiglieri comunali e provinciali agli atti e ai documenti delle rispettive amministrazioni locali (art. 43 d.lg. n. 267/2000, corrispondente all'art. 31, commi 5, 6 e 6 *bis*, l. n. 142/1990).

Una delle richieste presentate risulta di particolare interesse riguardando specificamente la possibilità di accedere a dati, quali quelli relativi all'AIDS o all'infezione da HIV, per i quali l'ordinamento ha previsto già prima dell'entrata in vigore della legge n. 675 particolari cautele.

L'Autorità ha rammentato che l'art. 8, comma 5, lett. b), del d.lg. n. 135/1999, in merito al trattamento di dati sensibili effettuato da soggetti pubblici, ha considerato di rilevante interesse pubblico il trattamento di dati "strettamente necessario allo svolgimento della funzione di controllo, di indirizzo politico e di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati, per consentire l'espletamento di un mandato elettivo".

Le amministrazioni sono tenute, a seguito delle disposizioni introdotte dal d.lg. n. 135/1990, ad identificare e rendere pubblici, secondo i rispettivi ordinamenti, i tipi di dati e le operazioni eseguibili nei trattamenti di dati sensibili strettamente necessari allo svolgimento della funzione di controllo, di indirizzo politico e di sindacato ispettivo e di altre forme di accesso riconosciute dalla legge o dai regolamenti degli organi interessati (art. 8, comma 5, lett. b), d.lg. n. 135/1990).

Solo in relazione a tale circostanza, quindi, il consigliere può accedere anche a tali dati.

Resta comunque fermo l'obbligo di rispettare il principio di pertinenza e non eccedenza con riferimento sia alle modalità del trattamento, sia alla natura dei dati, nonché il divieto di diffusione dei dati idonei a rivelare lo stato di salute (artt. 9, comma 1, lett. d), 23, comma 4, legge n. 675/1996; art. 4, comma 4, d.lg. n. 135/1999).

Il rispetto di questi principi deve essere particolarmente accurato anche quando si trattano altre informazioni (ad esempio quelle relative a soggetti tossicodipendenti o a malati psichiatrici) per le quali l'ordinamento prevede un particolare regime di tutela dalla cui circolazione può derivare un grave pregiudizio per la vita privata e la dignità personale degli interessati.

9. LA FORMAZIONE DI BANCHE DATI DI RILEVANTI DIMENSIONI

Si è già sottolineato nella relazione annuale per l'anno 1999 il forte sviluppo che negli ultimi tempi si è registrato in materia di costituzione di grandi banche dati.

È indubbio che esse, per l'elevato numero di dati detenuti e, soprattutto, per le sempre più agevoli interconnessioni che fra di loro possono operarsi, accanto agli indubbi vantaggi in termini di efficienza dell'attività amministrativa, rappresentano un elemento di preoccupazione per i cittadini ed inducono l'Autorità a rivolgere una vigile attenzione al fenomeno.

Le disponibilità offerte dalla tecnica, come si è riferito nella precedente relazione, non possono infatti non procedere di pari passo con una valutazione delle implicazioni sui diritti fondamentali della persona. Tale difficile cammino deve essere accompagnato da un coinvolgimento dell'opinione pubblica e da una cosciente valutazione dei diversi interessi in gioco.

È proprio per tale motivo che la legge n. 675, per rendere leciti taluni trattamenti, richiede l'esistenza di norme di carattere primario o secondario, le quali sono generalmente adottate con procedimenti che garantiscono una adeguata partecipazione e un idoneo controllo, anche successivo.

Con particolare riguardo alle pubbliche amministrazioni, ad esempio, l'art. 27 della legge n. 675 impone che l'istituzione e le modalità di utilizzo, specie esterno, di banche dati siano supportate da una norma legislativa o regolamentare. I presupposti previsti da tale norma costituiscono infatti, secondo quanto affermato dall'Autorità, "l'essenziale fondamento per realizzare un flusso trasparente di dati ispirato a criteri omogenei che garantiscano la protezione dei dati personali nel rispetto dei principi di pertinenza, completezza e non eccedenza sanciti dall'art. 9, lett. d) della legge n. 675".

L'esigenza di disporre di tale previsione normativa è stata rappresentata dal Garante, ad esempio, in occasione del parere reso al Ministero dell'interno sullo schema di decreto ministeriale istitutivo di un indice nazionale delle anagrafi-INA. Tale indice, predisposto dal Ministero dell'interno sulla base di un progetto intersettoriale ed inserito nell'ambito del Sistema di accesso e interscambio anagrafico-SAIA (sul quale, v. la Relazione per l'anno 1999, pp. 25-26), dovrebbe consentire di individuare più rapidamente il comune che detiene i dati dei cittadini presenti nelle anagrafi della popolazione ed un migliore esercizio, da parte del Ministero dell'interno, dei compiti di vigilanza ad esso affidati sulla tenuta delle anagrafi comunali.

Precisati i termini per la costituzione di tale banca dati, il Garante, nelle more di una disposizione legislativa che disciplinasse organicamente la materia, non ha ravvisato ostacoli alla realizzazione dell'Indice in via strettamente sperimentale, per un periodo di tempo delimitato e nell'ambito di una circoscritta area territoriale. In tale fase sperimentale, però, ha aggiunto l'Autorità, non avrebbero potuto avere accesso ai dati soggetti diversi dalle pubbliche amministrazioni e i dati stessi si sarebbero dovuti utilizzare esclusivamente per fini di pubblica utilità, secondo quanto previsto dall'art. 34 del d.P.R. n. 223/1989.

La previsione legislativa in questione ha poi trovato concretizzazione nel d.l. 27 dicembre 2000, n. 392, convertito in legge 28 febbraio 2001, n. 26, il quale, istituendo l'INA presso il Ministero dell'interno, ha anche espressamente previsto che ai fini dell'adozione del decreto del Ministro per la gestione di tale Indice sia sentito il Garante.

Nel 2000 le problematiche connesse all'istituzione di grandi banche dati in ambito pubblico sono venute stranamente in maggiore evidenza con prevalente riferimento alla sola materia anagrafica.

Poco tempo dopo l'emanazione del parere appena ricordato, infatti, il Garante è stato nuovamente consultato dal Ministero dell'interno in relazione ad un progetto trasmessogli dalla Prefettura di Firenze, relativo alla collaborazione tra la Rete telematica regionale toscana–RTRT e lo stesso Ministero, volto a consentire la consultazione per via telematica delle informazioni anagrafiche in possesso dei comuni.

Tale progetto prevedeva interconnessioni con il SAIA e avrebbe potuto avviare forme di collaborazione con altre regioni interessate.

Benché esso non stabilisse, secondo il Ministero, la costituzione di un'anagrafe regionale o comunque sovracomunale, l'Autorità ha dovuto ribadire (v. parere del 20 giugno 2000, in *Bollettino* n. 13, p. 12) alcune osservazioni già rese riguardo alla necessità di una disciplina organica finalizzata a ridurre il rischio del proliferare di iniziative non coordinate fra loro (e peraltro suscettibili di raggiungere gli obiettivi fissati, considerato che non vi è obbligo per i comuni di aderire a sistemi di interscambio anagrafico).

Essa ha poi precisato che la motivazione con la quale i vari enti avrebbero potuto richiedere il collegamento informatico e telematico avrebbe dovuto chiaramente indicare le norme di legge o di regolamento o le necessità istituzionali comportanti l'esigenza di acquisire dati anagrafici, non potendosi ritenere sufficiente il generico riferimento alle "finalità istituzionali e/o di pubblica utilità".

Una conferma della necessità di disporre di un quadro normativo omogeneo si è poi avuta, sempre in materia anagrafica, in occasione dell'approvazione della legge della Regione Friuli-Venezia Giulia n. 97/2000 con la quale, integrando le disposizioni concernenti l'anagrafe dei beneficiari delle agevolazioni sul prezzo delle benzine già prevista dalla precedente legge n. 47/1996, si era inteso – secondo quanto riscontrato dal Garante – creare una nuova e ben più articolata banca dati regionale da utilizzarsi anche per "altre finalità di carattere istituzionale".

Si era previsto che i dati contenuti in tale banca dati potessero essere ceduti a chiunque ne facesse richiesta, seppur "nell'ambito di quanto previsto dalla normativa vigente in materia di *privacy*". L'impianto così costituito, secondo l'Autorità, oltre a confliggere con la normativa in materia anagrafica, trovava un limite (emergente anche dai lavori parlamentari di approvazione della legge n. 675/1996) legato al fatto che tra le attribuzioni delle regioni non rientrano compiti di disciplina, anche indiretta, della materia della protezione dei dati personali, neanche in materie di competenza regionale, restando semmai salvi eventuali provvedimenti regionali in funzione attuativa di obblighi normativi fissati a livello statuale o nella normativa comunitaria (v. segnalazione del 26 maggio 2000, in *Bollettino* n. 13, p. 16).

La Regione Friuli-Venezia Giulia ha poi fornito un riscontro alle osservazioni del Garante manifestando la volontà di attuare la predetta normativa in un quadro di pieno rispetto dei principi in materia di riservatezza e di trattamento dei dati personali.

Pur prendendo atto di tale assicurazione, il Garante ha ribadito la necessità di individuare un correttivo almeno in sede attuativa, regolando in una deliberazione di Giunta il ricorso a tecniche informatiche e telematiche tali da agevolare i flussi di dati, in piena conformità ai limiti ed alle modalità consentite dal regolamento anagrafico, chiedendo a tal fine di prendere visione preventivamente degli schemi di regolamenti ed atti amministrativi di attuazione (v. nota del 9 ottobre 2000, in *Bollettino* n. 14-15, p. 22).

La Regione Friuli-Venezia Giulia ha assicurato di volersi conformare a quanto indicato dall'Autorità ed ha inviato in data 4 dicembre 2000 un primo schema di deliberazione di Giunta volto ad individuare le modalità operative della comunicazione di dati anagrafici da parte dei comuni.

Il Garante nel dare atto, ancora una volta, della collaborazione istituzionale avviata, ha però dovuto rilevare che alcuni principi non hanno ancora trovato integrale attuazione. Il riferimento è in particolare alla necessità di garantire che i dati provenienti dalle anagrafi della popolazione siano utilizzati solo per usi di pubblica utilità e che il trattamento a livello regionale di ulteriori dati a fini di prestazioni di servizi al cittadino avvenga nel pieno rispetto della normativa sulla protezione dei dati personali, evitando la sostanziale formazione di una anagrafe regionale della popolazione, nonché improprie applicazioni della disciplina del consenso (v. parere del 10 dicembre 2001, in *Bollettino* n. 19).

Sempre relativamente alla costituzione di grandi archivi informatizzati, va ricordata la vicenda relativa all'istituzione di una banca dati sui sinistri stradali. Allo scopo infatti di rendere più efficace la prevenzione ed il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore, il d.l. 28 marzo 2000, n. 70, aveva inserito all'art. 12 della legge n. 990/1969 il comma 5-*quater*, istitutivo presso l'ISVAP di una banca dati dei sinistri relativi a tali assicurazioni.

La formulazione della norma è risultata tuttavia particolarmente carente sul piano della protezione dei dati personali. La legge di conversione 5 marzo 2001, n. 57, sebbene abbia apportato qualche correttivo, non è riuscita a fugare le perplessità iniziali.

In particolare, tale legge ha stabilito che le procedure e le modalità di funzionamento della banca dati in questione siano definite con provvedimento dell'ISVAP da pubblicare nella Gazzetta Ufficiale. Con lo stesso provvedimento devono essere stabilite le modalità di accesso alle informazioni raccolte per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore, nonché le modalità ed i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione. Il trattamento e la comunicazione dei dati personali ai soggetti indicati sono consentiti per lo svolgimento delle funzioni previste dalla medesima disposizione. La genericità dei limiti imposti è tale da alimentare alcune perplessità sul grado di tutela assicurato agli inte-

ressati, perplessità che potrebbero essere almeno in parte superate da una tempestiva ed accorta consultazione del Garante che, sebbene la legge non impone come obbligatoria, è stata tuttavia già oggetto di una prima richiesta dell'ISVAP.

Il Garante è stato poi chiamato a fornire il proprio avviso sullo schema delle istruzioni poi impartite dalla Banca d'Italia nel settore bancario e alla Società interbancaria per l'automazione S.p.a. (S.I.A.) per la gestione del sistema centralizzato per la rilevazione dei rischi creditizi per gli indebitamenti di importo compreso fra i 60 ed i 150 milioni di lire, in applicazione della deliberazione del Comitato interministeriale per il credito e il risparmio del 3 maggio 1999, pubblicata sulla *G.U.* n. 158 dell'8 luglio 1999 (v. oltre par. n. 36).

Un accenno va infine fatto al registro informatico dei protesti cambiari la cui disciplina, come già ricordato nel paragrafo 2, è stata innovata dalla legge 18 agosto 2000, n. 235, che ha stabilito un limite per la registrazione delle notizie dei protesti in tale archivio ed ha conferito precisi diritti in ordine alla cancellazione delle stesse nel caso di pagamento delle cambiali o di erroneo inserimento delle informazioni.

Da ultimo, nel quadro delle diverse e proficue collaborazioni in atto in particolare con la Banca d'Italia, il Garante è stato attivamente consultato nel quadro dei lavori preliminari per la redazione dello schema di regolamento del Ministro della giustizia con il quale saranno disciplinate le modalità di trasmissione dei dati all'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento irregolari istituito presso la Banca d'Italia dall'art. 36 del d.lg. n. 507/1999. Diverse indicazioni dell'Autorità sono state recepite prima del recente invio dello schema di regolamento al Consiglio di Stato, da parte del Ministero della giustizia, per il previsto parere.

10. CARTA D'IDENTITÀ ELETTRONICA E TESSERA ELETTORALE

In linea con l'attuale processo di consolidamento della c.d. *Società dell'informazione*, le amministrazioni pubbliche mostrano un crescente interesse ad utilizzare documenti elettronici per svolgere attività amministrative e per erogare *on-line* servizi ai cittadini; trattasi di una tendenza in atto da alcuni anni e già registrata nelle precedenti relazioni dell'Autorità, che persegue finalità di semplificazione, snellimento e razionalizzazione dell'attività amministrativa.

Tra i documenti elettronici della pubblica amministrazione già regolamentati ed introdotti in via sperimentale vi sono i documenti di riconoscimento muniti di supporto magnetico o informatico e le carte sanitarie elettroniche.

Vi è il rischio che l'istituzione e l'interconnessione dei documenti elettronici sacrifichi o comprima l'esigenza di tutela dei diritti della persona e della riservatezza dei dati personali; tale preoccupazione si fonda anche sul fatto che l'Italia è priva di una legislazione articolata ed organica in materia e ciò rende possibile la proliferazione e la duplicazione di archivi e documenti elettronici da parte dei soggetti pubblici.

Vi è dunque l'esigenza di armonizzare gli interventi attraverso una legislazione generale che contemperi le esigenze di efficienza e di razionalizzazione della pubblica amministrazione con quelle di tutela della riservatezza della persona, anche in attuazione delle prescrizioni e dei principi contenuti nella normativa comunitaria.

Il Garante, che già negli anni passati, nell'esercizio della sua funzione consultiva (art. 31, comma 2, legge n. 675/1996), aveva evidenziato la necessità di valutare con attenzione il tipo di informazioni da inserire nei documenti elettronici, le operazioni effettuabili su di essi, i soggetti che possono avere accesso alle diverse categorie di dati e i diritti dei cittadini in particolare rispetto ai dati sanitari e biometrici, più recentemente ha anche partecipato ad un gruppo di lavoro istituito presso la Presidenza del Consiglio dei ministri relativo all'ipotesi di introduzione di *carte intelligenti* nei Paesi membri dell'Unione europea.

Inoltre la Commissione europea, durante la presidenza portoghese dell'Unione europea, ha organizzato nel mese di aprile del 2000 un vertice sulle *carte intelligenti* al quale hanno partecipato autorevoli rappresentanti dei vari settori interessati; tali incontri sono stati l'occasione per arricchire il già vivace dibattito in sede comunitaria incentrato sull'individuazione di principi generali comuni, sulle garanzie di affidabilità e sicurezza e sullo sviluppo di specifiche tecnologie.

Con riferimento all'attività svolta sul piano interno dal Garante e in particolare alla carta d'identità elettronica e al documento d'identità elettronico, occorre ricordare che tali documenti sono stati già istituiti e parzialmente regolamentati negli anni scorsi (art. 2, comma 10, della legge 15 maggio 1997, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191; d.P.C.M. 22 ottobre 1999, n. 437).

Nel mese di giugno il Ministero dell'interno ha chiesto il parere dell'Autorità sullo schema di decreto ministeriale concernente le regole tecniche e di sicurezza relative alle tecnologie ed ai materiali utilizzati per la produzione delle carte e dei documenti d'identità elettronici.

L'Autorità nell'esprimere il parere allo schema di decreto, ha formulato alcune osservazioni relativamente alla gestione associata delle funzioni dei Comuni, all'interconnessione degli archivi, all'aggiornamento di un archivio nazionale (il citato Indice nazionale delle anagrafi) non previsto dalla normativa primaria e al trattamento dei dati sensibili.

Nel medesimo parere il Garante ha peraltro segnalato che, per quanto attiene i progetti di sperimentazione a livello locale, occorre una valutazione complessiva ed omogenea delle varie iniziative dei comuni che rende quindi necessaria la consultazione dell'Autorità da parte del Ministero ai sensi dell'art. 31, comma 2, della legge n. 675/1996. In tale occasione (*Provv.* del 12 luglio 2000) si è anche proposto – considerati i ristretti termini previsti per il procedimento – di individuare una soluzione secondo cui nel caso di specie, in caso di silenzio dell'Autorità protrattosi per oltre dieci giorni dalla ricezione della richiesta, il parere dell'Autorità stessa poteva considerarsi reso.

Tali osservazioni, tese ad un più attento bilanciamento delle esigenze di semplificazione e di snellimento dell'attività amministrativa con quelle di riservatezza della persona in conformità con la normativa vigente in materia, non sono state recepite nel testo del decreto emanato nel mese di luglio (cfr. d.m. 19 luglio 2000, pubblicato nella *G.U.* 21 luglio 2000, n. 169). Con una nota successiva, il Ministro si è tuttavia impegnato a tenere in massima considerazione le osservazioni formulate dall'Autorità in sede di attuazione delle disposizioni del decreto e ha manifestato l'intenzione del Governo di proporre un'apposita disposizione legislativa relativa all'indice nazionale delle anagrafi.

Di seguito a tale impegno non sono però pervenuti al Garante interpelli del Ministero relativi alla sperimentazione a livello locale di carte di identità.

Per quanto attiene alla tessera elettorale, documento sostitutivo e permanente del certificato elettorale, occorre premettere che esso è stato introdotto nel corso dell'anno in forma cartacea (cfr. d.P.R. 8 settembre 2000, n. 120), nonostante la previsione legislativa circa la possibilità di adottare la tessera su supporto informatico, anche attraverso l'utilizzazione congiunta della carta d'identità elettronica (art. 13 legge 30 aprile 1999, n. 120).

Tale questione ha a lungo impegnato l'Autorità lo scorso anno, dapprima in incontri con rappresentanti del Ministero dell'interno, e poi nell'elaborazione dell'articolato parere espresso sullo schema di regolamento concernente la tessera elettorale (cfr. parere del 17 novembre 1999; v. anche la Relazione sull'attività svolta e sullo stato di attuazione della legge n. 675/1996 relativa all'anno 1999, p. 22).

In tale occasione il Garante aveva formulato osservazioni critiche sull'ipotesi di introdurre, seppure per una fase transitoria, la tessera elettorale in forma cartacea e aveva suggerito di utilizzare direttamente il modello su supporto informatico.

L'Autorità aveva in particolare espresso la preoccupazione che la tessera cartacea, valida per un numero consistente di consultazioni elettorali e/o referendarie e riportante l'indicazione dell'avvenuto voto, diversamente dal modello informatico, comportasse una conoscibilità dei dati relativi al comportamento elettorale dell'interessato eccessiva rispetto alle finalità della legge istitutiva (l. n. 120/1999) e non pienamente conforme alla normativa sulla protezione dei dati personali.

Tali osservazioni, qui riportate in estrema sintesi, non sono state accolte nel regolamento emanato con d.P.R. 8 settembre 2000, n. 299 in quanto, come risulta dalla relazione del sottosegretario di Stato per l'interno, l'interesse al controllo sull'esercizio del diritto di voto è stato ritenuto prevalente sull'esigenza di tutela della riservatezza dei cittadini (cfr. resoconto stenografico Camera, I commissione, 27 ottobre 1999).

L'Autorità ha auspicato un riesame a breve dell'intera questione, anche in considerazione delle aspre e diffuse critiche successivamente intervenute sul documento così come adottato.

Si rammenta in particolare che in occasione delle ultime consultazioni elettorali (12 maggio 2001), l'Autorità ha ribadito che alcuni profili del nuovo modello di tessera elettorale non rispettano la disciplina sulla riservatezza dei cittadini e il principio della segretezza del voto, rendendo conoscibile il comportamento elettorale del cittadino. Il Garante ha pertanto sollecitato nuovamente il Ministero ad un complessivo riesame della questione, segnalando anche alcuni specifici accorgimenti per evitare che la certificazione della partecipazione al voto possa eventualmente evidenziare particolari condizioni dell'elettore, quali la degenza in ospedale e la detenzione in carcere (v. comunicato stampa del 24 aprile 2001).

11. ATTI ANAGRAFICI, DELLO STATO CIVILE E LISTE ELETTORALI

Una parte rilevante dell'attività del Garante nei riguardi del settore pubblico è stata rivolta a soddisfare numerose richieste di chiarimenti avanzate da enti locali con riferimento alla disciplina, parzialmente diversa, applicabile in relazione alle loro specifiche funzioni e caratteristiche, pur nella uniformità della disciplina relativa a tutti i soggetti pubblici non economici. In particolare, una serie di interventi del Garante hanno riguardato problemi relativi alla comunicazione e alla diffusione dei dati nell'ambito delle norme riguardanti gli atti anagrafici, lo stato civile e le liste elettorali.

Il Garante aveva già affrontato alla fine del 1999 la specifica questione della consultazione per via telematica degli atti anagrafici da parte delle forze dell'ordine (v. il parere reso al Comune di Pino Torinese, comunicato stampa n. 33, in *Bollettino* n. 10, p. 108). Sul tema il Garante è tornato per profili di carattere più generale riguardo alla possibilità di stipulare convenzioni fra archivi anagrafici, altre amministrazioni pubbliche, gestori ed esercenti di pubblici servizi. Il Comune di Novara ha chiesto un parere su una bozza di convenzione in attuazione della facoltà prevista dall'art. 2, comma 5, della l. 127/1997, per la trasmissione di dati e documenti tra gli archivi anagrafici e dello stato civile "garantendo il diritto alla riservatezza delle persone". Il Garante, nel parere del 22 marzo 2000 (in *Bollettino* n. 11-12, p. 18), ha chiarito che detta disposizione agevola semplicemente la possibilità di trasmissione di dati e documenti a cui i diversi soggetti possono già accedere sulla base della legislazione vigente, mentre una nuova forma di gestione e di accesso ai dati anagrafici "potrebbe essere invece introdotta solo da apposite norme modificative".

Sulla base di quanto previsto dal comma 3 dell'art. 27 della l. n. 675/1996, l'Autorità, con provvedimento del 10 luglio 2000, ha poi ritenuto conforme alla legge in materia di protezione dei dati personali la diffusione di una delibera della giunta comunale nella quale erano riportate alcune informazioni relative al pagamento di taluni tributi e ad un credito vantato nei confronti dell'amministrazione comunale. Oltre a non aver riscontrato una violazione delle norme in materia di pubblicità degli atti comunali o una inosservanza dei principi di pertinenza e non eccedenza dei dati inseriti nell'atto pubblicato, l'Autorità ha ricordato che ai fini della diffusione da parte di pubbliche amministrazioni non è prevista l'acquisizione del consenso degli interessati.

Per quanto riguarda la possibilità per un Comune di incaricare una cooperativa di effettuare, mediante convenzione, un servizio di protocollazione di atti di stato civile provenienti dall'estero giacenti presso gli uffici comunali, il Garante (provvedimento del 16 febbraio 2001) ha ricordato che nello svolgimento dei propri compiti istituzionali il soggetto pubblico può ricorrere a privati affidando ad essi determinate attività anche attraverso concessioni, appalti o convenzioni. In tal caso, a garanzia della tutela della riservatezza dei dati personali trattati dal soggetto privato, è necessario che la convenzione contenga espresse disposizioni relative alla nomina del responsabile e dei soggetti incaricati del trattamento e alle garanzie per la sicurezza dei trattamenti e dei dati ai sensi dell'art. 15 della l. n. 675/1996 e del d.P.R. n. 318/1999.

L'Autorità, come sopra detto, è intervenuta in più occasioni (provvedimenti del 26 maggio 2000, 5 dicembre 2000 e 10 aprile 2001, rispettivamente in Bollettino n. 13, p. 15; n. 14/15, p. 22; n. 19) in merito alla legge della Regione Friuli-Venezia Giulia n. 11/2000 con la quale, integrando le disposizioni con-

cernenti l'anagrafe dei beneficiari delle agevolazioni sul prezzo delle benzine, creerebbe una nuova e ben più articolata anagrafe regionale della popolazione, utilizzata anche per altre finalità di carattere istituzionale. Nel caso di specie, il Garante ha ritenuto che tali iniziative non sono compatibili con la disciplina anagrafica, tenendo anche conto dei limiti cui soggiace la potestà normativa regionale in materia di protezione dei dati personali e, conseguentemente, con i principi dell'articolo 27 della legge n. 675/1996. Non sono state ritenute ammissibili, pertanto, né la libera consultazione diretta delle anagrafi (attraverso, ad esempio, l'interrogazione individuale o di massa di qualsiasi dato contenuto negli archivi), né una loro indifferenziata interconnessione con le banche dati del soggetto richiedente le informazioni medesime.

Con un parere reso il 4 aprile 2001 (in *Bollettino* n. 19), il Garante ha precisato che il diritto di accesso alle liste elettorali di sezione utilizzate in precedenti elezioni per la votazione, nella quale sono contenuti dati idonei a rivelare l'effettiva partecipazione dei cittadini alle votazioni, è esercitabile da ogni elettore entro il termine di 15 giorni dal deposito nella cancelleria, al fine dell'eventuale controllo sulla regolarità delle operazioni elettorali. Fuori dal contesto e dai limiti descritti, pertanto, i titolari di cariche elettive che lo richiedano in occasione di successive consultazioni elettorali non possono consultare dette liste. Con l'occasione l'Autorità ha peraltro ricordato la libera consultabilità da parte di chiunque, con possibilità di estrarne copia, stamparle e metterle in vendita, delle liste elettorali custodite presso gli uffici comunali, nelle quali sono, come è noto, riportati i dati dei cittadini iscritti nel comune aventi diritto al voto.

Un tema ricorrente ha riguardato la possibilità per i comuni, mediante la stipula di convenzioni, di favorire la trasmissione di dati e documenti tra archivi anagrafici, nonché verso altre amministrazioni pubbliche e ai gestori ed esercenti di pubblici servizi. Sull'argomento l'Autorità ha risposto al Comune di Novara con provvedimento del 22 marzo 2000 (in *Bollettino* n. 11/12, p. 18) sottolineando che non è conforme alla disciplina anagrafica e alle norme sulla protezione dei dati la consultazione indiscriminata degli archivi anagrafici dei comuni e l'interconnessione tra questi archivi e le banche dati delle altre amministrazioni.

Sebbene l'impostazione seguita nella predisposizione della convenzione fosse da ritenere condivisibile tenendo conto della normativa sul rilascio dei certificati anagrafici, il Garante ha segnalato al Comune la necessità di evitare connessioni dirette con archivi o atti anagrafici e di prevedere, piuttosto, la possibilità di collegamenti informatici o telematici attraverso i quali rendere disponibili, su richiesta, la trasmissione o la consultazione in rete di un documento o di un certificato relativi, a seconda del soggetto convenzionato, ad elenchi di iscritti all'anagrafe oppure a singole posizioni anagrafiche. È stato, inoltre, precisato che occorre indicare la motivazione che giustifica il collegamento, il quale deve essere previsto da specifiche norme di regolamento, oppure legittimato da necessità istituzionali degli enti richiedenti.

Il tema ha richiesto un'ulteriore precisazione anche in relazione allo sviluppo dei servizi offerti da molte amministrazioni attraverso reti Intranet e Internet. Nel parere reso all'Associazione nazionale dei comuni italiani (ANCI) il 23 maggio 2000 (in *Bollettino* n. 13, p. 21), l'Autorità ha indicato le linee-guida che devono essere osservate per assicurare una corretta ed uniforme applicazione della normativa sulla protezione dei dati personali, in particolare per quanto riguarda la gestione dei flussi informativi delle c.d. reti civiche che consentono di accedere per via telematica anche ad informazioni, notizie, banche dati e archivi degli enti locali.

Nel provvedimento sono state esaminate anche altre questioni di rilievo per l'attività dei comuni, tra le quali la conoscibilità dei dati trattati dai servizi sociali e la comunicazione di quelli relativi agli stranieri minorenni ai fini del rimpatrio nei Paesi d'origine. In tale circostanza si è chiarito che, mentre la pubblicazione di elenchi nominativi riguardanti il rilascio di concessioni ed autorizzazioni edilizie non incontra ostacoli di fondo, è invece vietata la diffusione attraverso le reti civiche dei dati personali provenienti dagli archivi anagrafici o dai registri dello stato civile, la cui conoscibilità è soggetta all'osservanza di limiti e modalità fissati uniformemente da norme dello Stato.

L'Autorità ha precisato che nel regolamento per la gestione delle reti civiche l'ente locale può anche prevedere che la diffusione dei dati avvenga mediante la pubblicazione di riviste e di notiziari telematici. In tal caso il trattamento dei dati può essere basato su finalità di tipo giornalistico e i comuni possono adempiere agli obblighi previsti per gli editori e per i giornalisti dalla legge n. 675/1996 e dal codice di deontologia per l'attività giornalistica. Se l'accesso alla rete civica avviene attraverso una postazione pubblica il comune, oltre a dotarsi delle misure minime di sicurezza previste dal regolamento n. 318/1999 per prevenire la dispersione, la distruzione o l'uso illecito dei dati personali, deve attrezzare tali postazioni con sistemi che garantiscano la riservatezza delle operazioni effettuate dall'utente, impedendo ai successivi utilizzatori di conoscere o di poter ricostruire le informazioni che sono state acquisite dalla rete.

Il Garante è tornato sull'argomento in occasione della promozione da parte di alcune Regioni di collegamenti telematici tra gli archivi anagrafici dei comuni, allo scopo di semplificare l'attività amministrativa. Con il parere del 20 giugno 2000 (in *Bollettino* n. 13, p. 11), fornito al Ministero dell'interno in merito a un progetto di integrazione delle anagrafi elaborato nel caso di specie dalla rete telematica regionale toscana anche per permettere la comunicazione telematica di alcune informazioni tratte dalle anagrafi comunali, il Garante ha spiegato che l'interconnessione tra gli archivi è in linea generale compatibile con la legge sulla *privacy*, ma deve limitarsi alla comunicazione di dati secondo le modalità previste dalla legislazione anagrafica e non può dare luogo alla costituzione di una anagrafe autonoma su base regionale. Le altre amministrazioni connesse al sistema non partecipano, pertanto, alla diretta gestione degli archivi, ma vi possono accedere in tempo reale, pur sempre nel rispetto delle disposizioni fissate dalla legislazione anagrafica.

Un aspetto parimenti delicato è poi relativo all'attività di comunicazione verso i cittadini da parte delle istituzioni comunali. In proposito deve rilevarsi che nei tempi più recenti, anche al fine di istituire un rapporto più diretto tra amministratori ed amministrati, sono aumentate nei comuni alcune forme di comunicazione diretta da parte dei sindaci (lettere, riviste, giornali inviati nominativamente). Ciò è sicuramente un effetto delle leggi che hanno modificato l'ordinamento degli enti locali e il relativo sistema elettorale. La voluta personalizzazione delle funzioni dei sindaci ha avuto come conseguenza anche una forte personalizzazione delle loro comunicazioni, il che ha reso difficile tracciare netti confini tra comunicazione "istituzionale" e comunicazione "non istituzionale", sicché si è generata a volte incertezza nell'opinione pubblica e reazioni da parte di alcuni cittadini.

In relazione a tale quadro, il Garante ha ad esempio esaminato le segnalazioni di alcuni cittadini di Roma e di Milano che, avendo ricevuto una lettera da parte dei rispettivi sindaci, avevano chiesto all'Autorità di verificare se l'inoltro della lettera fosse avvenuto nel rispetto della normativa in materia di trattamento dei dati personali. Il Garante, con due provvedimenti del 19 aprile 2001 (in *Bollettino* n. 19), ha ritenuto di non poter escludere che le lettere in questione fossero riconducibili all'attività di informazione e di comunicazione delle pubbliche amministrazioni, pur osservando che, dall'esame della documentazione trasmessa dai due Comuni, potevano ravvisarsi alcuni punti incerti, se rigorosamente confrontati con il paradigma normativo, e tuttavia non tali da configurare un palese contrasto con le norme che regolano la materia.

12. L'ATTUAZIONE DELLA LEGGE NEGLI ENTI LOCALI

Come si è già osservato, l'attuale evoluzione tecnologica apre nuove possibilità di creare archivi e banche dati in grado di contenere un numero crescente di informazioni personali che possono essere poste in relazione fra loro per le finalità più diverse. Seppure ne deriva la possibilità di disporre di nuovi servizi in maniera più efficiente e rapida, ciò tuttavia comporta un aumento dei rischi intrinsecamente connessi con tali operazioni, le quali moltiplicano le possibilità che i dati vengano impropriamente comunicati o comunque utilizzati per finalità differenti da quelle consentite o autorizzate.

In relazione a tali problematiche, l'Autorità ha partecipato (v. Relazione annuale per il 1999, p. 20) alle attività del Comitato di coordinamento per l'indirizzo ed il controllo della fase di avvio e sperimentazione del Sistema di accesso e interscambio anagrafico-SAIA (art. 8 della Convenzione stipulata in data 4 novembre 1999 tra il Ministero dell'interno e l'Associazione nazionale comuni italiani-A.N.C.I.).

Nell'ambito del medesimo Sistema, il Ministero dell'interno ha posto l'esigenza di realizzare un Indice nazionale delle anagrafi per l'immediata individuazione del Comune che detiene i dati personali contenuti nelle anagrafi della popolazione di ciascun cittadino, nonché per facilitare l'esercizio dei compiti di vigilanza attribuiti sulla tenuta delle anagrafi comunali.

La rilevante incidenza di quest'ultima progettata innovazione sull'ordinamento anagrafico e l'ampia individuazione dei soggetti legittimati ad accedere all'Indice hanno originato una prima presa di posizione del Garante, il 2 novembre 1999, nei riguardi del Ministro dell'interno e due successive, l'8 marzo 2000 e il 29 maggio 2000, nelle quali l'Autorità ha fatto presente che la materia esige un intervento a livello legislativo che permetta anche di definire con chiarezza le finalità di utilizzo, i soggetti aventi accesso e il contenuto stesso di tale Indice, che comunque non può certo prefigurare la creazione di una vera e propria anagrafe nazionale. Successivamente a questi interventi, come si è già avuto modo di

ricordare, con il d.l. 27 dicembre 2000, n. 392, convertito in legge 28 febbraio 2001, n. 26, è stato istituito, presso il Ministero dell'interno, l'Indice nazionale delle anagrafi (INA). Tale disposizione legislativa ha espressamente previsto che ai fini dell'adozione del decreto del Ministro dell'interno per la gestione dell'INA, sia sentito il Garante per la protezione dei dati personali.

Il Garante, con provvedimento del 23 maggio 2000 (in *Bollettino* n. 13, p. 21), ha sollecitato i comuni italiani a dare rapida e compiuta attuazione alle norme sulla *privacy* ed ha fornito una serie di indicazioni e di chiarimenti volti a facilitare una corretta ed uniforme applicazione della normativa sul trattamento dei dati da parte delle amministrazioni comunali.

È stato riscontrato dall'Autorità che, come molte amministrazioni pubbliche, anche i comuni sono in forte ritardo nel porre in essere gli adempimenti previsti a garanzia dei cittadini. In tale occasione è stata ribadita l'esigenza di dare con tempestività attuazione alle previsioni della legge sulla protezione dei dati effettuando tra l'altro la nomina degli "incaricati del trattamento", cioè del personale che gestisce materialmente i dati.

L'attenzione del Garante si è però incentrata, in particolare, sulla necessità di una rapida adozione dei regolamenti previsti dal d.lg. n. 135/1999 in materia di utilizzo di dati sensibili da parte delle pubbliche amministrazioni. È stato così ricordato ai comuni che essi hanno l'obbligo di svolgere una puntuale ricognizione delle categorie delle informazioni raccolte, utilizzate e conservate e, proprio attraverso l'emanazione di questi regolamenti, di identificare e rendere pubblici i tipi di dati e le operazioni che con essi si possono eseguire. Tale adempimento, che ha lo scopo di garantire l'uso corretto dei dati più delicati dei cittadini da parte delle amministrazioni comunali, semplificando al tempo stesso le procedure, deve però avere caratteri di uniformità in modo da evitare, come si è già detto, diversità ingiustificabili e difformità nei trattamenti di dati fra comune e comune.

In questo senso, l'Autorità ha auspicato che l'ANCI avvii un'approfondita e rapida riflessione sugli schemi finora messi a punto e diffusi, che non sono risultati sempre conformi alle norme in materia di protezione dei dati personali.

In linea con gli impegni già assunti con l'ANCI in forza del protocollo d'intesa firmato il 1° luglio 1998, il Garante ha rinnovato in data 3 ottobre 2000 il proprio impegno con l'Associazione dei comuni, nonché con l'UPI e l'UNCEM, per definire un programma ed iniziative che favoriscano ulteriormente il processo di recepimento e di adeguamento della normativa in materia di protezione dei dati personali negli enti locali.

Un altro interessante aspetto è stato affrontato dall'Autorità in occasione dell'esame di una segnalazione relativa alla prassi, adottata dal comando di polizia municipale di una grande città, di non indicare nei verbali di accertamento delle violazioni al codice della strada (nell'esemplare redatto con strumenti automatizzati e comunicato in copia al proprietario del veicolo) le generalità dei vigili urbani che elevavano contravvenzione; su tale esemplare era riportata, invece, un'avvertenza che giustificava tale omissione come conseguenza dell'applicazione della legge sulla *privacy*.

L'Autorità ha affermato che nessuna disposizione della legge sul trattamento dei dati personali preclude alla polizia municipale di indicare nei verbali informatizzati le generalità degli agenti e che risulta anzi impropria l'avvertenza secondo cui la predetta omissione conseguirebbe all'applicazione della l. n. 675/1996.

È stato così precisato che il principio di pertinenza, in base al quale nei vari atti debbono essere riportati i dati indispensabili, opera anche nell'ambito dell'attività di polizia municipale e permette una "calibratura" delle informazioni da indicare, in considerazione della particolare natura dei procedimenti di tipo sanzionatorio e delle esigenze di tutela dei diritti degli automobilisti.

Il Garante ha quindi stabilito che la prassi adottata dal comando non era conseguenza della legge sulla *privacy* e che l'avvertenza presente nei verbali utilizzati doveva essere eliminata.

13. Attività fiscali e tributarie

Il Garante ha continuato, nel corso dell'anno 2000, la sua collaborazione con il Ministero delle finanze, con riguardo alla predisposizione dei modelli di dichiarazioni da presentarsi da parte dei contribuenti e dei sostituti d'imposta.

In particolare, l'Autorità ha reso il proprio parere in ordine ad alcune modifiche apportate alle informative inserite nei modelli 730, 770, CUD ed Unico, a seguito dell'intervenuta abrogazione, da parte dell'art. 7 della l. 3 giugno 1999, n. 157, della norma che consentiva ai contribuenti di destinare la quota del 4 per mille dell'Irpef al finanziamento dei partiti e dei movimenti politici (art. 1 l. n. 2/1997). Rispetto agli esemplari predisposti per il 1999, vi è stata un'ulteriore modifica riguardante la collocazione del testo completo dell'informativa nelle istruzioni in appendice, rimettendo ad una nota sintetica posta sul frontespizio il compito di fornire una prima informazione e di operare il necessario rinvio.

In data 3 febbraio 2000 il Garante si è espresso positivamente su tali modifiche, formulando alcune osservazioni di dettaglio. Con l'occasione, il Ministero ha manifestato all'Autorità l'intenzione di utilizzare per le dichiarazioni del 2000 lo stesso modello di busta impiegato nel 1999; anche in questa circostanza, l'Autorità ha preso atto delle assicurazioni fornite dall'Amministrazione rispetto alla non estraibilità delle dichiarazioni dalle aperture praticate su tale busta.

Per quanto concerne i contenuti delle dichiarazioni dei redditi, il Garante ha fornito un riscontro in relazione ai dubbi prospettati dal Ministero delle finanze in ordine alla legittimità della diffusione dei nominativi di contribuenti che hanno dichiarato redditi superiori ad una certa soglia, evidenziandone la destinazione ad un'ampia pubblicità, confermata dalla vigenza della disposizione che prevede la pubblicazione a cura del Ministero degli elenchi di contribuenti il cui reddito imponibile è stato accertato dai competenti uffici e di quelli sottoposti a controlli globali a sorteggio (art. 69, commi 1, 2 e 3, d.P.R. n. 600/1973). Tali elenchi comprendono, tra l'altro, i nominativi dei contribuenti che non hanno presentato la dichiarazione dei redditi o nei cui confronti è stato accertato un maggior reddito disponibile superiore a determinate soglie.

Il medesimo regolamento prevede altresì la formazione, per ciascun comune, di elenchi nominativi di tutti i contribuenti che hanno presentato la dichiarazione dei redditi o che esercitano imprese commerciali, arti e professioni, elenchi da depositarsi per un anno presso gli uffici delle imposte ed i comuni interessati per la consultazione da parte di chiunque (art. 69, comma 4, d.P.R. n. 600/1973); tali disposizioni, come il Garante ha precisato, non sono state modificate dall'entrata in vigore della legge n. 675/1996.

La prassi di collaborazione tra il Ministero delle finanze e l'Autorità garante è, d'altra parte, rispecchiata dalla decisione dell'Amministrazione di sottoporre a parere preventivo diversi provvedimenti concernenti attività rilevanti dal punto di vista del trattamento di dati personali.

Nel corso del 2000, il Ministero ha ad esempio chiesto al Garante di esprimere un parere su uno schema di convenzione di affidamento in concessione ad una società a partecipazione pubblica (*ex* art. 10, comma 12, l. n. 146/1998) dell'elaborazione di studi di settore e dell'effettuazione di studi e ricerche in materia tributaria. L'originario testo della convenzione prevedeva che la concessionaria potesse utilizzare dati, notizie ed informazioni presenti nel sistema informativo dell'Amministrazione, attenendosi alle direttive impartite da essa, nonché di dati, notizie ed informazioni fornite all'Amministrazione dall'Istat, dalle associazioni di categoria, da enti, istituzioni ed organismi pubblici e privati, o raccolti direttamente, attraverso indagini anche campionarie.

Esprimendosi in merito, il Garante ha rappresentato la necessità di specificare le categorie di dati messe a disposizione del concessionario, nel rispetto dei principi di pertinenza, proporzionalità e non eccedenza dei dati sanciti dall'art. 9 della legge n. 675/1996, dovendosi precisare altresì quali informazioni possono essere raccolte direttamente dal concessionario. A quest'ultimo possono essere resi comunque accessibili esclusivamente i dati che l'Amministrazione e gli altri soggetti pubblici detengono già e trattano in base ad altre specifiche disposizioni contenute in leggi o regolamenti. L'Amministrazione è stata invitata a precisare le modalità dell'accesso alle informazioni del proprio sistema e degli altri soggetti pubblici, nonché a chiarire se la concessionaria sarà tenuta a registrare le informazioni acquisite in appositi archivi elettronici.

L'Autorità ha inoltre chiarito che la concessionaria dovrà essere designata quale responsabile del trattamento dei dati di cui appariva unico titolare l'Amministrazione finanziaria nel suo complesso. È risultato inoltre necessario segnalare la necessità di introdurre puntuali indicazioni in ordine alle finalità e ai limiti dell'utilizzazione delle informazioni personali da parte del concessionario, con particolare riguardo all'individuazione di appropriate misure relative alla sicurezza dei dati, specificando che i trattamenti effettuati dal concessionario possono riguardare le finalità e i dati strettamente collegati all'espletamento di quanto previsto dalla convenzione. Il Garante ha infine ribadito che potranno essere diffusi dal concessionario soltanto dati anonimi (parere del 14 marzo 2001): il nuovo assetto organizzativo dei ministeri finanziari, che consente una limitata esternalizzazione di talune attività di elaborazione delle informazioni, non dovrebbe, in tal modo, avere significative conseguenze sul grado di tutela riconosciuto agli interessati.

Il conferimento di nuove competenze alle regioni in materia di accertamento dell'assolvimento degli obblighi in materia di tasse automobilistiche comporterà la condivisione degli archivi ad esse relativi, e la necessità di armonizzare le norme di gestione, onde garantire adeguate economie di spesa. Il Ministero delle finanze ha chiesto al Garante, in proposito, di esprimere un parere su uno schema di protocollo di intesa tra le regioni, le province autonome di Trento e Bolzano e lo stesso Ministero, concernente l'aggiornamento e la gestione degli archivi regionale e nazionale delle tasse automobilistiche, ai sensi dell'art. 5, commi 1 e 2, d.m. 25 novembre 1998, n. 418.

Nell'esprimersi sullo schema sottoposto alla sua valutazione (parere dell'11 dicembre 2000), l'Autorità si è richiamata ai precedenti pareri espressi sui provvedimenti di attuazione della legge n. 449/1997 ed ha precisato che occorre prevedere specificamente l'utilizzabilità dei dati per lo scopo unico ed esclusivo della gestione delle tasse automobilistiche. Ha altresì rilevato che il protocollo d'intesa, nonché la complessa disciplina della materia, prevedono una serie articolata di rapporti tra soggetti pubblici ed organismi istituiti *ad hoc*, rendendo assai incerta la determinazione dell'amministrazione o dell'organismo che svolge le funzioni di titolare del trattamento. In proposito, il Garante ha richiesto il necessario chiarimento, indispensabile ai fini della corretta applicazione della normativa sulla protezione dei dati, anche in relazione all'eventuale designazione dei responsabili del trattamento e all'esercizio dei diritti dell'interessato.

Le articolate attribuzioni del Ministero delle finanze comprendono, come è noto, anche l'attività di vigilanza e regolamentazione in materia di lotterie e giuochi. L'imminente avvio delle concessioni relative al "bingo" ha richiesto l'esercizio del potere regolamentare del Ministro, che vi ha provveduto con d.m. 31 gennaio 2000, n. 29. In applicazione di tale decreto, la competente direzione generale ha sottoposto all'attenzione del Garante uno schema di regolamento sul quale l'Autorità ha emesso un parere in data 25 ottobre 2000. Con riferimento all'effettuazione di riprese nelle sale mediante impianti televisivi a circuito chiuso, il Garante ha ritenuto necessario precisare che dette riprese dovranno riguardare solo il meccanismo di estrazione delle palline, anziché giocatori e visitatori presenti. L'Autorità ha poi giudicato non conforme al principio di non eccedenza e pertinenza del trattamento la prevista schedatura indiscriminata degli innumerevoli visitatori delle sale dislocate sul territorio nazionale e di tutti i loro singoli ingressi, attuata, in ipotesi, per impedire l'accesso alle sale di determinati soggetti (minori, persone in stato di ebbrezza, in possesso di armi). Peraltro, come ha segnalato il Garante, l'eliminazione delle schede personali per ciascun visitatore non preclude la possibilità, per il personale di sala, di chiedere a determinati soggetti, nell'esercizio della necessaria vigilanza, di esibire un documento di identità in determinate circostanze (ad esempio, per verificare l'età o per identificare persone moleste).

Conformemente a quanto disposto dall'art. 31 della legge n. 675/1996, la Presidenza del Consiglio dei ministri ha poi chiesto un parere in ordine ad uno schema di decreto legislativo in materia di criteri unificati di valutazione della situazione economica dei soggetti che richiedono prestazioni sociali agevolate, a norma dell'art. 59, comma 53, della legge 27 dicembre 1997, n. 449 (c.d. riccometro).

Il provvedimento mira a ridurre gli adempimenti a carico dei richiedenti determinate prestazioni agevolate in ambito pubblico, a chiarire alcuni criteri utili per accertare la loro situazione economica, nonché a perfezionare il sistema delle detrazioni.

Con il precedente d.lg. n. 109/1998 sono stati identificati alcuni "criteri unificati" per valutare tale situazione economica anche attraverso un indicatore della "situazione economica equivalente" (i.s.e.e.) dei soggetti interessati, rilevante ai fini dell'ammissione alle prestazioni.

Nel parere espresso il 26 marzo 1998 sul relativo schema, il Garante aveva manifestato già diverse perplessità sugli aspetti di propria competenza, rappresentando la necessità che il decreto bilanciasse direttamente, con norme primarie, le finalità pubbliche connesse all'istituzione del "riccometro" con i diritti fondamentali degli interessati.

Precisando di non voler interferire sulle scelte di politica economica e sociale, l'Autorità aveva chiesto di introdurre un quadro organico e facilmente ricostruibile di disposizioni sui tipi di prestazioni agevolate, sulle modalità osservate dai singoli enti per acquisire, utilizzare e scambiare i dati di carattere personale, nonché per costituire eventuali archivi o banche dati e per effettuare controlli.

Tale richiesta non ha però trovato accoglimento, nel complesso, nel d.lg. n. 109/1998, il quale rimane tuttora carente, come ha segnalato il Garante, per le parti che riguardano la protezione dei dati personali e presenta le caratteristiche di genericità e di frammentazione che erano state evidenziate nel parere.

Il d.lg. n. 109/1998 ha peraltro mantenuto aperta la possibilità, già prevista dalla legge-delega n. 449/1997, di introdurre specifiche disposizioni in tema di trattamento dei dati attraverso ulteriori decreti correttivi adottabili nel corso del successivo biennio.

Lo schema di decreto sottoposto al parere del Garante costituisce, per l'appunto, uno dei provvedimenti che il Governo si era riservato di adottare.

Il Garante, nel parere del 5 aprile 2000, ha richiamato l'attenzione sulla necessità di completare lo schema con norme che chiariscano con maggiore trasparenza le modalità di utilizzazione e di circolazione delle informazioni di carattere personale (modalità che vanno disciplinate poiché le amministrazioni raccoglieranno anche dati "comuni" diversi da quelli "sensibili").

Si prevedeva, con il decreto legislativo *in itinere*, l'introduzione di una banca dati centralizzata presso l'INPS di notevoli dimensioni e collegata con un vasto arco di enti; una novità che doveva essere quindi accompagnata da misure e garanzie adeguate, ulteriori rispetto al profilo della sicurezza e dell'integrità dei dati.

Nello specifico, l'Autorità ha così rilevato:

– che non sembrava in linea con la legge-delega la soluzione secondo cui l'INPS potesse delineare una "procedura informatica" per facilitare la raccolta e l'utilizzazione delle informazioni rilevanti per la determinazione dell'i.s.e.e. (procedura che secondo l'art. 59, comma 51, lett. a) della legge-delega n. 449 doveva essere invece predisposta a cura della Presidenza del Consiglio dei ministri);

– che la norma dello schema di decreto la quale disciplinava l'utilizzazione delle informazioni da parte dell'INPS per i controlli, facendo riferimento ad archivi di amministrazioni collegate, non poteva essere ritenuta una fonte "autorizzativa" di tali collegamenti. La base normativa e i limiti per tali intrecci di dati andavano necessariamente ritrovati in norme speciali che prevedessero espressamente l'interconnessione o il collegamento, oppure nella generale disciplina prevista dall'art. 27, comma 2, della legge n. 675/1996 (per i dati "comuni") e dal decreto n. 135/1999 (per quelli "sensibili"), da richiamare nella disposizione;

– che una considerazione analoga alla precedente andava formulata per quanto riguarda le comunicazioni INPS a (non meglio individuati) enti erogatori di prestazioni sociali agevolate.

Il Garante ha, così, conclusivamente rilevato l'esigenza di integrare e modificare lo schema in base alle osservazioni suesposte.

Nel corso del 2000 sono pervenuti all'Autorità numerosi reclami e segnalazioni da parte di cittadini e di associazioni di consumatori concernenti la comunicazione che la RAI – Radiotelevisione italiana S.p.A. invia alle persone che non risultano presenti negli elenchi degli abbonati al servizio radiotelevisivo ai fini del pagamento del canone. Il Garante ha esaminato, ove possibile, congiuntamente tali reclami e segnalazioni, in quanto spesso prospettanti, sotto vari profili, analoghe questioni.

Con una prima comunicazione oggetto di censura, la RAI ha invitato i destinatari a regolarizzare la propria posizione, allegando un bollettino di conto corrente per il versamento dell'importo dovuto e un questionario in cui indicare dati anagrafici e indirizzo (anche in riferimento a familiari conviventi titolari dell'abbonamento), con l'avvertimento che, in difetto di notizie che permettano di regolarizzare la posizione, la società si riserva di comunicare i dati del destinatario all'Amministrazione finanziaria per successivi accertamenti. I reclami e le segnalazioni hanno sollevato il problema della liceità del trattamento, da parte della società concessionaria del servizio pubblico radiotelevisivo, dei dati dei destinatari della comunicazione, lamentando, in particolare, che:

a) nessuna norma permetterebbe alla RAI, in quanto S.p.A., di raccogliere ed utilizzare i dati degli interessati senza il loro consenso (con specifico riferimento alla possibilità, per la stessa società, di accedere ai dati presenti nelle anagrafi comunali della popolazione e agli elenchi telefonici); non sarebbe inoltre previsto un obbligo per questi ultimi di fornire dati che li riguardano o che attengono a propri familiari o conviventi;

b) non sarebbero stati chiari i criteri e le modalità in base ai quali vengono acquisiti i dati dei potenziali utenti e vengono inviate le comunicazioni, in quanto i destinatari fanno parte spesso di un nucleo familiare o risiedono con un convivente già abbonati (es.: coniuge o figli maggiorenni) e non sono titolari di ulteriori utenze relative ad altri servizi di pubblica utilità (in alcuni casi, gli interessati dichiarano anche di non possedere apparecchi televisivi);

c) la comunicazione (di cui vengono anche contestati i toni considerati vessatori) ed il connesso trattamento dei dati non sarebbero stati in sintonia con il principio di correttezza sancito dalla disciplina sulla tutela dei dati personali poiché, pur in mancanza di informazioni attendibili circa la detenzione di apparecchi televisivi, la società presumerebbe da semplici elementi (es.: iscrizioni o variazioni anagrafiche relative alla residenza o al raggiungimento della maggiore età dei cittadini) una possibile evasione del canone;

d) il questionario da rispedire con i dati anche di terzi non avrebbe riportato una idonea informativa ai sensi della legge n. 675/1996 (art. 10) e sarebbe stato inoltre inserito in una cartolina visibile a chiunque (anziché in busta chiusa);

e) di fronte alle richieste degli interessati di conoscere la fonte dalla quale sono stati ricavati i dati (o di esercitare gli altri diritti di cui all'art. 13 della legge n. 675, ad esempio, per chiedere la cancellazione o il blocco dei dati, oppure per opporsi al loro trattamento), la società non avrebbe spesso fornito alcun riscontro o avrebbe risposto in modo negativo (affermando, ad esempio, di non dover "fornire indicazioni riguardanti le procedure adottate per individuare eventuali utenze TV abusive").

L'Autorità si era già occupata del trattamento dei dati connesso alla gestione e alla riscossione del canone di abbonamento al servizio radiotelevisivo in occasione del parere sui due atti aggiuntivi alla convenzione stipulata tra il Ministero delle finanze e la RAI il 23 dicembre 1988 per regolare i rapporti relativi alla gestione del canone (parere del 9 maggio 2000).

La materia è disciplinata da un complesso di disposizioni normative, talvolta di diversi anni or sono, le quali stabiliscono che chiunque detiene "uno o più apparecchi atti o adattabili alla ricezione delle radioaudizioni" deve pagare un canone (in particolare, il r.d.l. 21 febbraio 1938, n. 246, convertito nella legge 4 giugno 1938, n. 880 e la legge 14 aprile 1975, n. 103, in cui sono regolati gli adempimenti relativi alle modalità e ai termini di pagamento, al c.d. libretto di iscrizione alle radiodiffusioni, alle denunce all'ufficio del registro dei cambiamenti di residenza o del domicilio, oppure della cessazione dell'uso dell'apparecchio e alle sanzioni applicabili).

L'amministrazione degli abbonamenti è stata affidata per tutto il territorio nazionale ad un unico ufficio dell'Amministrazione finanziaria istituito con d.m. del 16 dicembre 1953, già denominato URAR-TV di Torino (Ufficio registro abbonamenti radio TV, ora I Ufficio entrate Torino S.A.T Sportello Abbonamento T.V.), il quale si avvale di strutture, mezzi e personale messi a disposizione dalla società. Quest'ultima svolge inoltre, per conto di tale ufficio ed in base alla predetta convenzione, diversi compiti relativi alla riscossione degli abbonamenti e al recupero delle somme dovute, a vario titolo, dai detentori degli apparecchi e può inviare ad essi comunicazioni ed avvisi.

La convenzione prevede l'obbligo per la RAI di costituire, sempre per conto del predetto ufficio (e in base alla documentazione dallo stesso fornita), un ruolo magnetico degli abbonati residenti nel territorio nazionale, che deve essere periodicamente aggiornato per quanto riguarda i pagamenti, le cancellazioni e le situazioni anagrafiche (sulla base di tale ruolo vengono poi predisposti i libretti di iscrizione ed effettuati i controlli su coloro che hanno omesso, ritardato od effettuato in misura insufficiente il pagamento).

Con il primo atto aggiuntivo alla convenzione (stipulato il 17 giugno 1999 ed approvato con decreto del Ministero delle finanze il 23 luglio 1999), sono stati precisati alcuni aspetti relativi al trattamento dei dati. L'Amministrazione finanziaria-URAR-TV di Torino ha designato la RAI–Direzione produzione abbonamenti e attività per le pubbliche amministrazioni quale responsabile del trattamento dei dati contenuti nell'archivio informatico risultante dal ruolo magnetico degli abbonati (art. 8 l. n. 675/1996), anche per ciò che attiene ai dati anagrafici relativi a cittadini maggiorenni acquisiti dalla RAI per conto dell'URAR TV o direttamente da quest'ultimo, dati ricavati dagli archivi comunali o dalle banche dati di società che erogano servizi di pubblica utilità (ai sensi della l. n. 127/1997 e della l. n. 166/1991 di conversione del d.l. n. 103/1991 sullo scambio di dati tra l'amministrazione finanziaria ed altri soggetti pubblici e privati ai fini del recupero di contributi previdenziali).

In qualità di responsabile del trattamento, la società deve attenersi alle istruzioni impartite dall'amministrazione, la quale può effettuare verifiche. Deve inoltre predisporre una relazione periodica sulle attività relative ai dati personali ed individuare per iscritto le persone fisiche incaricate di compiere le operazioni necessarie per attuare la convenzione (art. 19 l. n. 675/1996).

Il primo dei due atti aggiuntivi prevede inoltre che la RAI debba ricevere periodicamente dall'URAR TV i dati dei soggetti che non risultano titolari di abbonamento e (per conto dello stesso ufficio, ma a proprio nome e spese) debba inviare a tali soggetti "comunicazioni contenenti l'indicazione degli obblighi discendenti dalla detenzione di apparecchi radiotelevisivi e dei vantaggi conseguenti alla regolarizzazione spontanea", comunicando all'URAR TV i risultati della verifica con i dati aggiornati dei soggetti contattati e di coloro che hanno risposto (v. l'art. 1, commi 6 e 7). Quale responsabile del trattamento, la RAI collabora con l'Amministrazione titolare del trattamento nello svolgimento dei compiti relativi alla gestione e alla riscossione dei canoni. La società non può essere dunque considerata, secondo il Garante, come un soggetto privato che persegue ulteriori finalità e che può decidere autonomamente in ordine al trattamento delle informazioni personali, dovendo la stessa attenersi rigorosamente alle prescrizioni normative e alle istruzioni impartite all'Amministrazione finanziaria.

Limitatamente a questi rapporti, alla società deve ritenersi quindi applicabile il particolare regime previsto per le amministrazioni pubbliche che, a differenza dei privati (i quali possono trattare informazioni personali in presenza del consenso degli interessati o di uno degli altri presupposti equipollen-

ti: artt. 12 e 20 l. n. 675), possono effettuare solo i trattamenti di dati connessi all'esercizio delle proprie funzioni istituzionali, nei limiti stabiliti dalle previsioni di legge o di regolamento (art. 27 l. n. 675/1996).

Il trattamento da parte della RAI dei dati relativi agli abbonati è risultato quindi lecito in termini generali, anche per quanto concerne la raccolta, per conto dell'URAR TV, di ulteriori informazioni sui cittadini nell'ambito delle convenzioni che l'amministrazione finanziaria può stipulare per la trasmissione di dati o di documenti (sulla base delle citate disposizioni della l. n. 127/1997 e in tema di scambio dei dati per il recupero di contributi previdenziali), rispettivamente con i comuni (in riferimento agli archivi anagrafici e dello stato civile, con le modalità e nei limiti stabiliti dalle relative discipline normative, su cui il Garante si è più volte pronunciato) e con soggetti erogatori di servizi (ad es., per l'energia elettrica o la telefonia).

Le informazioni personali raccolte possono essere utilizzate dalla società, seppur esclusivamente per le finalità perseguite dall'Amministrazione finanziaria, ai fini della gestione degli abbonamenti e della riscossione dei canoni con adozione, però, di tutti gli accorgimenti richiesti dalla normativa sulla tutela del diritto alla riservatezza (individuazione degli incaricati, informativa, misure di sicurezza, diritti di accesso ai dati personali, ecc.).

Sul piano della corretta e completa attuazione degli adempimenti in materia di protezione dei dati la comunicazione della RAI e le collegate iniziative segnalate dai cittadini, presentano tuttavia diverse lacune ed anomalie.

In considerazione del fatto che varie comunicazioni inviate ai cittadini ed il relativo trattamento di dati sono basati su accertamenti preliminari e valutazioni presuntive, il Garante ha segnalato, anzitutto, l'esigenza che, in linea con il principio di correttezza sancito dall'art. 9 della legge n. 675/1996, la RAI indichi con chiarezza gli obblighi relativi alla detenzione di apparecchi radiotelevisivi e i vantaggi conseguenti ad una regolarizzazione spontanea, riformulando la comunicazione in modo da evidenziare meglio al destinatario le relative finalità, evitando toni ed espressioni con le quali si attribuisca all'interessato una possibile evasione del canone.

Pur restando impregiudicata la doverosa attività di verifica del corretto pagamento del canone, occorre disporre, come ha rimarcato l'Autorità, prima di inviare una comunicazione del tipo di quella segnalata, lo svolgimento di riscontri più attenti ed approfonditi sotto i profili della completezza, dell'esattezza e della pertinenza delle informazioni raccolte. La comunicazione in questione (contenente dati personali raccolti presso terzi) e l'allegato questionario (volto all'acquisizione di dati direttamente dagli interessati) non recavano le informazioni agli interessati necessarie ai sensi dell'art. 10 della legge n. 675/1996; non precisavano, inoltre, la natura facoltativa od obbligatoria del conferimento dei dati, né le conseguenze dell'eventuale rifiuto di fornirli. I destinatari della comunicazione devono essere altresì informati sulla possibilità di esercitare i diritti di accesso ai dati previsti dall'art. 13 della legge n. 675. Deve essere poi agevolato tale accesso anche attraverso opportune misure volte a semplificare le modalità e a ridurre i tempi delle risposte (art. 17, comma 9, del d.P.R. n. 501/1998).

Quanto all'interpretazione secondo cui la società ha fornito un riscontro negativo a talune richieste volte a conoscere l'origine dei dati relativi a nominativi ed indirizzi (ritenendo tali informazioni concernenti atti preparatori di un procedimento tributario, considerati sottratti al diritto di accesso ai sensi degli artt. 13, comma 2, e 24, comma 6, della legge n. 241/1990), l'Autorità ha ribadito le differenze che contraddistinguono, in termini di oggetto e di presupposti, il diritto di accesso di cui alla legge n. 241 (che si riferisce alla documentazione amministrativa e può essere esercitato dal portatore di un interesse personale e qualificato, per la tutela di situazioni giuridicamente rilevanti, salvi i casi di esclusione previsti) e i diritti introdotti dalla legge n. 675/1996. Tali diritti riguardano infatti i dati personali e possono essere esercitati dalle persone cui si riferiscono senza particolari formalità e limitazioni, ad eccezione di taluni diritti che richiedono una specifica situazione e dei casi di esclusione tassativamente indicati dalla legge, nei quali non può però rientrare il trattamento svolto dalla RAI, in qualità di responsabile del Ministero delle finanze, ai fini della gestione degli abbonamenti.

Il Garante ha così confermato l'obbligo, per la società concessionaria e per l'Amministrazione finanziaria, di fornire senza ritardo un riscontro alle richieste avanzate in base al predetto art. 13 della legge n. 675 ricordando che, in caso di mancata risposta o di riscontro negativo, dopo cinque giorni dalla richiesta, gli interessati possono rivolgersi all'autorità giudiziaria o al Garante ai sensi dell'art. 29 della medesima legge.

Infine, il Garante si è occupato di un altro aspetto evidenziato in alcuni reclami, indicando la necessità dell'adozione di misure idonee ad evitare un'inutile divulgazione di dati personali attraverso la restituzione del questionario contenente dati anche di terzi (di familiari o conviventi già abbonati) in una cartolina leggibile da chiunque, anziché in una busta chiusa o con modalità che, comunque, non ne rendano possibile una facile ed immediata consultazione da parte di estranei (*Provv.* del 12 luglio 2000).

Successivamente, il Garante si è espresso in ordine agli schemi di comunicazione e del questionario, riformulati dalla società in conformità al provvedimento (segnalazione del 13 dicembre 2000). In tale occasione, l'Autorità è tornata a chiarire che l'informativa dovrà specificare la possibilità di comunicare dati degli utenti alla Guardia di finanza, per i controlli di competenza, solo sulla base di precisi elementi e riscontri circa la presunta evasione del canone, come richiede la vigente disciplina di riferimento, onde evitare condizionamenti della volontà della persona contattata nel comunicare i dati del terzo cui è intestato l'abbonamento. Il Garante ha quindi segnalato alla società l'opportunità di specificare che la compilazione del questionario facilita l'identificazione dell'abbonamento di riferimento e può rendere superflue ulteriori verifiche.

L'Autorità ha chiesto da ultimo chiarimenti alla società sui presupposti giuridici in base ai quali RAI-radiotelevisione italiana S.p.a. sollecita, nell'ambito di altri tipi di comunicazioni, il rilascio di una dichiarazione sostitutiva dell'atto di notorietà per le situazioni di convivenza con persone titolari di abbonamento al servizio radiotelevisivo, in riferimento a quanto disposto dagli artt. 9 e 10 della legge n. 675/1996.

Il Garante è in procinto di definire conclusivamente tutti i procedimenti attivati sulle varie questioni relative al canone radiotelevisivo, in relazione agli elementi forniti dalla RAI in un quadro di piena collaborazione rispetto alle verifiche effettuate.

14. ARCHIVI RELATIVI A CITTADINI EXTRACOMUNITARI

L'Autorità ha affrontato nel corso dell'anno anche alcune delicate questioni relative alle modalità di costituzione, di gestione e di interconnessione di archivi relativi ai cittadini extracomunitari da parte di soggetti pubblici.

Trattasi di un tema complesso, che può implicare il trattamento dei dati sensibili di persone straniere e che richiede il coordinamento tra l'ampia e articolata legislazione di settore, anche in materia di tutela dell'ordine pubblico e di immigrazione, e le prescrizioni e i principi sulla protezione di dati personali.

Il Garante, nel mese di marzo, ha espresso un parere favorevole sullo schema di decreto poi adottato nel mese di dicembre dal Ministro dell'interno e relativo alle modalità di comunicazione, anche in via telematica, dei dati concernenti i cittadini stranieri fra gli uffici di anagrafe dei comuni, gli archivi dei lavoratori extracomunitari e gli archivi dei competenti organi centrali e periferici del Ministero dell'interno (G. U. 11 gennaio 2001, n. 8).

Il Garante ha poi segnalato al Ministero dell'interno-Dipartimento di pubblica sicurezza la necessità di adeguare i trattamenti dei dati relativi ai permessi di soggiorno per motivi di protezione sociale alla normativa sulla protezione dei dati personali attraverso il ricorso a codici alfanumerici idonei ad identificare la tipologia di permesso ai soli uffici interessati (art. 18, d.lg. n. 286/1998).

L'Autorità ha quindi ritenuto lesive del generale principio di pertinenza e di non eccedenza previsto dall'art. 9 della legge n. 675/1996 le modalità con le quali un ufficio periferico di pubblica sicurezza ha rilasciato alcuni permessi speciali.

In particolare è stata contestata l'apposizione a margine di uno schedario degli estremi della normativa sul soggiorno per motivi di protezione sociale e l'indicazione delle associazioni impegnate nel reinserimento dello straniero. Tale procedura rendeva infatti facilmente desumibile la tipologia del permesso, esponendo gli interessati al rischio di essere facilmente individuati quali persone sottratte ai condizionamenti di organizzazioni criminali.

Il Ministero dell'interno ha recepito le osservazioni formulate dall'Autorità, diramando una circolare con la quale ha disposto che all'atto del rilascio dei permessi di soggiorno per motivi di protezione sociale si debba fare riferimento solo a codici alfanumerici e alla locuzione "motivi umanitari".

Sempre con riferimento a questo argomento, è in via di definizione un procedimento attivato da una segnalazione relativa ad un rilevamento effettuato nelle scuole pubbliche da parte degli insegnanti di religione cattolica. Si tratta di uno studio volto ad acquisire elementi utili per predisporre i nuovi progetti formativi rivolti ad una scuola sempre più multietnica e multireligiosa. I dati raccolti riguardano il numero di studenti immigrati – anche in riferimento alla provenienza geografica – che si avvalgono o meno dell'insegnamento della religione cattolica.

FORZE DI POLIZIA, UFFICI GIUDIZIARI E SERVIZI DI INFORMAZIONE E DI SICUREZZA

15. PROFILI GENERALI

Come è noto, la legge n. 675/1996 prevede, all'art. 4, alcuni trattamenti svolti in ambito pubblico che sono ancora parzialmente sottratti alla disciplina in materia di protezione dei dati personali (ci si riferisce, in particolare, ai trattamenti effettuati per ragioni di giustizia, per finalità di prevenzione e repressione dei reati, a quelli relativi a dati memorizzati o destinati a confluire nel Centro elaborazione dati del Dipartimento della pubblica sicurezza, nonché ai trattamenti effettuati dai servizi di informazione e di sicurezza).

A tali trattamenti, tuttavia, si applicano alcune disposizioni della legge n. 675, in particolare quelle attinenti ai requisiti di liceità e alla sicurezza dei trattamenti di dati personali, nonché quelle che prevedono l'esercizio da parte del Garante di verifiche e controlli (art. 4, comma 2, l. n. 675/1996). Gli uffici giudiziari o di polizia hanno, in particolare, il dovere di rispettare il principio di "proporzionalità" nel trattamento dei dati (in base al quale, fra l'altro, si possono trattare solo i dati *"pertinenti ... e non eccedenti"* rispetto alle finalità istituzionali, secondo quanto previsto dall'art. 9 l. n. 675/1996) e l'obbligo di adottare le cautele necessarie a garantire la sicurezza dei dati trattati (art. 15, commi 1 e 2, l. n. 675/1996 e d.P.R. n. 318/1999 sulle misure minime di sicurezza).

Sulla portata e sui limiti dell'attuale applicabilità di tali disposizioni ai trattamenti dell'art. 4 si è rivolta l'attenzione del Garante, in attesa che sia completato il quadro normativo. La recente legge 24 marzo 2001, n. 127, infatti, al fine di ultimare il processo di piena attuazione dei principi previsti dalla legge n. 675 nell'ambito di specifici settori, già avviato con le leggi-delega n. 676/1996 e n. 344/1998, ha previsto un ulteriore differimento del termine per l'esercizio della delega al 31 dicembre 2001.

16. PROTEZIONE DEI DATI E ATTIVITÀ GIUDIZIARIA

I principi descritti si applicano ai trattamenti di dati personali svolti *"per ragioni di giustizia"*, sebbene la normativa processuale antecedente alla legge n. 675/1996 non sia stata ancora modificata alla luce delle nuove garanzie in materia di trattamento dei dati personali.

Come già riportato nella relazione per l'anno 1999, il Garante si è espresso in tal senso in particolare nel provvedimento del 29 febbraio 2000 rispetto ai trattamenti effettuati nell'ambito di un giudizio instaurato da persone che avevano contratto particolari sindromi a causa della somministrazione di emoderivati infetti.

Data la delicatezza della materia, il legale delle parti aveva richiesto che fossero adottate nel processo misure idonee a tutelare la riservatezza dell'identità dei ricorrenti e, in proposito, l'Autorità ha sottolineato che i principi previsti dalla legge n. 675, benché non ancora compiutamente articolati nelle norme processuali civili e penali, dovrebbero comunque concretizzarsi in misure anche di carattere organizzativo, pur nei limiti delle prerogative dell'autorità giudiziaria. La non integrale adozione in giudizio di efficaci cautele può condizionare, infatti, il diritto del cittadino alla propria difesa o addirittura comportare la rinuncia della parte lesa a chiedere il risarcimento dei danni per timore dell'ampia conoscibilità delle patologie sofferte.

L'Autorità ha comunque segnalato al Governo e al Parlamento l'opportunità che siano introdotte disposizioni processuali volte a contemperare meglio le esigenze processuali con quella di garantire la riservatezza dei soggetti coinvolti in vicende giudiziarie riguardanti aspetti particolarmente delicati della persona.

Sull'argomento il Garante, nel luglio 2000, ha anche avuto un proficuo incontro con l'Associazione nazionale magistrati, nel corso del quale quest'ultima ha sottolineato l'esigenza di integrare, anche sul piano normativo, la disciplina processuale e deontologica al fine di assicurare il pieno rispetto dei dirit-

ti della personalità e in particolare della riservatezza. Il Garante e l'Associazione hanno poi concordato sulla necessità di operare un attento bilanciamento, anche sul piano delle prassi applicative, tra la tutela della riservatezza e la specificità della funzione giudiziaria che è preposta alla tutela di interessi anch'essi costituzionalmente garantiti.

Il Garante non ha rinvenuto, invece, elementi per intervenire in ordine alle disposizioni che un tribunale aveva impartito in tema di accesso degli operatori giudiziari e, in particolare, degli avvocati, alle notizie sullo stato dei procedimenti civili e penali inserite nel sistema informativo del medesimo ufficio giudiziario; ciò anche in considerazione delle precedenti prese di posizione con le quali l'Autorità ha richiamato l'attenzione sul rapporto fra le norme processuali sulla richiesta di atti e di notizie e le disposizioni della legge n. 675.

Sotto il profilo dei controlli sui trattamenti svolti *"per ragioni di giustizia"*, il Garante, anche nel decorso anno, ha precisato che è consentito inviare all'Autorità una segnalazione o un reclamo (art. 31, l. n. 675/1996) per sollecitare il controllo sulla liceità dei trattamenti, ma non è possibile esercitare i diritti nelle forme previste dagli articoli 13 e 29 della legge n. 675 rivolgendosi direttamente all'ufficio giudiziario o presentando un formale ricorso all'Autorità stessa.

Con provvedimento del 14 febbraio 2001, il Garante ha ritenuto tuttavia che i diritti di cui all'articolo 13 si possono esercitare rispetto ai dati contenuti in una nota-circolare del Consiglio superiore della magistratura quale quella esaminata, con la quale si informavano gli uffici giudiziari dell'avvenuta nomina dei referenti per la formazione decentrata. La decisione era ovviamente basata sul presupposto che i trattamenti di dati non erano effettuati per "ragioni di giustizia". Con il relativo ricorso al Garante, il magistrato interessato aveva chiesto il blocco del trattamento dei dati personali e la rettifica delle informazioni diffuse sul proprio conto con la circolare, ritenendo che si trattasse di dati incompleti e non pertinenti e comunque implicanti discredito alla propria persona. Nel merito, l'Autorità ha poi respinto la richiesta di blocco anche in quanto il provvedimento inibitorio non sarebbe comunque risultato necessario alla luce dell'iniziativa assunta dal CSM di sostituire la circolare "impugnata". Ha inoltre respinto anche la richiesta di rettifica in quanto, per le modalità con cui era stata formulata, avrebbe determinato la diffusione di ulteriori dati anch'essi non pertinenti rispetto alla finalità da perseguire; ciò sul presupposto che l'applicazione di un principio previsto dalla legge n. 675 non può comportare un'ulteriore inosservanza degli altri principi di protezione dei dati.

Anche sotto il profilo dei controlli, con l'attuazione della legge-delega n. 127/2001, si avrà la possibilità di sperimentare nuovi strumenti di garanzia per gli interessati volti, ad esempio, a consentire loro un esercizio più immediato dei diritti previsti dall'articolo 13 della legge n. 675, tenendo comunque conto della specificità dei trattamenti svolti per *"ragioni di giustizia"*.

Sono da ricordare inoltre, nell'ambito delle diverse iniziative dell'Autorità garante sul tema dei trattamenti di dati personali a fini di giustizia:

– le indicazioni espresse dall'Autorità stessa sullo schema di regolamento recante disposizioni per l'uso di strumenti informatici e telematici nel processo civile (regolamento poi approvato con decreto del Ministro della giustizia 13 febbraio 2001, n. 123);

– il parere reso sullo schema di decreto ministeriale riguardante le regole procedurali relative alla tenuta dei registri informatizzati dell'Amministrazione della giustizia (decreto del Ministro della giustizia 27 marzo 2000, n. 264);

– il provvedimento del 17 febbraio 2000, con il quale il Garante ha riconosciuto la liceità del trattamento di dati personali relativi a minori da parte di un Ufficio per la mediazione penale costituito su iniziativa di alcuni soggetti pubblici, in quanto la normativa di settore consente agli uffici giudiziari di avvalersi della collaborazione di esperti per accertare la personalità di minori e di promuoverne la conciliazione con le persone offese dal reato;

– il provvedimento del 30 marzo 2000 con cui l'Autorità, in risposta ad un quesito posto da un ufficio giudiziario, ha chiarito (in senso diverso da quanto pure ritenuto dall'Ufficio legislativo del Ministero della giustizia) che l'articolo 4 della legge n. 675 si riferisce inequivocamente a tutte le attività comunque effettuate nell'ambito di uffici giudiziari, anche dalla magistratura amministrativa e contabile, ribadendo la diretta applicabilità delle disposizioni della legge n. 675 richiamate nel comma 2 dell'art. 4 a tutti i trattamenti svolti per "ragioni di giustizia" e non solo a quelli amministrativi strumentali alla funzione giurisdizionale, fermi restando, in ogni caso, gli opportuni adattamenti resi indispensabili dalla specificità degli interessi perseguiti previsti dalla più volte ricordata legge delega;

– la nota del 9 novembre 2000 con la quale il Garante ha richiamato l'attenzione del Ministro della giustizia sulla pubblicazione, sul sito Internet di un tribunale, di un avviso relativo all'udienza preliminare di un complesso procedimento penale connesso all'utilizzazione di emoderivati infetti. Nell'occasione l'Autorità ha ribadito che, pur nella consapevolezza che la validità dei relativi atti deve essere verificata nella competente sede giudiziaria, l'applicazione – seppure parziale – della legge n. 675/1996 ai trattamenti di dati per ragioni di giustizia impone agli uffici giudiziari di adottare modalità applicative delle norme processuali più consone alle libertà fondamentali e alla dignità degli interessati.

17. LE MODALITÀ DI NOTIFICAZIONE DI ATTI

La tematica delle cautele da osservare a garanzia della riservatezza delle persone interessate da notifiche di atti giudiziari è, com'è noto, fra quelle cui il Garante ha dedicato maggiore attenzione, sin dal provvedimento del 22 ottobre 1998 (v. Relazione per l'anno 1998, p. 23), considerato il generale interesse dei cittadini manifestato. Il Garante era già tornato sull'argomento nel corso del 1999 chiarendo, con una nota del 26 ottobre 1999, che le cautele richieste nelle notifiche a garanzia della riservatezza della persona interessata, e in particolare nei confronti del terzo cui venga notificato l'atto (ad es. busta chiusa), sono da ritenersi applicabili anche al processo contabile ed amministrativo (v. Relazione per l'anno 1999, p. 62). La questione è stata portata anche all'attenzione del Ministero della giustizia.

Alcune indicazioni dell'Autorità sono state sostanzialmente recepite in un disegno di legge presentato nella decorsa legislatura il quale, tuttavia, è stato approvato solo da un ramo del Parlamento (XIII^ legislatura, AC 6735). Tale iniziativa, che si auspica venga riproposta, opportunamente aggiornata, nel corso della nuova legislatura, prevede alcune soluzioni rispetto alle notificazioni degli atti del processo (si era prevista infatti la modifica di alcune disposizioni dei codici di rito e della normativa sulle notifiche a mezzo posta) e nell'ambito di procedimenti amministrativi, dove il problema è altrettanto sentito (ad es. notifica di sanzioni a carattere amministrativo, cartelle esattoriali, ecc.).

18. ATTIVITÀ DI POLIZIA

Per quanto riguarda i trattamenti svolti per finalità di polizia, hanno assunto un particolare rilievo gli accertamenti svolti dal Garante a seguito di alcune segnalazioni di militari e di cittadini in ordine a taluni trattamenti di dati personali effettuati dall'Arma dei Carabinieri riguardanti, in particolare, le c.d. "pratiche permanenti".

Dagli accertamenti effettuati non sono emersi trattamenti sostanzialmente difformi dalla normativa vigente. Sono stati però evidenziati alcuni problemi che derivano da un quadro normativo non ancora pienamente armonizzato ai principi introdotti dalla legge sulla riservatezza dei dati. In tal senso, il Garante ha segnalato al Governo la necessità di un sollecito intervento normativo, anche in via regolamentare, sia per quanto riguarda i trattamenti a fini amministrativi, sia per quelli attinenti alle attività di polizia.

In particolare, dalle notizie fornite dall'Arma in un quadro di collaborazione, è emerso che alcune prassi da lungo tempo adottate hanno portato alla conservazione di un numero elevato di pratiche e di informazioni ormai in contrasto con i sopravvenuti principi in materia di protezione dei dati. L'Autorità ha pertanto indicato – accanto alle auspicate soluzioni normative – la necessità di interventi anche sul piano organizzativo, volti, fra l'altro, ad individuare termini più adeguati di conservazione dei dati, nonché livelli diversificati di consultazione dei documenti, a consentire verifiche periodiche della pertinenza delle informazioni e ad assicurare idonee cautele rispetto ai dati più risalenti nel tempo, specie se di natura sensibile. L'Arma ha già fornito alcuni primi utili riscontri con due note pervenute nel marzo di quest'anno.

Analogamente a quanto appena descritto in ordine alle "pratiche permanenti" dell'Arma, il Garante non ha rinvenuto elementi di illiceità nei trattamenti di dati effettuati dall'Ufficio per la garanzia peni-

tenziaria del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia, in ordine ai quali un sindacato di categoria aveva segnalato presunte "schedature" del personale con l'asserita creazione di fascicoli riportanti informazioni di carattere privato (*Provv.* del 30 ottobre 2000).

Un'altra problematica della quale il Garante è tornato ad occuparsi è quella delle richieste di informazioni formulate nell'ambito di attività di indagine di polizia giudiziaria o avanzate da pubbliche autorità per altre finalità istituzionali.

Il Garante aveva già chiarito alcuni importanti aspetti applicativi della disciplina in materia allorché, nel 1999, aveva fornito una prima risposta ad una compagnia aerea circa i limiti di acquisibilità da parte delle forze di polizia di dati relativi ai passeggeri dei voli (v. Relazione per l'anno 1999, p. 63).

Più di recente, l'Autorità ha nuovamente distinto due categorie di richieste: a) quelle riconducibili ad un'attività di polizia giudiziaria, cui si applica l'art. 4 della legge n. 675, alle quali deve darsi corso in base al codice di procedura penale non ostandovi l'applicabilità della stessa legge n. 675, salva l'applicabilità, in ogni caso, del principio di pertinenza (per cui le richieste devono, nei limiti del possibile, essere circostanziate sotto il profilo oggettivo e temporale); b) quelle avanzate da forze di polizia o da altre pubbliche autorità non riconducibili all'esercizio di poteri di polizia giudiziaria (o, comunque, alle altre funzioni indicate nell'art. 4), cui si applica l'intera disciplina della legge n. 675 e, in particolare, quella prevista per i flussi informativi fra soggetti pubblici e privati (artt. 27 e 20, l. n. 675).

La questione verrà nuovamente approfondita a breve con particolare riguardo alla richiesta di acquisire sistematicamente dati sui passeggeri di voli aerei.

Per quanto attiene al profilo dei controlli sui trattamenti effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o su trattamenti comunque riconducibili ad attività di polizia considerate nell'art. 4 della legge, il Garante, in relazione ad un ricorso avverso il trattamento dei dati personali utilizzati per un avviso orale del questore, ha ribadito che per i trattamenti effettuati dal predetto C.e.d. o riconducibili a *"finalità ... di prevenzione, accertamento e repressione dei reati"* (art. 4, comma 1, lett. e)) l'interessato può esercitare i suoi diritti di verifica e di rettifica direttamente nei confronti del Dipartimento della pubblica sicurezza, Ufficio per il coordinamento e la pianificazione delle forze di polizia, ovvero sollecitare l'instaurazione da parte del Garante di un autonomo procedimento di verifica su quanto segnalato dall'interessato in ordine ai dati che lo riguardano (art. 31, comma 1, lett. d) e p) e art. 32), ma non può presentare ricorso al Garante ai sensi dell'art. 29 della legge n. 675 e 18 e ss. del d.P.R. n. 501/1998.

Resta ferma l'esigenza che anche attraverso i decreti delegati previsti dalla citata legge-delega, siano introdotte modifiche alle attuali procedure tali da rendere più snelle, ma anche più efficaci le verifiche.

19. Sistema di informazione Schengen

Nel corso dell'anno il Garante, quale Autorità di controllo sulla sezione nazionale del Sistema informativo Schengen (N.SIS), ha ricevuto numerose richieste di verifica dell'eventuale registrazione, nei predetti archivi, di dati personali dei richiedenti e della liceità dei relativi trattamenti in base ai principi contenuti nella Convenzione di applicazione dell'Accordo di Schengen e nella legge n. 675 (art. 11, l. 30 settembre 1993, n. 388).

La gran parte delle richieste sono state presentate dagli interessati direttamente al Garante, mentre in alcuni casi esse sono pervenute dalle omologhe Autorità di controllo degli altri Paesi alle quali i richiedenti si sono rivolti in base alla procedura di consultazione fra Autorità di controllo prevista dall'art. 114, comma 2, della Convenzione.

Si tratta, in molti casi, di istanze relative al diniego del rilascio di visti; altre richieste sono finalizzate a conoscere l'esistenza e le cause di provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno nel nostro Paese ovvero si riferiscono a casi di usurpazione d'identità o di omonimia.

Anche nel decorso anno si è riscontrato un notevole incremento del numero delle richieste pervenute al Garante rispetto all'anno precedente (n. 59 nel periodo 1999-10 aprile 2000), anche a seguito della proficua azione del nostro Paese nell'ambito della campagna informativa sui diritti del cittadino nei confronti del Sistema d'informazione Schengen, a suo tempo deliberata dall'Autorità comune di controllo in tutti i Paesi aderenti all'Accordo.

L'Autorità garante e l'ufficio SIRENE del Dipartimento della pubblica sicurezza, all'esito di proficui incontri su taluni aspetti applicativi della materia, hanno convenuto circa la necessità che sia assicurata una maggiore speditezza alle procedure per il riscontro agli interessati delle verifiche effettuate, in particolare nei casi in cui l'Ufficio del Garante fornisce tale riscontro sulla base degli elementi forniti dal Dipartimento.

Nel quadro delle verifiche effettuate con la piena collaborazione del Dipartimento non sono emerse specifiche violazioni nelle modalità del trattamento dei dati. Il Garante ovviamente proseguirà nell'esercizio delle proprie funzioni di controllo approfondendo, anche sulla base degli orientamenti dell'Autorità comune di controllo Schengen, la piena corrispondenza alla Convenzione di applicazione dell'Accordo di Schengen delle varie modalità di raccolta e trattamento di specifiche categorie di dati.

20. SERVIZI DI INFORMAZIONE E DI SICUREZZA

Il Garante ha svolto anche nel corso del 2000 l'attività di verifica su specifici trattamenti di dati personali effettuati presso gli organismi competenti in materia di informazioni e di sicurezza (SISMI, SISDE e CESIS), effettuando accertamenti rispetto alle segnalazioni dei soggetti interessati, in conformità alla legge n. 675/1996. I controlli sono stati effettuati con le modalità già osservate nel corso dei precedenti anni, anche nei casi più recenti con la piena collaborazione dei predetti organismi.

Al termine di tali accertamenti, che sono stati concentrati nel terzo gruppo di verifiche effettuate dal Garante a decorrere dalla sua istituzione (per un totale di circa trenta persone fisiche e giuridiche che hanno chiesto accertamenti), l'Autorità, nel riscontrare la sostanziale liceità e correttezza del trattamento dei dati personali, ha rivolto alle autorità di Governo, nel maggio del 2000, alcune valutazioni d'insieme sull'applicazione della normativa in materia di protezione dei dati personali. In particolare è stata richiamata l'attenzione sull'opportunità di impartire nuove istruzioni agli uffici periferici per evitare l'acquisizione di informazioni non pertinenti rispetto alle finalità di tutela della sicurezza e difesa dello Stato.

È stata inoltre rilevata l'esigenza di una maggiore attenzione al profilo della conservazione nel tempo dei dati raccolti, raccomandando una maggiore selezione delle informazioni disponibili anche sulla base di tecniche informatiche e un accesso o una conservazione diversificata del materiale riguardante vicende remote.

Un'indicazione ha riguardato il potenziamento delle tecniche di classificazione di fascicoli, che pure sono risultati conservati in modo ordinato e ricostruibile.

Agli interessati che hanno chiesto accertamenti è stato fornito un riscontro nel rispetto di quanto previsto dall'art. 32, comma 6, della legge n. 675/1996.

Infine, anche per quanto attiene ai controlli esercitabili sui trattamenti svolti dagli organismi di sicurezza ovvero su dati coperti da segreto di Stato, il Garante, con un provvedimento del 28 febbraio 2000, ha precisato che è possibile inviare all'Autorità una segnalazione o un reclamo per sollecitarne il controllo sulla legittimità dei trattamenti, ma non è consentito esercitare i diritti previsti dall'articolo 13 della legge n. 675 rivolgendosi direttamente ai predetti organismi ed eventualmente con ricorso al Garante in base all'articolo 29 della stessa legge n. 675.

SANITÀ

21 PROFILI GENERALI

Il nuovo assetto normativo delineato dal legislatore delegato nel 1999 per la disciplina del trattamento dei dati idonei a rivelare lo stato di salute da parte degli organismi sanitari pubblici, nonché degli organismi sanitari e degli esercenti le professioni sanitarie operanti in regime di convenzione o di accreditamento con il Servizio sanitario nazionale, ha incontrato non poche difficoltà applicative.

Invero, l'efficacia delle disposizioni degli artt. 22 e 23 della legge n. 675, così come riformulate a seguito delle integrazioni e modificazioni introdotte dai dd.lg. 11 maggio 1999, n. 135, in materia di "*trattamento dei dati sensibili da parte dei soggetti pubblici*" e 30 luglio 1999, n. 282 recante "*disposizioni per garantire la riservatezza dei dati personali in ambito sanitario*", è rimessa all'adozione di un regolamento del Ministro della sanità con il quale dovranno essere definite le semplificazioni introdotte dall'art. 2, comma 1, del citato d.lg. n. 282.

Alla stesura di tale regolamento, che sarà emanato previo parere della Conferenza Stato-Regioni e del Garante, lavora un'apposita commissione istituita presso il Ministero della sanità. Quest'ultima, nonostante l'impegno, non è ancora addivenuta ad un testo definitivo che, nell'individuare modalità semplificate per il trattamento dei dati sulla salute e, in particolare, per le informative di cui all'art. 10 della legge n. 675 e per la raccolta del consenso, tenga conto delle diverse esigenze di tutti i titolari coinvolti nella "catena sanitaria" – anche in relazione alle diverse finalità – nonché della necessaria previsione di un periodo non breve per la messa a regime del sistema.

Il lavoro è reso peraltro più complesso dal fatto che al medesimo regolamento del Ministero della sanità, anziché alle singole aziende ed organismi sanitari ed ospedalieri, spetta il compito di provvedere alla ricognizione di tutti i trattamenti dei dati sulla salute effettuati nell'ambito del Servizio sanitario nazionale e, quindi, alla specificazione "dei tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi", ai sensi dell'art. 22, comma 3-*bis*, della legge n. 675/1996.

È evidente che, allo stato, la mancata emanazione del suddetto regolamento – che pure sembra poter giungere a rapida definizione – rende priva di concreta efficacia la volontà del legislatore delegato di prevedere, per il trattamento dei dati sulla salute, una disciplina uniforme per i soggetti pubblici e per quelli privati convenzionati o accreditati con il Servizio sanitario nazionale. A tale riguardo deve aggiungersi che la proroga al 31 dicembre 2001 – disposta con legge 24 marzo 2001, n. 127 – per l'esercizio della delega prevista dalla legge n. 676/1999, potrebbe costituire una preziosa occasione per apportare eventuali altri interventi di carattere integrativo e correttivo (art. 2 l. n. 676/1996) alla vigente disciplina sul trattamento dei dati personali in ambito sanitario.

L'assimilazione sopra detta tra soggetti pubblici e privati operanti nell'ambito del Servizio sanitario nazionale non ha invece interessato i professionisti sanitari operanti in regime di libera professione e tutti gli altri soggetti privati per i quali resta valida la regola generale della doppia condizione del consenso scritto e dell'autorizzazione del Garante o, se del caso, la disciplina speciale prevista dall'art. 23, comma 1, della legge n. 675/1996.

Va rammentato tuttavia che la normativa delegata ha preso comunque in considerazione gli organismi sanitari privati e gli esercenti le professioni sanitarie estranei al S.S.N., laddove ha previsto l'emanazione di appositi codici di deontologia e buona condotta da adottarsi ai sensi dell'art. 31, comma 1, lett. h), della legge n. 675/1996. Questi dovranno, da un lato, prevedere una disciplina integrativa dell'emanando regolamento del Ministro della sanità e, dall'altro, in coordinamento con quest'ultimo, introdurre alcune semplificazioni per il trattamento dei dati sulla salute anche da parte degli organismi sanitari ed esercenti le professioni sanitarie non facenti parte del Servizio sanitario nazionale (art. 17, comma 3, d.lg. n. 135/1999, come modificato dal d.lg. n. 282/1999).

In questo intricato quadro normativo il Garante ha proseguito la sua attività autorizzatoria rinnovando anzitutto, con provvedimento del 20 settembre 2000, l'autorizzazione generale per il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione n. 2/2000, pubblicata sulla Gazzetta

Ufficiale n. 229 del 30 settembre 2000). La nuova formulazione dell'autorizzazione n. 2/2000 non si discosta sostanzialmente dalla precedente. Il termine di efficacia è stato fissato al 31 dicembre 2001.

Sempre nell'ambito dell'attività autorizzatoria il Garante, con provvedimento del 5 dicembre 2000 (pubblicato nel *Bollettino*, nn. 14/15, p. 10), pronunciandosi in ordine ad una specifica richiesta di autorizzazione, ha accolto soltanto parzialmente la richiesta stessa. In particolare, mentre da un lato ha chiarito che il trattamento dei dati idonei a rivelare lo stato di salute per finalità di gestione degli ordini dei clienti è già autorizzato dal provvedimento n. 2/2000 (punto 1.2 lett. e)) alle condizioni ivi indicate, ha d'altra parte opposto un diniego al trattamento dei dati sulla salute finalizzato ad analisi di *marketing* e di statistica, alla creazione dei profili dei clienti, nonché a proposte commerciali ed offerte di vendita in base alle tipologie di acquisto effettuate da ciascun cliente.

Relativamente a questi ultimi trattamenti, infatti, il Garante ha ritenuto che non sussistessero circostanze particolari o situazioni eccezionali tali da giustificare il rilascio di un'autorizzazione specifica in deroga a quella generale e che la richiesta di autorizzazione non era stata predisposta secondo il modello approvato dall'Autorità ai sensi dell'art. 14 del d.P.R. n. 501/1998.

Un'altra istanza di autorizzazione ha fornito al Garante l'occasione per precisare alcuni aspetti relativi al corretto utilizzo dei dati sulla salute da parte di una società che intendeva fornire ai propri clienti un servizio di messa in rete dei profili sanitari dei clienti stessi in un'area ad accesso riservato di un sito Internet, alla quale poter accedere (in caso di necessità anche dall'estero) tramite un codice identificativo personale.

Al riguardo, con nota del 7 febbraio 2001, il Garante ha chiarito che l'accesso al profilo sanitario dell'interessato via Internet dall'estero configura un'ipotesi di trasferimento transfrontaliero dei dati per il quale è di regola necessario il consenso scritto dell'interessato (art. 28, comma 4, lett. e)), eventualmente cumulato con quello più generale previsto nell'ambito del rapporto contrattuale.

Inoltre, con riferimento ai profili della sicurezza e alle misure minime previste dal d.P.R. n. 318/1999, l'Autorità ha precisato che l'assegnazione del codice identificativo e la sua gestione, anche rispetto all'obbligo di disattivazione in caso di "*mancato utilizzo per un periodo superiore a sei mesi*" (art. 4, comma 1, lett. b), d.P.R. n. 318/1999), riguardano ciascun utente a prescindere dalla circostanza che l'utente medesimo o una persona delegata acceda solo ai dati che lo riguardano. Ne deriva che il rapporto contrattuale dovrà prevedere che all'assegnazione del codice identificativo segua anche l'autorizzazione all'accesso prevista dall'art. 5 del d.P.R. sopra citato ("*accesso ai dati particolari*").

Il richiamo all'adozione delle misure minime di sicurezza, nonché al rispetto dei principi generali fissati dal d.lg. n. 135/1999, è contenuto anche in un parere reso dal Garante al Ministero della sanità nell'esercizio della sua funzione consultiva (art. 31, comma 2, l. n. 675/1996). Si tratta, in particolare, del parere sullo schema di decreto ministeriale recante modiche al certificato di assistenza al parto (in *Bollettino*, n. 11-12, p. 34), nel quale l'Autorità ha sottolineato la necessità che nei *nuovi* certificati siano adottate misure idonee a garantire la massima riservatezza delle informazioni per le quali già esiste una disciplina speciale (l. n. 194/1978 sull'interruzione di gravidanza e art. 2, comma 1, l. n. 127/1997 sul diritto della madre all'anonimato).

Va fatta menzione, inoltre, di alcune precisazioni fornite dal Garante nell'ambito dell'esame di alcuni ricorsi presentati ai sensi dell'art. 29 della legge n. 675.

In particolare l'Autorità, nel decidere in merito ad una richiesta di accesso con la quale l'interessato intendeva acquisire copia di un'indagine ecografica effettuata presso un presidio ospedaliero realizzata su un supporto che per la tecnologia usata non permetteva l'estrazione di copia ha precisato che l'art. 13 della legge n. 675 non prevede – in linea di principio – la necessaria consegna della documentazione o dei supporti sui quali i dati sono conservati. Tuttavia, il titolare e il responsabile del trattamento sono tenuti ad estrapolare dai propri archivi e documenti tutte le informazioni su supporto cartaceo o informatico che riguardano il richiedente e a riferirle a quest'ultimo con modalità idonee a rendere i dati facilmente comprensibili, specie quando le informazioni, se non messe a disposizione nella loro interezza a mezzo dell'esibizione o consegna di copia di documenti, non siano agevolmente ricostruibili o siano snaturate del loro contenuto (*Provv.* dell'11 aprile 2000, in *Bollettino* 11-12, p. 58). Nel caso di specie, la soluzione è stata quindi individuata nella visione diretta delle immagini riprodotte sull'unico supporto, da parte del medico designato.

Inoltre, esaminando il ricorso con il quale un ricorrente chiedeva la cancellazione dei dati contenuti nella relazione medica stilata da un centro di igiene mentale, perché trattati senza il suo consenso, il Garante ha chiarito che, in base alla disciplina vigente all'epoca in cui si erano svolti i fatti (artt. 22, comma 3, e 41, comma 5, della l. n. 675/1996), la struttura sanitaria pubblica aveva potuto legittimamente svolgere un'attività di trattamento rientrante tra i propri compiti istituzionali senza il consenso del soggetto interessato (decisione del 29 settembre 2000).

In altra occasione l'Autorità ha invece dichiarato la fondatezza del ricorso presentato da due coniugi nei confronti di un'azienda sanitaria e della relativa società assicurativa, che non avevano fornito riscontro alla richiesta di accesso formulata dai ricorrenti ai sensi dell'art. 13 della legge n. 675/1996. In particolare, il Garante ha riconosciuto il diritto dei ricorrenti di accedere alle informazioni personali contenute in alcune relazioni cliniche, purché e nella misura in cui esse siano direttamente o indirettamente riferibili agli interessati. D'altra parte, invece, il diritto di accesso non riguarda altre parti delle relazioni cliniche che siano riferibili soltanto a rapporti interni all'azienda sanitaria o a circostanze attinenti unicamente al personale medico o paramedico coinvolto nella vicenda (decisione del 12 dicembre 2000).

22. DATI GENETICI

Come è noto, anche con riferimento ai dati genetici è intervenuto il legislatore delegato introducendo il principio secondo cui il trattamento dei dati genetici, da chiunque effettuato, dovrà essere oggetto di una nuova ed apposita autorizzazione del Garante (art. 17, comma 5, d.lg. 11 maggio 1999, n. 135, come integrato e modificato dall'art. 16 del d.lg. 30 luglio 1999, n. 281).

Tale autorizzazione, che avrà carattere generale e dunque troverà applicazione senza la necessità di una apposita richiesta, sarà rilasciata dal Garante a seguito di un complesso procedimento nel quale deve essere "*sentito il Ministro della sanità che acquisisce, a tal fine, il parere del Consiglio superiore di sanità*".

Con deliberazione del 2 maggio 2000 (in *Bollettino* n. 13, p. 19) l'Autorità ha avviato tale procedura stabilendo, peraltro, che l'autorizzazione al trattamento dei dati genetici dovrà: *a*) disciplinare le finalità e le modalità di raccolta, di utilizzazione e di eventuale comunicazione di questi dati; *b*) prevedere misure che consentano all'interessato di esprimere in modo consapevole il consenso all'uso dei dati e che possano prevenire discriminazioni nei suoi confronti o di terzi; *c*) garantire il rispetto della volontà dell'interessato di non essere informato sull'esito degli accertamenti e, infine, *d*) disciplinare le cautele da adottare sul piano della sicurezza nel trattamento dei dati e per assicurare il rispetto del segreto professionale.

Fino all'adozione di una regolamentazione più compiuta, il trattamento dei dati genetici resta tuttavia disciplinato dall'autorizzazione n. 2/2000. Il legislatore delegato ha infatti previsto (art. 17, comma 5, sopracitato) che, nelle more dell'autorizzazione specifica, i trattamenti dei dati genetici possono essere proseguiti sulla base dell'attuale autorizzazione generale del Garante (punto 2, lett. *b*), dell'autorizzazione n. 2/2000).

Al momento, sulla base dell'autorizzazione n. 2/2000 (che prevede il consenso scritto ai sensi degli artt. 22 e 23 della legge n. 675, nonché alcune esclusioni soggettive e limitazioni nelle finalità perseguibili), il trattamento dei dati genetici resta temporaneamente consentito sino al 31 dicembre 2001 "*limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività*". La medesima autorizzazione n. 2/2000 non opera, invece (e il titolare del trattamento deve quindi richiedere previamente al Garante un'apposita autorizzazione), se manca il consenso dell'interessato e il trattamento dei dati genetici è finalizzato alla tutela della salute di un terzo o della collettività. L'inosservanza delle prescrizioni impartite dal Garante attraverso lo strumento autorizzatorio resta punita con la sanzione penale (art. 37 legge n. 675/1996).

L'intervento del Garante in materia di dati genetici si è poi avuto in relazione a talune notizie, apparse sulla stampa nazionale ed internazionale, secondo cui alcune popolazioni sarde sarebbero oggetto di indagini genetiche destinate ad essere proiettate sul mercato anche internazionale.

Avvalendosi dei poteri conferitigli dal legislatore (art. 32, comma 1, legge n. 675/1996), l'Autorità è quindi intervenuta chiedendo ai soggetti coinvolti informazioni e precisazioni circa le finalità e le modalità del complesso trattamento di dati genetici denunciato dalla stampa.

Sebbene gli accertamenti e gli approfondimenti siano ancora in corso l'Autorità, che ha proceduto anche ad un sopralluogo, ha potuto registrare la disponibilità dei ricercatori a collaborare e a fornire ogni utile elemento di valutazione.

Occorre infine ricordare che nel giugno 2000 il Garante, in collaborazione con il Comitato nazionale per la bioetica e Legambiente, ha promosso un convegno sul tema "I nostri dati genetici: opportunità, rischi e diritti".

In tale occasione, sulla base di uno studio presentato da Legambiente dal quale è emerso che oltre 50 siti Internet, quasi tutti statunitensi, vendono *on-line* kit "fai da te" per test genetici, tutti i relatori hanno espresso forte preoccupazione per il diffondersi del fenomeno anche nel nostro Paese, dove peraltro negli ultimi anni i test genetici sono aumentati del 99,7%.

In relazione a ciò sono stati sottolineati i rischi connessi all'effettuazione di analisi genetiche indipendentemente dall'intermediazione di medici e specialisti e, quindi, l'importanza della consulenza genetica; la necessità di avviare controlli di qualità sui laboratori di analisi, di stabilire regole per la ricerca e, infine, di scongiurare il pericolo di una commercializzazione anche internazionale di informazioni genetiche. A tale proposito il Presidente di questa Autorità ha rammentato che la normativa in materia di protezione dei dati personali prevede che le informazioni possano essere trasferite solo in Paesi che assicurino un adeguato livello di protezione e che comunque i dati genetici non fanno parte dell'accordo "*Safe Harbor*".

23. Ricerca medica

I riferimenti normativi per il trattamento dei dati sulla salute finalizzati a scopi di ricerca medica ed epidemiologica sono rimasti sostanzialmente immutati: da un lato, la semplificazione introdotta dall'art. 5 del d.lg. n. 282/1999 secondo cui il trattamento può essere effettuato senza il consenso dell'interessato qualora "*la ricerca sia prevista da un'espressa previsione di legge o rientri nel programma di ricerca biomedica o sanitaria di cui all'articolo 12-bis del d.lg. 30 dicembre 1992, n. 502*"; dall'altro, nelle more di eventuali modificazioni conseguenti all'adozione del regolamento del Ministro della sanità di cui si è fatto cenno al paragrafo 17, le prescrizioni contenute e richiamate nel capo 1.2 dell'autorizzazione n. 2/2000 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale.

A queste disposizioni il Garante ha fatto pertanto riferimento nel provvedimento del 18 maggio 2000 (in *Bollettino* n. 13, p. 32), in risposta ad una azienda ospedaliera che chiedeva di verificare la possibilità, per alcune aziende farmaceutiche che sponsorizzano la sperimentazione di farmaci, di accedere alle cartelle cliniche dei pazienti. In particolare l'Autorità ha ricordato che il consenso dei pazienti interessati è sempre necessario, salvo che la ricerca sia svolta al fine di tutelare l'incolumità fisica degli stessi ovvero ricorrano le condizioni previste dall'art. 5 del d.lg. n. 282 sopra richiamato.

Deve rammentarsi inoltre che, per la ricerca medica ed epidemiologica, il quadro normativo dovrà essere integrato dalle disposizioni dei codici di deontologia e buona condotta, il cui rispetto "è condizione essenziale per la liceità del trattamento dei dati".

Sarà infine opportuno un coordinamento con le norme riguardanti la ricerca medica ed epidemiologica contenute nei codici dei deontologia per le attività statistiche e di ricerca scientifica.

24. Tessera sanitaria

Anche in quest'ambito è intervenuto il legislatore delegato, colmando la lacuna esistente nelle disposizioni che disciplinavano l'introduzione della carta sanitaria elettronica (art. 59, comma 50, lett. i) l. n. 449/1997 e d.l. n. 450/1998 convertito, con modificazioni, dalla l. n. 39/1999).

Tali disposizioni infatti, come più volte sottolineato da questa Autorità in diversi pareri espressi nell'esercizio della funzione consultiva (art. 31, comma 2, l. n. 675), non prevedevano alcun quadro di garanzie a tutela della riservatezza dei cittadini interessati.

L'art. 6 del d.lg. n. 282/1999 ha quindi fissato alcuni principi fondamentali in materia di protezione dei dati sanitari, stabilendo alcune limitazioni all'inserimento dei dati nella carta sanitaria elettronica e prevedendo garanzie per la sua corretta utilizzazione.

Successivamente questa Autorità, nel parere reso al Ministero dell'Interno il 12 luglio 2000 sullo schema di decreto ministeriale concernente le regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici, ha rappresentato il rischio di una proliferazione di più documenti elettronici contenenti dati sanitari e di una possibile sovrapposizione con la disciplina delle carte sanitarie elettroniche.

È quindi intervenuta la legge finanziaria 2001 (l. 23 dicembre 2000, n. 388) che ha previsto l'abrogazione delle disposizioni sopracitate delle leggi n. 449/1997 e n. 39/1999 e l'inserimento dei dati sanitari nel "documento d'identità elettronico" (*Provv.* del 7 settembre 2000).

25. AIDS

È noto che l'entrata in vigore della normativa in materia di protezione dei dati personali non ha abrogato le previgenti disposizioni di legge che tutelavano in modo specifico e più rigoroso la riservatezza e la dignità delle persone. Tra queste, in particolare, il legislatore ha espressamente fatto salve, in quanto compatibili, quelle contenute nella legge 5 giugno 1990, n. 135, in materia di Aids (art. 43, comma 2, l. n. 675).

In più occasioni tuttavia, come già evidenziato nelle precedenti relazioni annuali, l'Autorità è stata chiamata ad esprimersi su questioni relative al rapporto tra le disposizioni della legge n. 675 e quelle della normativa in materia di prevenzione e lotta contro l'Aids.

Ancora recentemente, con nota dell'8 febbraio 2001 (in *Bollettino* n. 17, p. 5), l'Autorità ha chiarito che le garanzie di riservatezza previste dalla legge sull'Aids si applicano anche in caso di richiesta di accesso da parte di consiglieri comunali agli atti e ai documenti in possesso di enti locali. Nel provvedimento il Garante ha aggiunto che le medesime garanzie devono essere rispettate quando il trattamento riguardi altre informazioni (tossicodipendenza o malattie mentali) per le quali l'ordinamento prevede un particolare regime di tutela.

Esprimendo preoccupazione per l'inadeguata sensibilità prestata nei confronti della riservatezza e della dignità delle persone offese, l'Autorità si è poi rivolta, come già accennato in un precedente paragrafo, al Ministro della giustizia in occasione della pubblicazione sul sito Internet del Tribunale di Trento di un avviso relativo all'udienza preliminare di un complesso procedimento penale per somministrazione di emoderivati infetti.

In tale nota il Garante ha rammentato la necessità di integrare con urgenza le norme processuali attualmente vigenti; ciò al fine di consentire che persone danneggiate a seguito di emotrasfusioni possano esercitare con piena tranquillità il diritto di difesa e non siano piuttosto indotte a rinunciarvi per evitare ulteriori danni legati ad un'ampia conoscenza della propria condizione di salute.

L'intervento dell'Autorità si è reso infine necessario quando sulla stampa sono state riportate notizie relative alla messa in atto, da parte di alcune strutture sanitarie, di sistemi di sorveglianza delle infezioni Hiv che comportavano l'archiviazione dei dati personali dei soggetti sieropositivi o affetti da Aids.

Il Garante, che ha inviato immediatamente richieste di informazioni alle strutture interessate, sta tuttora svolgendo una serie di approfondimenti sulla conformità dei suddetti sistemi alla specifica disciplina in materia di Aids e di sorveglianza epidemiologica, sulle precise finalità perseguite, sulle modalità di trattamento utilizzate per i flussi di dati e per la conservazione dei dati stessi (anche per ciò che riguarda la sicurezza), sui diritti delle persone interessate e sulle modalità di informazione delle stesse.

LAVORO E PREVIDENZA SOCIALE

26 LA PROTEZIONE DEI DATI NEL RAPPORTO DI LAVORO

Anche nel corso dell'anno 2000, vivo è stato l'interesse del Garante nei confronti delle esigenze di protezione dei dati personali nel settore del lavoro, sia pubblico, sia privato.

Oltre ad aver rinnovato per il periodo 1° ottobre 2000–31 dicembre 2001 le autorizzazioni generali rilasciate negli anni precedenti, rivelatesi strumento idoneo non solo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, ma anche per semplificare gli adempimenti che la legge n. 675/1996 pone a carico di determinate categorie di titolari (tra cui, con specifico riferimento al settore che qui interessa, i datori di lavoro in relazione al trattamento dei dati sensibili e dei dati a carattere giudiziario), il Garante è stato chiamato a pronunciarsi su specifiche problematiche, tra cui quella della conoscibilità delle note di qualifica.

In particolare, il Garante, sviluppando temi e principi già affermati in precedenti occasioni, nel ribadire che la previsione di cui all'art. 13, comma 1, lett. c), n. 1 della legge n. 675/1996 attribuisce a ciascun interessato – e quindi a ciascun lavoratore – il diritto di accedere ai propri dati personali, senza però che ciò possa tramutarsi in un diritto al rilascio di copia integrale degli atti o di altri documenti contenenti tali dati (soltanto ove l'estrazione dei dati personali dai documenti e la conseguente trasposizione su supporto cartaceo o informatico risulti particolarmente difficoltosa, allora l'adempimento alla richiesta di accesso può avvenire anche tramite la modalità dell'esibizione e/o della consegna in copia della documentazione, come già precisato da questa Autorità in tema di diritto d'accesso alle perizie medico-legali nel settore assicurativo e, da ultimo, in materia di lavoro, con *Provv.* del 28 dicembre 2000), ha altresì affermato che, ai sensi dell'art. 13 della legge n. 675/1996 e dell'art. 17 d.P.R. n. 501/1998, il datore di lavoro, quale titolare del trattamento, è tenuto a comunicare al lavoratore i dati relativi alla sua persona in forma completa, "mettendo in chiaro" tutte le informazioni personali comunque collegate al rapporto di lavoro o allo stato giuridico ed economico del dipendente, compresi quelli relativi allo sviluppo di carriera, alla rilevazione delle presenze, alle domande di ferie, ai turni di servizio, alla copia dei ruoli paga, ai certificati di malattia, ai moduli di autorizzazione alle missioni", nonché le informazioni riportate in eventuali progetti formativi (in tal senso, vedi *Provv.* del 17 ottobre 2000). In tale occasione, inoltre, il Garante, a fronte di specifica richiesta, ha avuto modo di chiarire che, tra le pretese azionabili dal lavoratore ex art. 13 legge n. 675/1996, non rientra quella volta a conoscere il nominativo degli eventuali "incaricati" del trattamento dei dati personali, sicché la relativa richiesta deve ritenersi inammissibile.

Sempre in tale ottica, inoltre, va considerato anche il provvedimento adottato il 28 giugno 2000, con il quale il Garante, in consapevole difformità con l'interpretazione fornita dal Tribunale di Fermo con decreto del 26 ottobre 1999, ha ribadito il diritto del lavoratore ad essere posto a conoscenza di tutti i "fattori valutativi" impiegati dal datore di lavoro ai fini della formulazione del giudizio complessivo finale contenuto nelle note di qualifica annuali. Va sottolineato che il caso in questione è identico ad altra precedente fattispecie, nella quale il giudice di merito, adìto da un istituto di credito ex art. 29, comma 6, legge n. 675/1996 (in sede di opposizione avverso una precedente pronunzia del Garante, di tenore analogo a quella oggetto di trattazione), ha affermato che "forma dato personale la valutazione finale del dipendente attribuita dall'amministrazione, ma non le operazioni effettuate al fine di giungere alla valutazione complessiva finale ...".

Al contrario, il Garante, nel ribadire che l'art. 1, comma 2, lett. c), legge n. 675/1996 definisce espressamente dato personale "qualunque informazione relativa a persona fisica, persona giuridica ...", ha affermato che si deve ricomprendere in tale ampia accezione "ogni notizia, informazione od elemento che abbia comunque un'efficacia informativa tale da fornire un contributo di conoscenza rispetto ad un soggetto identificato o identificabile" (principio, questo, già manifestato dall'Autorità in tema di giudizi espressi su docenti e sull'efficacia didattica di determinati corsi, in materia di giudizi su profili della personalità dell'interessato relativamente a test psico-attitudinali, nonché in tema di riscontri diagnostici di tipo medico e, segnatamente, di valutazioni medico-legali), sicché ad ogni elemento valutativo non potrebbe disconoscersi la natura di dato personale; e ciò "a prescindere dal loro successivo confluire nella qualifica sintetica annuale di cui costituiscono presupposti e articolazioni dotati, però, di autonomo significato", e come tali suscettibili di eventuali richieste d'integrazione ex art. 13 della legge n.

675/1996. Ulteriore conferma di tale impostazione, poi, può rinvenirsi nel provvedimento del 19 giugno 2000, con il quale il Garante ha ordinato ad una società di porre a disposizione di un suo ex dipendente gli attestati di qualificazione professionale conseguiti durante il pregresso rapporto lavorativo.

In ogni caso, trattasi di questione giuridica di enorme rilevanza, rispetto alla quale risulteranno di particolare interesse le future valutazioni della Suprema Corte di cassazione, già adita dai lavoratori interessati, che si spera possano tenere presente anche la Risoluzione adottata il 22 marzo 2001 dal Gruppo dei garanti europei, che ha riconosciuto a Bruxelles, appunto, la natura di "dato personale" delle predette valutazioni.

Infine, sempre in tema di "note di qualifica", è opportuno segnalare anche il provvedimento adottato in data 6 febbraio 2001, con il quale il Garante ha avuto modo di chiarire che il diritto del lavoratore (ex art. 13 legge n. 675/1996) ad accedere alle note di qualifica ed ai giudizi può essere esercitato soltanto in relazione ai propri dati personali, e non con riferimento ai dati contenuti in note di qualifica o, comunque, in giudizi relativi ai colleghi di lavoro, a meno che l'istante non sia munito di una delega o di una procura *ad hoc*, all'uopo rilasciatagli dall'interessato.

Analogamente, con riferimento al diritto del lavoratore ad accedere anche ai dati di tipo valutativo e, corrispondentemente, all'obbligo del datore di lavoro di porre a disposizione dell'interessato, "in chiaro", tutte le informazioni personali oggetto di trattamento, meritano di essere richiamati anche i provvedimenti adottati dal Garante in data 9 ottobre 2000, 12 dicembre 2000 e 7 marzo 2001, che si pongono nel già richiamato solco interpretativo.

27. SISTEMI INFORMATIVI E CONTROLLO A DISTANZA DEL PERSONALE

Altro profilo che assume particolare importanza nel settore del lavoro è quello del c.d. controllo a distanza dei lavoratori, il quale risulta strettamente connesso alla più ampia tematica della videosorveglianza.

In proposito, occorre premettere che in materia trova già applicazione l'art. 4 della legge n. 300/1970 che, nel vietare "il controllo a distanza dell'attività dei lavoratori" (anche come mera possibilità di controllo ad insaputa del prestatore), disciplina distintamente le due ipotesi dell'impianto di apparecchiature finalizzate al controllo a distanza (primo comma) e di apparecchiature per fini produttivi, ma tali comunque da presentare la possibilità di fornire anche il controllo a distanza del dipendente (secondo comma). Mentre le apparecchiature di cui al primo comma sono vietate, data la loro "odiosità", il loro contrasto con i principi della Costituzione e gli stessi effetti che possono arrecare alla produttività, quelle di cui al secondo comma sono consentite a condizione che il datore di lavoro osservi quanto tassativamente previsto nello stesso secondo comma ed, eventualmente, dai successivi.

Il Garante, chiamato nuovamente ad occuparsi della questione, ha anzitutto rammentato che la direttiva comunitaria n. 95/46/CE e la Convenzione n. 108/1981 del Consiglio d'Europa rendono obbligatoria l'applicazione della disciplina sul trattamento dei dati personali anche ai suoni ed alle immagini (quali quelle registrate nei controlli video), qualora permettano di identificare un soggetto anche in via indiretta, evidenziando che la legge n. 675/1996, attuativa della citata Convenzione, ha considerato quale "dato personale" qualunque informazione che permetta l'identificazione, anche in via indiretta, dei soggetti interessati, ivi compresi i suoni e le immagini (art. 1, comma 1, lett. c)).

L'Autorità ha proseguito l'analisi di una problematica già lungamente affrontata nel corso del 1999 e che è bene richiamare anche in questa Relazione. Chiamata infatti ad esprimere un parere in relazione ad un impianto di video-sorveglianza da installare sui mezzi di trasporto di un'azienda comunale, diretto a garantire la sicurezza dei viaggiatori, a prevenire reati ed atti di vandalismo alle fermate, l'Autorità aveva infatti sottolineato la necessità che tali sistemi fossero attivati in presenza di un articolato quadro di garanzie. In particolare, il Garante, nel richiamare i fondamentali divieti sanciti dall'art. 4 della legge n. 300/1970 (con specifico riferimento all'eventuale stabile ripresa della posizione di guida degli autisti), aveva sollecitato il richiedente a determinare la localizzazione delle telecamere e le modalità di ripresa televisiva in aderenza con le finalità sottese all'installazione del sistema stesso, tenendo conto dei principi fissati dall'art. 9 della legge n. 675/1996 in tema di pertinenza e non eccedenza dei dati: di conseguenza, aveva auspicato una predisposizione di modalità di ripresa tali da consentire una visione puramente panoramica dell'interno delle vetture o dell'ambito

della fermata, dovendosi ritenere inibite riprese più particolareggiate, atte a realizzare un'intrusione nella riservatezza delle persone, ovvero una visione di particolari irrilevanti. Inoltre, stante la stretta connessione tra l'eventuale visione "in chiaro" delle immagini (originariamente registrate solo in modo codificato) e la commissione di atti criminosi denunciati all'autorità di polizia, il Garante aveva altresì sollecitato l'installazione di un modulo di accesso ai computer della c.d. "stazione di lettura" secondo un sistema di "doppia chiave" congiunta (una in possesso dell'azienda e l'altra in possesso delle forze dell'ordine), con predeterminazione, tra l'altro, di idonee misure di sicurezza per la salvaguardia dei dati.

Negli ultimi tempi, il problema del controllo a distanza sul luogo di lavoro è tornato all'attenzione del Garante – come pure di altri Paesi e di molte altre autorità di garanzia straniere- in relazione agli accessi alle reti telematiche da parte del personale e all'uso della posta elettronica.

L'Autorità ha già avviato specifici accertamenti richiedendo, sia a società distributrici di appositi software, sia ad aziende risultate utilizzatrici dello stesso, tutte le informazioni utili per una piena valutazione delle caratteristiche del *software* e delle opzioni da esso consentite, nonché delle concrete forme di utilizzazione con specifico riguardo alle modalità di informativa verso i dipendenti, all'istituto del consenso, all'eventuale consultazione delle rappresentanze sindacali aziendali, alle finalità perseguite ed alla conservazione dei dati relativi agli accessi ai siti.

Il Garante si riserva di adottare a breve termine un provvedimento di carattere generale in riferimento ai diversi aspetti emersi nei vari procedimenti, tenendo presenti le nuove implicazioni che la legge n. 675/1996 pone per quanto riguarda l'informativa ai lavoratori interessati, il principio di proporzionalità nel trattamento dei dati, la trasparenza dei controlli e i limiti entro i quali essi sono consentiti, ed eventuali suggerimenti operativi che potranno essere formulati per bilanciare i diritti e le libertà fondamentali degli interessati con le esigenze connesse alla prestazione lavorativa e all'osservanza degli obblighi del rapporto di lavoro.

Il Garante terrà anche conto, a questo riguardo, degli approfondimenti in atto su scala europea, anche alla luce delle prime quattro iniziative intraprese in altri Paesi da altre autorità di garanzia in materia di protezione dei dati, dei risultati dell'apposito Gruppo di lavoro costituito dalle quindici autorità garanti, nonché delle prime riflessioni che l'Autorità italiana ha formulato nel corso della recente Conferenza europea di Atene del 10-11 maggio 2001.

28. Il Sistema informazione lavoro

Nell'ambito dell'attività consultiva (art. 31, comma 2, legge n. 675/1996), il Garante ha avuto modo di proseguire gli approfondimenti relativi ai sistemi informativi in materia di lavoro.

Già in passato l'Autorità aveva espresso un parere in relazione allo schema di regolamento concernente, nell'ambito della delegificazione della materia, il riordino di alcune procedure per il collocamento pubblico; tale regolamento, infatti, avrebbe lo scopo di facilitare l'incontro della domanda e dell'offerta di lavoro nel rispetto della competenza delle Regioni (art. 1 legge 15 marzo 1997, n. 59), attraverso un'efficace attivazione sul territorio nazionale del Sistema informativo lavoro (Sil).

È opportuno richiamare quanto già riportato nella Relazione per l'anno 1999 circa la necessità di chiarire, in via generale, il complessivo rapporto tra flussi di dati previsti e l'organizzazione del SIL, trattandosi di un sistema che, per espressa previsione di legge, dev'essere improntato ai principi di cui alla legge n. 675/1996 (vedi art. 11, comma 1, d.lg. 469/1997).

Analogamente, sono state ribadite le perplessità già sollevate in relazione sia all'istituzione di una "scheda professionale" del lavoratore (non essendo ancora chiara non solo la funzione di tale scheda, ma anche le connesse modalità di trattamento dei dati in essa riportati), sia all'autonomo rilascio, su base regionale, di una "carta elettronica personale" del lavoratore, soprattutto in assenza di un primo quadro normativo d'insieme che poteva essere meglio armonizzato con la recente disciplina della carta d'identità elettronica.

Con provvedimento del 24 aprile 2001, il Garante ha nuovamente ribadito principi analoghi esprimendo il parere su due schemi di decreti ministeriali attuativi del regolamento di semplificazione della disciplina per il collocamento ordinario dei lavoratori con d.P.R. 7 luglio 2000, n. 442. L'Autorità ha

anzitutto evidenziato il mancato recepimento – con il d.P.R. n. 442/2000 - di varie considerazioni formulate con il parere del 30 novembre 1999, in particolare per quanto riguarda il rapporto tra i flussi di dati personali previsti e la peculiare organizzazione del Sil, e la delimitazione degli obblighi di verifica dell'esattezza e della pertinenza delle informazioni, anche in termini di uniformità di disciplina sull'accesso da parte di regioni ed enti locali. Altre osservazioni hanno riguardato la titolarità del trattamento dei dati relativi all'elenco anagrafico delle persone in cerca di lavoro e, sotto altro profilo, alcuni aspetti dello schema di decreto concernente la scheda professionale.

29. CARTELLINI IDENTIFICATIVI

Infine, particolare rilievo merita il provvedimento dell'11 dicembre 2000, con il quale il Garante, sollecitato da molte richieste di parere avanzate da pubbliche amministrazioni, aziende sanitarie, compagnie aeree, aziende di trasporto, servizi di ristorazione e singoli lavoratori, ha affrontato il problema dei c.d. cartellini identificativi.

Alcune norme contrattuali o disposizioni organizzative, in vigore sia nel settore pubblico, sia in quello privato, prevedono che il personale a contatto con il pubblico appunti sull'abito o sulla divisa di lavoro un cartellino identificativo, contenente vari dati personali del dipendente: trattasi di norme aventi lo scopo di migliorare il rapporto tra operatori (pubblici o privati) ed utenti dei servizi o clienti degli esercizi commerciali, comportando una maggiore responsabilizzazione del personale ed una più agevole possibilità di tutela dei terzi.

Però, poiché tale esposizione al pubblico di alcuni dati personali degli interessati risulta anche idonea a determinare un'agevole identificazione dell'operatore che, di fatto, può divenire anche destinatario di improprie pressioni da parte di terzi o di successivi contatti anche per ragioni estranee all'attività lavorativa, il Garante, nel riportarsi ai principi di pertinenza e non eccedenza dei dati rispetto alla finalità perseguita attraverso il trattamento (art. 9 l. n. 675/1996), ha ribadito che la limitazione della riservatezza, anche se collegata al perseguimento di una legittima finalità, dev'essere comunque ridotta al minimo indispensabile. Pertanto, la diffusione dei dati personali dei dipendenti attraverso l'imposizione dei cartellini identificativi può trovare giustificazione, nel settore privato, soltanto in caso di adempimento di un obbligo previsto da una legge, da un regolamento o dalla normativa comunitaria (art. 20 l. n. 675/1996), mentre nel settore pubblico ciò è possibile solo ove sia previsto da norme di legge o di regolamento (art. 27, commi 3 e 4).

Nell'ambito del lavoro privato, l'obbligo dell'apposizione del cartellino identificativo trova fondamento in alcune prescrizioni contenute in accordi sindacali aziendali o in regolamenti aziendali, che hanno esplicito riguardo o a finalità interne all'azienda (controlli sulle entrate e le uscite dall'azienda, riconoscimento del personale, accesso ad aree riservate) ovvero ad altre concernenti i rapporti con gli utenti o con i clienti. Pertanto, proprio con specifico riguardo a quest'ultima finalità, il Garante ha ritenuto che non presenti alcuna utilità l'evidenziazione sul cartellino dei dati dei dipendenti concernenti le generalità o gli estremi anagrafici, mentre risulta senz'altro utile ai terzi che entrino in contatto con il personale la conoscibilità dell'immagine fotografica dell'interlocutore, l'indicazione del ruolo professionale, nonché il nome ed il numero (o la sigla) identificativi.

Analoghe considerazioni, inoltre, valgono anche per il settore pubblico. Infatti, anche ove siano stati emanati atti amministrativi d'organizzazione che prevedano l'adozione, da parte del personale, di cartellini identificativi, la limitazione della riservatezza dei dipendenti dovrà sempre avvenire nel rispetto dei principi di pertinenza e non eccedenza, soprattutto laddove non sussistano precise disposizioni di legge o di regolamento che prescrivano puntualmente il contenuto di detti cartellini.

STATISTICA, RICERCA SCIENTIFICA E RICERCA STORICA

30. STATISTICA E RICERCA SCIENTIFICA

Con il provvedimento pubblicato nella G.U. n. 46 del 25 febbraio 2000 (in *Bollettino* n. 11/12, p. 115), l'Autorità ha promosso la sottoscrizione di codici deontologici e di buona condotta relativi al trattamento di dati personali utilizzati in vari settori di rilevante interesse generale tra cui la statistica e la ricerca scientifica. Tali codici rivestono un particolare rilievo giuridico poiché il loro rispetto diviene *"condizione essenziale per la liceità del trattamento dei dati"* (art. 6, comma 2, d.lg. n. 281/1999). Così come previsto dal provvedimento del Garante, i soggetti pubblici e privati maggiormente rappresentativi ed interessati a questo tipo di trattamenti (comprese le società scientifiche e le associazioni professionali), hanno partecipato nel corso dell'anno 2000 all'elaborazione dei codici deontologici che nei suddetti settori sono giunti ad una fase molto avanzata e sono oramai prossimi all'emanazione.

Il Garante, inoltre, ha affrontato la tematica della statistica e della ricerca scientifica in vari provvedimenti, rispondendo a quesiti o fornendo i prescritti pareri in ordine agli atti suscettibili di incidere sulla materia della protezione dei dati personali.

In tal senso il Garante ha espresso parere favorevole allo schema di regolamento governativo che stabilisce i criteri e le procedure per l'individuazione dei soggetti privati che partecipano al Sistema statistico nazionale (Sistan), nell'ambito del quale opera l'Istat insieme ad altri organismi pubblici impegnati nell'attuazione del Programma statistico nazionale.

Nel parere, fornito su richiesta dalla Presidenza del Consiglio dei ministri-Dipartimento della funzione pubblica, l'Autorità ha richiamato l'attenzione del Governo sull'esigenza di rafforzare ulteriormente le misure di tutela della *privacy* presenti nello schema di regolamento, e ciò anche attraverso un esplicito richiamo alle disposizioni del d.lg. n. 281/1999 riguardante il trattamento dei dati personali a scopo di ricerca storica, statistica e scientifica.

Con un parere fornito poi su richiesta del Ministero della sanità, in merito allo schema di decreto ministeriale che modifica il contenuto e la struttura del certificato di assistenza al parto ai fini delle rilevazioni statistiche sulle nascite, sulla mortalità infantile e sui nati affetti da malformazioni (parere del 10 aprile 2000, in *Bollettino* n. 11/12, p. 34), il Garante – come già riferito in altra parte della presente Relazione – ha chiarito che il trattamento dei dati personali contenuti nei nuovi certificati dovrà avvenire in modo tale da garantire la riservatezza delle informazioni più delicate come quelle riguardanti le interruzioni di gravidanza e l'anonimato delle madri che non consentono di essere nominate. L'Autorità ha, quindi, rilevato che il provvedimento risultava carente di apposite previsioni volte a garantire l'anonimato e la riservatezza delle informazioni che saranno inserite nel certificato. A tale riguardo il Garante ha chiesto al Ministero della sanità di inserire nel decreto misure che consentano di evitare l'identificazione, anche indiretta, della donna che ha partorito attraverso il collegamento tra i suoi dati personali e le altre informazioni contenute nel certificato di parto. I dati anagrafici dovranno, pertanto, essere conservati separatamente da quelli sensibili che possono rilevare a fini di ricerca statistica, come ad esempio le indagini sul numero delle interruzioni volontarie di gravidanza. L'Autorità ha inoltre sollecitato l'amministrazione ad integrare lo schema di decreto con una norma che estenda anche alle regioni l'obbligo di eliminare gli elementi identificativi diretti dai certificati di assistenza al parto che vengono trasmessi ogni sei mesi al Ministero della sanità e successivamente comunicati all'Istituto nazionale di statistica.

Il Garante, in un parere fornito su richiesta dell'Istat in merito allo schema di regolamento predisposto per disciplinare il quinto censimento generale dell'agricoltura (parere del 28 marzo 2000, in *Bollettino* n. 11/12, p. 71), ha inoltre rilevato che le modalità della raccolta non contrastano, in linea generale, con la disciplina sulla protezione dei dati personali ed ha suggerito all'Istat di modificare il regolamento al fine di garantire il trattamento delle informazioni soggette ad una speciale tutela. Nel corso della raccolta potrebbero, infatti, essere trattati anche dati sensibili riguardanti la libertà di opinione, come nel caso in cui l'azienda agricola censita aderisca ad un'associazione sindacale di categoria. In particolare, è stato chiesto di prevedere la possibilità di raccogliere le informazioni riguardanti le aziende iscritte direttamente dalle associazioni, subordinando la comunicazione dei dati sensibili al preventivo consenso scritto degli imprenditori agricoli.

L'Autorità, il 21 febbraio 2000 (in *Bollettino* n. 11/12, p. 70), ha fornito all'Istat il prescritto parere sul Programma statistico nazionale 2000-2002, ai sensi dell'art. 6-*bis*, comma 2, del d.lg. n. 322/1989, che prevede anche l'inserimento nel Programma delle finalità perseguite e delle garanzie previste, nonché i dati "*particolari*" da trattare, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento. In tale occasione l'Autorità, esprimendo parere favorevole al Programma, ha segnalato l'opportunità di una maggiore attenzione all'esplicitazione delle garanzie che l'ordinamento ha predisposto a tutela degli interessati, con particolare riferimento ai diritti di accesso e rettifica previsti dalla l. n. 675/1996.

In merito alla richiesta di parere avanzata dall'Istituto nazionale di statistica sullo schema di regolamento di esecuzione del 14° censimento della popolazione, del censimento generale delle abitazioni e dell'8° censimento dell'industria e dei servizi (parere del 14 marzo 2001, in *Bollettino* n. 18, p. 37), richiesto ai sensi dell'art. 37 della legge 17 maggio 1999, n. 144, il Garante ha rilevato la necessità di prevedere che gli organismi esterni, ed in particolare quelli privati cui verranno affidate fasi di rilevazione censuaria tramite convenzione o contratti, possiedano requisiti di esperienza, capacità ed affidabilità tali da fornire idonee garanzie del pieno rispetto delle istruzioni ricevute specie in materia di riservatezza e sicurezza dei trattamenti. Analoghi requisiti devono essere opportunamente richiesti ai rilevatori e ai coordinatori i quali dovranno assumere anche la necessaria qualifica di "*incaricati del trattamento*" ai sensi degli artt. 8 e 19 della l. n. 675/1996, essendo tenuti alla stretta osservanza delle istruzioni ricevute e soggetti alla vigilanza sul corretto svolgimento dei compiti loro assegnati, nonché al segreto d'ufficio.

L'Autorità si è anche espressa su un quesito posto in ordine alla possibilità che un istituto scolastico di istruzione secondaria possa consegnare ad un docente universitario, che li aveva richiesti al fine di effettuare una ricerca sui "destini sociali" dei diplomati stessi, gli elenchi delle persone diplomatesi nel corso di alcuni anni scolastici (parere del 1° febbraio 2000, in *Bollettino* n. 11/12, p. 47). In proposito il Garante ha osservato che l'art. 17 del d.lg. 30 luglio 1999 n. 281, che ha inserito il nuovo art. 330-*bis* nel d.lg. 16 aprile 1994 n. 297, concernente "*l'approvazione del testo unico delle disposizioni legislative in materia di istruzione, relative alle scuole di ogni ordine e grado*", specifica che i dati degli studenti, già diplomati alla data di entrata in vigore della medesima disposizione, "*possono essere comunicati o diffusi decorsi trenta giorni dalla notizia che le scuole e gli istituti scolastici, ovvero il Ministero della pubblica istruzione, rendono nota mediante annunci al pubblico*". Le finalità della ricerca condotta dall'Università si colloca tra le iniziative volte a favorire (anche con il contributo dell'indagine statistica) la formazione, l'aggiornamento e la riqualificazione degli studenti e dei lavoratori, finalità che rientrano, infatti, fra quelle prese in considerazione dal citato art. 17 del d.lg. n. 281. Il Garante ha infine sottolineato come il ricercatore, nel ricevere i dati, è tenuto all'osservanza di tutti gli obblighi fissati, in via generale, dalla legge n. 675 e più specificamente dal citato d.lg. n. 281, con particolare riguardo alle modalità di trattamento e alla conservazione dei dati, nonché all'adozione delle prescritte misure di sicurezza.

31. Ricerca storica e attività archivistiche

L'applicazione della normativa sui dati personali ai trattamenti effettuati per scopi storici ha avuto da sempre bisogno di un approccio particolare, conseguente all'esigenza di contemperare la tutela della riservatezza con l'attività di ricerca storica, che di per sé si pone in contrapposizione con il principio di conservazione temporanea del dato personale previsto dalla legge n. 675/1996.

Il legislatore comunitario, nei "considerando" nn. 29 e 40 e nell'art. 6 della direttiva 95/46/CE del 24 ottobre 1995, ha previsto – purché gli Stati membri forniscano garanzie appropriate- che il trattamento dei dati personali per scopi storici non è ritenuto incompatibile con le finalità per le quali i dati sono stati precedentemente raccolti, ed ha attenuato l'obbligo di fornire l'informativa alla persona interessata qualora ciò risulti impossibile o implichi uno sforzo eccessivo.

Il Governo, sulla base delle leggi-delega nn. 676/1996 e 344/1998, ha emanato il decreto legislativo 30 luglio 1999, n. 281 che ha innovato nel settore storico con disposizioni volte al bilanciamento delle diverse esigenze, sia attraverso modifiche alla legge n. 675/1996 (cfr., per esempio, art. 9, comma 1-*bis*), sia attraverso modifiche alla normativa previgente in materia archivistica (cfr. d.lg. 30 settembre 1963, n. 1409). Oltre ai cambiamenti relativi all'accesso alla documentazione contenente dati personali, il d.lg. 281/1999 ha previsto anche l'adozione di un importante codice deontologico per i trattamenti di dati personali per scopi storici, cui dovranno attenersi gli archivisti e gli utenti.

Tale codice, pubblicato a cura del Garante sulla *G.U.* n. 80 del 5 aprile 2001, è stato elaborato da un gruppo di lavoro composto da rappresentanti di soggetti pubblici e privati, società scientifiche ed associazioni professionali che operano nel settore della ricerca storica e degli archivi. Esso completa, integra e specifica la disciplina già introdotta con norma primaria dal d.lg. n. 281/1999. Si compone di tre parti rispettivamente dedicate ai principi generali, alle regole di condotta per gli archivisti e a quelle per gli utenti. Fra i principi generali è da sottolineare la necessità che l'utilizzazione di dati personali acquisiti nell'ambito della ricerca storica e dell'accesso ad atti e documenti si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

Le disposizioni del codice si riferiscono ai trattamenti effettuati in relazione ai documenti conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico. Gli archivi privati possono comunque comunicare alla competente sovrintendenza archivistica l'intenzione di applicare anch'essi le norme presenti nel codice.

Per quanto riguarda gli archivisti, il codice definisce regole di correttezza e di non discriminazione nei confronti di coloro che richiedano la consultazione di fonti storiche, e prevede che gli archivisti debbano tutelare l'integrità degli archivi e l'autenticità dei documenti - anche attraverso l'adozione di idonee misure di sicurezza - ed astenersi dal fare un uso personale delle informazioni di cui dispongano in ragione della propria attività, non disponibili agli utenti. Gli archivi che acquisiscono fonti orali sono tenuti a richiedere all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti e del consenso manifestato dagli interessati.

Per gli utenti, cioè per chiunque faccia ricerca storica, il codice individua cautele per la raccolta, l'utilizzazione e la diffusione dei dati contenuti nei documenti. Essi devono utilizzare i documenti conformandosi agli scopi perseguiti e delineati nel progetto di ricerca, sotto la propria responsabilità, nel rispetto dei principi di pertinenza ed indispensabilità di cui all'art. 7 del d.lg. n. 281/1999. Il principio del libero accesso agli archivi pubblici subisce talune eccezioni, introdotte con norme primarie, con riferimento ai documenti di carattere riservato relativi alla politica interna ed estera dello Stato (consultabili dopo cinquanta anni dalla loro data) e quelli che contengono dati sensibili e di carattere giudiziario (consultabili dopo quaranta anni). Il termine è di settanta anni se i dati sono relativi allo stato di salute o alla vita sessuale o a rapporti riservati di tipo familiare. Prima della scadenza dei termini è possibile consultare i documenti di cui sopra, con apposita autorizzazione rilasciata dal Ministro dell'interno, previo parere della Commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati, cui partecipa, fra gli altri, anche un rappresentante del Garante. È importante sottolineare che quando viene concessa l'autorizzazione alla consultazione in deroga ai limiti previsti, questa, a parità di condizioni, deve essere rilasciata ad ogni altro richiedente. Tale autorizzazione può contenere cautele volte a consentire la comunicazione dei dati senza ledere i diritti, le libertà e la dignità delle persone interessate, come l'obbligo di non diffondere i nomi o di utilizzare solo le iniziali, tenendo comunque sempre presente il principio di pertinenza. Infine, nella diffusione dei dati, gli utenti devono astenersi dal pubblicare dati analitici di interesse strettamente clinico o dal descrivere abitudini sessuali riferite ad una determinata persona. La sfera privata delle persone note o che abbiano esercitato funzioni pubbliche deve essere poi rispettata nel caso in cui le notizie o i dati non abbiano alcun rilievo sul loro ruolo o sulla loro vita pubblica.

In conclusione, sembra opportuno evidenziare che l'Ufficio del Garante, nel marzo del 2000, ha segnalato alla Presidenza del Consiglio e al Ministero per i beni e le attività culturali l'esigenza di aggiornare il testo unico in materia di beni culturali e ambientali. Il d.lg. 29 ottobre 1999, n. 490 (recante, appunto, il nuovo testo unico in materia), infatti, ha inserito nel medesimo t.u. le disposizioni legislative vigenti alla data del 31 ottobre 1998, abrogando diversi articoli del d.P.R. n. 1409/1963 tra cui gli artt. da 21 a 25, riformulati negli artt. 107 ss. del medesimo testo unico. Tale riformulazione però non ha tenuto conto delle modifiche ed integrazioni apportate al d.P.R. n. 1409/1963 (artt. 21 e 21-*bis*) dal d.lg. n. 281/1999. Al fine di evitare tale situazione di incertezza, l'Autorità ha pertanto chiesto un intervento normativo di adeguamento, peraltro già previsto dalla legge-delega n. 352/1997 entro tre anni dalla data della sua entrata in vigore.

ASSOCIAZIONI, MOVIMENTI POLITICI, PARTITI E CONFESSIONI RELIGIOSE

32. PROTEZIONE DEI DATI E REALTÀ ASSOCIATIVE

Il Garante è tornato a pronunciarsi (v. già *Provv.* 29 settembre 1999, in *Bollettino*, n. 10, p. 35), stabilendone l'illegittimità, in ordine all'utilizzo di dati (segnatamente, contenuti in elenchi) degli iscritti ad un'associazione, utilizzati per finalità diverse, nella specie di propaganda elettorale, da quelle indicate nell'informativa o comunque in presenza di un'informativa che, per genericità e indeterminatezza, non rende possibile individuare con sufficiente precisione la finalità del trattamento effettuato (*Provv.* 5 ottobre 1999; v. anche *Provv.* 9 ottobre 2000, in *Bollettino* n. 14/15, p. 17). In tale occasione l'Autorità ha potuto altresì precisare che anche le operazioni di stampa di etichette adesive dei nominativi personali e la loro apposizione su buste già predisposte da parte di soggetti terzi rispetto al titolare integrano gli estremi di una operazione di "comunicazione" di dati (v. ancora *Provv.* 9 ottobre 2000).

Più in generale, queste vicende (ed altre di seguito rappresentate) hanno indotto il Garante a ribadire in un c.d. "decalogo" (provvedimento 7 marzo 2001, in *Bollettino*, n. 18, p. 24) che, in caso di uso di dati di aderenti ad organizzazioni diverse da quelle politiche (ad es. associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politico-partitica), l'utilizzazione a fini di propaganda elettorale di dati relativi agli iscritti è possibile qualora detta eventualità venga espressamente prevista nell'informativa resa agli iscritti al momento dell'adesione o del rinnovo della stessa (e qualora gli organi dirigenti dell'associazione decidano, con loro autonoma determinazione, di prevedere una tale possibilità).

Il Garante ha avviato poi alcuni procedimenti in relazione all'improprio uso di dati per finalità di propaganda elettorale da parte di medici o di strutture sanitarie che disponevano di dati per finalità di cura.

33. L'USO DI DATI PER FINALITÀ POLITICO-ELETTORALI

Lo svolgimento delle consultazioni elettorali ha determinato ulteriori e significativi interventi dell'Autorità in materia di trattamento di dati personali, il cui contenuto può rinvenirsi, negli aspetti salienti, nel menzionato provvedimento del 7 marzo 2001, attraverso il quale il Garante ha ritenuto opportuno segnalare ai partiti e ai movimenti politici alcuni dei principi più significativi ai quali ispirare i trattamenti dei dati personali nel corso della campagna elettorale, per renderli armonici con la disciplina introdotta dalla l. n. 675/1996.

In questa cornice deve collocarsi il provvedimento del 7 febbraio 2001 (pubblicato in *G.U.* 13 febbraio 2001, n. 36 e in *Bollettino*, n. 17, p. 7) con il quale, in virtù del potere accordato al Garante dall'art. 10, comma 4, della legge n. 675/1996, si sono esonerati fino al 30 giugno 2001 partiti, movimenti politici, comitati promotori, sostenitori di liste e di candidati (come ogni altro soggetto intento anch'esso ad effettuare, in occasione delle consultazioni elettorali, operazioni di trattamento di dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, per esclusive finalità di comunicazione politica o di propaganda) dall'obbligo di rendere l'informativa prevista dall'art. 10, comma 3, l. n. 675/1996 all'interessato, lasciando sussistere detto obbligo nei casi di spedizione di messaggi di posta elettronica o di lettere articolate, assolvibile, in questi casi, con l'inserzione dell'informativa nella comunicazione medesima.

Variegate sono state poi le tipologie di modalità trasmissive utilizzate a fini di propaganda elettorale. Non sempre i dati personali sono stati attinti dalle fonti appena menzionate (o si è fatto ricorso al previo consenso espresso da parte dei cittadini). Invero, da un lato sono giunte al Garante segnalazioni in ordine all'invio, specie nel periodo elettorale, di messaggi propagandistici sulle utenze telefoniche mobili degli abbonati, fatti per i quali è attualmente in corso un'istruttoria da parte dell'Autorità; per

altro verso, forme di comunicazione politica sono state altresì realizzate ricorrendo alla messaggeria elettronica.

A quest'ultimo riguardo, e muovendo dalla considerazione che anche gli indirizzi di posta elettronica devono essere considerati dati personali ai fini dell'applicazione della legge n. 675/1996, si è accertata l'assenza dei presupposti di liceità e di correttezza nel loro trattamento che l'Associazione politica nazionale Lista Marco Pannella (*Provv.* 11 gennaio 2001, in *Bollettino*, n. 16, p. 39) ha operato reperendo sulla rete Internet, tramite un software appropriato, oltre 390.000 indirizzi di posta elettronica a scopo di successiva comunicazione politica.

In particolare si è rilevato che gli indirizzi di posta elettronica degli interessati non provengono da *"pubblici registri, elenchi, atti o documenti conoscibili da chiunque"* (art. 12, comma 1, lett. c), legge n. 675/1996) di tal che la loro utilizzazione nel caso in esame non era da ritenersi consentita (mancando una previa manifestazione positiva di consenso ed essendo altresì inoperanti gli ulteriori presupposti elencati nell'art. 12 della medesima legge).

La previsione contenuta nella citata lettera c) non si riferisce, infatti, a qualunque dato personale che sia *di fatto* consultabile da una pluralità di persone, ma ai soli dati personali desumibili da registri, elenchi, atti o documenti *"pubblici"* (quali ad esempio gli elenchi degli iscritti a vari albi e collegi professionali, taluni registri detenuti dalle camere di commercio e, soprattutto, le liste elettorali che chiunque, come precisato dall'art. 51 del d.P.R. 20 marzo 1967, n. 223, può visionare ed ottenere in copia presso i competenti uffici comunali) o sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque (si pensi ai dati ricavati dagli elenchi telefonici) (art. 20, comma 1, lett. b), legge n. 675/1996).

In senso analogo si era già pronunciato il Gruppo europeo delle autorità garanti per la protezione dei dati nel parere n. 1/2000 (adottato a Bruxelles il 3 febbraio 2001) in tema di reti e di commercio elettronico, secondo cui la mera rinvenibilità di un indirizzo *e-mail* in uno spazio pubblico di Internet non comporta un uso libero dell'indirizzo stesso per *mailing* elettronici.

Nel caso commentato, poi, il Garante ha altresì rilevato che, al di là del profilo appena trattato, l'Associazione politica nazionale Lista Marco Pannella non provvedeva, attraverso un servizio attivo ed efficace, alla cancellazione degli indirizzi di posta elettronica di coloro che, ricevute le comunicazioni a contenuto politico, ne facevano richiesta ai sensi dell'art. 13 della legge n. 675/1996.

Merita precisare, in ordine a detto provvedimento, che lo stesso è stato impugnato dalla menzionata associazione politica dinanzi al Tribunale di Roma. Il giudizio è in una fase introduttiva nella quale il giudice deve esprimersi anche sulla costituzione in giudizio di un'associazione di utenti e consumatori.

In altra sede, il Garante ha appurato l'infondatezza di una segnalazione relativa ad un trattamento di dati solo apparentemente effettuato dall'Osservatorio sulla legalità e la questione morale, pur evidenziando la necessità di perfezionare l'informativa e il modello di consenso presenti nel sito www.antoniodipietro.org (cfr. *Provv.* 11 gennaio 2001, in *Bollettino*, n. 16, p. 42).

In occasione di un quesito formulato dal Presidente del Tribunale di Napoli si è poi puntualizzato (v. lettera del 4 aprile 2001) che, diversamente dalle liste elettorali generali e sezionali (contenenti i nominativi degli elettori aventi diritto al voto), tenute presso i competenti uffici comunali e la cui conoscibilità è sancita dal menzionato art. 51 d.P.R. n. 223/1967, gli esemplari delle liste elettorali di sezione sulle quali, nei singoli seggi, sono stati annotati in occasione di precedenti elezioni i dati relativi ai cittadini che hanno votato, sono utilizzabili al solo fine del controllo sulla regolarità delle operazioni elettorali, nei termini stabiliti dall'art. 62 del d.P.R. 16 maggio 1960, n. 570 (recante il testo unico delle leggi per la composizione e la elezione degli organi delle amministrazioni comunali), applicabile anche con riferimento alle elezioni regionali ai sensi dell'art. 1, comma 5, della legge 17 febbraio 1968, n. 108, con conseguente insussistenza del diritto d'accesso a favore dei titolari di cariche elettive che chiedano al Tribunale di accedervi per ipotizzati fini di espletamento del proprio mandato o per finalità di propaganda elettorale.

Conclusivamente, devono essere ricordate anche in questo paragrafo le riserve espresse dal Garante (v., da ultimo, il comunicato stampa del 24 aprile 2001), e già precedentemente formulate nel novembre 1999 al Ministero dell'interno in occasione del parere reso sullo schema di regolamento sulla tessera elettorale, per quanto riguarda la *privacy*, la libertà e la segretezza del voto. Il nuovo modello – cartaceo- di tessera elettorale, rendendo nota una sequenza di informazioni relativi a diverse consultazioni elettorali precedenti, potrebbe esporre il cittadino al rischio che la scelta di partecipare o meno alla consultazione elettorale sia facilmente conoscibile anche fuori della sezione elettorale, consentendo altresì di dedurne sostanzialmente l'orientamento politico, con conseguente violazione della segretezza del voto.

Alcune consultazioni elettorali, infatti, possono assumere particolare significato per l'oggetto (si pensi a determinati referendum o a votazioni di ballottaggio) o per il contesto in cui cadono (alcune forze politiche possono esprimere specifici orientamenti invitando gli elettori al voto o all'astensione), tanto che anche il solo dato dell'avvenuta partecipazione alle operazioni di voto può risultare idoneo a svelarne le preferenze politiche. Di qui la ragione di una nuova nota, inviata dal Garante al Ministro dell'interno, con l'auspicio di un riesame urgente dell'intera tematica.

34. CONDOMINI E SOCIETÀ

In relazione al trattamento dei dati personali in ambito condominiale il Garante (*Provv.* 19 maggio 2000, in *Bollettino*, n. 13, p. 7) ha osservato che, ai fini della normativa contenuta nella l. n. 675/1996, possono formare oggetto di trattamento i dati personali raccolti ed utilizzati per il conseguimento delle finalità riconducibili agli artt. 1117 e ss. del codice civile, dei quali l'amministratore ha la diretta gestione e del cui trattamento i condomini devono essere considerati contitolari.

Muovendo da questo assunto, si è altresì evidenziato che la legge n. 675/1996 non ha modificato la normativa relativa al condominio degli edifici, segnatamente in relazione alle norme dettate in materia di costituzione dell'assemblea e di validità delle deliberazioni (artt. 1136 ss. cod. civ.). Pertanto devono potersi individuare con esattezza i nominativi dei condomini (ad es. anche tramite la previa esibizione di copia o estratti degli atti notarili), trattandosi di dato indispensabile ai fini della regolare convocazione assembleare, nonché per la verifica della validità delle stesse deliberazioni. Le modalità per procedere a dette verifiche possono essere stabilite anche attraverso il regolamento di condominio, nella piena osservanza, però, dei principi di pertinenza e non eccedenza sanciti dall'art. 9 della legge n. 675/1996. In tal modo è consentito procedere all'accertamento dei soli dati realmente necessari a verificare gli elementi idonei a individuare la titolarità dei singoli soggetti a partecipare all'assemblea e l'ammontare delle singole quote rappresentate (tali non sono, ad es., salvo il consenso degli interessati, i numeri telefonici dei singoli condomini o dei loro familiari).

Del pari è risultato lecito, in termini generali, il trattamento di dati personali attinenti alla situazione debitoria dei soggetti appartenenti ad un consorzio, in quanto funzionale all'adempimento degli obblighi derivanti dall'adesione al consorzio medesimo. Tuttavia, come messo in luce in un provvedimento del 7 dicembre 2000 (conseguente allo svolgimento di ulteriori accertamenti disposti con provvedimento del 18 maggio 2000), detti dati devono essere trattati sulla base di un'idonea informativa (assente nel caso di specie), anche orale, volta a rappresentare tutti gli elementi contenuti nell'art. 10 della legge n. 675/1996, ed in particolare le modalità del trattamento, inclusa l'eventuale comunicazione o diffusione dei dati personali dei consorziati. Dagli accertamenti svolti, inoltre, è stato possibile rilevare che, in assenza di previsioni statutarie, le posizioni debitorie dei consorziati erano affisse in una bacheca di fatto accessibile a chiunque anziché ai soli interessati afferenti al consorzio, integrandosi da questo punto di vista una illecita diffusione di dati personali.

Il Garante ha altresì precisato (*Provv.* 19 dicembre 2000 e, nello stesso senso, nota del 12 gennaio 2001) che la l. n. 675/1996 è compatibile con la disciplina contenuta nel codice civile in materia di documentazione societaria (artt. 2421, 2422, 2490 e 2516 c.c.), di tal che non viene pregiudicato il diritto del socio ad acquisire (in conformità a quanto previsto da leggi, regolamenti o normative comunitarie in materia societaria) dati, notizie e documenti inerenti all'attività sociale: in particolare il socio può accedere, indipendentemente dal consenso dell'interessato, a dati e documenti riportati nei libri, dovendo la società adempiere ad un obbligo normativo (art. 20, comma 1, lett. c), l. n. 675/1996). Tale comunicazione può avvenire senza il consenso dei soci anche quando attenga a dati relativi allo svolgimento di attività economiche o provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque (art. 20, comma 1, lett. b), l. n. 675/1996).

ATTIVITÀ FORENSE, INVESTIGAZIONE PRIVATA E LIBERI PROFESSIONISTI

35. L'ATTIVITÀ DEI LIBERI PROFESSIONISTI

Il Garante ha avuto modo di occuparsi nuovamente dell'impatto della legge n. 675/1996 sull'attività svolta dai liberi professionisti, a cominciare dal regime di pubblicità degli albi professionali e degli atti connessi allo "status" d'iscritto all'albo.

In particolare, il Garante (*Provv.* del 29 marzo 2001) ha nuovamente ribadito che la legge 675/1996 "non ha modificato la disciplina legislativa relativa al regime di pubblicità degli albi professionali e alla conoscibilità degli atti connessi", sottolineando che "tali albi sono destinati 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", con la conseguenza che "le disposizioni normative relative ai vari albi permettono ai diversi ordini professionali di comunicare e diffondere a soggetti pubblici e privati i dati personali" in essi contenuti, "in armonia con quanto stabilito dall'art. 27, commi 2 e 3, della legge n. 675".

Inoltre il Garante, nell'affrontare nuovamente la questione del regime di pubblicità dei provvedimenti disciplinari adottati nei confronti degli iscritti agli albi professionali (tematica già esaminata ad esempio con parere del 16 giugno 1999, in *Bollettino* n. 9, p. 72), ha riaffermato che la *ratio* sottesa alla pubblicità dei medesimi albi e dei periodici aggiornamenti relativi a nuove iscrizioni e cancellazioni ricorre anche per i provvedimenti che comportano una sospensione o l'interruzione dell'esercizio della professione, i quali, per loro stessa natura, devono considerarsi soggetti anch'essi ad un regime di ampia conoscibilità.

Più specificamente, con riferimento alla posizione degli iscritti all'albo degli avvocati, l'Autorità, nel rammentare che il r.d.l. n. 1578/1933 prevede, oltre alla preventiva comunicazione degli albi ai Ministri della giustizia e del lavoro, nonché ai presidenti della corte d'appello e del tribunale del distretto, la loro affissione "nelle sale d'udienza della corte, dei tribunali e delle preture del distretto medesimo per mezzo di ufficiale giudiziario", ha sottolineato che l'art. 46, commi primo e terzo, del citato r.d.l. stabilisce che i provvedimenti di radiazione e di sospensione sono "comunicati a tutti i consigli dell'ordine degli avvocati e procuratori della Repubblica ed alle autorità giudiziarie del distretto al quale il professionista appartiene". Inoltre, proprio in relazione a tale tipo di provvedimenti, il Garante ha richiamato le disposizioni del r.d. 22 gennaio 1934, n. 37, che prevede un apposito regime di pubblicità – da attuarsi a mezzo deposito presso i rispettivi uffici di segreteria – per le decisioni adottate sia dai consigli dell'ordine (in primo grado) che dal Consiglio nazionale forense (in sede d'impugnazione).

Ciò premesso, nel rilevare come tali provvedimenti disciplinari siano atti pubblici soggetti ad un regime di conoscibilità (sia da parte di altri professionisti, sia di terzi) "che si fonda su rilevanti motivi di interesse pubblico connessi anche a ragioni di giustizia ed al regolare svolgimento dei procedimenti in ambito giudiziario", il Garante ha affermato che, nel caso di specie, non poteva ritenersi prevalente l'interesse alla riservatezza del singolo professionista destinatario di una misura disciplinare (ferma restando la necessità che, ai sensi dell'art. 9 della legge n. 675/1996, la menzione del provvedimento disciplinare fosse attuata in modo corretto ed in termini esatti e completi) sicché, stante il regime di conoscibilità di detti provvedimenti, doveva ritenersi lecita la loro divulgazione tramite riviste, notiziari o altre pubblicazioni curate dal Consiglio dell'ordine che, integrando un trattamento di dati personali finalizzato alla pubblicazione o diffusione occasionale di articoli, saggi o altre manifestazioni del pensiero, sono soggette alla disciplina prevista dall'art. 25 l. 675/1996 per l'attività giornalistica e d'informazione.

Inoltre, con particolare riferimento ai c.d. "dati sensibili", giova anche ricordare che il Garante, visti i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti, ha reiterato le autorizzazioni n. 4 e n. 6, concernenti proprio il trattamento di tali dati da parte dei liberi professionisti e degli investigatori privati. Trattasi di provvedimenti che, nella sostanza, riproducono il contenuto delle precedenti autorizzazioni e che avranno efficacia sino al 31 dicembre 2001.

36. La raccolta di dati per finalità di difesa

Altro argomento di particolare importanza, su cui il Garante è stato chiamato a pronunziarsi ripetutamente nel corso del 2000, è quello della raccolta dei dati per l'esercizio del diritto di difesa.

In uno di detti casi, l'Autorità ha avuto ad esempio modo di riscontrare la liceità dell'attività informativa svolta da un investigatore privato, all'uopo incaricato da una società, al fine di verificare l'esistenza o meno di una condizione patologica ostativa allo svolgimento di prestazione lavorativa da parte di un dipendente (*Provv.* del 9 novembre 2000). In particolare, nell'accertare che il trattamento in questione andava ricondotto nell'alveo degli artt. 12, comma 1, lett. h) e 20, comma 1, lett. g), nonché dell'art. 22, comma 4, l. n. 675/1996, il Garante ha ritenuto che l'attività investigativa, svolta sulla base di uno specifico mandato conferito dalla società, si era sostanziata in un trattamento di dati personali (in particolare nello scatto di alcune fotografie e nella redazione di brevi annotazioni circa gli spostamenti del lavoratore nei periodi e negli orari indicati all'atto del conferimento dell'incarico) pertinenti rispetto all'intento della società di dimostrare in giudizio (come poi avvenuto) l'insussistenza di una patologia addotta dal lavoratore, sicché la mera possibilità di desumere dalle fotografie riprese a distanza o dalle annotazioni alcuni occasionali riferimenti a familiari compresenti durante gli spostamenti non poteva considerarsi circostanza eccedente rispetto alla finalità del trattamento.

In altri casi, il Garante è stato chiamato a valutare la liceità di una diversa tipologia di trattamenti di dati personali collegati all'espletamento di un'attività giudiziaria.

In particolare, in relazione ad un ricorso con cui l'interessato lamentava il mancato riscontro, da parte di un giudice di merito, ad una richiesta di accesso ai dati personali conservati in un fascicolo avente ad oggetto l'eventuale convalida di un trattamento sanitario obbligatorio, il Garante (*Provv.* del 27 aprile 2000), nell'appurare che il trattamento in questione doveva farsi rientrare fra quelli svolti "per ragioni di giustizia, nell'ambito degli uffici giudiziari, del Consiglio superiore della magistratura e del Ministero di grazia e giustizia" (art. 4, comma 1, l. 675/1996), ha ricordato anche in questo caso che a tale categoria di trattamenti si applicano solo alcune disposizioni della l. n. 675/1996, fra le quali non sono al momento compresi né l'art. 13 (esercizio del diritto di accesso ai dati), né l'art. 29 (ricorso al Garante) della medesima legge. Pertanto, nei confronti dell'attività degli uffici giudiziari e dei magistrati ivi addetti non può essere proposto ricorso ex art. 29, né può essere presentata una previa istanza ai sensi del citato art. 13, essendo possibile sollecitare, attraverso una richiesta o l'invio di una segnalazione o reclamo al Garante, la verifica della rispondenza dei trattamenti di dati ai requisiti stabiliti dalla legge o dai regolamenti (artt. 31, comma 1, lett. d) e p) e 32, in relazione all'art. 4, comma 2).

Analoghe considerazioni sui trattamenti finalizzati all'esigenza di far valere o difendere un diritto in sede giudiziaria sono state espresse nei provvedimenti del 18 aprile 2000 e dell'8 giugno 2000.

Ulteriori e proficui spunti per l'intervento del Garante saranno forniti dalla nuova disciplina sulle indagini difensive nel procedimento penale, introdotta dalla l. n. 397/2000.

Premesso che la normativa in questione ha innovato sensibilmente la vecchia impostazione codicistica in materia, originariamente basata sull'art. 38 disp. att. c.p.p., si deve osservare che a seguito dell'introduzione di tale disciplina si è posto un problema di raccordo con la l. n. 675/1996 (per molti aspetti risolvibile sul piano meramente applicativo o su quello di nuove regole deontologiche), soprattutto con riferimento alle garanzie, agli adempimenti ed ai limiti che i difensori, gli investigatori privati ed i consulenti tecnici (incaricati dal difensore) dovranno tenere presenti all'atto della raccolta di informazioni di carattere personale. In particolare, stante la stretta interazione esistente tra la l. n. 675 e la l. n. 397, sembrano opportuni alcuni accorgimenti per consentire agli operatori di fornire con un unico atto una sola informativa che unisca, nella sostanza, l'"informativa" ex art. 10 l. n. 675 e le varie "avvertenze" di cui all'art. 391-*bis* c.p.p. (introdotto dalla l. 397/2000), tenendo conto degli elementi delle due informative sostanzialmente comuni, come pure di altre notizie che devono essere fornite agli interessati al momento della raccolta dei dati, e che sono distintamente previste da ciascuno dei predetti articoli, in termini che potrebbero essere condensati, con formulazioni esaurienti, ma sintetiche, in unico atto di informativa.

37. I CODICI DEONTOLOGICI

Altre questioni aperte (che sono all'esame anche del gruppo di lavoro che è in procinto di completare i lavori preparatori dei due codici di deontologia in materia di esercizio del diritto di difesa e di investigazione privata, promossi dal Garante il 10 febbraio 2000) riguardano, tra l'altro, i tempi di conservazione dei dati, la raccolta di determinati dati sensibili e i diversi doveri dei soggetti che a vario titolo collaborano al trattamento dei dati per le predette finalità.

Il fenomeno dei codici di deontologia e di buona condotta, quali fonti sostanzialmente normative (seppur di rango inferiore) create con il contributo di singole categorie, nel settore d'appartenenza, secondo principi di rappresentatività, non è infatti estraneo né al settore forense, né a quello dell'investigazione privata.

Già l'Unione delle Camere penali italiane, a seguito dell'entrata in vigore della legge n. 397/2000, ha approvato alcune prime "Norme di comportamento" del penalista nelle indagini difensive (successivamente integrate e coordinate con altre approvate in precedenza), che contengono alcuni utili riferimenti in materia di protezione dei dati, in particolare per quanto riguarda il contenuto delle informative e il richiamo, nel conferimento agli investigatori privati autorizzati ed ai consulenti tecnici dell'incarico di cui all'art. 327-*bis*, comma 3, c.p.p., al dovere d'osservanza delle disposizioni di legge sulle indagini difensive, "incluse quelle in materia di tutela dei dati personali".

Queste prime iniziative risulteranno utili per condurre a termine in breve tempo il codice deontologico dedicato al tema dell'utilizzazione di dati per finalità di difesa di un diritto in sede giudiziaria, non solo penale, ma anche civile ed amministrativa, da coordinare ovviamente con gli esistenti strumenti deontologici per la categoria forense.

In avanzato stato di predisposizione è, anche, l'ulteriore schema di codice deontologico per l'investigazione privata che, sulla base delle prime bozze inviate al Garante e degli approfondimenti in atto per armonizzarlo al codice poc'anzi citato, dovrebbe vedere la luce prima della fine del corrente anno.

SETTORE DEL CREDITO, FINANZIARIO ED ASSICURATIVO

38. PROFILI GENERALI

Gli operatori del settore creditizio, finanziario ed assicurativo sono tra quelli maggiormente coinvolti dai principi e dalle disposizioni della legge n. 675/1996 sulla raccolta e sul trattamento dei dati, la quale ha comportato l'attuazione di diversi adempimenti che hanno avuto immediati e profondi riflessi nella loro normale attività imprenditoriale e nei quotidiani rapporti con la clientela.

Si tratta anche dei settori economici in cui, proprio per l'importanza rivestita dalle informazioni di carattere personale rispetto ai servizi erogati e la necessaria ampiezza degli archivi e dei flussi di dati che riguardano pressoché tutti i cittadini italiani, è emersa con grande evidenza la diffusa sensibilità dell'utente-consumatore verso le nuove forme di tutela introdotte dalla legge sulla *privacy*, con una sempre più frequente attivazione degli strumenti di difesa dei propri diritti e degli interessi fondamentali.

Nel corso del 2000, sono continuati ad affluire numerosi all'Ufficio del Garante i ricorsi, le segnalazioni, i reclami ed i quesiti in questi ambiti, con particolare riguardo a due filoni, per così dire, "patologici", nei quali a breve-medio termine (prima, cioè che vengano introdotti eventuali correttivi in sede legislativa, oppure stabilite da parte dell'Autorità regole uniformi mediante una valutazione più generale), sembra purtroppo destinato ad aumentare il già vasto contenzioso esistente:

– per quanto concerne gli istituti di credito e finanziari, le questione legate al funzionamento ed all'operatività dai sistemi di rilevazione dei rischi creditizi, nonché le c.d. centrali rischi, gestite da privati, soprattutto con riferimento al credito al consumo;

– per quanto riguarda il settore assicurativo, i problemi connessi all'accesso da parte degli assicurati interessati alle perizie medico-legali predisposte dai sanitari di fiducia delle compagnie di assicurazioni, in relazione alle richieste di risarcimento dei danni ed alla liquidazione dei sinistri (sia per le assicurazioni auto, sia per le polizze sanitarie).

Rispetto a questi due principali filoni, occorre segnalare alcuni altri significativi temi affrontati dall'Autorità nel decorso anno con riguardo ai trattamenti di dati svolti da banche e società finanziarie.

Sul fronte della semplificazione degli adempimenti per la tutela della *privacy* in questo settore, l'Autorità è tornata sul tema delle modalità alternative di informativa ai clienti interessati, utilizzabili in relazione a complesse operazioni di cartolarizzazione dei crediti (tema già ampiamente trattato nella Relazione per l'anno 1999, par. 2.6.2, p. 50). Il Garante ha infatti adottato il 4 aprile 2001 un provvedimento di carattere generale, con il quale ha autorizzato le società cessionarie di crediti a fornire l'informativa mediante pubblicazione nella *Gazzetta Ufficiale*, con modalità sostanzialmente analoghe a quelle previste dal testo unico in materia bancaria e finanziaria (che prevede tale forma di pubblicazione per rendere note le cessioni in blocco di rapporti giuridici: art. 58 d.lg. n. 385/1993).

Nel richiamare i propri precedenti orientamenti in materia (*Provv.* del 26 novembre 1998 e del 5 giugno 1999), l'Autorità ha precisato che l'autorizzazione si intende automaticamente concessa anche per le altre società che – trovandosi nelle medesime condizioni- ne abbiano fatto richiesta, decorsi trenta giorni dal ricevimento delle istanze senza che il Garante abbia chiesto chiarimenti o comunicato il rigetto. L'informativa da pubblicare nella *Gazzetta Ufficiale* -e da trasmettere prima in copia all'Ufficio del Garante- dovrà essere messa a disposizione degli interessati e resa agevolmente visibile nelle filiali e negli uffici delle società cessionarie, nonché pubblicata su almeno due quotidiani nazionali ed uno locale (del luogo in cui sono insediate le filiali che hanno intrattenuto il maggior numero di rapporti con i clienti interessati).

Riguardo alle segnalazioni presentate dai cittadini nei confronti del mondo bancario, va poi evidenziato un altro dato relativo al grave aumento, negli scorsi mesi, dei ricorsi e dei reclami contro le violazioni delle norme poste a tutela della riservatezza e della segretezza nei rapporti bancari, relativamente alla divulgazione a terzi di informazioni su operazioni o conti dei clienti, spesso, in collegamento a procedimenti pendenti presso l'autorità giudiziaria.

Nell'esaminare i diversi reclami pervenuti, il Garante ha spesso riscontrato che le lamentele degli interessati non potevano essere prese in considerazione in quanto riferite a circostanze generiche e non

documentate -ad es., una telefonata effettuata ad alta voce da un impiegato in un locale della filiale dove potevano essere presenti altre persone oppure un colloquio tenutosi all'interno di un'agenzia di banca per la stipulazione di un mutuo richiesto da un familiare del cliente (*Provv.* del 6 febbraio 2001 in *Bollettino* n. 17, p. 28 e dell'11 dicembre 2000, in *www.garanteprivacy.it*). In uno specifico caso, l'Autorità ha ritenuto altresì infondate le doglianze di una società sulla presunta eccedenza delle informazioni riportate nella dichiarazione prodotta da una banca in una procedura esecutiva presso terzi (*Provv.* del 19 settembre 2000).

In un'altra ipotesi, è stato invece chiarito che anche gli eredi del cliente deceduto possono accedere ai dati relativi ai depositi e conti di quest'ultimo, in base all'art. 13, comma 3, della legge n. 675/1996, che permette a chiunque vi abbia interesse di esercitare i diritti ivi previsti relativamente a dati di persone decedute. Tuttavia, l'Autorità ha precisato che non è allo stesso modo conoscibile il nominativo del percettore del saldo di deposito, in quanto tale informazione non riguarda il cliente deceduto, ma un terzo (*Provv.* del 27 ottobre 2000, pubblicato sul sito *www.garanteprivacy.it*).

L'Autorità ha definito da ultimo un procedimento relativo ad interessanti questioni sul c.d. segreto bancario e sugli obblighi di riservatezza nel trattamento dei dati dei clienti, appurando che (*Provv.* del 23 maggio 2001, in corso di pubblicazione) una banca aveva operato una comunicazione illecita di dati ad un legale relativamente a rapporti di conto corrente e di deposito titoli di una cliente.

Quest'ultimo provvedimento potrà risultare utile per definire criteri di comportamento e procedure uniformi nell'interesse sia dei cittadini sia delle banche, da poter sviluppare e fissare anche in sede di predisposizione da parte degli istituti di credito e finanziari del codice deontologico, i cui lavori sono stati avviati l'anno scorso (a seguito del provvedimento del 10 febbraio 2000 per la promozione della sottoscrizione di codici di buona condotta in diversi settori, allegato alla Relazione per l'anno 1999, par. 6.2.2, p. 223), e la cui adozione risulterà positiva anche per le scelte dei consumatori che, rivolgendosi agli istituti aderenti al codice, potranno vedere maggiormente tutelata la riservatezza dei dati relativi alla propria situazione economica o finanziaria.

39. PERIZIE MEDICO-LEGALI E CONTROVERSIE ASSICURATIVE

Nel corso dell'ultimo anno di attività numerosi sono stati i ricorsi presentati in relazione al trattamento dei dati personali nel settore assicurativo; si è quindi confermata quella tendenza ad un diffuso contenzioso in tale ambito già evidenziata da questa Autorità nello scorso anno (v. Relazione per l'anno 1999, p. 47).

È frequente, infatti, il caso di un soggetto coinvolto in un sinistro, o comunque interessato ad un risarcimento di danni fisici, che adisce l'Autorità per poter accedere ai propri dati personali contenuti nella perizia medico-legale redatta dal medico fiduciario della società di assicurazione cui è stata richiesta la liquidazione del danno. Se nel corso del precedente anno le modalità di presentazione e il contenuto delle richieste avanzate al titolare del trattamento e del ricorso successivamente presentato all'Autorità potevano risentire di una conoscenza ancora superficiale dei contenuti della legge, tali problematiche sono nettamente diminuite nel corso del 2000.

Questa circostanza, unita ad un orientamento giurisprudenziale costante dell'Autorità in materia, ha consentito di poter approfondire e specificare alcuni aspetti significativi.

L'Autorità ha infatti avuto modo di qualificare la natura delle informazioni contenute nelle perizie medico-legali fornendo chiarimenti sull'esatta portata della definizione di "dato personale".

Tali perizie contengono un complesso di informazioni che, pur nella loro eterogeneità, forniscono un insieme di elementi informativi, diretti e indiretti, sul soggetto interessato, sulle sue eventuali patologie, sul rapporto fra di esse ed altri eventi della vita del medesimo. In particolare le perizie sono composte di più parti. In esse compaiono infatti: 1) dati personali identificativi di tipo anagrafico; 2) dati storici sull'evento che ha dato luogo alla richiesta di risarcimento; 3) dati personali riferiti allo stato di salute; 4) elementi valutativi veri e propri in cui il medico legale esprime le sue considerazioni sul nesso di causalità fra eventi traumatici e danno, su importanti profili della sfera psicofisica dell'assicurato rilevati prima e nel corso della visita medica.

Il Garante, fin dalle sue prime decisioni concernenti il settore, ha evidenziato che si potevano ricomprendere nella nozione di "dato personale" tutte le informazioni contenute nelle perizie medico-legali,

comprese quelle espresse in forma di valutazioni o di giudizi sull'invalidità o sull'inabilità dell'interessato (decisioni del 25 maggio e del 4 dicembre 2000). Infatti, la nozione di "dato personale" che è stata adottata dalla legge n. 675 – in ossequio ai principi espressi nell'art. 2, lettera a), della direttiva 95/46/CE – è particolarmente ampia. Essa comprende non solo l'informazione di tipo anagrafico o comunque oggettivo, ma anche ogni notizia o elemento che abbia un'efficacia informativa tale da fornire un contributo aggiuntivo di conoscenza rispetto ad un soggetto identificato o identificabile.

Anche nella parte in cui la perizia contiene elementi valutativi veri e propri nei quali il medico-legale esprime le proprie considerazioni su profili rilevanti della sfera psicofisica dell'interessato, tali valutazioni forniscono ulteriori elementi informativi che completano e arricchiscono il quadro di riferimento, clinico e personale, dell'interessato. Tali elementi che derivano dal libero convincimento del medico non possono essere per ciò stessi considerati espressione di conoscenze impermeabili all'accesso dell'interessato (*Provv.* del 22 novembre 2000 pubblicata sul sito dell'Autorità).

Tale opinione è inoltre ora supportata dalla *Raccomandazione sui dati valutativi dei dipendenti* approvata il 22 marzo 2001 dal Gruppo dei Garanti europei di cui all'art. 29 della direttiva n. 95/46/CE. Da tale documento si evince in maniera chiara che devono essere considerati dati personali anche i giudizi o le valutazioni sintetizzate attraverso un punteggio o una classifica, ovvero espressi attraverso criteri valutativi.

Ulteriore problema affrontato dall'Autorità nelle decisioni sui ricorsi è stato quello derivante dall'applicazione dell'art. 14, comma 1, lettera e) della legge n. 675, concernente il differimento del diritto di accesso di cui all'art. 13 della medesima legge n. 675/1996, limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio per lo svolgimento delle investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria.

Il Garante ha affermato che la valutazione del pregiudizio deve essere effettuata caso per caso e di esso il titolare del trattamento deve fornire adeguata motivazione (decisioni del 14 aprile 2000, 9 maggio 2000 e 25 ottobre 2000).

Nei ricorsi presentati, il Garante ha talvolta appurato che dalle deduzioni svolte non emergevano elementi idonei a considerare provato il pregiudizio. Non si poteva ad esempio ritenere sufficiente il mero disaccordo delle parti sull'esistenza del danno risarcibile (*Provv.* del 9 maggio 2000) per prevedere un temporaneo differimento del diritto di accesso dell'interessato ai dati personali contenuti nella perizia medico-legale. In altre situazioni, il Garante ha invece previsto che, al fine di garantire una tutela completa del diritto di difesa, occorre non pregiudicare le deduzioni delle parti in ordine alle prove e alle modalità della loro esibizione in giudizio, talora anche in una fase iniziale di una controversia giudiziaria (*Provv.* del 14 aprile 2000).

Se da un lato la legge n. 675 pone infatti limiti al diritto di accesso, dall'altro, nel bilanciamento tra le due situazioni giuridiche contrapposte (quella dell'interessato di conoscere i propri dati personali; quello della società di non vedere pregiudicato il proprio diritto di difesa in una causa sull'accertamento del diritto al risarcimento), si deve evitare che l'eccezione basata sul diritto di difesa possa vanificare la tutela dei diritti riconosciuti nell'art. 1 della medesima legge.

Va segnalato infine che le impugnative al giudice ordinario di decisioni riguardanti questo settore rappresentano, come si vedrà nello specifico paragrafo, un numero esiguo.

40. Raccolte di dati in ambito assicurativo

A parte gli accennati problemi dell'accesso alle perizie medico-legali, nel campo assicurativo si sono poste in questi anni una serie di questioni relative agli adempimenti previsti dalla disciplina sulla tutela dei dati personali analoghe a quelle affrontate nel settore del credito, con – probabilmente- una maggiore criticità, dovuta alla più ampia presenza ed utilizzo in ambito assicurativo di informazioni personali di natura sensibile e, in particolare, di quelle riferite allo stato di salute degli interessati.

Come per le banche, l'Autorità è in procinto di completare, in collaborazione con la competente associazione di categoria, l'A.N.I.A., alcuni approfondimenti per addivenire ad una modulistica-tipo ancora più semplificata per l'informativa ed il consenso, che tenga conto della molteplicità di trattamenti di dati personali, anche sanitari, posti in essere dalle compagnie assicurative e da un complesso di soggetti coin-

volti nella c.d. catena assicurativa (a partire dagli agenti e dalla variegata rete di intermediari assicurativi per finire ai periti, ai legali ed alle autofficine).

Come già detto, è connaturato all'attività assicurativa anche un ampio trattamento di dati sensibili relativi alla salute del cliente e di terzi, raccolti e trattati nel momento iniziale di specifici rapporti contrattuali (relativi ad esempio a polizze infortuni o sanitarie) o nell'ambito di operazioni di liquidazione dei sinistri e di risarcimento dei danni, che spesso sfociano in procedimenti arbitrali o giudiziari.

Di qui la specifica attenzione dedicata dal Garante nelle sette autorizzazioni generali sui dati sensibili rinnovate il 30 settembre 2000 (cfr. le autorizzazioni nn. 2/2000 e 5/2000, riportate nella documentazione allegata alla presente Relazione) o relativi a provvedimenti penali a carico degli assicurati. Categorie di dati che le compagnie possono trattare, tra l'altro, per accertare responsabilità in relazione a sinistri o ad eventi attinenti alla vita umana o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, relativamente ad illeciti direttamente connessi all'attività medesima (v. capo IV autorizzazione n. 7/2000).

Per quanto concerne il trattamento dei dati relativi allo stato di salute da parte delle compagnie, l'Autorità ha avuto modo di chiarire, esaminando un ricorso, alcuni aspetti relativi agli obblighi di conservazione dei dati contenuti nella documentazione e nelle certificazioni sanitarie nell'ambito delle assicurazioni r.c. auto (*Provv.* del 14 settembre 2000 e del 24 ottobre 2000).

Sulla base delle disposizioni contenute nelle predette autorizzazioni generali nn. 2 e 5, il Garante ha infatti ritenuto che nel caso sottoposto alla sua attenzione, relativo non ad un cliente attuale della compagnia, ma ad un terzo danneggiato in un sinistro stradale risarcito più di cinque anni prima, non ricorressero né particolari ipotesi (ad es. impresa assicuratrice in liquidazione), né ragioni specifiche che avrebbero potuto giustificare un'ulteriore conservazione dei dati sanitari dell'interessato, essendo trascorsi appunto cinque anni dalla liquidazione dei danni (con prescrizione, peraltro, del termine per l'esercizio dei diritti relativi al risarcimento del sinistro) e non essendo in atto alcun contenzioso tra le parti.

Il Garante, avendo disposto il blocco dei dati, ha invitato la società a cancellare o a trasformare in forma anonima le informazioni relative allo stato di salute del ricorrente, non essendo risultata più giustificata la conservazione di dati eccedenti rispetto alle finalità dell'originaria raccolta e del loro attuale trattamento.

Occorre poi segnalare, come novità normativa di assoluto rilievo per i riflessi in materia di tutela dei dati personali, l'art. 2, commi 5-*quater* e 5-*quinquies*, della legge 26 maggio 2000, n. 137 (di conversione, con modificazioni, del d.l. 28 marzo 2000, n. 70, recante disposizioni urgenti per il contenimento delle spinte inflazionistiche: v. il testo coordinato pubblicato sulla *G.U.* n. 122 del 27 maggio 2000), con il quale è stata istituita presso l'ISVAP una banca dati dei sinistri relativi all'assicurazione obbligatoria per i veicoli a motore immatricolati in Italia, al fine di rendere più efficace la prevenzione ed il contrasto di comportamenti fraudolenti in tale settore. Le compagnie di assicurazioni sono obbligate, pena l'applicazione di sanzioni amministrative pecuniarie, a trasmettere periodicamente alla banca dati le informazioni riguardanti i sinistri dei propri assicurati a partire, come periodo di riferimento, dal 1° gennaio 2001.

Le concrete procedure e modalità di funzionamento devono essere stabilite con un provvedimento attuativo dell'Istituto di vigilanza. Tale problema assume quindi una particolare rilevanza anche per la definizione di delicati profili come, ad esempio, l'individuazione delle informazioni di carattere personale che dovranno confluire nella banca dati e la delimitazione dei soggetti pubblici e privati che potranno avervi accesso. Come già precisato nel par. 9, la questione verrà approfondita a breve termine con l'ISVAP.

Alla fine di quest'anno, il Garante ha inoltre attivato immediati accertamenti sulle notizie di stampa circa l'annunciata intenzione delle imprese assicuratrici di inviare moduli o questionari per la raccolta di dati personali da utilizzare, dopo la loro compilazione da parte della clientela, ai fini della gestione dei rapporti assicurativi o in relazione a frodi assicurative. In particolare, l'Autorità ha voluto verificare quali fossero le ipotizzate modalità di acquisizione ed utilizzazione dei dati in correlazione all'informativa fornita agli assicurati (con specifico riferimento alla natura obbligatoria o facoltativa del conferimento dei dati), nonché l'ambito di circolazione delle informazioni anche in relazione alle novità normative in materia di frodi assicurative. L'associazione di categoria ha al momento evidenziato che le imprese assicurative non hanno elaborato alcun questionario e che le notizie di stampa si riferivano a procedure adottate nel mercato inglese dell'assicurazione obbligatoria r.c. auto e non ancora presenti in quello italiano.

41. CENTRALI RISCHI E SOCIETÀ FINANZIARIE

Anche nell'anno 2000, una parte considerevole – peraltro ancora in costante crescita – del complessivo numero dei ricorsi e dei reclami presentati al Garante ha riguardato i trattamenti di dati personali svolti, per finalità di tutela connesse ai rapporti di finanziamento, dagli istituti di credito e finanziari, nonché dai soggetti che, in ambito pubblico (la Banca d'Italia) e privato (alcune note società, come Crif, Ctc, Experian, ecc.), gestiscono sistemi di rilevazione dei rischi creditizi.

Le attività degli operatori in questo settore sono incentrate sulla capillare raccolta ed ampia circolazione, in un medesimo circuito finanziario, di informazioni sulle esposizioni debitorie dei potenziali nuovi clienti, che dovrebbero essere finalizzate ad individuare eventuali posizioni di inadempimento ed a prevenire effettive situazioni di rischio nell'erogazione dei prestiti.

Tali attività, e i connessi trattamenti di dati, hanno una rilevante incidenza sui consumatori interessati, determinando in non pochi casi – nelle ipotesi, ad esempio, di segnalazione di dati inesatti o di annotazioni e giudizi sproporzionati rispetto a lievi inadempimenti relativi, magari, mancata informazione ed acquisizione del consenso degli interessati – non solo un'ingiustificata preclusione verso ogni forma di finanziamento, ma anche un'inaccettabile violazione dei più elementari principi di riservatezza, in relazione a fondamentali diritti relativi pure all'identità personale e alla dignità umana.

Come già evidenziato lo scorso anno (v. Relazione per l'anno 1999, par. 2.6.3, p. 51), l'introduzione di specifiche regole a tutela della sfera privata dell'individuo ha reso più evidenti alcuni punti critici delle attività svolte dalle c.d. centrali rischi private, soprattutto nel campo del credito al consumo, rendendo improcrastinabile l'individuazione di criteri e procedure omogenee per trovare un più adeguato equilibrio tra le equivalenti, ma contrapposte esigenze di tutela collegate ad una sana e prudente gestione del rischio creditizio, da un lato, e un lecito e corretto trattamento delle informazioni a carattere personale.

In questo senso, può risultare utile, anche al fine di prevenire una parte del vasto contenzioso esistente, l'inserimento nel citato codice deontologico in fase di predisposizione (*v. par. 38*), di apposite regole di comportamento per i gestori delle centrali di rischi, per quanto attiene ai tipi di dati che possono essere lecitamente annotati e conservati, i tempi di conservazione, l'ambito di comunicazione delle informazioni, il riscontro tempestivo alle richieste di accesso ai dati e la pronta rettificazione e cancellazione.

Riguardo ai problemi legati all'operatività delle centrali rischi private, il Garante ha nel frattempo avviato numerosi accertamenti a seguito, in particolare, di alcuni ricorsi relativi a richieste di cancellazione di dati rivolte da singoli cittadini a società finanziarie e ai gestori delle centrali (*Provv.* 26 luglio 2000).

Si tratta di questioni analoghe a quelle già esaminate lo scorso anno (v. Relazione per il 1999, par. 2.6.3, p. 52), concernenti spesso trattamenti di dati iniziati prima dell'entrata in vigore della legge n. 675, per i quali sono emerse clausole di "autorizzazione" con i quali gli interessati, prima dell'8 maggio 1997, avevano acconsentito a far registrare nelle centrali alcuni dati personali per finalità di tutela del credito e a farli comunicare a società di rilevazione dei rischi finanziari e ad altre società aderenti al circuito delle centrali.

Per questi casi e in riferimento a contratti di finanziamento più recenti, il Garante ha avviato procedimenti nei confronti di alcune società finanziarie e di centrali rischi private, chiedendo notizie e chiarimenti circa le formule di informativa e di consenso, sulla durata della conservazione dei dati nella centrale rischi (anche in rapporto ad inadempimenti lievi o temporanei) e su appositi codici utilizzati per distinguere i semplici ritardi nei pagamenti dalle situazioni più o meno gravi di morosità, magari sanate.

Il Garante è stato invece attivamente coinvolto dalla Banca d'Italia all'atto del varo delle istruzioni con le quali l'Istituto ha impartito disposizioni relative al sistema centralizzato per la rilevazione dei rischi creditizi affidato, su proposta dell'A.B.I., alla Società interbancaria per l'automazione S.p.a. (S.I.A.).

Il sistema è stato istituito con deliberazione del Cicr del 3 maggio 1999 (già richiamata nella Relazione per il 1999, par. 2.6.3, p. 52) per indebitamenti di importo inferiore a quelli censiti presso la centrale rischi della Banca d'Italia (150 milioni) e superiore al limite massimo stabilito per il credito al consumo (60 milioni).

L'Autorità ha potuto esprimere un generale parere favorevole, poiché nello schema delle istruzioni sono state recepite varie indicazioni già fornite, limitatamente ai profili della tutela dei dati personali, nel corso di precedenti consultazioni informali (così come previsto anche dall'art. 31, comma 6, l. n. 675).

Le banche e gli intermediari finanziari devono segnalare alla nuova centrale rischi i prestiti erogati per somme nei limiti degli importi sopra indicati. Il trattamento dei dati può essere quindi svolto senza acquisire il consenso dei clienti i quali devono però ricevere un'adeguata informativa.

Nelle predette istruzioni, che per gli aspetti procedurali richiamano quelle già emanate per il sistema di rilevazione dei rischi creditizi gestito dalla Banca d'Italia, sono contenute disposizioni in ordine alle misure di sicurezza e di riservatezza delle informazioni, nonché all'esercizio del diritto di accesso riconosciuto agli interessati.

42. L'"ANAGRAFE DEI CONTI CORRENTI"

Nell'ottobre del 2000 è entrato in vigore il regolamento istitutivo dell'anagrafe dei rapporti di conto e di deposito (adottato dal Ministro del tesoro di concerto con i Ministri delle finanze e dell'interno con d. 4 agosto 2000, n. 269, pubblicato sulla *G.U.* 2 ottobre 2000, n. 230), incisivamente corretto dopo il parere espresso nel 1999 con il quale il Garante metteva in luce una serie di carenze per quanto riguarda gli aspetti della tutela dei dati personali e, in particolare, le finalità e modalità di accesso all'archivio (v. Relazione per l'anno 1999, par. 2.6.4, p. 53).

Il Ministero del tesoro, indicato nel regolamento come il titolare del trattamento, si avvale della rete telematica e del servizio forniti dalla Società interbancaria per l'automazione S.p.a. (S.I.A.), nominata a sua volta, con lo stesso regolamento, come responsabile del medesimo trattamento. È stato istituito un comitato di garanzia chiamato ad esprimere pareri su questioni rilevanti relative alle attività del centro, anche in tema di sicurezza e segretezza, presieduto da un magistrato e composto da diversi rappresentanti dei ministeri e delle autorità interessate (non è stata prevista la presenza di un rappresentante del Garante).

Sono stati inoltre stabiliti alcuni criteri per le richieste di accesso all'anagrafe (nelle quali devono essere evidenziati gli specifici motivi sottostanti), con individuazione dei soggetti abilitati e dei tempi -ancora ampi- di conservazione delle informazioni raccolte.

Sono stati altresì previsti obblighi di riservatezza per il personale addetto ad accedere alle informazioni, anche presso i soggetti e le autorità pubbliche richiedenti, nonché misure di sicurezza per la protezione delle informazioni e della loro trasmissione in rete.

L'Autorità mantiene un alto livello di attenzione in relazione all'anagrafe e al funzionamento dell'intero sistema, considerato anche che la disciplina di alcuni delicati profili, legati ad esempio alla comunicazione e all'acquisizione dei dati, è stata rimessa a fonti ulteriori. Per la completa attuazione dell'anagrafe sono stati infatti previsti ben tre ulteriori decreti ministeriali (di cui uno di approvazione della convenzione stipulata tra il centro operativo e la S.I.A.), per i quali dovrà obbligatoriamente essere acquisito il parere del Garante ai sensi dell'art. 31, comma 2, della legge n. 675/1996.

43. ANAGRAFE DEGLI ASSEGNI BANCARI E POSTALI

Come accennato nel par. 9, la collaborazione istituzionale con la Banca d'Italia e con il Ministero della giustizia si è sviluppata positivamente anche a proposito del costituendo archivio informatizzato degli assegni bancari e postali, che sarà concretamente istituito una volta entrato in vigore il regolamento attualmente all'esame del Consiglio di Stato.

Nel quadro degli ulteriori interventi di decriminalizzazione degli illeciti in materia di emissione di assegni, il d.lg. n. 507/1999 ha previsto (art. 36) una base dati informatizzata per rendere effettive le revoche e le temporanee interdizioni conseguenti ad atti illeciti.

Varie osservazioni e proposte dell'Autorità sono state già recepite nel quadro di un'attiva consultazione.

GIORNALISMO

44. PROFILI GENERALI

Il Garante ha continuato a ricevere numerosi quesiti, reclami, segnalazioni e ricorsi inerenti al trattamento dei dati per finalità giornalistiche. Il fatto che, pur in assenza di sostanziali modifiche al quadro normativo sui trattamenti svolti in ambito giornalistico (quali si erano invece verificate nel 1998 con l'approvazione del codice deontologico sui trattamenti realizzati nell'ambito dell'attività giornalistica), si sia evidenziata una così diffusa domanda di tutela da parte dei cittadini, testimonia il fatto che tali trattamenti sono avvertiti come particolarmente incisivi sulla sfera privata dei singoli.

D'altra parte, in una società come la nostra, nella quale i mezzi di informazione assumono un ruolo di così grande importanza e possono anche per questo arrecare danni notevoli alla vita privata dei singoli, appare evidente che i trattamenti svolti nell'esercizio della professione giornalistica costituiscano uno degli ambiti maggiormente problematici fra quelli affidati alla tutela del Garante. Ciò, anche in considerazione del delicato vaglio che l'Autorità è chiamata a compiere nei singoli casi, a proposito dell'essenzialità dell'informazione diffusa con riferimento all'interesse pubblico alla sua conoscenza.

Si deve altresì rilevare che sempre più spesso problematiche di questa natura vengono segnalate con riguardo alla diffusione di informazioni personali tramite Internet. Ciò è indice del grande sviluppo che stanno avendo in rete i mezzi di comunicazione ed insieme dei rischi che tale diffusione reca con sé per quanto attiene alla tutela dei dati personali (si veda in proposito il *Provv.* del 30 ottobre 2000, relativo alla diffusione su un sito Internet di un articolo di carattere giornalistico del quale l'interessato lamentava la volgarità, la falsità nonché il coinvolgimento di persone estranee alla sua sfera personale).

45. SEGRETO D'UFFICIO, SEGRETO PROFESSIONALE E C.D. SEGRETO INVESTIGATIVO

Limiti del segreto dei giornalisti in materia di indagini della magistratura

Il Garante ha avuto modo di occuparsi dei giornalisti non solo in quanto soggetti che diffondono notizie riguardanti terzi, e quindi come ordinarie controparti di coloro che lamentano una violazione della propria riservatezza e dignità, ma anche in quanto potenziali destinatari di una tutela sotto il profilo della tutela della segretezza delle fonti.

Uno dei profili di maggiore delicatezza ed interesse in materia attiene certamente al segreto professionale dei giornalisti ed al suo rapporto con le indagini della magistratura. Come è noto, infatti, i giornalisti, in ragione della propria attività, godono di una particolare tutela per quanto attiene alla segretezza delle fonti da cui ricavano le informazioni utilizzate nell'esercizio della professione. Essa, tuttavia, è suscettibile di essere compressa qualora il giudice ordini al giornalista di indicare l'origine delle sue informazioni nel caso in cui le notizie siano indispensabili ai fini della prova del reato e la loro veridicità possa essere accertata solo attraverso l'identificazione della fonte della notizia (art. 200, comma 3, c.p.p.).

A questo riguardo, si può ricordare il caso in cui un giornalista ha lamentato una violazione del segreto in occasione di perquisizioni disposte da una Procura della Repubblica che procedeva per il reato di rivelazione ed utilizzazione di segreti di ufficio commesso da un pubblico ufficiale non identificato. Ciò, in seguito alla pubblicazione da parte dello stesso giornalista di un articolo nel quale aveva riferito di un arresto nell'ambito di un'indagine penale.

Il Garante ha proceduto, attenendosi strettamente al profilo di propria competenza attinente al trattamento dei dati personali, ad una verifica del corretto rispetto della normativa in materia di protezione dei dati.

Gli accertamenti, dopo alcune iniziali perplessità di ordine giuridico manifestate dall'ufficio interessato, per certi aspetti fisiologiche considerata la delicatezza delle questioni di diritto coinvolte, sono stati completati con la fattiva cooperazione del medesimo ufficio ed hanno permesso di dichiarare non fondato il reclamo alla luce proprio delle risultanze processuali e dell'andamento dei fatti (*Provv.* del 28 maggio 2000).

ta, come è argomentabile dall'art. 20, comma 1, lett. g) della legge n. 675/1996, che non prevede la diffusione senza consenso dei dati acquisiti per finalità di difesa. Pertanto, mentre sarebbe stato possibile consegnare la videocassetta all'autorità giudiziaria, non era lecito allegare la stessa ad una rivista. Di qui, la conferma del provvedimento di blocco e l'accoglimento del relativo ricorso.

46. ATTIVITÀ GIORNALISTICA E RISPETTO DEI PRINCIPI DELLA LEGGE N. 675/1996

In diverse circostanze, il Garante ha dovuto ribadire la necessità di applicare la normativa – in ampia parte di carattere speciale – dettata con riguardo ai trattamenti di dati personali svolti nell'ambito dell'attività giornalistica. Così, ad esempio, nel dichiarare infondato un ricorso presentato contro alcune importanti testate nazionali da parte di una testimone all'interno di un procedimento penale per gravi reati (*Provv.* del 3 luglio 2000), l'Autorità ha chiarito che il trattamento doveva essere valutato alla luce di quanto disposto dall'art. 25 della legge n. 675/1996 e dal codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*Provv.* del 29 luglio 1998, in *G.U.* del 3 agosto 1998).

Pertanto, quando gli articoli o i servizi pubblicati costituiscono una legittima espressione del diritto di cronaca, magari in relazione – come nel caso di specie – a delicate indagini volte ad appurare l'attendibilità di una testimone (l'interessata) e di sue rilevanti dichiarazioni ai fini processuali, e il trattamento è finalizzato ad informare l'opinione pubblica sugli sviluppi di una vicenda che ha richiamato l'attenzione a livello nazionale, nel rispetto dell'essenzialità dell'informazione e della pertinenza dei dati riferiti, lo stesso trattamento deve considerarsi legittimo. In tal caso, quindi, non può invocarsi il mancato conferimento, da parte dell'interessata, del preventivo consenso al trattamento dei dati, essendo questo esplicitamente escluso dalle disposizioni appena richiamate. Ciò, anche quando attraverso gli articoli e le trasmissioni vengano diffusi dati di carattere sensibile, essendo anche in questa ipotesi consentito prescindere dal consenso, naturalmente ove sia rispettato il limite posto al diritto di cronaca dall'essenzialità dell'informazione e si evitino riferimenti a congiunti o ad altri soggetti non interessati ai fatti (art. 5 del citato codice deontologico).

Argomentazioni analoghe hanno fondato la decisione originata da un ricorso – poi dichiarato infondato – presentato da alcuni consiglieri di amministrazione, dirigenti e giornalisti di una delle principali aziende radiotelevisive nazionali che lamentavano l'avvenuta pubblicazione su un quotidiano di una serie di articoli in cui venivano evidenziate asserite appartenenze politiche degli stessi, nonché rapporti e relazioni personali (amichevoli od ostili) esistenti all'interno dell'azienda televisiva medesima (*Provv.* del 31 maggio 2000). Anche in tal caso l'Autorità, applicando la disciplina sopra richiamata, ha ritenuto che gli articoli fossero espressione di una legittima modalità di esercizio del diritto di cronaca – per quanto opinabili potessero essere i toni utilizzati – con riferimento alla personalità, alle esperienze professionali ed agli incarichi ricoperti dalle persone su indicate, le quali occupavano appunto posti di rilievo in un'azienda di primaria rilevanza sociale.

Nel caso di specie, non sussistevano gli estremi per censurare il diritto dei mezzi di informazione di esprimere valutazioni, anche critiche, riferite alle singole persone, atteso che, peraltro, le notizie riportate potevano essere acquisite correttamente dai giornalisti attraverso la consultazione di giornali, interviste, colloqui, dichiarazioni o attingendo alle consuete fonti lecitamente utilizzate nella cronaca giornalistica. Tale pronuncia del Garante, come altre analoghe, non era ovviamente preclusiva per gli interessati della possibilità di adire il giudice ordinario per rivolgere eventuali diverse istanze in sede civile o penale che esulano dall'ambito di competenza del Garante.

In questo contesto, merita infine di essere ricordata la decisione con la quale l'Autorità ha dichiarato non fondato un ricorso presentato dal titolare di una ditta artigiana. Questi aveva infatti lamentato l'avvenuta pubblicazione su un quotidiano locale della notizia secondo la quale alcuni consiglieri comunali avevano segnalato alla Corte dei conti il comportamento di un comune concernente una transazione con il ricorrente, relativamente al versamento di una penale contrattuale legata a "gravi motivi di salute" del ricorrente medesimo (*Provv.* del 22 gennaio 2001, in *Bollettino* n. 16, p. 8). In tale circostanza il Garante ha constatato che l'articolo riguardava una contestata vicenda amministrativo-erariale che traeva spunto da atti e documenti accessibili al pubblico. La vicenda era quindi riferita ad un fatto di interesse generale relativo al corretto svolgimento dell'attività amministrativa comunale e, nel caso di specie, non era stata descritta ricorrendo a particolari o dettagli non pertinenti; il generico riferimento ai "motivi di salute" del ricorrente (origine della controversa riduzione della penale, contestata dai consi-

Al di là dell'esito, tale pronuncia merita di essere ricordata per alcuni chiarimenti di carattere generale offerti dal Garante sulle proprie competenze in relazione ai trattamenti svolti dalla magistratura. Come è noto, infatti, gli uffici giudiziari sono tenuti al rispetto di alcune disposizioni della legge n. 675/1996 che riguardano anche la pertinenza e la non eccedenza dei dati trattati; l'Autorità può accertare la rispondenza dei trattamenti ai requisiti di legge, ove necessario verificando l'attuazione da parte del titolare o del responsabile di modificazioni o integrazioni dirette a rendere il trattamento conforme alle disposizioni vigenti (artt. 4, comma 2; 31, comma 1, lett. b), c), p) e 32, commi 6 e 7, l. n. 675/1996).

A questo riguardo, l'Autorità ha chiarito che tale delicata attività di verifica è stata però inserita dal legislatore – e deve essere conseguentemente esercitata- in un quadro di cooperazione e di rispetto delle reciproche attribuzioni che non permette, ad esempio, di invocare dinanzi al Garante un sindacato sull'ampiezza del materiale probatorio acquisito nel corso delle indagini preliminari o di sollevare davanti all'Autorità questioni attinenti alla validità di atti procedimentali, alla loro riforma o all'utilizzabilità nel processo degli elementi di prova, dovendo tali questioni essere invece esaminate nelle sedi processuali utilizzando gli ordinari strumenti di impugnazione.

Segreto professionale dei giornalisti ed esercizio dei diritti ex art. 13

La tutela del segreto professionale dei giornalisti può venire in considerazione anche con riguardo all'esercizio dei diritti previsti dall'art. 13 della legge n. 675/1996. Infatti, come ha avuto modo di ricordare il Garante anche nel corso del 2000, la possibilità accordata ai giornalisti di opporre il segreto sulle fonti di informazione non li esime dal dare riscontro alle richieste degli interessati.

È stato ad esempio sottoposto all'Autorità un caso di pubblicazione su un quotidiano locale di un articolo in cui il giornalista aveva fatto riferimento all'esistenza di una lettera riservata di un cittadino. Questi aveva chiesto di conoscere in che modo il giornalista fosse entrato in possesso della lettera medesima senza ottenere una risposta soddisfacente e, per tale ragione, ha presentato ricorso al Garante. Seppure parzialmente, il ricorso è stato accolto sulla base del presupposto che, anche nel caso dei giornali, l'interessato ha sempre il diritto di ottenere, a cura del titolare del trattamento, senza ritardo ed in maniera adeguata, la comunicazione dell'esistenza e dell'origine dei dati che lo riguardano, salvo dichiarare che la fonte dalla notizia è coperta dal segreto professionale in ragione del carattere fiduciario del rapporto con il soggetto che la ha fornita (comunicato n. 2 del 10 gennaio 2000, in *Bollettino*, n. 11-12, p. 81).

Liceità delle modalità di raccolta dei dati successivamente diffusi con i mezzi di informazione

Uno dei profili più delicati con riferimento alla disciplina della tutela dei dati personali con riguardo ai mezzi di informazione, attiene alle modalità con cui sono raccolte le informazioni successivamente diffuse. In merito, si deve ricordare il ricorso con cui un avvocato aveva richiesto il blocco della diffusione, tramite una videocassetta allegata ad un giornale, della registrazione di un colloquio fra il ricorrente medesimo ed un suo collega che dichiarava essere avvenuta a sua insaputa mediante una telecamera nascosta.

In tale occasione il Garante, dopo aver disposto il blocco della pubblicazione in via cautelare (*Provv.* del 20 settembre 2000), ha successivamente accolto il ricorso e confermato il blocco, giudicando contraria alla disciplina sui dati personali la diffusione di tale videocassetta attraverso i mezzi di informazione (*Provv.* 30 ottobre 2000).

In proposito, l'Autorità ha innanzitutto ricordato che la registrazione a fini di difesa giudiziaria da parte di una persona impegnata in una conversazione non richiede il necessario consenso del proprio interlocutore (v. anche *Provv.* del 12 luglio 2000). Infatti, anche nelle ipotesi in cui è stato esplicitamente previsto che tale registrazione è illecita in determinati contesti, come nel caso di riunioni tra avvocati, che possono essere registrate solo con il consenso di tutti i presenti (art. 22, par. 3, codice deontologico approvato dal Consiglio nazionale forense il 17 aprile 1997), si deve ritenere che la registrazione non consensuale da parte di uno dei presenti sia consentita quando avviene per una reale esigenza di tutela di un diritto in sede giudiziaria (art. 12, comma 1, lett. h).

Nel caso di specie non è stata dimostrata l'effettiva esigenza di tutela in sede giudiziaria – e, quindi, della liceità della registrazione – a causa dell'insufficienza degli elementi prodotti nel corso del procedimento, rendendosi pertanto necessario rinviare tale aspetto all'esame delle competenti autorità giudiziarie. Tuttavia, si è potuto chiarire che, anche quando la registrazione è effettuata lecitamente per tutelare un diritto in sede giudiziaria, essa può essere utilizzata senza il consenso dell'interessato solo per le medesime finalità, in particolare dandone comunicazione all'autorità competente. Non è pertanto consentito fare uso dei dati in altro modo, avviandoli ad una diffusione indiscrimina-

glieri comunali) non è stato reputato, proprio in ragione della sua genericità, tale da recare lesione alla dignità dell'interessato: in virtù di ciò l'Autorità ha considerato lecita la pubblicazione dell'articolo, dichiarando pertanto infondato il ricorso.

L'applicazione della normativa ai trattamenti svolti in ambito giornalistico, alle fotografie pubblicate dai giornali ed alle riprese televisive

In altre circostanze l'Autorità ha applicato la normativa a trattamenti di dati personali, realizzati nell'ambito della professione giornalistica, sotto forma di fotografie o di immagini diffuse attraverso i mezzi di informazione.

Anche in tali eventualità all'autore delle fotografie (o delle riprese) si applica la previsione dell'art. 25, comma 4, della legge n. 675/1996; quest'ultima disposizione, infatti, estende le norme relative all'esercizio della professione di giornalista ai *"trattamenti temporanei finalizzati esclusivamente alla pubblicazione di articoli, saggi o altre manifestazioni del pensiero"* e fra queste, possono essere appunto inserite anche le attività dirette a realizzare un servizio fotografico, atteso che anche le fotografie che ritraggono persone sono trattate dalla legge alla stregua di documenti contenenti dati personali (art. 1, comma 2, lett. c), l. n. 675/1996).

Per tale ragione, colui che scatta fotografie, al pari di chi raccoglie notizie, è tenuto a rendere note la propria identità, la propria professione e le finalità della raccolta, senza ricorrere ad "artifici o pressioni indebite" (art. 2 del codice deontologico dei giornalisti).

Al riguardo, con particolare riferimento all'informativa semplificata prevista per i trattamenti svolti nell'ambito dell'attività giornalistica, il Garante ha chiarito che questa trova applicazione anche nelle ipotesi in cui i dati sono raccolti presso un soggetto diverso dall'interessato (*Provv.* del 21 febbraio 2000).

Nel caso di specie, il Garante era stato investito dell'esame di una vicenda che aveva visto la pubblicazione, da parte di un organo di stampa, delle copie di alcune fotografie relative ad un noto personaggio dello spettacolo conservate presso l'abitazione dei genitori di questo. Poiché, dunque, le fotografie ritraevano una persona diversa rispetto a coloro che vivevano nella casa in cui erano conservate, esse non potevano considerarsi raccolte presso l'interessato, con conseguente inoperatività dell'obbligo di informativa ai sensi dell'art. 10, comma 1, della legge n. 675/1996.

La disciplina sulla riservatezza per i personaggi pubblici e le persone note

Analogamente a quanto accade in altri ordinamenti, anche nel nostro la sfera privata delle persone che ricoprono determinate cariche pubbliche o che hanno acquisito una particolare notorietà risulta essere per certi aspetti più ridotta rispetto a quella delle persone la cui vita privata è protetta maggiormente. Tenendo conto di tale principio, il codice deontologico dei giornalisti ha però previsto che la sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se la notizia o di dati non hanno alcun rilievo sul ruolo o sulla loro vita pubblica (art. 6).

Nel corso del 2000 il Garante si è trovato più volte ad applicare tale disposizione, a fronte di reclami presentati da alcuni personaggi pubblici che denunciavano una lesione della propria vita privata. È questo, ad esempio, il caso di un quesito sottoposto all'Autorità da un noto parlamentare che aveva preso parte ad una cerimonia in cui erano presenti altri personaggi pubblici, e che aveva visto il suo nome riprodotto, insieme a quello di altri, in un articolo di giornale che riferiva della cerimonia medesima. In tale occasione, il Garante ha constatato che non vi era stata alcuna violazione delle disposizioni del codice deontologico appena richiamate e che una parte dell'articolo sembrava anzi scaturire da una precisazione fornita direttamente dall'interessato.

Più in generale, l'Autorità ha ricordato che, con riguardo al principio dell'essenzialità dell'informazione, può considerarsi lecita anche un'informazione molto dettagliata, qualora ricorrano determinati presupposti, tra i quali rileva la qualificazione dei protagonisti come personaggi pubblici (*Provv.* del 21 febbraio 2000 e, per un caso analogo, *Provv.* del 20 ottobre 2000).

Fatti resi noti direttamente dagli interessati o attraverso i loro comportamenti in pubblico

Con riguardo alla diffusione operata dai mezzi di informazione, nell'ipotesi in cui gli stessi interessati abbiano in qualche modo reso pubbliche le notizie che li riguardano, viene precluso in alcuni casi un intervento dell'Autorità diretto a ridurre la diffusione delle informazioni medesime (v., in proposito, il comunicato n. 5 del 17 gennaio 2000, in *Bollettino* n. 11-12, p. 83).

La legge n. 675/1996, mentre ha previsto in generale che i giornalisti devono rispettare i limiti del diritto di cronaca, con particolare riferimento a quello dell'essenzialità dell'informazione riguardo a fatti di interesse generale, ha lasciato ferma la possibilità di trattare i dati relativi a circostanze e fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico (art. 25, comma 1). Tale ipotesi ha trovato anche riscontro nel codice di deontologia dei giornalisti che ha fatto salvo il diritto di addurre successivamente motivi legittimi di tutela, ma non ha ribadito il limite dell'essenzialità dell'informazione, richiamato invece con particolare pregnanza per quanto attiene ai dati sensibili (art. 5 del codice di deontologia).

A questo riguardo, si può ricordare un ricorso riguardante le dichiarazioni fatte dal padre naturale di un minore durante alcuni programmi televisivi. Chiarito che in tale ipotesi non sarebbe stato in ogni caso applicabile l'art. 3 della legge n. 675/1996 (in tema di trattamento di dati per fini esclusivamente personali), l'Autorità ha constatato che la vicenda alla quale era stata fatta menzione durante la trasmissione era notoria, in quanto già oggetto di cronaca giornalistica, anche a seguito di dichiarazioni dei relativi protagonisti (v. *Provv.* del 28 febbraio 2000). Di qui l'impossibilità di accogliere la richiesta di opposizione al trattamento formulata dalla ricorrente (in quanto trovava applicazione il già citato art. 5, comma 2, del codice deontologico), che lascia però impregiudicata l'esigenza che giornalisti e conduttori delle trasmissioni televisive operino in modo da evitare o ridurre il rischio di trattare i dati riferiti ai minori in modo da non incidere sul corretto sviluppo della personalità degli stessi (ciò, in particolare, con riferimento all'art. 7 del codice dei giornalisti, sul quale si tornerà fra breve).

Un altro caso che merita di essere menzionato è quello in cui il Garante è stato chiamato a decidere sul ricorso presentato da una madre nei confronti di una televisione a diffusione nazionale, in relazione ad un servizio relativo al rimpatrio in Italia della propria figlia minore a seguito della decisione di una Corte distrettuale statunitense. Anche in tale frangente l'Autorità ha dichiarato infondato il ricorso in quanto, sebbene le fotografie riprodotte nel filmato trasmesso riguardassero un minore, erano state mostrate da uno dei genitori, per di più in un contesto di sentita prospettazione di una complessa vicenda familiare che aveva destato in più occasioni il pubblico interesse (*Provv.* del 23 novembre 2000).

Pubblicazione a mezzo stampa dei provvedimenti disciplinari assunti dagli ordini professionali

Come il Garante ha avuto modo di chiarire altre volte, non sempre l'applicazione della normativa sulla tutela dei dati personali porta ad una minore conoscibilità delle informazioni. In alcune circostanze, infatti, quando devono essere tutelati altri diritti e valori, la disciplina sulla riservatezza può farsi veicolo di una maggiore trasparenza. E ciò può riguardare anche trattamenti particolarmente delicati per la protezione dei dati, quali la diffusione attraverso i mezzi di informazione.

Al riguardo, si può ricordare il caso in cui l'Autorità è stata chiamata a decidere sul ricorso presentato da un'avvocato per lamentare l'avvenuta pubblicazione – su una rivista dell'ordine di appartenenza – del provvedimento di sospensione dalla professione adottato nei suoi confronti. In tale occasione, il Garante ha avuto modo di ribadire che la legge n. 675/1996 non ha modificato la disciplina legislativa relativa al regime di pubblicità degli albi professionali ed alla conoscibilità degli atti connessi. Per tale ragione, deve ancora ritenersi che tali albi siano destinati per loro natura e funzione ad un regime di piena pubblicità, anche della tutela dei diritti di coloro che a vario titolo hanno rapporti con gli iscritti agli albi (*Provv.* del 29 marzo 2001).

Molte delle disposizioni che regolano tale forma di pubblicità sono spesso risalenti nel tempo e necessitano pertanto di essere aggiornate anche al fine di individuare in modo più preciso le diverse forme di diffusione consentite, secondo la logica sottesa alla legislazione in materia di riservatezza (art. 27, comma 3, l. n. 675/1996). Ciò, tuttavia, non fa venir meno la qualificazione degli albi professionali come atti pubblici non solamente conoscibili da chiunque, ma anche oggetto di doverosa pubblicità.

Più specificamente, il Garante ha chiarito che la *ratio* sottesa alla pubblicità degli albi e dei periodici aggiornamenti relativi a nuove iscrizioni e cancellazioni ricorre anche per i provvedimenti che comportano la sospensione o l'interruzione dell'esercizio della professione. Sebbene l'ordinamento preveda al riguardo specifiche forme di pubblicità (es. comunicazione a tutti i consigli dell'ordine degli avvocati ed alle autorità giudiziarie del distretto al quale il professionista appartiene: art. 46, commi 1 e 3, r.d.l. n. 1578/1933), è chiaro che le stesse consentono a chiunque di venire lecitamente a conoscenza di determinati provvedimenti e di darne legittimamente ulteriore notizia.

Il Garante ha potuto così affermare che i provvedimenti disciplinari dei consigli dell'ordine e del Consiglio nazionale forense devono essere considerati quali atti pubblici soggetti ad un regime di conoscibilità. Ciò, pur in assenza di disposizioni più analitiche di legge o di regolamento in cui siano previste particolari modalità di diffusione a favore di determinati soggetti, ulteriori rispetto a quelli specificamente indicati come destinatari dalle norme vigenti.

L'interesse alla riservatezza del professionista destinatario di una misura disciplinare non può ritenersi quindi prevalente rispetto all'interesse generale alla conoscenza del provvedimento medesimo ed è pertanto lecita la divulgazione della notizia del provvedimento stesso attraverso riviste, notiziari o altre pubblicazioni curate anche dagli ordini interessati. Ciò, ovviamente, nel presupposto che la diffusione del provvedimento avvenga in modo corretto ed in termini esatti e completi, secondo quanto disposto dall'art. 9 della legge n. 675/1996.

Pubblicazione a mezzo stampa dei dati relativi ai redditi dichiarati

Nel corso del 2000 (nonché nei primi mesi del 2001), il Garante è stato chiamato ad occuparsi della diffusione, ad opera dell'Amministrazione finanziaria, dei dati relativi al reddito delle persone fisiche anche con riguardo alla loro pubblicazione da parte degli organi di informazione. Tale tema è stato già affrontato dall'Autorità in diverse occasioni, chiarendo che la disciplina vigente prevede espressamente la pubblicazione di determinati elenchi di taluni contribuenti e del relativo reddito. La stessa normativa dispone inoltre la formazione, da parte di ciascun comune, degli elenchi nominativi di tutti i contribuenti che hanno presentato la dichiarazione dei redditi o che esercitano imprese commerciali, arti e professioni (v. *par. 13* della presente Relazione), elenchi, questi, che devono essere depositati per un anno presso gli uffici delle imposte e i comuni interessati ai fini della consultazione da parte di chiunque (art. 69 d.P.R. n. 600/1973 come successivamente modificato in particolare dall'art. 19 l. n. 413/1991).

L'esistenza di siffatte disposizioni – espressione di una scelta normativa volta ad un'ampia conoscibilità di determinati dati- integra gli estremi richiesti dall'art. 27, comma 3, della legge n. 675/1996 e rende quindi allo stato lecita, salve eventuali modifiche normative, la comunicazione degli elenchi da parte dell'amministrazione finanziaria, anche dal punto di vista della normativa in materia di riservatezza (v. lettera del 13 ottobre 2000, in *Bollettino*, n. 14-15, p. 9).

Sulla base di tali presupposti, l'Autorità ha pertanto dichiarato infondato un ricorso presentato da un imprenditore che aveva chiesto il blocco dei dati relativi al proprio reddito diffusi da un quotidiano locale sulla base di quanto pubblicato dall'amministrazione finanziaria (*Provv.* 17 gennaio 2001, in *Bollettino* n. 16, p. 5). Il Garante ha infatti affermato che, essendo le informazioni rese accessibili dall'amministrazione finanziaria destinate ad un'ampia pubblicità, la successiva pubblicazione di dati estratti lecitamente da elenchi accessibili a chiunque è da ritenersi lecita anche senza il consenso degli interessati e senza che sia necessario per la testata che li riproduce dimostrare la sussistenza del requisito dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico (art. 20, comma 1, lett. d), l. n. 675/1996).

Decisioni di carattere procedurale e limiti alle competenze del Garante

Non di rado il Garante è stato investito di istanze di tutela che eccedevano le proprie specifiche competenze: si pensi alle ipotesi in cui il suo intervento è stato invocato in relazione alla diffusione di informazioni denigratorie o diffamatorie, oppure al fine di ottenere dall'Autorità il risarcimento di un danno subito in ragione della diffusione di dati personali attraverso i mezzi di informazione (si veda, per tutti, il *Provv.* del 20 ottobre 2000).

In questi casi l'Autorità ha chiarito ancora una volta l'ambito delle proprie competenze e della tutela amministrativa accordata in relazione al trattamento dei dati personali, ricordando comunque la possibilità di far valere i propri diritti di fronte ad altre autorità (nella specie il giudice ordinario).

In altre circostanze, sono giunte all'Autorità richieste di provvedimenti (ad esempio di blocco della diffusione di talune informazioni) che non potevano essere emanati a causa della mancanza di presupposti procedurali a tal fine necessari (si possono vedere, per tutti, i *Provv.* adottati il 5, il 22 aprile e il 21 settembre 2000; nel terzo di questi casi, l'interessato lamentava di essere stato ripreso durante una trasmissione televisiva a sua insaputa; un altro ricorso è stato dichiarato inammissibile il 30 ottobre 2000, relativamente ad un'intervista dell'ex moglie del ricorrente, mandata in onda durante una nota trasmissione televisiva, nella quale l'intervistata faceva menzione di fatti e circostanze tali da permettere l'identificazione del ricorrente stesso e di suo figlio). Altre volte, invece, sono risultati insufficienti gli elementi di valutazione forniti (*Provv.* 21 febbraio 2000).

In molte di tali ipotesi il Garante, oltre ad indicare le procedure di volta in volta necessarie per ottenere il provvedimento richiesto, ha cercato, ove le circostanze lo consentivano e la questione sottoposta lo richiedeva, di offrire comunque una tutela agli interessati, ad esempio considerando anche alla stregua di segnalazioni i ricorsi proposti in maniera non conforme all'art. 29 della legge e al d.P.R. n. 501/1998.

In ogni caso, quando ciò era possibile, il Garante ha sempre tenuto a chiarire che il pronunciamento dell'Autorità, magari riferito ad un particolare aspetto della vicenda, non precludeva a coloro che avessero avuto interesse di instaurare, anche dinanzi alla competente autorità giudiziaria, specifiche controversie dirette ad ottenere giudizi di cui il Garante non poteva farsi carico anche a causa dell'insufficienza degli elementi di valutazione sottoposti al suo vaglio (si veda, per tutti, il *Provv.* del 21 febbraio 2000).

In alcuni casi, infine, l'Autorità ha avviato autonomamente procedimenti distinti da quello aperto su istanza degli interessati, al fine di accertare il rispetto della normativa sulla riservatezza con riguardo a profili in parte diversi da quelli segnalati o che comunque richiedevano di essere autonomamente valutati (si veda, per tutti, la decisione adottata il 27 agosto 2000 su un ricorso presentato dai genitori di una minore, in relazione ad alcuni articoli dedicati ad un procedimento giudiziario, pubblicati da un quotidiano locale).

47. La tutela dei minori

I minori restano tra i soggetti più esposti e indifesi rispetto al rischio di lesione dei propri diritti fondamentali (ed in particolare del diritto alla riservatezza) da parte dei mezzi di informazione.

Indebite ingerenze nella vita privata dei minori possono comportare danni irreparabili nella relativa vita di relazione e nello sviluppo della personalità, derivanti a volte dalla tendenza a spettacolarizzare vicende che meriterebbero invece maggiori cautele da parte dei *media*. Per tale ragione, anche nel corso del 2000 il Garante si è visto più volte obbligato a richiamare al rispetto dei precisi limiti alla diffusione dei dati personali sui minori (si veda, in particolare, il *Provv.* del 22 aprile 2000).

Come è noto, infatti, al fine di tutelarne la personalità, i giornalisti non devono pubblicare i nomi dei minori coinvolti in fatti di cronaca, né fornire particolari in grado di condurre alla loro identificazione. Questo, nella consapevolezza che la tutela della personalità del minore si estende anche ai fatti che non sono specificamente reati, tenuto conto della qualità della notizia e delle sue componenti. Inoltre, per espressa previsione normativa, il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca. Quando, tuttavia, per motivi di rilevante interesse pubblico e fermi restando i limiti di legge, il giornalista decide di diffondere notizie o immagini riguardanti minori, deve farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi ed i limiti stabiliti anche dalla cosiddetta "Carta di Treviso" (art. 7 del codice di deontologia sul trattamento dei dati personali nell'esercizio dell'attività giornalistica).

In applicazione di questi principi, l'Autorità ha disposto il blocco dei dati relativi alle molestie subite da una minore ad opera dei suoi rapitori nei confronti di una serie di testate giornalistiche (*Provv.* 20 giugno 2000). Alcuni organi di stampa a diffusione nazionale avevano reso note, nei titoli e nel corpo degli articoli, talune circostanze relative alle molestie sessuali che apparivano perpetrate dai rapitori di una minore. Il Garante ha disposto il blocco muovendo dalla considerazione che la possibile ed ulteriore divulgazione dei dati relativi alle molestie, a prescindere dalla loro eventuale rilevanza sotto il profilo penale (profilo per il quale è stata investita la competente autorità giudiziaria in relazione all'art. 734-*bis* c.p.), avrebbe comportato il concreto rischio di un pregiudizio rilevante per l'interessata. Un provvedimento, dunque, da cui derivava per gli editori titolari del trattamento e per i responsabili del medesimo, un preciso obbligo di sospendere ogni ulteriore operazione di trattamento diversa dalla mera conservazione delle informazioni già raccolte e, in particolare, di astenersi dal diffondere ulteriormente i medesimi dati anche in modo indiretto, attraverso la pubblicazione delle corrispondenti parti dello stesso provvedimento del Garante.

In questo contesto merita di essere infine ricordata anche una decisione assunta dall'Autorità nell'agosto 2000, con riguardo all'avvenuta pubblicazione su taluni organi di informazione di liste di soggetti responsabili di gravi atti di violenza a danno di minori. In merito a tali vicende, il Garante era intervenuto con un comunicato stampa per ricordare che la diffusione indiscriminata di informazioni non trova fondamento nel nostro ordinamento. Tali notizie, infatti, a prescindere dalla loro reale efficacia sul piano della prevenzione e dalla circostanza che i dati possano essere desunti anche da fonti accessibili (quali, ad es. pronunce giudiziarie), sono suscettibili di valutazione critica e fonte di contenzioso potendo anche, a seconda dei casi, oltre che determinare danni agli stessi minori indirettamente identificabili, comportare responsabilità per eventuali inesattezze dei dati, oppure per giudizi indifferenziati su situazioni in realtà difformi o per la lesione del diritto all'oblio di persone interessate rispetto a fatti talvolta assai risalenti nel tempo (comunicato stampa del 23 agosto 2000).

SORVEGLIANZA E SISTEMI BIOMETRICI

48. VIDEOSORVEGLIANZA

Il tema della videosorveglianza è stato nello scorso anno tra quelli con riferimento ai quali il Garante ha profuso un particolare impegno, sia per la diffusione del fenomeno, sia in ragione della particolare sensibilità manifestata al riguardo da parte di numerosi cittadini.

In attesa di una specifica normativa che disciplini l'utilizzo dei sistemi di videosorveglianza, le regole previste in via generale dalla disciplina sul trattamento dei dati personali risultano (anche sulla scorta delle indicazioni comunitarie contenute nella direttiva n. 95/46/CE) già applicabili alle immagini ed ai suoni, nel caso in cui le apparecchiature che li rilevano permettano di identificare, in modo diretto o indiretto, un determinato soggetto.

In questo quadro, anche in uno spirito di collaborazione che molte amministrazioni hanno sino ad oggi dimostrato, taluni enti locali hanno ritenuto di interpellare preventivamente il Garante con riferimento ad iniziative di controllo del territorio da realizzare attraverso l'impiego di dispositivi elettronici.

In particolare, il Comune di Mantova ha sottoposto al Garante un progetto di installazione di un sistema di tele-sorveglianza in alcune zone della città, basato su dodici telecamere, in parte destinate ad effettuare rilevazioni a fini statistici e di studio degli accessi dei veicoli al centro storico e nelle zone a traffico limitato, in parte utilizzate per finalità di controllo a distanza "con funzioni di prevenzione e repressione di attività illecite".

Nella specie, il Garante, con provvedimento del 7 marzo 2000, ha fatto presente che per gli aspetti concernenti l'installazione e l'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, occorreva tener conto della nuova disciplina introdotta dal d.P.R. n. 250/1999, il quale prevede, tra l'altro, per i comuni interessati, l'obbligo di munirsi di un'autorizzazione rilasciata dal Ministero dei lavori pubblici, nonché il vincolo di utilizzazione degli impianti per raccogliere dati riguardanti il luogo, il tempo e l'identificazione dei veicoli che accedono al centro storico o nelle zone a traffico limitato, rilevando immagini solamente in caso di infrazione. Alla luce di ciò, il Garante ha chiesto di rivedere l'impostazione del progetto, nella parte in cui ipotizzava una rilevazione sistematica di tutte le targhe dei veicoli transitati, con la previsione di una verifica a posteriori al fine di redigere una lista dei soggetti "sanzionabili" e una rilevazione anonima prevista solo in una fase successiva, per fini statistici e di studio.

La vicenda ha offerto l'occasione all'Autorità per ribadire che la legge n. 675/1996 è applicabile anche ai trattamenti di immagini effettuati attraverso i sistemi di videosorveglianza, a prescindere dalla circostanza che le informazioni siano registrate in un archivio elettronico o eventualmente comunicate a terzi dopo la loro temporanea raccolta e conservazione attraverso circuiti di controllo.

Benché sia vero che le registrazioni effettuate mediante l'uso di telecamere non contengono sempre e necessariamente dati di carattere personale, in quanto la distanza, l'ampiezza dell'angolo visuale e la qualità degli strumenti possono rendere non identificabili le persone inquadrate, la c.d. legge sulla *privacy* considera "dato personale" qualunque informazione relativa a persone anche non identificate, ma identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione. Sicché, ai fini dell'applicazione della legge n. 675/1996, non è necessario che le persone vengano identificate in maniera chiara ed univoca, essendo al contrario sufficiente che i soggetti risultino identificabili attraverso, ad esempio, il collegamento con altre fonti conoscitive, quali foto segnaletiche, *identikit* o archivi di polizia contenenti immagini.

L'Autorità ha quindi invitato il Comune di Mantova a compiere un'attenta verifica, in riferimento alle finalità indicate nel progetto (in particolare con riguardo a quelle di "prevenzione e repressione di attività illecite criminali"), al fine di accertare quali di esse rientrassero effettivamente tra le funzioni istituzionali demandate all'ente stesso, alla luce dell'ordinamento degli enti locali all'epoca dei fatti vigente, dell'ordinamento della polizia municipale, nonché dagli statuti e dai regolamenti comunali (v. art. 27, comma 1, l. n. 675/1996), sollecitando altresì l'ente locale ad individuare misure di sicurezza idonee ad assicurare un uso corretto dei dati da parte dei soggetti legittimati (art. 15, l. n. 675/1996 e d.P.R. n. 318/1999), nonché di modalità volte a fornire agli interessati, in modo efficace, l'informativa prevista dall'art. 10 della legge n. 675/1996.

In relazione alla prevista installazione degli impianti di tele-sorveglianza nel Comune di Mantova, il Garante ha in conclusione segnalato la necessità di apportare talune modifiche al progetto, al fine di renderlo conforme a quanto rilevato in sede di esame preventivo, evidenziando in particolare:

a) la necessità di introdurre una limitazione delle modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine), anche al fine di assicurare il rispetto dei principi fondamentali fissati dall'art. 9 della legge n. 675/1996, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;

b) la necessità di istituire una correlazione tra liceità e pertinenza della raccolta di informazioni e il previsto livello elevato di precisione e di dettaglio della ripresa dei tratti somatici delle persone (si parlava infatti di "*zoom e/o brandeggio motorizzato, con la conseguente possibilità di gestire al meglio l'inquadratura*"), nonché di tener conto dei precisi limiti posti all'installazione di impianti audiovisivi dall'art. 4 della legge n. 300/1970 (c.d. Statuto dei lavoratori), evitando altresì la ripresa sistematica di luoghi privati;

c) la necessità di individuare i soggetti legittimati all'accesso, alla custodia ed all'utilizzazione alle registrazioni anche all'interno dell'ente, escludendo persone diverse dai responsabili e dagli incaricati;

d) la necessità di precisare che, ai fini dell'analisi dei flussi di traffico, il trattamento è effettuato con modalità volte a salvaguardare l'anonimato, ma solo successivamente alla fase della raccolta, giacché le immagini registrate possono contenere dati di carattere personale.

Diversamente dal Comune di Mantova, che si era limitato a predisporre un progetto (sul quale ci si è soffermati in questa sede anche perché presenta profili poi risultati comuni ad altre iniziative), quello di Portici ha trasmesso al Garante la delibera della Giunta comunale con la quale era stato approvato uno schema di regolamento per l'installazione e l'utilizzo di impianti di videosorveglianza del territorio, di telecontrollo ambientale e di pannelli a messaggi variabili.

Dall'esame di tale provvedimento è emerso che con tali impianti il Comune intendeva monitorare le zone nevralgiche del traffico cittadino ed i punti di maggiore concentrazione abitativa, per una pluralità di finalità, tra le quali: *a)* dotarsi di uno strumento attivo di protezione civile; *b)* identificare, in tempo reale, luoghi e ragioni di ingorghi per consentire, fra l'altro, il pronto intervento della polizia municipale; *c)* rilevare infrazioni al codice della strada; *d)* rilevare situazioni di pericolo per la sicurezza pubblica, consentendo l'intervento degli operatori. Anche in tal caso, l'Autorità, con provvedimento del 17 febbraio 2000, ha segnalato la necessità di apportare talune modificazioni allo schema di regolamento, al fine di renderlo armonico con le previsioni della legge n. 675/1996.

Queste vicende, che hanno offerto un'ulteriore attestazione dell'interesse sviluppatosi attorno al tema della videosorveglianza, hanno stimolato altresì una valutazione istituzionale delle dimensioni e delle caratteristiche del fenomeno, basata anche sull'ausilio di esperti esterni. È stata curata, così, un'importante esperienza di ricerca "sul campo", condotta con la collaborazione della società Ipermedia. La ricerca, condotta tra il 20 marzo e il 20 maggio 2000, ha avuto lo scopo di fornire una valutazione preliminare circa la presenza dei sistemi di videosorveglianza visibile esterna nei luoghi pubblici di alcune città italiane: Milano, Verona, Roma, Napoli. Più specificatamente, si è trattato di uno studio pilota volto a fornire, attraverso i dati raccolti, alcune indicazioni sulla presenza di tali strumenti nel nostro Paese e porre, quindi, le basi per un eventuale studio di più ampio respiro, destinato alla misurazione esaustiva del fenomeno ed alla valutazione del suo "impatto ambientale".

Il campo d'indagine è stato individuato nelle zone centrali e semicentrali di Milano, Roma, Napoli e Verona.

Data la dimensione esplorativa della ricerca, nell'ambito di ciascuna città si è optato per un campionamento a scelta ragionata: sono stati selezionati alcuni itinerari, assunti in qualità di casi-campione, con riferimento al centro commerciale, storico, politico (nel caso di Roma) e residenziale di ciascun ambito cittadino, all'interno dei quali è stato rilevato il numero di videocamere presenti, poi assunte ad unità di analisi. Sono state oggetto d'indagine tutte le videocamere esterne e visibili che riprendevano le strade e le piazze campionate, sicché la ricerca tiene conto anche dei casi di videocamere interne a recinzioni, ma rivolte verso l'esterno, o presenti nelle strade adiacenti a quelle percorse, ma rivolte verso queste ultime.

L'obiettivo principale della ricerca, consistente nel fornire una valutazione preliminare circa la presenza dei sistemi di controllo video visibili ed esterni nelle quattro città italiane indicate, scontava evidentemente la carenza, creatasi per effetto dell'interazione negativa di molti fattori, di uno dei presupposti necessari all'identificazione dell'universo di riferimento: la possibilità di delimitare le unità che lo compongono. In concreto, ci si è trovati di fronte ad un universo "sconosciuto", non essendo note, oltre

al numero delle unità che lo costituiscono, anche la loro localizzazione e le loro caratteristiche. Ciò nonostante, i campioni relativi alle quattro città oggetto di rilevazione possono considerarsi sufficientemente validi (considerando anche la dimensione esplorativa della ricerca) per fornire dati utili ad elaborare (ancorché su un piano certamente non scientifico, ma congetturale) una prima stima riguardo alla diffusione di tali sistemi.

I dati sono stati raccolti tramite una scheda di rilevazione composta da otto variabili relative alla città, zona, ubicazione, collocazione, identificabilità, posizione, visibilità e tipologia della videocamera. Per mezzo di essa è stato possibile raccogliere informazioni non solo sull'affollamento, ma anche sul grado di percettibilità degli strumenti di videosorveglianza, specie attraverso l'analisi della posizione e della visibilità degli apparecchi.

Le videocamere individuate sono complessivamente 1095: 726 a Roma, 213 a Milano, 89 a Napoli e 67 a Verona. Considerando il carattere campionario dell'indagine, questi numeri consentono di stimare, a livello di attendibile proiezione statistica, la presenza in Italia di circa un milione di impianti di videosorveglianza.

Non si sono peraltro evidenziate significative differenze tra le quattro città (pur trattandosi di tre grandi capoluoghi e una città di minori proporzioni). In ciascun ambito cittadino, invero, i sistemi di videosorveglianza risultano collocati principalmente a vigilanza di sportelli bancari, sono posti ad altezza portone, facilmente individuabili e di grandi dimensioni. Inoltre, fatta eccezione per Milano, dove le telecamere sono equamente distribuite tra zone centrali e semicentrali, si è riscontrata una maggiore concentrazione di meccanismi di controllo video nelle aree poste al centro delle città.

I risultati della ricerca sono stati presentati ai rappresentanti delle istituzioni e alla stampa in occasione di un apposito incontro promosso dal Garante presso la Camera dei deputati nel luglio 2000, che ha visto la partecipazione anche di rappresentanti di governo, di gruppi parlamentari, del mondo accademico e della cultura.

L'iniziativa ha avuto risalto sulla stampa quotidiana, periodica e radiotelevisiva che, sull'esempio dell'Autorità, ha promosso specifiche ricerche a campione sottoposte all'attenzione dell'opinione pubblica, che hanno altresì riscosso l'interesse delle istituzioni.

Ad essa hanno fatto seguito da un lato alcuni progetti di legge coerenti con l'impostazione data dal Garante; dall'altro, talune linee-guida che, su richiesta del Consiglio d'Europa, sono state predisposte dal segretario generale del Garante unitamente ad un rapporto, che il Consiglio stesso si accinge ad approvare definitivamente (v. www.coe.fr).

Anche in considerazione dei riscontri ottenuti, e per venire incontro alla forte domanda di informazione sul tema, il Garante ha quindi provveduto a stilare una sorta di "decalogo" valevole per tutti coloro che intendono installare impianti stabili (o comunque non occasionali), cioè sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini, in particolare a fini di sicurezza, di tutela del patrimonio, di controllo di determinate aree e di monitoraggio del traffico o degli accessi di veicoli nei centri storici. In sintesi, fermo restando innanzitutto il principio di proporzionalità tra mezzi impiegati e fini perseguiti, anche per evitare l'applicazione delle sanzioni previste dalle norme vigenti, sono state indicate ai titolari del trattamento le seguenti cautele:

a) occorre chiarire gli scopi che si intendono perseguire e verificare se sono leciti in base alle norme vigenti. Se l'attività è svolta, ad esempio, per prevenire pericoli concreti o specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche;

b) il trattamento dei dati deve avvenire per scopi determinati, espliciti e legittimi;

c) i titolari del trattamento tenuti a notificare al Garante l'esistenza di trattamenti devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza;

d) i cittadini devono essere informati, in maniera chiara anche se sintetica, della presenza di telecamere e dei diritti che possono esercitare sui propri dati, tanto più se le apparecchiature non sono immediatamente visibili;

e) per il controllo a distanza dei lavoratori rimangono comunque validi i divieti e le garanzie previsti dallo Statuto dei lavoratori;

f) i dati raccolti devono essere quelli strettamente necessari agli scopi perseguiti: vanno pertanto registrate solo le immagini indispensabili, va limitato l'angolo visuale delle riprese, vanno evitate immagini

dettagliate o ingrandite e, di conseguenza, vanno stabilite in maniera adeguata la localizzazione delle telecamere e le modalità di ripresa;

g) va stabilito con precisione entro quanto tempo le immagini devono essere cancellate e occorre prevedere la loro conservazione solo in relazione ad illeciti che si siano verificati o a indagini giudiziarie o di polizia;

h) vanno individuate, con designazione scritta, le persone che possono utilizzare gli impianti e prendere visione delle registrazioni; deve essere vietato l'accesso alle immagini ad altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia;

i) i dati raccolti per determinati fini (ad esempio sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio per pubblicità o analisi dei comportamenti di consumo), fatte salve le esigenze di polizia o di giustizia e non possono essere diffusi o comunicati a terzi;

l) le immagini registrate per la rilevazione degli accessi dei veicoli ai centri storici devono rispettare l'apposito regolamento (d.P.R. 250/1999) ed essere conservate per il solo periodo necessario alla contestazione delle infrazioni.

Nel caso, invece, di impianti di videosorveglianza finalizzati esclusivamente alla sicurezza individuale (si pensi, ad esempio, al controllo dell'accesso alla propria abitazione), questi, ove perseguano effettivamente solo tale scopo, non rientrano nell'ambito di applicazione della legge sulla riservatezza, essendo il trattamento effettuato a fini personali. Le persone che possono divenire oggetto di indebiti controlli possono comunque tutelare i propri diritti dinanzi all'autorità giudiziaria. Anche in queste ipotesi vanno quindi rispettati alcuni obblighi: le riprese devono essere limitate al solo spazio antistante tali accessi, evitando forme di videosorveglianza su aree circostanti che potrebbero limitare la libertà altrui; le informazioni raccolte, inoltre, non devono essere comunicate o diffuse ad altri.

49. Impronte digitali e rilevazioni biometriche

Attraverso l'analisi delle caratteristiche biometriche (geometria del volto, della mano, dell'iride, etc.), è possibile, a distanza, acconsentire all'esecuzione di operazioni o confrontare le informazioni rilevate con quelle memorizzate in apposite banche di dati, al fine di attivare gli opportuni rimedi.

La questione tocca anche il tema della sicurezza di operazioni e transazioni e della sicurezza in determinati ambienti, avvertito soprattutto da talune categorie di aziende, in ragione della particolare natura dell'attività da esse svolta.

Anche per questi motivi l'introduzione di sistemi di lettura e/o raccolta di impronte digitali (che di regola operano contestualmente ad altre apparecchiature di rilevazione di informazioni personali, specie in forma di controllo video) è fenomeno che ha interessato, sino ad oggi, soprattutto gli istituti di credito.

Nel corso del 2000, anche su segnalazione dell'utenza (il cui grado di attenzione si dimostra crescente di fronte al diffondersi dell'uso di tecnologie sofisticate), il Garante si è occupato del problema in alcune occasioni (provvedimenti dell'11 dicembre 2000, del 7 marzo 2001 e del 28 febbraio 2001). In relazione alle modalità con le quali si sono sviluppate le prime esperienze applicative, sono emersi anzitutto tre profili:

a) un problema di rispetto del principio di proporzionalità sancito dall'art. 9 della legge n. 675/1996, tra almeno uno dei sistemi in concreto impiegati (quello di rilevazione delle impronte digitali, a volte associate ad immagini) e le finalità perseguite, essendo apparse esorbitanti, nei pochi casi esaminati, le intraprese attività indifferenziate di raccolta di dati significativi – quali le impronte associate alle immagini – imposte a tutti coloro che entrano nella banca, ivi compresi i soggetti diversi dai clienti in senso proprio, di per sé non legittimate da generiche esigenze di sicurezza non accompagnate da elementi che evidenzino una concreta situazione di rischio;

b) la tendenziale insufficienza, quando non addirittura la carenza, dell'informativa prescritta dall'art. 10 della legge n. 675/1996, tanto più vistosa se si considera la particolare natura delle informazioni personali che vengono raccolte, anche grazie a recenti acquisizioni scientifiche che in linea astratta potreb-

bero consentire di ricavare elementi conoscitivi di sicura "sensibilità" relativamente alla persona cui i dati si riferiscono. Le informative sono risultate inidonee ad avvertire gli interessati della presenza di dispositivi elettronici di rilevazione dell'impronta e dell'immagine dei clienti, come della loro eventuale associazione (effettuata contemporaneamente o successivamente all'ingresso nei locali della banca), nonché carenti delle indicazioni concernenti l'esercizio dei diritti di cui all'art. 13 della legge n. 675/1996;

c) il complessivo profilo relativo alle modalità di rilevazione e all'eventuale classificazione dei dati, al tempo di conservazione, alle misure di sicurezza, all'accesso da parte del personale interno e/o del personale di polizia.

In considerazione di ciò, il Garante ha vietato con alcuni primi provvedimenti, con effetto immediato, l'ulteriore utilizzazione dei dispositivi di rilevazione delle impronte digitali utilizzati dagli istituti di credito interessati dalle verifiche dell'Autorità, determinandone la disattivazione. Altre disattivazioni sono state comunicate da taluni istituti richiesti di fornire elementi di valutazione.

Resta da completare l'esame del delicato problema dell'individuazione di un ragionevole punto di equilibrio che salvaguardi – segnatamente dal punto di vista delle modalità da seguire in concreto – anche le istanze di sicurezza rappresentate in casi particolari da alcuni soggetti.

Il Garante ha pertanto ripreso di recente la valutazione complessiva del problema e si riserva di formulare a breve alcune ulteriori indicazioni a completamento, sviluppo ed arricchimento di quanto già affermato in precedenza.

50. Braccialetto elettronico

Particolare interesse ha destato, in un momento che ha fatto registrare un picco di crescita della domanda di sicurezza da parte dei cittadini, la controversa introduzione di forme di controllo a distanza – che comportano una massiccia attività di raccolta e trattamento di dati personali – di soggetti sottoposti alla misura cautelare degli arresti domiciliari o alla detenzione domiciliare, in attuazione di quanto disposto a seguito delle modifiche al c.p.p. e all'ordinamento penitenziario operate con d.l. 24 gennaio 2000, n. 341, emanate al dichiarato scopo di decongestionare l'apparato di vigilanza, alle prese con l'esigenza di dislocare ad altri servizi di controllo del territorio risorse umane impegnate nella sorveglianza a domicilio.

Le nuove disposizioni sono state rese operative con il già menzionato (*v. par.* 2) d.m. 2 febbraio 2001, adottato dal Ministro dell'interno di concerto con il Ministro della giustizia e pubblicato sulla *G.U.* del 15 febbraio 2001, recante "modalità di installazione ed uso e descrizione dei tipi e delle caratteristiche dei mezzi elettronici e degli altri strumenti tecnici destinati al controllo delle persone sottoposte alla misura cautelare degli arresti domiciliari nei casi previsti dall'art. 275-*bis* del codice di procedura penale e dei condannati nel caso previsto dall'art. 47-*ter*, comma 4-*bis*, l. 26 luglio 1975, n. 354".

Il decreto rappresenta un'importante testimonianza del positivo rapporto di collaborazione instauratosi tra il Garante ed altri soggetti istituzionali, che nella specie non si sono limitati a dare formale attuazione all'art. 31, comma 2, della legge n. 675/1996 (ove è stabilito che "*il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla presente legge*"), ma hanno recepito diverse indicazioni formulate dall'Autorità. Indicazioni ispirate alla necessità di contemperare le perseguite necessità di controllo con l'esigenza di evitare forme di vigilanza inutilmente oppressive, in particolare per quanto concerne il rispetto dei principi sanciti nell'art. 9 della legge n. 675/1996, con specifico riguardo alle modalità di raccolta e trattamento, alle finalità e alla durata della conservazione dei dati raccolti, nonché agli aspetti attinenti alla sicurezza delle informazioni personali, ai sensi dell'art. 15 della medesima legge e del d.P.R. n. 318/1999.

MARKETING

51. INFORMATIVA E SPECIFICITÀ DEL CONSENSO

L'innovazione introdotta dall'erompere delle tecnologie dell'informazione e della comunicazione, determinando tempi e modalità di trattamento delle informazioni una volta impensabili, ha coinvolto ormai la società nella sua interezza, con rilevanti implicazioni in relazione allo svolgimento delle attività economiche in generale e del *marketing* in particolare. Per esso, a ben vedere, si sono schiuse nuove prospettive; non solo, infatti, è ormai agevole l'elaborazione di volumi di dati personali prima difficilmente gestibili (se non a costi elevati), ma è altresì possibile rendere destinatari di flussi informativi non più una generalità indistinta di potenziali acquirenti, quanto *target* sempre più mirati di potenziale clientela, sino a giungere a forme di comunicazione individualizzata.

La rilevanza, quindi, della raccolta e dell'utilizzo dei dati personali è di tutta evidenza nel *marketing* moderno, la cui attività è tesa appunto ad offrire alle imprese informazioni, possibilmente sempre più complete, afferenti a soggetti che si ritengono compatibili, in relazione alle relative caratteristiche personali, con i beni e servizi prodotti ed offerti.

Con l'introduzione nell'ordinamento nazionale della disciplina sul trattamento dei dati personali, da un lato, i destinatari dell'attività di *marketing* (che dei loro stessi dati personali in larga misura si alimenta) hanno preso coscienza di disporre di nuovi strumenti di difesa nei confronti dei trattamenti caratterizzati da finalità pubblicitarie, promozionali e commerciali (avendo oggi il diritto di consentire in modo libero e consapevole all'uso di detti dati per tali fini, come anche di opporvisi). Dall'altro lato, anche le imprese acquisiscono sempre più coscienza del valore aggiunto che può rappresentare una banca dati di qualità e selettiva in cui siano inseriti specifici e "mirati" dati personali di coloro i quali hanno liberamente ed espressamente manifestato un consenso al trattamento, compilando questionari articolati.

Sul fenomeno, in particolare in relazione alla raccolta dei dati effettuata attraverso questionari e *coupon* mediante i quali vengono richiesti dati anagrafici, recapiti telefonici e telematici, informazioni sulle attività professionali svolte, redditi, composizione del nucleo familiare, gusti e preferenze, l'Autorità era già intervenuta alla fine del 1999 (v. Relazione per il 1999). Si è reso così evidente un ricorso crescente a tali tecniche in numerosi settori merceologici e si è constatato che detta raccolta non è sempre svolta conformemente alla normativa sulla protezione dei dati personali.

I rilievi critici riguardano soprattutto l'informativa all'interessato, spesso mancante o inidonea (per incompletezza o inesattezza) a rendere conto compiutamente delle modalità e delle finalità del trattamento effettuato, riflettendosi così sulla validità delle dichiarazioni di consenso rilasciate.

In un provvedimento a carattere generale emesso il 13 gennaio 2000, trasmesso anche ad organismi, istituzioni ed organizzazioni dei settori interessati, sono state pertanto fornite precise indicazioni alle quali si è conformata nel corso dell'anno l'attività di verifica del Garante.

In ordine a ciò sono stati altresì emessi provvedimenti *ad hoc* nei quali si è di volta in volta segnalata la necessità di: *a)* apportare modifiche alla clausola di informativa e consenso presente nei modelli utilizzati; *b)* correggere l'impostazione seguita da società che esercitano, in particolare, attività di *telemarketing* (*Provv.* 14 settembre 2000) e che non forniscono l'informativa agli interessati contattati telefonicamente neppure al momento della promozione, pur essendo tenute ad indicare le principali caratteristiche del trattamento dei dati, anche se temporaneo (si è evidenziato in tal caso che il mancato rispetto delle disposizioni sull'informativa agli interessati, di cui all'art. 10 della legge n. 675/1996, comporta l'illiceità del trattamento e, tra l'altro, la violazione amministrativa prevista dall'art. 39, comma 2, della legge medesima); *c)* richiedere il consenso all'interessato rispetto ad ulteriori ed eventuali trattamenti promozionali ed alla comunicazione a terzi dei dati con una formula "in positivo", anziché "in negativo", ovvero dando per presupposto il consenso salvo eventuale diniego.

Gli stessi principi sono stati poi estesi a società che effettuano selezione del personale e che, nello svolgimento della propria attività, raccolgono *curricula* anche tramite annunci riportati su quotidiani o periodici, realizzando in tal modo una raccolta di dati personali; pure in questa evenienza si rende infat-

ti necessario assolvere all'obbligo di informativa nei termini più volte indicati dal Garante, considerando che, in caso di inottemperanza, le dichiarazioni di consenso spesso richieste (e rese) per i *curricula* sono da ritenersi invalide.

Nel giugno del 2000 il Garante, sempre al fine di fornire indicazioni riguardo all'esatto adempimento della normativa sulla protezione dei dati personali, ha svolto due audizioni con operatori direttamente interessati ai provvedimenti sopra richiamati e con organismi ed associazioni operanti nei settori maggiormente coinvolti.

Nella prima audizione, gli operatori hanno formulato un giudizio positivo e di condivisione delle indicazioni fornite dal Garante in ordine al contenuto e alle modalità di predisposizione dell'informativa, soprattutto per quanto concerne l'esigenza di completezza, semplificazione, sintesi e chiarezza delle informazioni. In tale sede, sono stati forniti ulteriori chiarimenti, in particolare sui seguenti aspetti:

– elementi essenziali da riportare nell'informativa, contemperando le esigenze di sintesi e di semplicità;

– indicazione delle categorie dei soggetti a cui i dati sono comunicati, evitando la generica formula *"aziende di nostra fiducia"*;

– eliminazione della richiesta di consenso per i trattamenti derivanti dall'esecuzione di obblighi di natura contrattuale o dall'acquisizione di informative precontrattuali su richiesta degli interessati;

– inidoneità di alcune correnti formule di consenso con riferimento ai trattamenti svolti da altre società destinatarie dei dati.

In particolare il Garante ha ribadito l'esigenza che il consenso degli interessati, per essere validamente manifestato, deve essere espresso, libero e specifico. Le disposizioni vigenti, infatti, richiedono l'acquisizione e la documentazione per iscritto dell'atto di assenso al trattamento dei dati da parte dell'interessato.

Nella seconda audizione, le associazioni di categoria hanno manifestato la propria disponibilità a costituire un gruppo di lavoro sulle problematiche applicative della legge n. 675/1996 nel settore del *direct marketing*, che potrebbe curare anche la predisposizione di linee-guida e modelli semplificati utilizzabili dalle società associate. In particolare, una di queste ha segnalato l'esigenza di distinguere tra le vere e proprie ricerche di mercato, svolte dai propri associati (i quali acquisirebbero dati personali solo nella fase iniziale, mediante interviste effettuate previo consenso degli interessati, con una loro successiva analisi o divulgazione in forma anonima ed aggregata secondo metodi statistici e scientifici), e le indagini di *marketing* eseguite tramite modulistica analoga a quella esaminata dal Garante, che avrebbero invece la finalità di "profilazione" dei comportamenti delle persone, ricerca di clientela e gestione delle relative banche dati.

In materia, quindi, l'Autorità persevera nella propria opera volta, da un lato, a sensibilizzare gli operatori di settore e, dall'altro, a vigilare per assicurare il rispetto delle disposizioni sulla tutela del trattamento dei dati personali.

Il Garante apprende poi con soddisfazione che emerge progressivamente un moderno concetto di *marketing*, finalizzato a prestare al consumatore un servizio attraverso forme selettive di consenso, più rispettose della personalità degli interessati, nelle quali l'elemento di adeguata informativa è prevalente rispetto al mero profilo promozionale e pubblicitario.

COMMERCIO ELETTRONICO

52. PROFILI GENERALI E LINEE DI TENDENZA

Dei vari argomenti coinvolti dalla problematica riguardante la tutela dei dati personali, due presentano particolari aspetti di ampiezza e di costante mutevolezza: l'incidenza nei confronti del commercio elettronico e del *direct marketing* (1).

La globalizzazione dei mercati coincide con quella delle reti telematiche di comunicazione anche interattiva. Assistiamo a modifiche di tecniche contrattuali per la vendita dei prodotti, nonché all'evoluzione di tecniche informative e promozionali degli stessi prodotti, in forme sempre più personalizzate.

Da un lato emerge la necessità di standardizzare le tecniche contrattuali al fine di automatizzare un numero crescente di affari e dall'altra preme la contemporanea esigenza di personalizzare gli approcci promozionali dell'offerta. Ciò comporta una costante attenzione da parte di autorità garanti come il Garante italiano, che assumono una caratteristica peculiare: di essere, nel medesimo tempo, applicatrici del diritto e creatrici di "giurisprudenza", ma anche sollecitatrici di tempestivi adeguamenti legislativi a causa dell'incalzare delle innovazioni di prodotto e di processo.

In un mondo sempre più interconnesso e quindi globalizzato dalla velocità delle conoscenze e dal movimento degli uomini, capitali, merci e servizi, l'aumento globale del valore aggiunto è direttamente proporzionale all'aumento della velocità e della quantità degli scambi. Tutto ciò si riflette nell'aumento della quantità dei beni prodotti e, quindi, nella riduzione dei costi di produzione, nonché nella dilatazione delle utilità – e conseguentemente di rischi – per utenti e consumatori.

Le problematiche relative alla tutela dei dati personali e riguardanti la trasparenza e correttezza del loro uso sia in sede di offerta di prodotti, sia in sede di conclusione ed esecuzione contrattuale nelle compravendite, sono destinate ad incidere sempre più nell'immediato futuro e ciò è legato anzitutto alla diffusione dei *personal computer* ed ai collegamenti Internet.

Dall'indagine pubblicata di recente dalla X Commissione attività produttive della Camera dei deputati sul commercio elettronico, si apprende che gli utenti Internet a livello mondiale nel luglio del 2000 erano già 360 milioni (2). Per quanto riguarda l'Europa, alla stessa data il numero degli utenti era di 95 milioni ed è previsto che salirà a 140 milioni nel 2003.

Già ora in Italia il 32% delle famiglie possiede un *personal computer* e si stima che circa 14 milioni di individui, pari al 25% della popolazione, abbia navigato in Internet nell'ultimo trimestre del 2000. Si prevede che tale numero raddoppierà nel 2003.

Da questi dati ci rendiamo facilmente conto come, nel prossimo futuro, l'incidenza della problematica riguardante la tutela della *privacy* aumenterà ancora, impegnando da un lato l'adeguamento legislativo e, dall'altro, l'attività giurisprudenziale e di indirizzo del Garante italiano.

Il problema che si pone è quello di garantire libertà di sviluppo ai mercati riducendo al minimo i vincoli e gli adempimenti e garantendo, dall'altro, la necessaria tutela ai diritti fondamentali dell'individuo. Si tratta dunque di una vera e propria navigazione tra Scilla e Cariddi, tra la libertà di intraprendere e i diritti di riservatezza del singolo.

Per quanto riguarda il valore del commercio elettronico in Europa si stima che nei prossimi quattro anni passerà da 25 a 510 miliardi di euro, cioè dagli attuali 50 mila miliardi di lire ad oltre un milione di miliardi di lire.

---

(1) Il presente paragrafo riproduce ampi brani dell'intervento del prof. Gaetano Rasi, componente del Garante, al convegno su "Diffusione dell'e-commerce, tecniche di direct marketing e protezione dei dati", tenutosi a Roma in occasione del Forum P.A. del 7-11 maggio 2001.

(2) Camera dei Deputati, Servizio Commissioni indagini conoscitive e doc. leg.va, n. 40, "Il commercio elettronico", X Commissione, Atti parlamentari, XIII Legislatura. All'indagine ha preso parte anche il prof. Rasi prima della elezione quale componente del Garante.

aumento del 42% sullo stesso dato mensile dell'anno precedente. Tutto ciò sembra dunque dare adito a considerazioni riguardanti una espansione del sistema purché, naturalmente, vi siano condizioni favorevoli e non ostative.

Un recente studio curato dal Gruppo dei Garanti europei (*Privacy on the Internet, An integrated approach to on-line data protection*, menzionato nella documentazione allegata alla presente Relazione), relativo anche al fenomeno dello *spamming* (ossia dei messaggi di posta elettronica contenenti comunicazioni pubblicitarie indesiderate), ha posto in luce dati secondo cui il fenomeno stesso negli USA sarebbe in declino perché gli stessi operatori preferiscono ricorrere ad attività di *marketing* più corrette anche in termini di protezione dei dati. Si allude all'introduzione del concetto di *marketing* su autorizzazione, ossia l'istituzione di canali di comunicazione con i consumatori su base volontaria passando per gradi da un rapporto fondato sull'interesse ad un rapporto basato sulla fiducia.

Con il crescere della fiducia, il consumatore viene convinto ad autorizzare una gamma sempre più ampia di attività di *marketing*, raccolta di dati sulle abitudini di vita, su *hobbies* e interessi, invio di messaggi pubblicitari relativi a nuovi prodotti e servizi, ecc. Questo tipo di *marketing* basato su un approccio di "*opt-in*" (ossia, sulla possibilità per il cliente di scegliere se aderire o meno) è espressione di una parola d'ordine crescente fra gli operatori del settore negli USA (che permette probabilmente di superare le conclusioni dell'ultimo rapporto su Internet redatto dall'USIC-*United States Internet Council*-, contenente una serie di raccomandazioni ai Governi, tra cui quella secondo cui una rete soggetta ad eccessive restrizioni – anche in materia di *privacy* – renderebbe impossibile il commercio elettronico).

Il marketing basato su un approccio di "*opt-in*", dopo essere stato la parola d'ordine degli operatori americani può diventare anche l'approccio più adatto ad una prassi europea, conformemente alle norme giuridiche che vanno già in questa direzione in diversi Stati membri tra cui l'Italia.

Quattro sono attualmente gli strumenti comunitari rilevanti: *a)* la direttiva generale sulla protezione dei dati (95/46/CE); *b)* la direttiva sulle telecomunicazioni (97/66/CE); *c*) la direttiva sulle vendite a distanza (97/7/CE) e *d)* la direttiva sul commercio elettronico (2000/31/CE).

Le direttive non sono pienamente armonizzate tra loro (le prime due, ed in parte anche la terza, adottano un approccio sostanzialmente basato sull'*opt-in*, mentre quella sul commercio elettronico sembra favorire un approccio di tipo *opt-out*). Si è creata così una qualche ambiguità di fondo, posta in evidenza anche dagli estensori dello studio da ultimo citato, che non facilita l'individuazione di condotte chiare ed univoche da parte delle imprese che operano in questo settore. Alcune disposizioni riguardano poi solo la legittimità dell'invio di comunicazioni commerciali indesiderate nell'ambito di determinate relazioni *business-to-consumer* o *business-to-business*, e non disciplinano a monte la più complessa questione della raccolta e del trattamento dei dati personali.

Non vi sono, tuttavia, rilevanti conflitti di tipo giuridico, giacché la direttiva n. 2000/31/CE (e tale aspetto dovrà essere tenuto presente all'atto del suo recepimento in Italia) non si applica nei settori disciplinati dalle due citate direttive sulla protezione dei dati.

Occorrerà però grande attenzione nell'interpretare ed armonizzare sul piano applicativo questo complesso di regole.

Per eliminare le menzionate ambiguità occorre anche che il dibattito si sposti dalla mera correttezza dell'invio di messaggi pubblicitari alla liceità e correttezza della raccolta di dati.

Esplicitando le circostanze in cui è possibile raccogliere legittimamente dati personali (come l'indirizzo di *e-mail*), l'operatore commerciale ed il destinatario dell'*e-mail* possono già scegliere in modo trasparente la natura e gli sviluppi futuri del rapporto instauratosi.

Appare poi naturale estendere su scala europea al *marketing* diretto via *e-mail* le stesse regole valide per il *marketing* diretto effettuato attraverso dispositivi automatici di chiamata o *fax* – poiché in entrambi i casi si tratta di attività di natura invasiva che non possono essere interrotte dai destinatari.

Alcune prime considerazioni conclusive e riassuntive sembrano quindi possibili:

1) la tutela della riservatezza non solo non contrasta, ma costituisce il necessario presupposto per lo sviluppo del commercio elettronico.

2) sempre più spesso gli utenti ed i consumatori scelgono l'operatore o il fornitore di servizi a cui si rivolgono tenendo conto della politica in materia di *privacy* da questo adottata. Ciò fa sì che oggi l'adozione di pratiche rispettose dei diritti delle persone sia divenuta un fattore stesso – importante – di concorrenza fra gli operatori del settore.

Sempre nella stessa indagine della X Commissione della Camera dei Deputati, si prevede che per l'Italia, nel periodo 1999-2004 le vendite *on-line* passeranno da 1,8 a 53 miliardi di euro, ossia da 3.600 miliardi di lire a oltre 110 mila miliardi di lire.

In cifre individuali gli acquirenti via Internet dovrebbero passare da meno di 1 milione di fine 1999 a circa 10 milioni dell'inizio del 2004.

Attualmente il 65% delle transazioni elettroniche riguarda il *business to business* ed il 35% del *business to consumer*. Si prevede che alla fine del 2003 il *business to business* raggiungerà un peso percentuale pari al 77%. In altre parole sono soprattutto le aziende ad usarlo fra loro, piuttosto che il cliente finale.

Questi dati corrispondono con altro recente studio – curato dall'IPSOS – il quale indica addirittura che vi sarebbe una generale tendenza da parte del pubblico dei consumatori a non sviluppare il commercio elettronico. Nel 1999 a livello europeo infatti il 27% degli intervistati dichiarava di voler fare a breve un acquisto via Internet mentre, alla distanza di un anno, la percentuale è scesa al 20% (i francesi dal 48% delle intenzioni di acquisto sono passati al 16%; gli inglesi dal 24% al 16%; i portoghesi dal 42% al 31%; gli italiani dal 31% al 25%).

Comunque, si tratti di commercio tra imprese o di vendite ai consumatori, il problema riguarda non solo i dati relativi ai mezzi di pagamento utilizzati (carta di credito), ma anche le altre informazioni personali quali, per esempio, i gusti presumibili dai consumi abituali. E ciò non direttamente nei confronti dei consumatori, ma attraverso i loro fornitori che acquistano i dati elaborati da terzi. Sono tutti dati utilizzati per definire il profilo dei clienti ai fini del *marketing*.

Mentre inizialmente – da parte di coloro che si pongono come ditte fornitrici – si era registrato un atteggiamento di diffidenza nei confronti delle disposizioni poste a tutela della riservatezza, successivamente si è potuto riscontrare un progressivo mutamento di posizioni.

Oggi sono sempre più gli operatori che comprendono l'importanza di instaurare con gli utilizzatori – ossia con altre imprese e pure con i consumatori – un rapporto impostato in termini di lealtà e trasparenza nell'uso dei loro dati personali.

Dobbiamo constatare che progressivamente si avverte la necessità di passare da sistemi di raccolta occulta dei dati ad altri che prevedono l'informazione preventiva del consumatore sui trattamenti, consentendogli di prestare, al riguardo, forme differenziate di consenso.

Si realizza così un sistema per il quale il destinatario dei prodotti e dei servizi è in grado di valutare esplicitamente i vantaggi, in termini di informazione, assistenza, servizi aggiuntivi che possono derivare all'interessato proprio da un corretto utilizzo dei suoi dati.

Tutto questo non costituisce solamente un modo per attrarre più consumatori, evitando di "spaventarli" attraverso pratiche eccessivamente aggressive di raccolta dei dati e successivo trattamento ai fini di *marketing*. Ma anche la sola via per ottenere dagli stessi consumatori informazioni attendibili, evitando che essi – secondo quanto a volte accade – ricorrano a forme di "difesa" basate sul conferimento di dati errati. Col risultato di vanificare le strategie di *marketing* adottate.

Le considerazioni fatte spiegano anche perché le politiche della *privacy* in materia di commercio elettronico siano oggi divenute uno strumento di competizione fra i diversi operatori. Ossia un elemento ulteriore per caratterizzarsi di fronte ai consumatori, conquistandone la fiducia e mantenendola nel tempo.

Una prima soluzione proposta è già sul tappeto e riguarda l'adozione del marchio internazionale di garanzia a tutela dei consumatori *on-line* e rientra nelle iniziative riguardanti il commercio elettronico della Commissione dell'Unione Europea. La *Better Business Bureau on-line* (*BBB on-line*) ed *Eurochambres* (*Association of european chambers of commerce and industry*), come molti altri soggetti, hanno ad esempio proposto un primo marchio di fiducia internazionale, che dovrebbe attestare che l'impresa che lo espone *on-line* aderisce a specifici standard commerciali e garantisce il rispetto di un codice di condotta nella risoluzione di eventuali controversie.

La correttezza e riuscita di queste iniziative dipende tra l'altro dalla scelta dei parametri per il rilascio del "marchio": assai utile, in tal senso, è la serie di prescrizioni contenute nella recente Raccomandazione sui requisiti minimi per la raccolta di dati attraverso siti *web*, approvata dai Garanti europei e riportata nella documentazione allegata alla presente Relazione.

Passando al *direct marketing* va osservato che l'andamento della pubblicità via Internet e la collaterale attività di vendita on-line ha subito negli USA una crescita: a febbraio di quest'anno si è avuto un

3) anche al di là di ogni considerazione sui profili inerenti alla protezione dei diritti fondamentali delle persone, le pratiche troppo aggressive di *marketing* via Internet si rivelano inefficaci e controproducenti per chi le attua sul piano della riuscita commerciale (rifiuto generalizzato nei confronti del cosiddetto *spamming*).

4) il conferimento all'utente di un'informativa completa ed esauriente sui trattamenti che verranno svolti sui suoi dati, ed il riconoscimento a questi della facoltà di dare il proprio consenso informato ai trattamenti medesimi costituiscono ormai un presupposto necessario anche per chi intenda perseguire una politica di fidelizzazione dei clienti nel tempo.

53. CASI APPLICATIVI

Il Garante ha concluso nel corso del 2000 un primo monitoraggio di alcuni siti *web* volto ad accertare le modalità di informativa degli utenti e di raccolta del consenso, ove necessario.

Sulla base di una circostanziata segnalazione di un'associazione di consumatori, l'Autorità ha avviato di recente un'ulteriore serie di verifiche con particolare riguardo ai c.d. "trattamenti invisibili" che sarebbero effettuati da altri siti *web*, nonché relativamente all'informativa per finalità di *marketing* e di commercio elettronico, alla c.d. profilazione di clienti anche in relazione a dati sensibili.

Gli accertamenti verranno conclusi – e abbinati ai risultati del predetto monitoraggio – applicando i principi in materia di esauriente informativa e di libero e consapevole consenso richiamati nei par. 51 e 55 della presente Relazione in relazione al *marketing*, al *telemarketing* e alle reti di telecomunicazione e telematiche.

Numerosi altri procedimenti sono in corso per specifiche violazioni segnalate da persone che ricevono *e-mail* indesiderate – a volte, addirittura in presenza di un'espressa opposizione – o fax anche a ripetizione, nell'inosservanza dei principi di cui, in particolare, al d.lg. n. 171/1998 e al d.lg. n. 185/1999.

RETI TELEMATICHE E SERVIZI DI TELECOMUNICAZIONE

54. PROFILI GENERALI

L'universo delle telecomunicazioni e, al suo interno, il settore della telefonia e delle reti informatiche è stato oggetto di particolare attenzione da parte del Garante anche nel corso del 2000: numerose sono state invero le segnalazioni pervenute, a dimostrare la particolare sensibilità dell'opinione pubblica e a testimoniare la crescente familiarità dei cittadini con l'utilizzo delle tecnologie dell'informazione.

L'evoluzione tecnologica in questo settore, notoriamente, mentre rende disponibili nuovi servizi e funzioni di interesse per i cittadini, evidenzia al contempo i rischi collegati ad una pervasiva ed automatica raccolta di dati personali. Laddove, poi, ciò avviene attraverso l'offerta agli utenti di prestazioni gratuite in cambio dell'uso delle informazioni, raccolte senza una esauriente informativa ed impiegate ormai come una vera e propria merce di scambio, è evidente la necessità di assicurare garanzie ancor più adeguate a tutela della sfera privata, dell'identità e della dignità personale.

Emerge, così, il ruolo centrale delle normative a tutela della riservatezza, anche in relazione alla possibilità che i dati raccolti siano utilizzati per operare classificazioni sempre più sofisticate di utenti e consumatori, anche al fine di porre ciascuno in grado di esercitare consapevolmente la propria facoltà di scelta. Occorre infatti considerare che ad una crescente alfabetizzazione degli utenti in riferimento all'uso dei principali servizi di telecomunicazione, non sembra ancora affiancarsi un'adeguata informazione rispetto ai meccanismi di funzionamento ed all'utilizzo delle informazioni trattate da fornitori e gestori nel corso dell'erogazione.

Anche nell'anno trascorso, perciò, l'attività del Garante è stata rivolta soprattutto alla verifica della conformità delle modalità di attivazione ed erogazione dei servizi di telecomunicazione alla normativa sulla protezione dei dati, anche attraverso l'opportuna attività di informazione e di divulgazione generale indirizzata agli operatori e agli utenti, con particolare riguardo ad Internet ed ai servizi di telefonia fissa e mobile.

Nel quadro delle sue competenze nell'ambito del Gruppo europeo delle autorità garanti istituito dall'art. 29 della direttiva n. 95/46/CE, e dei gruppi di lavoro presso il Consiglio dell'Unione europea, il Garante partecipa inoltre attivamente alla rielaborazione del quadro europeo della direttiva in materia di protezione dei dati personali nei servizi di telecomunicazione, attualmente in corso ad opera del Consiglio e del Parlamento europeo.

55. TRASPARENZA E CORRETTEZZA VERSO GLI UTENTI INTERNET

Proprio con riferimento ad Internet si può cogliere con maggiore nettezza il fatto che da strumento di isolamento dagli altri, quale diritto ad essere lasciati soli, la *privacy* si trasforma in strumento di controllo dinamico e di comunicazione. Allo stesso modo, nell'area del commercio elettronico, la riservatezza diventa lo strumento attraverso il quale, con fiducia, l'utente accede all'acquisto di beni o di servizi, con la garanzia che quelle informazioni non verranno impropriamente utilizzate, fatte circolare, elaborate per costruire profili della personalità che potrebbero avere anche effetti discriminatori.

Attualmente è assai difficile utilizzare Internet senza doversi misurare con pratiche invasive della *privacy* individuale ed operazioni di trattamento dei dati personali effettuate con modalità tali da restare invisibili all'interessato. In altre parole, l'utente Internet non sa spesso che i suoi dati personali sono stati raccolti e successivamente elaborati e che potrebbero essere utilizzati per scopi a lui non resi noti. L'interessato per lo più non sa nulla di tale trattamento e non può, di riflesso, assumere decisioni "libere" al riguardo. Il Gruppo europeo dei garanti si è non a caso espresso sulla questione già nel Parere n. 1/1999 del 23 febbraio 1999, incoraggiando l'industria del *software* e dell'*hardware* a lavorare su prodotti Internet rispettosi della *privacy*, fornendo i necessari strumenti per conformarsi alla normativa europea sulla protezione dei dati.

Una prima condizione per un trattamento lecito dei dati personali è che il soggetto dei dati sia informato e messo compiutamente al corrente del trattamento in questione. Il Gruppo si è quindi particolarmente interessato a tutti i tipi di operazioni di trattamento attualmente effettuate da *software* ed *hardware* su Internet privi di queste caratteristiche.

In questa materia anche la CNIL (*Commission nationale pour l'informatique et les libertés*) francese ha svolto una preziosa ricerca, concentrandosi soprattutto sul trattamento automatico ed invisibile dei dati personali attraverso *software* ed *hardware* nel corso della navigazione su Internet. La ricerca è stata presentata al Garante, nello spirito di collaborazione che anima l'operato delle autorità europee, nell'ambito di un seminario svoltosi il 13 novembre 2000 presso la sede dell'Autorità.

Sul versante dell'attività interna, il Garante è intervenuto per valutare le procedure di corretta e trasparente acquisizione e di pertinente trattamento dei dati da parte dei fornitori di servizi di accesso ad Internet. L'Autorità aveva avviato già nel luglio del 1999 un procedimento di indagine nei confronti del servizio di accesso gratuito ad Internet ("*Libero*" di Infostrada), a seguito di diverse segnalazioni concernenti l'acquisizione, al momento dell'attivazione del servizio, di varie informazioni personali, nonché il successivo monitoraggio delle connessioni ai siti visitati dagli abbonati, allo scopo dell'individuazione delle loro preferenze per determinare il profilo dei fruitori del servizio, o per programmare l'invio di messaggi *e-mail* a sfondo pubblicitario (v. Relazione per l'anno 1999, p. 72).

Al termine di un'approfondita istruttoria, nel corso della quale è stato affrontato il tema della raccolta e dell'utilizzazione di dati personali nell'ambito di servizi di accesso gratuito ad Internet offerti dagli operatori nel settore delle telecomunicazioni, il Garante ha indicato alla società titolare del trattamento alcune modalità necessarie ad assicurare la liceità e la correttezza dei comportamenti nei confronti degli utenti (*Provv.* del 13 gennaio 2000).

Il Garante ha chiarito che, fermo restando il rispetto della volontà dei cittadini di consentire alla cessione di dati identificativi o attinenti a gusti, preferenze ed interessi, in particolare per ottenere gratuitamente determinati servizi, gli interessati devono, comunque, essere messi in grado di esprimere le proprie scelte sull'uso dei dati che li riguardano, consapevolmente e liberamente. Per questo è anzitutto necessario che essi ricevano tutte le informazioni necessarie per la piena comprensione delle finalità e delle modalità di trattamento dei dati, compresi quelli acquisiti in un momento successivo – giacché l'obbligo di informazione al cliente permane, anche quando non venga richiesto alcun consenso –, dovendosi verificare attentamente se taluni dati, indicati come asseritamente "obbligatori" dalle società del settore, siano realmente indispensabili per attivare e mantenere il servizio principale offerto.

In particolare, le segnalazioni pervenute al Garante avevano prospettato un contrasto con la normativa, sia sotto l'aspetto dell'insufficienza delle informazioni fornite agli interessati, sia riguardo alla possibilità di raccogliere dati sui siti frequentati e di controllare l'effettiva lettura, da parte degli abbonati, dei messaggi pubblicitari inviati dalla società.

Nel corso del procedimento, la società titolare ha peraltro provveduto ad eliminare alcune incongruenze ed anomalie presenti nella documentazione sottoposta al potenziale cliente all'atto dell'iscrizione, specificando che l'analisi degli accessi ai siti *web* sarebbe stata svolta tra quelli presenti in un catalogo predisposto dalla stessa società, in modo da evitare il riferimento a siti dal cui contenuto fosse possibile ricavare il riferimento a dati sensibili, e negandosi, d'altra parte, che fosse effettuata alcuna verifica circa il ricevimento e la visualizzazione dei messaggi pubblicitari da parte degli utenti.

Nel provvedimento finale il Garante ha tuttavia ritenuto necessaria l'ulteriore revisione di alcuni profili relativi alle informazioni e ai documenti sottoposti ai clienti all'atto della richiesta dell'attivazione del servizio, fornendo al riguardo diverse indicazioni che debbono ritenersi estensibili a tutti gli operatori che offrono servizi analoghi.

In particolare si è segnalato che l'informativa, riferita a tutti gli aspetti del complessivo trattamento svolto dal fornitore nell'ambito del servizio (attraverso la riepilogazione chiara delle notizie ad esso attinenti presenti nel contratto, nonché integrata con un richiamo, anche sintetico, ai diritti di accesso attribuiti agli interessati dall'art. 13 della legge n. 675/1996, con l'indicazione dell'ufficio o servizio presso cui esercitare tali diritti), deve essere collocata prima della richiesta di registrazione dei propri dati.

L'obbligo di informazione impone inoltre di precisare tutte le categorie di ulteriori soggetti ai quali potranno essere comunicate le informazioni raccolte e che dovrebbero, a loro volta, acquisire il consenso degli interessati, salvo che sia la prima società titolare del trattamento a richiedere il consenso dei clienti anche per conto delle successive, fornendone una precisa indicazione, anche predisponendo un elenco a parte da rendere agevolmente consultabile per gli interessati.

La richiesta del consenso nei confronti degli abbonati che abbiano accettato le condizioni contrattuali, autorizzando l'invio di messaggi pubblicitari sulla propria casella di posta elettronica, pur potendo essere circoscritta alle sole operazioni di trattamento dei dati per finalità commerciali non collegate al servizio ed alla loro divulgazione all'esterno, dovrebbe essere poi riferita anche alle disposizioni in materia di pubblicità e di chiamate indesiderate, introdotte dalle recenti normative sulla riservatezza delle telecomunicazioni (d.lg. n. 171/1998) e sui contratti a distanza (d.lg. n. 185/1999).

Riguardo ai dati acquisiti con i moduli di adesione al servizio, il Garante ha segnalato la necessità di rendere ben edotti gli interessati che determinate informazioni sono, poi, raccolte non in virtù di specifici obblighi normativi (non ravvisabili nella mera opportunità di rendere accessibili alcune informazioni sugli abbonati ad organi ed autorità preposte ad indagini ipoteticamente interessate in futuro a raccoglierle), quanto in vista dell'intenzione del fornitore di procedere al trattamento sulla base di un'autonoma scelta di caratterizzazione del servizio, anche quando l'abbonato non presti il consenso a trattamenti e comunicazioni per finalità commerciali.

Inoltre, in relazione agli aspetti connessi ai dati relativi ai siti consultati dagli abbonati, il Garante ha confermato la necessità che si assumano tutte le misure idonee ad evitare una raccolta di informazioni sensibili.

Nel fornire tali indicazioni, il Garante ha segnalato la necessità di fornire a ciascun utente già abbonato al servizio il nuovo testo di informativa messo a punto per i nuovi clienti e rispettoso della normativa sulla protezione dei dati personali, assicurando ai vecchi abbonati la possibilità di esprimere nuovamente il consenso o di revocare attraverso un meccanismo agevole le precedenti manifestazioni di volontà.

L'Autorità ha altresì disposto che copia del provvedimento fosse trasmessa anche agli altri operatori che offrono servizi analoghi, allo scopo di sensibilizzarli al maggior rispetto della normativa vigente.

Sotto altro profilo, è emerso che la diffusione crescente delle connessioni onerose o gratuite ad Internet, unitamente alla maggiore attenzione rivolta al potenziale mercato degli utenti telematici da parte delle imprese e delle associazioni, comporta talvolta frizioni tra l'interesse alla comunicazione pubblicitaria, la libertà di manifestazione del pensiero ed il diritto alla riservatezza, che vengono portate all'attenzione dell'Autorità.

Nell'anno trascorso, si è potuto ad esempio assistere ad un incremento dell'utilizzo dei sistemi informatici e di telefonia fissa e mobile per finalità di comunicazione politica e di propaganda elettorale, con l'impiego di metodologie non sempre conformi alla normativa vigente sulla tutela delle informazioni personali. Ci si trova in questi casi, in rete, di fronte all'esigenza di tutelare due diversi interessi: da una parte quello di chi comunica; dall'altra l'interesse di chi, essendo destinatario della comunicazione, ha diritto di preservare la propria sfera privata difesa da ingiustificate invasioni altrui.

Come già riferito in altro paragrafo, in data 15 novembre 2000 il Garante ha avviato accertamenti per verificare la fondatezza di una segnalazione relativa ad un trattamento di dati effettuato dall'Osservatorio sulla legalità e la questione morale, in relazione alla ricezione non gradita di un messaggio di posta elettronica proveniente dal sito dell'associazione.

Sulla base dei riscontri effettuati e degli elementi forniti dall'Osservatorio, la segnalazione non è poi risultata fondata. Si è accertato, infatti, che il messaggio oggetto della segnalazione, non era stato inviato direttamente dall'Osservatorio o dal relativo sito, ma da un privato che aveva ritrasmesso la *newsletter* dell'Osservatorio ad un limitato numero di destinatari, nel quadro di una probabile attività interpersonale di informazione.

Il Garante, constatando che i documenti sottoposti all'utente all'atto dell'adesione non erano pienamente conformi alla normativa, ha però proceduto, sulla base della documentazione acquisita, a segnalare autonomamente all'Osservatorio, ai sensi dell'art. 31, comma 1, lett. c), della legge n. 675/1996, la necessità che l'informativa e la formula di consenso inserite sul sito, in calce al modulo di adesione all'Osservatorio, fossero riformulate in modo da contenere, anche sinteticamente e con eventuale stile colloquiale, tutti gli elementi richiesti dall'art. 10 della legge n. 675/1996.

La Raccomandazione sulla raccolta di dati personali

Il 17 maggio 2001 Il Gruppo delle autorità per la protezione dei dati dell'Unione europea, presieduto da Stefano Rodotà, ha adottato una Raccomandazione (n. 2/2001, riprodotta nella documentazione allegata), indirizzata al Consiglio d'europa, alla Commissione, al Parlamento europeo ed agli Stati membri, che fissa alcuni requisiti minimi per la raccolta di dati personali *on-line*.

La Raccomandazione nasce dall'esigenza di fornire indicazioni concrete sia agli operatori del settore responsabili del trattamento di dati personali nell'ambito di siti *web* (i "titolari", secondo la definizione della direttiva), sia ai singoli cittadini. Essa è rivolta anche agli enti che intendono creare un "bollino di qualità" che certifichi la rispondenza delle procedure di trattamento utilizzate alle direttive dell'Ue in materia.

L'aspetto significativo risiede anzitutto nella distinzione tra un primo gruppo di notizie che ciascun sito deve fornire a tutti i visitatori, in modo snello e visibile, ed un nucleo più articolato di informazioni che il sito può fornire in altre pagine *web* evidenziando l'intera *privacy policy* del sito stesso.

Le indicazioni riguardano, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari devono fornire agli utenti quando questi si collegano a pagine *web*, indipendentemente dagli scopi del collegamento. I Garanti sottolineano che i requisiti indicati rappresentano solo un nucleo "minimo" e che potranno essere integrati, in futuro, da ulteriori raccomandazioni di natura più specifica (ad esempio, per quanto riguarda il trattamento di dati "sensibili" o relativi a minori, oppure i trattamenti per scopi di natura sanitaria).

La Raccomandazione si applica a tutti i trattamenti effettuati da titolari che siano stabiliti in uno degli Stati dell'UE, oppure che non siano stabiliti nell'UE, ma utilizzino, ai fini del trattamento, apparecchiature o dispositivi situati sul territorio di uno Stato membro dell'UE.

I Garanti raccomandano pertanto:

– di fornire preventivamente a chiunque si colleghi ad un sito *web* che preveda la raccolta di dati personali le informazioni indicate nella direttiva: identità e indirizzo (elettronico o meno) del titolare; finalità del trattamento; "obbligatorietà" del conferimento delle informazioni richieste all'utente (vi possono essere dati necessari per fornire un servizio richiesto da un utente, mentre altri sono opzionali); modalità per esercitare i diritti di accesso, rettifica, cancellazione, opposizione al trattamento; destinatari eventuali delle informazioni raccolte (e in tal caso l'utente deve avere la possibilità di opporsi alla trasmissione dei suoi dati ad altri soggetti, per scopi diversi da quelli per cui gli vengono richiesti dal sito – ad esempio cliccando su una specifica casella); eventuale utilizzo di procedure automatiche per la raccolta dei dati (è il caso, ad esempio, dei *cookies*); misure di sicurezza adottate per garantire l'integrità e la riservatezza dei dati richiesti;

– di fornire le informazioni sopra elencate direttamente sul *monitor* del singolo utente, prima che avvenga la raccolta dei suoi dati, così da garantire che il trattamento avvenga in modo leale come prescrive la direttiva; per farlo si può ricorrere alle varie possibilità messe a disposizione dalle attuali tecnologie: finestre "a scomparsa", caselle da cliccare, messaggi "*pop-up*". È opportuno inoltre che sulla pagina di accoglienza del sito vi sia un'indicazione chiara e comprensibile dell'esistenza di un'informativa sulla *privacy* (ad esempio: "Questo sito raccoglie e tratta dati personali che la riguardano. Per ulteriori informazioni, clicchi qui");

– di tenere presente che i titolari hanno anche altri obblighi sanciti sempre dalla direttiva, oltre al dovere di informare adeguatamente gli interessati. In particolare, è necessario che la raccolta di dati personali sia necessaria per le finalità specificate: pertanto, se l'obiettivo che il titolare si prefigge (fornire un servizio, un'informazione, ecc.) può essere raggiunto senza elaborare dati personali, questi non devono essere raccolti. Nella stessa ottica, si sottolinea l'opportunità di favorire ed accettare l'impiego di pseudonimi quando questi ultimi permettano comunque di svolgere determinate transazioni. Inoltre, non devono essere raccolti più dati di quelli necessari per lo scopo dichiarato (in base al c.d. principio di "pertinenza"), e i dati raccolti devono essere conservati solo per un periodo giustificato dalle finalità del trattamento;

– di non utilizzare indirizzi di posta elettronica ricavati da "aree pubbliche" di Internet (ad esempio, gruppi di discussione) per attività di *marketing*, nel caso in cui i diretti interessati non sono stati informati; se invece gli interessati sono stati informati della possibilità che i dati forniti in una sede determinata vengono utilizzati per scopi di *marketing* diretto, e hanno avuto la possibilità di esprimere il proprio consenso a questa forma di utilizzazione (magari cliccando *on-line* su una casella apposita), in tal caso l'uso di indirizzi di *e-mail* per fini di *marketing* è da ritenersi lecito. I titolari devono inoltre garantire che l'utente abbia la possibilità di revocare il consenso all'uso dei suoi dati per fini commerciali.

La diffamazione in Internet

Occorre tenere conto che la dimensione della *privacy* non è da considerare soltanto da parte del soggetto attivo in rete, ma deve essere valutata anche dal punto di vista dei soggetti che possono essere a loro volta oggetto della comunicazione in rete.

Come è noto, la libertà di manifestazione del pensiero rimane soggetta, anche quando esplicata su Internet, ai limiti previsti dalle leggi civili e penali e i poteri attribuiti al Garante dalla legge n. 675/1996 devono essere coordinati con le tecniche di tutela ordinariamente previste dal codice civile e dal codice penale, diverse da quelle contenute negli artt. 13 e 29 della legge n. 675/1996, e non invocabili dinanzi all'Autorità perché esorbitanti dalle competenze per essa legislativamente predeterminate.

Il Garante ha precisato questa posizione in un provvedimento del 30 ottobre 2000. Il caso riguarda una persona che aveva lamentato la diffusione, su un sito Internet, di un comunicato dedicatogli, contenente notizie ritenute non veritiere o offensive e riferentesi anche a persone estranee alla sua sfera professionale. L'interessato aveva perciò richiesto all'Autorità di bloccare la diffusione delle informazioni, ma il Garante ha sottolineato che la normativa sulla *privacy* e il codice di deontologia per l'attività giornalistica, nel tutelare la riservatezza, l'identità e la dignità personale, si riferiscono al trattamento illecito e non corretto dei dati e, in particolare, alla diffusione di dati riservati.

Tali disposizioni non possono essere invece invocate rispetto alla diffusione di informazioni denigratorie o diffamatorie, pure altrimenti sanzionata dall'ordinamento in sede civile e penale. Per tale motivo, il Garante non si è avvalso del potere di "blocco" di cui all'articolo 31, comma 1, lettera l), della legge. Tuttavia, l'Autorità ha fatto presente ai ricorrenti che resta in loro disponibilità, ove lo reputino opportuno, l'instaurazione di specifiche controversie a tutela della loro onorabilità presso le competenti autorità giudiziarie.

In un'altra occasione (*Provv.* del 16 gennaio 2001) il Garante è tornato ad occuparsi di una fattispecie di pretesa diffamazione a mezzo Internet.

I ricorrenti hanno chiesto al Garante di disporre la cancellazione o il blocco dei dati personali diffusi tramite alcune pagine *web*: gli autori di tali pagine (identificati in esse con il solo nome di battesimo), nel raccontare la propria esperienza di obiettori di coscienza, avevano divulgato alcune notizie ritenute false e lesive della reputazione di alcune persone e che non sembravano rispettare i limiti posti al diritto di cronaca e di critica (con riferimento ai requisiti di interesse pubblico, verità e correttezza dell'informazione e delle espressioni utilizzate), nonché i principi di protezione dei dati applicabili all'attività giornalistica e ai trattamenti temporanei di dati personali a scopo di pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero.

Chiamato dapprima a pronunciarsi sulla richiesta di adottare in via d'urgenza il blocco dei dati chiesto dalle ricorrenti (ai sensi dell'art. 29, comma 5, l. n. 675/1996), con provvedimento del 6 dicembre 2000 il Garante ha accertato l'insussistenza dei presupposti per adottare il blocco stesso in quanto, anche a seguito della richiesta di informazioni formulata dall'Autorità nei confronti del fornitore del servizio, le pagine *web* accessibili tramite gli indirizzi segnalati erano state disattivate. Da un ulteriore indirizzo risultavano accessibili nuove pagine *web*, che non includevano però dati personali relativi agli interessati; le vicende descritte nell'articolo in contestazione erano state riportate nelle medesime pagine, in un nuovo testo recante una narrazione *impersonale* senza riferimento ad alcun dato *personale*. I resistenti assumevano l'impegno a non divulgare dati delle ricorrenti anche in occasione di eventuali, futuri articoli, pagine e documenti pubblicati tramite Internet.

In sede di valutazione del ricorso il Garante ha dichiarato così non luogo a provvedere, ritenendo accolte le richieste degli interessati formulate ai sensi dell'art. 13 della legge n. 675/1996 e precisando, altresì, che la decisione di non luogo a provvedere non pregiudica il diritto dei ricorrenti di rivolgersi all'autorità giudiziaria in relazione ad altri eventuali profili (come quelli inerenti all'onore e alla reputazione o al risarcimento del danno) per i quali la legge n. 675/1996 non attribuisce competenza all'Autorità.

56. Trattamento e accesso ai dati di traffico

Le modalità tecniche di erogazione dei servizi di telecomunicazione elettronica, si tratti di quelli Internet o dei servizi di telefonia mobile e fissa, consentono ai fornitori e talora a terzi interessati di accedere alle informazioni sul traffico dell'utenza. Si tratta di dati personali dotati di un notevole valore aggiunto, in quanto idonei anche a rivelare gusti ed interessi del consumatore, come pure a consentire la ricostruzione dell'intera trama delle relazioni private di un soggetto, o addirittura a permettere la rilevazione di informazioni particolarmente "sensibili" senza che l'interessato, avendone conoscenza, sia messo in condizione di esercitare i propri diritti.

Come è noto, peraltro, il d. lg. n. 171/1998 (v. Relazione per l'anno 1998) definisce con precisione quali dati personali (indirizzo, numero dell'abbonato, numero totale degli scatti nel periodo ecc.) possono essere utilizzati per le esigenze di fatturazione, essendo altrimenti obbligatorio cancellare o anonimizzare al termine della chiamata ogni altro dato personale eventualmente memorizzato. Tale trattamento a fini di fatturazione è consentito, peraltro, "sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento" (art. 4, comma 2, d.lg. n. 171/1998). Allo scopo di garantire maggiormente le esigenze di riservatezza degli utenti la normativa impone ai fornitori dei servizi di adottare anche modalità di pagamento alternative alla tradizionale fatturazione, tali da permettere di utilizzare il terminale con altra modalità di pagamento anche anonimo (ad esempio carte di credito, carte telefoniche prepagate ecc.).

Per quanto concerne l'invio della fattura ordinaria, il d.lg. n. 171/1998 prevede invece il diritto di ricevere, gratuitamente e dietro richiesta, l'indicazione dettagliata degli elementi dimostrativi degli oneri addebitati. Però, se ci si avvale di questo servizio, a garanzia soprattutto della riservatezza dei diversi utenti, devono essere mascherate le ultime tre cifre del numero chiamato. Quest'ultima prescrizione ha tenuto presente sia le indicazioni provenienti dal confronto in ambito europeo, sia il rapporto fra cifre mascherate e lunghezza totale dei numeri delle utenze telefoniche.

Diversi cittadini, liberi professionisti, imprenditori, associazioni, enti ed altri organismi (pubblici e privati) abbonati al servizio telefonico, tuttavia, continuano a lamentare gli ostacoli frapposti dai fornitori di servizi di telefonia all'accesso ai dati concernenti le chiamate addebitate nella bolletta, non in linea con le indicazioni dell'Autorità.

Proprio in risposta alla segnalazione di un cittadino che, dovendo tutelare un suo diritto in sede giudiziaria, aveva chiesto invano ad un gestore telefonico il rilascio della documentazione del traffico in entrata e in uscita relativamente ad un'utenza a lui intestata, il Garante ha rilevato che la legge sulla *privacy* permette all'abbonato di accedere ai dati di traffico sia in entrata, sia in uscita dalle proprie utenze telefoniche, senza necessità di un'autorizzazione o di altro provvedimento giudiziario.

In tale occasione il Garante, ribadendo quanto stabilito in diversi provvedimenti in materia di telecomunicazioni, ha specificato che rientra nella nozione di dato personale "qualunque informazione relativa all'interessato" (art. 1, l. n. 675/1996) e, come tale, se richiesta, essa deve essere messa a disposizione. Il diritto di accesso deve essere esercitato dall'interessato direttamente nei confronti del titolare o del responsabile del trattamento, personalmente o tramite un terzo cui sia stata conferita delega o procura per iscritto.

Nel caso in cui il gestore telefonico non dia soddisfazione alla richiesta ci si può rivolgere all'autorità giudiziaria o al Garante che ha ritenuto illegittimo, invece, l'accesso diretto a dati relativi a utenze intestate a terzi, i quali restano conoscibili esclusivamente tramite provvedimento giudiziario.

In un provvedimento adottato l'8 giugno 2000 a seguito di un ricorso, il Garante ha nuovamente affrontato tale questione, in riferimento alla comunicazione di alcuni dati di traffico telefonico in entrata e in uscita relativi ad alcune utenze fisse, chiesta dal difensore con un'istanza, formulata ai sensi dell'art. 38 disp. att. c.p.p., in materia di indagini difensive per l'esercizio del diritto alla prova, nonché con una successiva nota sottoscritta dallo stesso difensore. A seguito dell'invito ad aderire formulato dall'Autorità, la società ha comunicato agli interessati l'intendimento di non voler aderire alla richiesta formulata ai sensi del citato art. 38 disp. att. c.p.p. Con successiva memoria, la società resistente ha poi evidenziato, in particolare, che:

– la richiesta di acquisizione dei dati sarebbe stata volta all'esercizio di un eventuale diritto di difesa da parte di uno dei ricorrenti, che non sarebbe risultato, però, intestatario delle utenze telefoniche e non aveva, quindi, il diritto di accedere ai dati dell'abbonato (il quale, a sua volta, pur avendo sottoscritto le richieste e il ricorso, non sarebbe risultato titolare di alcun diritto nella sede processuale penale alla quale si è fatto riferimento);

– relativamente ai dati delle chiamate in entrata, vi era un'esigenza di tutelare la riservatezza degli abbonati chiamanti, per cui tali dati potevano essere comunicati "previo ordine del giudice" e, comunque, essere ricavati dal fornitore del servizio telefonico "a seguito di una procedura di elaborazione tecnicamente complessa ed onerosa, nell'ordine di centinaia di milioni" (di cui si sono illustrate, in termini generali, le modalità);

– le norme della legge n. 675/1996 sui presupposti di liceità del trattamento e della comunicazione dei dati personali non farebbero sorgere in capo al titolare del trattamento "alcun obbligo giuridico di adempimento". Tale obbligo, considerato quanto illustrato nella memoria della società, non poteva derivare neanche dall'art. 38 disp. att. c.p.p., che non attribuirebbe al difensore "alcun potere idoneo a costringere terzi a fornire le informazioni che vengono richieste".

Il Garante ha dichiarato il ricorso inammissibile, per difetto dei presupposti di cui all'art. 29 della legge n. 675/1996 (richiesta di esercitare il diritto di accesso ai dati che riguardano le proprie utenze telefoniche ai sensi dell'art. 13, l. n. 675/1996, e proposizione del ricorso solo in caso di inerzia o rigetto di tale specifica richiesta), atteso che il difensore si era limitato a chiedere l'accesso ai dati relativi al traffico di alcune utenze telefoniche intestate ad un altro ricorrente, con specifico riferimento, però, alla facoltà di raccogliere elementi di prova a fini investigativi ai sensi dell'art. 38 disp. att. c.p.p.

Il Garante ha precisato che una richiesta ai sensi del citato art. 38 disp. att. c.p.p. può permettere di ottenere la comunicazione "in chiaro" dell'intera sequenza dei numeri telefonici composti, senza il mascheramento delle ultime cifre (art. 20, comma 1, lett. g), l. n. 675/1996: cfr. *Provv.* del Garante del 5 ottobre 1998 e 5 ottobre 1999, in *Bollettino*, 1998, n. 6, p. 101 ss. e n. 10, p. 51 ss.), ma non crea nel titolare del trattamento destinatario della richiesta un obbligo di adempiere ed è, comunque, inidonea a giustificare un ricorso ai sensi dell'art. 29.

L'inammissibilità del ricorso, però, come ha tenuto a chiarire l'Autorità, ha lasciato impregiudicato il diritto di far valere in altra sede ulteriori istanze, in merito alle quali la legge n. 675/1996 non ha attribuito competenze al Garante, e non ha precluso inoltre all'abbonato di esercitare i diritti di cui all'art. 13 nei termini sopra indicati.

A tale riguardo, in riferimento alla particolare categoria di dati oggetto della controversia (dati relativi al traffico telefonico in entrata), il Garante ha osservato che la legge garantisce il diritto di accedere anche ai dati personali non ancora registrati (art. 13, comma 1, lett. c), n. 1), l. n. 675/1996) oltre che, ovviamente, ai dati disseminati in più luoghi o archivi, ovvero conservati in modo disorganico (casi in riferimento ai quali l'art. 17, comma 9, d.P.R. n. 501/1998 impone al titolare del trattamento di adottare opportune misure per agevolare l'accesso, tenendo presente la definizione di "dato personale" contenuta nell'art. 1 della legge).

L'accesso non può, invece, riguardare dati personali non ancora raccolti o che divengono materialmente esistenti solo a seguito di una specifica attività creativa notevolmente complessa e che potrebbe essere realizzata solo con la collaborazione di altri soggetti. Tali valutazioni vanno ovviamente condotte caso per caso, nel quadro delle condizioni tecniche del settore interessato.

Da ultimo, è intervenuto in materia il regolamento emanato con d.P.R. n. 77 dell'11 gennaio 2001 (in *G. U.* 29 marzo 2001). Fatte salve le disposizioni della normativa in materia di protezione dei dati personali e della vita privata, ai sensi della legge n. 675/1996 e del d.lg. n. 171/1998, tale regolamento ha disposto che le fatture debbono contenere dati particolareggiati, in modo da permettere la verifica e il controllo dei costi inerenti all'uso della rete telefonica pubblica fissa e dei servizi telefonici pubblici fissi.

Nella sua versione di base (definita con delibera dell'Autorità per le garanzie nelle comunicazioni) la fattura dettagliata deve essere fornita senza costi supplementari per l'utente, cui può eventualmente essere proposta una fattura ancora più particolareggiata a condizioni economiche ragionevoli o a titolo gratuito. Le chiamate gratuite per l'abbonato, comprese quelle dirette a numeri di emergenza, non sono indicate nella fattura dettagliata dell'abbonato (art. 28 d.P.R. n. 77/2001).

Constatato che il regolamento in questione interessa aspetti riguardanti la *privacy* e il trattamento dei dati personali nell'ambito delle telecomunicazioni, l'Autorità ha rilevato che tale decreto è affetto da un vizio che lo rende annullabile perché adottato senza che sia stato rispettato, come già avvenuto in altri casi segnalati, l'obbligo di consultazione del Garante previsto dalla legge sulla *privacy*. Al tempo stesso, il Garante ha interessato l'Autorità per le garanzie nelle comunicazioni per una valutazione comune sulla questione della formazione degli elenchi di telefonia mobile, al fine di prevenire incertezze operative e un diffuso contenzioso riguardo ai diritti degli interessati.

I dati sul traffico nel progetto di convenzione europea sulla cybercriminalità

La cybercriminalità è il rovescio della medaglia della Società dell'informazione. L'utilizzo di nuove tecnologie, infatti, mentre reca enormi benefici, offre la possibilità di perpetrare nuovi tipi di reati, ovvero di rendere più insidiosi i reati tradizionali sfruttando i nuovi strumenti disponibili. Il Consiglio d'Europa è impegnato dal 1997 nella stesura di un progetto di Convenzione internazionale sul *cybercrime*, che potrà essere sottoscritto anche da Paesi che non sono membri del Consiglio d'Europa. Sul progetto di Convenzione il Gruppo europeo dei Garanti si è espresso da ultimo con il Parere n. 4/2001, del 22 marzo 2001, che ha fatto seguito all'intervento del 7 settembre 1999 (Raccomandazione n. 3/1999), relativo alla conservazione dei dati sulle comunicazioni a fini giudiziari da parte dei fornitori di servizi Internet.

Nella sua più recente versione, il progetto di convenzione non contiene più, a differenza che in precedenza, un obbligo generale di sorveglianza consistente nella conservazione sistematica di tutti i dati relativi al traffico. Tuttavia, i Garanti europei hanno manifestato preoccupazione in riferimento alle disposizioni contenute nel progetto di Convenzione in merito ai dati di traffico, laddove, riferendosi alla conservazione e diffusione rapide di dati di traffico e di altra natura, non contemplano la possibilità, per la parte contraente cui sia presentata la richiesta di assistenza, di rifiutarsi di fornirla per motivi legati alla tutela dei dati (es.: inadeguatezza della tutela nel Paese di provenienza della richiesta), bensì soltanto per ragioni di ordine generale (ordine pubblico).

Allo stesso modo, l'imposizione dell'obbligo di conservare per almeno 60 giorni, su richiesta, dati informatici archiviati e dati relativi al traffico, al fine di consentire l'adozione di un provvedimento motivato delle autorità giudiziarie in ordine alla necessità dell'acquisizione ed alle modalità del loro utilizzo, comportano un onere per le imprese e per i privati cittadini interessati non coordinato con le disposizioni della direttiva 97/66/CE; preoccupazioni analoghe sono sollevate dalla disposizione che obbliga i fornitori di servizi a raccogliere o registrare, in tempo reale, nei limiti delle condizioni tecniche, dati relativi al traffico.

È evidente, in merito, che i consumatori non potranno nutrire una sufficiente fiducia nei servizi offerti dai fornitori, qualora non sia chiaro l'ambito dei soggetti legittimati ad accedere a dati e comunicazioni riservate, come e quando ciò sia possibile. Il Gruppo europeo ha espresso in merito l'auspicio, alla luce del forte impatto di tali disposizioni sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, che il Consiglio d'Europa consulti i propri esperti nel campo della tutela dei dati prima di definire la propria posizione sul progetto di Convenzione.

57. ELENCHI PUBBLICI E DIRITTI DEGLI INTERESSATI

In data 15 novembre 2000 il Garante ha avviato accertamenti nei confronti dell'Associazione politica nazionale Lista Marco Pannella, per verificare la liceità e la correttezza di alcuni trattamenti di dati relativi ad indirizzi di posta elettronica, in relazione a numerose segnalazioni che lamentavano la ricezione non gradita di messaggi per via telematica per finalità di comunicazione politica. Molti cittadini hanno fatto inoltre presente che non è stato loro possibile cancellarsi dagli elenchi dei destinatari secondo le modalità indicate nelle *e-mail* non gradite, o di essere stati costretti a reiterare invano più richieste di cancellazione.

All'esito dell'istruttoria, il Garante ha riscontrato che le segnalazioni pervenute erano fondate (Provv. 11 gennaio 2001).

L'Associazione ha fatto presente di aver reperito oltre 390.000 indirizzi di posta elettronica a scopo di comunicazione politica, utilizzando un software il quale archivierebbe indirizzi *e-mail* visualizzati su pagine *web* con suffissi ".it", ".org", ".com" e ".net" accessibili a chiunque in rete senza l'uso di *password* o di altri sistemi di protezione. La circostanza, peraltro, non ha trovato pieno riscontro in quanto, da accertamenti tecnici effettuati, in diversi casi non è stato possibile reperire in rete gli indirizzi di posta elettronica dei cittadini che hanno inviato una segnalazione.

A prescindere da tale aspetto, tuttavia, l'Autorità ha ritenuto che l'utilizzazione per finalità di comunicazione politica di tali indirizzi non fosse comunque lecita e corretta. Gli indirizzi di posta elettronica dei segnalanti non provenivano da "pubblici registri, elenchi, atti o documenti conoscibili da chiunque" (art. 12, comma 1, lett. c), l. n. 675/1996) e la loro utilizzazione nel caso in esame non poteva ritenersi consentita in mancanza di una previa manifestazione positiva di consenso da parte degli interessati (essendo altresì inoperanti gli ulteriori presupposti elencati nell'art. 12 della medesima legge).

Il Garante ha precisato che la previsione contenuta nella citata lettera c) si riferisce non a qualunque dato personale che sia di fatto consultabile da una pluralità di persone, ma ai soli dati personali che, oltre ad essere desunti da registri, elenchi, atti o documenti "pubblici" (in particolare in quanto formati o tenuti da uno o più soggetti pubblici), siano sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque, regime che può peraltro prevedere modalità o limiti temporali per il trattamento, da rispettare anche in caso di comunicazione o diffusione dei dati.

Le disposizioni richiamate, ha osservato il Garante, possono semmai trovare applicazione in altri casi – di stretta analogia – in cui un determinato registro, elenco, atto o documento sia reso ad esempio accessibile a chiunque sulla base della determinazione di un soggetto pubblico adottata in base ad una norma

(come avviene per l'elenco degli abbonati al servizio di telefonia vocale, per il quale l'Autorità per le garanzie nelle comunicazioni provvede affinché sia reso disponibile agli utenti: art. 17, comma 1, d.P.R. 19 settembre 1997, n. 318).

Una legittimazione all'utilizzazione pubblica di determinati dati può derivare anche dal consenso espresso degli interessati, manifestato in modo specifico ed informato.

Al contrario, le citate disposizioni non possono essere applicate in modo da poter trattare liberamente qualsiasi dato personale di natura non sensibile in base alla sola circostanza che il dato sia stato conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti.

L'utilizzazione per finalità di comunicazione politica degli indirizzi di posta elettronica dei segnalanti non poteva pertanto avvenire senza un preventivo consenso manifestato dagli interessati eventualmente anche nei confronti di più soggetti. Non era pertanto corretto gravare l'utente dell'onere di chiedere all'Associazione di interrompere l'invio dei messaggi non richiesti.

Parimenti, la conoscenza di fatto degli indirizzi che si realizza attraverso la partecipazione a *newsgroup* e *forum*, allo stesso modo, non poteva essere disgiunta dalla finalità per cui essa è stata resa possibile.

Contrastava, pertanto, con i principi di correttezza e finalità del trattamento raccogliere i dati che singoli utenti "lasciano" in un newgroup, forum, ecc. solo per le finalità di specifica discussione su determinati temi, hobbies, ecc., ed utilizzarli per altri scopi che nulla hanno a che vedere – anche indirettamente – con l'argomento per il quale l'utente partecipa ad una discussione più o meno "pubblica" ed indica il proprio recapito e le proprie generalità (art. 9, comma 1, lett. b), l. n. 675/1996).

Ad una conclusione analoga il Garante è giunto per i casi nei quali gli indirizzi di posta elettronica risultavano acquisiti dall'Associazione in quanto pubblicati su alcuni siti *web* per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale ed associativa.

La pubblicità di alcuni indirizzi resi conoscibili attraverso tali siti doveva essere collegata anch'essa, infatti, agli scopi per cui essa si verifica, non potendosi sostenere, anche in tali casi, che i dati posti a disposizione del pubblico per circoscritte finalità siano liberamente utilizzabili per l'invio generalizzato di *e-mail* anche quando queste non abbiano un contenuto commerciale o pubblicitario.

Il Garante ha poi rilevato che, a prescindere dalla liceità o meno dell'utilizzazione dei dati, l'Associazione era comunque tenuta a soddisfare senza ritardo le richieste di cancellazione ai sensi dell'art. 13 della legge n. 675/1996, curando un servizio attivo ed efficace di eliminazione degli indirizzi dei reclamanti.

Elenchi di abbonati ai servizi di telefonia mobile

Nell'ambito dei servizi di telefonia vocale, analogamente a quanto disposto dal d.P.R n. 318/1997, il recente regolamento emanato con d.P.R. n. 77 dell'11 gennaio 2001 (in *G.U.* 29 marzo 2001) ha previsto la possibilità di pubblicazione degli elenchi degli abbonati ai servizi di telefonia mobile. Il decreto prevede la possibilità per tali abbonati di decidere se e come (ad esempio, con il solo cognome, con l'indicazione dell'iniziale del nome proprio) comparire negli elenchi, escludendo altresì l'utilizzo delle stesse informazioni per fini pubblicitari (art. 20). È inoltre prevista la possibilità di verificare ed eventualmente di correggere i dati o di chiedere di essere radiati dagli elenchi.

Gli elenchi di tutti gli abbonati che non si siano espressamente opposti al fatto di esservi inseriti, con i numeri dei telefoni fissi e mobili e i numeri personali, dovrebbero essere messi a disposizione del pubblico su supporto cartaceo o elettronico, o su entrambi, in una forma approvata dall'Autorità per le garanzie nelle comunicazioni, e aggiornati periodicamente.

In proposito, il Garante ha richiesto immediatamente notizie ai fornitori di telefonia mobile sulle iniziative intraprese in ordine alla predisposizione di tali elenchi, alle modalità ipotizzate o utilizzate per informare le persone interessate e per garantire alle stesse un efficace esercizio dei diritti previsti dalla normativa sulla protezione dei dati personali, nonché dallo stesso regolamento che introduce la pubblicazione degli elenchi.

Constatato che il regolamento in questione interessa aspetti riguardanti la *privacy* e il trattamento dei dati personali nell'ambito delle telecomunicazioni, l'Autorità ha poi rilevato che tale decreto è affetto da un vizio che lo rende annullabile perché adottato senza che sia stato rispettato, come già avvenuto in altri casi segnalati, l'obbligo di consultazione del Garante previsto dalla legge sulla *privacy*.

Il Garante ha rilevato il rischio che il regolamento venga applicato, riguardo alla formazione degli elenchi, con modalità non idonee ad una piena protezione dei diritti degli interessati; al tempo stesso, ha interessato l'Autorità per le garanzie nelle comunicazioni per una valutazione comune al fine di prevenire incertezze operative e un diffuso contenzioso riguardo ai diritti degli interessati.

In particolare, come osservato dal Gruppo dei garanti europei nel Parere n. 7/2000, adottato il 2 novembre 2000, occorre rendere effettiva la possibilità per gli abbonati di decidere se essere inclusi o meno negli elenchi cartacei o elettronici; inoltre, vista la portata degli elenchi elettronici, gli abbonati dovranno essere informati sul loro eventuale uso ulteriore, ed i dati trattati dovranno essere limitati allo stretto necessario per identificare l'utente, senza rivelare informazioni strettamente "private".

Il Garante, come altre autorità per la protezione dei dati, si sta occupando anche di casi di "ricerche inverse" negli elenchi. Si tratta di nuovi servizi del mercato liberalizzato che offrono, con facilità e a basso costo, capacità estesa per il trattamento di tutte le informazioni contenute negli elenchi telefonici, anche attraverso l'associazione delle metodologie di ricerca a criteri multipli. Si rende, così, possibile risalire al nome e all'indirizzo dell'abbonato da un determinato numero, ovvero ai nomi e numeri telefonici degli abitanti in uno stesso quartiere, e così via.

L'orientamento del Gruppo europeo è quello di considerare tale nuova finalità degli elenchi come non compatibile con la finalità iniziale, considerando il trattamento illecito a meno che l'interessato non abbia manifestato un proprio specifico consenso al trattamento dei dati personali per tali nuove finalità. Il Gruppo ha adottato una posizione comune in merito, nel Parere n. 5/2000, approvato il 13 luglio 2000.

Un altro aspetto rischioso è legato alla possibilità per chiunque di modificare gli elenchi su supporto elettronico: si rende pertanto necessario garantire che le trasmissioni di elenchi rispettino le scelte espresse gratuitamente dagli utenti e dagli abbonati presso il fornitore iniziale. Inoltre, la possibile cessione dei dati sotto forma di CD ROM solleva ulteriori problemi legati alla durata dell'autorizzazione al trattamento, che deve essere determinata in modo da non consentire l'uso di dati non più utilizzabili in relazione alle scelte espresse dagli interessati.

La stessa proposta di revisione della direttiva 97/66/CE, partendo dall'implicito presupposto che non è opportuno l'inserimento in via automatica degli utenti dei servizi di telefonia mobile o dei servizi di comunicazione elettronica (posta elettronica) in elenchi pubblici, prevede che siano gli abbonati a decidere se vogliono figurare in un elenco pubblico e specificare quali dei loro dati personali debbano esservi riportati. Per tener conto delle varie possibilità di utilizzo degli elenchi pubblici, in particolare di quelli elettronici, è necessario informare gli abbonati circa gli scopi per i quali gli elenchi sono stati predisposti e garantire che il consenso ad essere inclusi venga prestato sulla base di un'accurata ed esauriente informazione circa le modalità di utilizzo dei propri dati personali.

58. SERVIZI DI LOCALIZZAZIONE

Nelle reti di comunicazioni mobili odierne, i dati relativi alla localizzazione dell'utente sono già disponibili. Questo tipo di informazione è necessaria per consentire la trasmissione di comunicazioni che sono originate e destinate ad un utente che non ha una postazione fissa. Si tratta di un informazione "grezza" sulla localizzazione, che è in realtà un sottoprodotto del servizio di trasmissione delle comunicazioni, e deve ritenersi disciplinato dalla vigente direttiva 97/66/CE e dal d.lg. n. 171/1998, nella parte riguardante i dati sul traffico.

Esiste tuttavia un nuovo tipo di servizi forniti dalle reti cellulari e satellitari che consentono di individuare esattamente l'ubicazione dell'apparecchiatura terminale dell'utente mobile. In questo caso i dati relativi alla localizzazione sono molto più precisi e vengono specificamente sottoposti a trattamento da parte dei fornitori della rete allo scopo di fornire servizi a valore aggiunto agli utenti e agli abbonati.

Nel corso del 1999, il Garante ha avviato le procedure di accertamento relative al delicato problema della "localizzazione" degli apparecchi di telefonia mobile, con la richiesta indirizzata ai gestori italiani di servizi di telecomunicazioni mobili di dettagliate informazioni (v. Relazione per l'anno 1999, p. 66).

L'Autorità si è riservata di effettuare una valutazione complessiva del problema alla luce dei chiarimenti, anche tecnici, forniti dai gestori, in modo da verificare la presenza di eventuali irregolarità rispet-

to alla normativa sulla protezione dei dati personali e prospettare misure idonee ed accorgimenti per la tutela dei diritti degli interessati.

Nel maggio 2000, con riferimento alle notizie apparse sui principali organi di informazione concernenti l'avvio di programmi di localizzazione per telefoni mobili, resi disponibili in Internet e via rete mobile, sulla base della tecnologia *CellPoint Finder* (che consentirebbe di localizzare con precisione i detentori degli apparecchi di telefonia cellulare), il Garante, in collaborazione con i fornitori/gestori, ha avviato un'ulteriore procedura di accertamento, chiedendo alla società interessata particolareggiate informazioni riguardo alle caratteristiche del programma in questione, ai fornitori di servizi ai quali esso sia stato già fornito sul territorio nazionale, alle modalità di conservazione dei dati, in ordine agli strumenti a disposizione dell'utente per disattivare il programma, nonché alle tecniche ideate per informare i singoli abbonati ed utenti interessati al servizio ed acquisirne il consenso.

Nell'ambito del procedimento, inoltre, il Garante ha richiesto ai principali gestori di telefonia mobile di fornire elementi circa: la tipologia dei dati veicolati sulle infrastrutture di rete dai quali è possibile individuare, direttamente o tramite ulteriori elaborazioni, la posizione geografica delle apparecchiature terminali mobili; le precise modalità di acquisizione, registrazione ed elaborazione dei dati, con particolare riferimento al grado di precisione della localizzazione spaziale delle apparecchiature terminali e alla persistenza in qualunque modo nel sistema informativo dei dati grezzi o dell'elaborazione su di essi svolta; l'esistenza o la previsione di accordi con altre società per la fornitura di servizi di localizzazione delle apparecchiature terminali, anche attraverso la predisposizione di idonei programmi informatici. L'Autorità ha inoltre convocato per un'audizione le società interessate ed altri qualificati rappresentanti del settore per procedere ad un approfondito esame congiunto degli elementi forniti.

In merito, la Commissione europea, nel preambolo alla proposta di revisione della direttiva n. 97/66/CE, ha espresso la preoccupazione che la capacità di trattare dati estremamente precisi in ordine all'ubicazione dell'utente nelle reti di comunicazione mobili porti ad una situazione in cui questi resti sotto sorveglianza permanente, al punto da trovarsi costretto a non utilizzare affatto detti servizi di comunicazione pur di tutelare la propria vita privata. La proposta precisa che i dati relativi alla localizzazione dell'utente possono essere utilizzati esclusivamente con il consenso informato dell'abbonato, prescrivendo che l'utente deve anche disporre di uno strumento semplice per rifiutare temporaneamente il trattamento dei dati relativi alla localizzazione, analogamente a quanto previsto per l'identificazione della linea chiamante. Le uniche deroghe a tale principio generale sono l'utilizzo dei dati relativi alla localizzazione dell'utente da parte dei servizi di emergenza e le deroghe vigenti ai fini della sicurezza pubblica e delle indagini di natura penale.

Sul punto si è recentemente pronunciato anche il Gruppo dei Garanti europei, nel Parere n. 7/2000 del 2 novembre 2000, rilevando che in linea di principio i dati relativi all'ubicazione non devono essere sottoposti a trattamento per la fornitura di servizi a valore aggiunto, ma eccezionalmente possono essere sottoposti a trattamento per finalità chiaramente specificate che richiedano tecnicamente l'uso dei dati relativi all'ubicazione e sempre che vengano messi in atto controlli di sicurezza consoni ai rischi per la vita privata. In considerazione del carattere "sensibile" dei dati in relazione alla libertà di movimento del cittadino e del fatto che non si tratta di dati necessari per stabilire la comunicazione, l'utente/abbonato deve avere il pieno controllo sulle finalità e modalità del trattamento cui essi vengono sottoposti con la possibilità, qualora sia interessato, di consentire liberamente al trattamento dei dati sull'ubicazione in relazione ad ogni fornitura di un servizio a valore aggiunto e con necessità di integrare l'attuazione tecnica di tale diritto nell'apparecchiatura dell'abbonato e non nella rete, come avviene invece nel caso dell'identificazione della linea chiamante.

SICUREZZA DEI DATI E DEI SISTEMI

59. LO STATO DELL'ARTE NELL'APPLICAZIONE DELLE MISURE DI SICUREZZA

La legge del 31 dicembre 1996, n. 675 ha assegnato una precisa base giuridica agli obblighi relativi alle misure di sicurezza che riguardano il trattamento automatizzato e non automatizzato di dati.

La disciplina prevede il dovere di custodire e controllare i dati trattati mediante l'adozione di idonee e preventive misure di sicurezza tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 15, comma 1, l. n. 675/1996); la mancata predisposizione di tali misure comporta la responsabilità per danni eventualmente cagionati (art. 18, l. n. 675/1996). Lo stesso art. 15, inoltre, ai commi 2 e 3, individua tramite un apposito regolamento le *"misure minime di sicurezza"* la cui violazione costituisce sicura esposizione al rischio di lesione del diritto alla tutela dei dati personali e comporta l'applicazione di sanzioni di carattere penale (art. 36, l. n. 675/1996).

Il previsto regolamento, emanato con il d.P.R. 28 luglio 1999, n. 318, entrato in vigore il 29 marzo 2000, comporta per il titolare del trattamento non solo l'obbligo di adottare le misure minime previste al comma 2 dell'art. 15 della legge n. 675/1996, ma anche di custodire e controllare i dati adottando le idonee e preventive misure di sicurezza di cui all'art. 15, comma 1.

L'Autorità, con deliberazione del 29 maggio 2000 (in *Bollettino* n. 13, p. 30), ha chiarito che nei confronti dei soggetti interessati non sussiste alcun obbligo di comunicare sistematicamente al Garante le determinazioni eventualmente adottate in attuazione del regolamento ed ha precisato che gli atti previsti dal regolamento, come il documento programmatico sulla sicurezza o la designazione dei responsabili e degli incaricati del trattamento, devono essere esibiti all'Autorità solo a seguito di un'eventuale e specifica richiesta in sede di ispezione o di controllo.

Successivamente, la legge 3 novembre 2000, n. 325 recante: *"Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste all'art. 15 della legge 31 dicembre 1996, n. 675"*, ha consentito a coloro i quali non avevano adottato le misure minime entro il predetto termine del 29 marzo 2000 di beneficiare, seppure non in modo automatico, ma adempiendo a determinate prescrizioni, di un differimento del termine fino al 31 dicembre 2000. Tale differimento, non direttamente rilevante ai fini della responsabilità civile per danno derivante da mancata o inidonea adozione di misure di sicurezza, ha permesso di prorogare al 31 dicembre 2000 l'applicabilità delle previste sanzioni penali (art. 36, l. n. 675/1996). Per contribuire alla corretta applicazione della legge il Garante è intervenuto, con un provvedimento del 5 dicembre 2000 (in *Bollettino* n. 14/15, p. 19), precisando le modalità applicative per l'adozione del documento previsto dall'art. 1 della legge n. 325/2000 con un atto avente data certa.

60. PRIMI CASI APPLICATIVI

Il Garante nel corso dell'anno 2000 ha affrontato l'argomento delle misure minime di sicurezza in varie occasioni, sia rispondendo a quesiti, sia formulando pareri su gli atti cui è richiesta la consultazione dell'Autorità.

In un parere pronunciato su richiesta della Lega italiana per la lotta all'AIDS (LILA) (in *Bollettino*, n. 11/12, p. 7) ha ricordato che gli organismi sanitari sono tenuti al rispetto dei principi di correttezza e di pertinenza richiesti per il trattamento di dati sensibili da parte dei soggetti pubblici, e devono adottare specifiche cautele a tutela della riservatezza degli interessati. Tra queste assume carattere di priorità la separazione dei dati anagrafici da quelli sanitari e la cifratura delle informazioni contenute in elenchi o banche dati. Per quanto riguarda, invece, il regolamento sulle misure minime di sicurezza, l'Autorità ha precisato che esso impone l'adozione, da parte di chi utilizza i dati, di idonee cautele e

accorgimenti di tipo organizzativo e tecnico, allo scopo di evitare la distruzione, la perdita e l'uso illecito delle informazioni raccolte, elaborate e conservate. Il Garante ha richiamato, infine, l'attenzione sull'accesso ai dati "*particolari*" (sensibili e giudiziari) che richiede al titolare o, se designato, al responsabile del trattamento l'obbligo di rilasciare specifiche autorizzazioni agli incaricati del trattamento o della manutenzione dei dati sensibili o di carattere giudiziario. Il rispetto di questi principi dovrà essere ancora più accurato quando si trattano informazioni inerenti all'AIDS o all'infezione da HIV, dalla cui circolazione può derivare un grave pregiudizio per la vita privata e la dignità personale degli interessati.

L'Autorità garante, in un provvedimento del 28 febbraio 2000 (in *Bollettino*, n. 11/12, p. 9), ha fornito analoghe raccomandazioni agli uffici giudiziari, richiamando il rispetto dei principi di correttezza e di pertinenza in base ai quali possono essere trattati e diffusi i soli dati necessari al perseguimento delle finalità istituzionali, precisando altresì che, al fine di tutelare la sicurezza dei dati raccolti, ciascun ufficio giudiziario, come ogni altra amministrazione, è tenuto al rispetto del regolamento in materia di misure minime di sicurezza e all'adozione delle idonee cautele organizzative e tecniche in modo da ridurre al minimo i rischi di distruzione dei dati e di accessi non autorizzati.

Il Garante, inoltre, nell'esprimere il prescritto parere allo schema di d.P.R. concernente "*Disposizioni relative all'uso di strumenti informatici e telematici nel processo civile*" (v. *Provv.* del 4 ottobre 2000, in *Bollettino*, n. 14/15, p. 13) ha ravvisato la necessità che nello stesso venisse effettuato un espresso richiamo all'art. 15 della legge n. 675/1996 e al connesso d.P.R. n. 318/1999, in quanto il suddetto provvedimento è applicabile ai trattamenti di dati personali effettuati per ragioni di giustizia presso uffici giudiziari (art. 4, comma 2, l. n. 675/1996). Nel medesimo provvedimento il Garante ha richiamato la necessità di precisare che i dati personali acquisiti presso i difensori delle parti a seguito di accesso al sistema informatico civile o, comunque, di ricezione di atti e documenti per via telematica, siano utilizzati in modo lecito e corretto da parte dei vari soggetti che vi possono accedere (sostituti ausiliari, tirocinanti, praticanti, colleghi operanti presso studi associati, associazioni di professionisti; personale amministrativo, ecc.). In tale occasione il Garante ha ricordato di aver impartito in proposito alcune prescrizioni nell'autorizzazione generale n. 4/2000, rilasciata ai sensi dell'art. 22, l. n. 675/1996 in tema di trattamento dei dati sensibili da parte di liberi professionisti. Nuove regole potrebbero essere adottate in materia in occasione del varo del codice di deontologia per il trattamento di tutti i dati personali trattati a fini di indagine difensiva e di difesa di un diritto in sede giudiziaria, promosso dal Garante con provvedimento del 10 febbraio 2000 e attualmente in fase di predisposizione.

Da ultimo l'Autorità, in data 23 febbraio 2001 (v. parere, in *Bollettino*, n. 17, p. 32), nel rispondere ad un quesito posto da dipendenti di una società, ha chiarito che, ai sensi del regolamento sulle misure minime di sicurezza, non è possibile vietare ai propri dipendenti che devono utilizzare gli strumenti informatici servendosi di *password* loro singolarmente assegnate, l'autonoma modifica delle stesse. Il Garante ha infatti ricordato che la parola chiave per l'accesso ai dati personali deve essere autonomamente sostituibile ed ha suggerito anche modalità per la prevista comunicazione della sostituzione al soggetto preposto alla sua custodia.

I TRASFERIMENTI ALL'ESTERO DI DATI

61. PAESI CHE OFFRONO UNA PROTEZIONE ADEGUATA

La Commissione europea ha constatato con due decisioni che alcuni Paesi terzi garantiscono un livello di protezione adeguato. A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

Queste decisioni non eliminano però la rilevanza dell'attività delle autorità di garanzia dei Paesi membri, poiché queste possono esercitare i loro poteri per sospendere il trasferimento verso l'estero nel caso in cui, ad esempio, la competente autorità del Paese terzo abbia accertato che il destinatario dei dati viola le norme vigenti in materia di protezione dei dati, ovvero in altre ipotesi assai complesse, nelle quali, tra l'altro, una violazione sia molto probabile, si possano ritenere inadeguate e non tempestive le misure che la competente autorità del Paese terzo intenda adottare e il trasferimento comporti il rischio imminente di gravi danni per gli interessati.

Il 26 luglio 2000 la Commissione ha adottato la decisione 2000/519/CE, riguardante l'adeguatezza della protezione dei dati personali in Ungheria (*G.U.C.E.* n. L 215 del 25 agosto 2000), sulla base del parere espresso nel 1999 dal Gruppo di lavoro previsto dall'art. 29.

La Commissione ha considerato in particolare che il principio della tutela della vita privata è contemplato dalla costituzione ungherese; che l'Ungheria ha ratificato la Convenzione del Consiglio d'Europa sulla protezione delle persone riguardo al trattamento automatizzato di dati di carattere personale (Convenzione n. 108/1981 del Consiglio d'Europa), volta a rafforzare la tutela dei dati personali e ad assicurare la libera circolazione tra le parti contraenti; che le norme vigenti in quel Paese incorporano i principi fondamentali necessari per assicurare un adeguato livello di protezione delle persone fisiche; che l'applicazione di tali norme è garantita dai ricorsi giurisdizionali, nonché dal controllo indipendente esercitato dal commissario nominato dal Parlamento.

Da notare che nei confronti dell'Ungheria la decisione riguarda tutti i trasferimenti di atti personali, mentre la decisione di seguito menzionata nei confronti degli Usa è relativa ai trasferimenti verso imprese ed organizzazioni aderenti al *"Safe Harbor"*.

Per vari aspetti simile è la decisione n. 2000/518/CE relativa alla Svizzera, resa in pari data (26 luglio 2000, in *G.U.C.E.* n. *L 215* del 25 agosto 2000) dalla Commissione: anche in questo caso la Commissione, conformemente al parere del Gruppo di lavoro previsto dall'art. 29, ha ritenuto adeguato il livello di protezione offerto da quell'ordinamento per tutte le attività rientranti nel campo di applicazione della direttiva, dopo aver considerato la costituzione, l'adesione alla Convenzione n. 108/1981 sopra menzionata, le norme federali e quelle cantonali e l'indipendenza dell'autorità di controllo competente in materia.

Non ancora a livello di Commissione, bensì di Gruppo di lavoro previsto dall'art. 29, sono invece le valutazioni relative a Canada ed Australia.

La prima, del 26 gennaio 2001 (parere n. 2/2001), in qualche misura interlocutoria, nella sostanza segnala alla Commissione alcuni aspetti essenziali dell'ordinamento canadese in materia di protezione di dati personali. Anzitutto si fa presente che le norme relative al trattamento effettuato da privati, contenute nel *Personal Information and Electronic Documents Act*, saranno pienamente in vigore nel 2004 e che il loro ambito di applicazione è relativo solo a soggetti privati che trattano dati personali nel corso di attività a scopo di lucro.

Si è poi richiamata l'attenzione sul rapporto tra norme federali e norme delle diverse province, attesa la non omogeneità della disciplina, occorrendo pertanto verificare l'opportunità di una valutazione dell'adeguatezza con riferimento ai singoli ordinamenti; si è poi sottolineata l'esigenza di monitorare l'evoluzione normativa riguardante i dati sensibili, valutando favorevolmente iniziative volte ad assicurare una più organica tutela degli stessi, anche con riferimento al loro trasferimento dal Canada ad altro Paese.

Il medesimo gruppo di lavoro, col parere 3/2001 del 26 gennaio 2001, ha invece ritenuto non ancora adeguata la protezione offerta dall'ordinamento australiano, o, più precisamente, ha indicato alcuni punti critici da superare per giungere ad una valutazione di adeguatezza.

Tra i punti va ricordata la non applicazione ad alcune materie, segnatamente alle piccole imprese ed ai dati dei dipendenti, degli strumenti normativi di protezione dei dati (*Privacy Act, Privacy Amendment*), ancorché questi possano essere di natura sensibile. In particolare non è chiara la definizione australiana di "piccola impresa", che diventa quindi potenzialmente di vastissima applicazione. È inoltre consentito in termini piuttosto ampi che l'informativa agli interessati sia fornita successivamente alla raccolta dei dati medesimi e per i dati sensibili le limitazioni relative alla raccolta non escludono che possa farsene un uso ulteriore, per scopi diversi da quelli originari. Gli strumenti di tutela, inoltre, non risultano applicabili a soggetti che non siano cittadini australiani o che non risiedano in Australia.

Questa valutazione non favorevole risulta ovviamente modificabile in futuro ma, al di là delle specifiche considerazioni sulle quali si basa, appare senz'altro significativa della complessità e delicatezza delle analisi richieste.

62. "*SAFE HARBOR*"

Di rilievo, anche nel corso del 1999 e del 2000, è stata l'attività svolta dal Garante in seno ad organismi comunitari ed internazionali, relativamente ai trasferimenti di dati verso Paesi terzi.

È nota, al riguardo, la disciplina contenuta nell'art. 25 della direttiva 95/46/CE secondo la quale lo stato di destinazione deve presentare un livello di protezione "adeguata", da valutarsi con riferimento a tutte le circostanze, segnatamente alla natura dei dati, protezione in mancanza della quale gli Stati membri devono adottare tutte le misure per impedire il trasferimento di dati della stessa natura verso tale Paese, a meno che ricorrano altri presupposti che permettano di trasferire comunque i dati (l'art. 26 prevede ad esempio che il trasferimento possa avvenire anche verso Paesi la cui legislazione non presenti un adeguato livello di protezione, in particolare quando l'interessato abbia manifestato il suo consenso, o quando il trasferimento sia accompagnato da clausole contrattuali idonee ad assicurare tale protezione).

Per valutare l'adeguatezza della protezione offerta da un Paese terzo possono essere considerati sia la legislazione nazionale, sia, dopo l'accertamento della situazione di inadeguatezza, gli impegni internazionali assunti con la Commissione in negoziati volti a porvi rimedio.

In questo quadro si è collocata l'attività del Garante in seno agli organismi comuni previsti dalla citata direttiva 95/46: il Gruppo consultivo di cui all'art. 29 (composto da un rappresentante di ciascuna autorità nazionale e da un rappresentante della Commissione, e presieduto nel periodo considerato dal Presidente del Garante italiano), al quale, tra l'altro, spetta formulare un parere sul livello di tutela nella Comunità e nei Paesi terzi; il comitato di cui all'art. 31, composto da rappresentanti degli Stati membri, è presieduto da un rappresentante della Commissione.

La presente esposizione sintetizza ed in parte rielabora il materiale disponibile sul sito Internet della competente Direzione generale della Commissione (*http://europa.eu.int/comm/internal-market*), cui si fa doveroso rinvio per ogni dettaglio.

Anche quest'anno, nell'ambito di quest'ultimo gruppo il Garante ha operato in continuo raccordo con il Ministero della giustizia, che rappresenta il Governo, nell'espressione di un orientamento comune al Governo ed all'Autorità di garanzia.

Si riassumono di seguito i momenti essenziali di tale attività, con costante riferimento ad alcuni atti di particolare importanza, che in qualche misura indicano la rilevanza non solo comunitaria della disciplina sulla protezione dei dati personali e quindi chiamano le autorità garanti, dopo un'impegnativa fase di elaborazione, ad una non meno rilevante funzione di verifica nell'applicazione di tali strumenti, volti ad assicurare un più ampio ambito di applicazione dei principi e delle regole fondamentali contenuti nella normativa comunitaria in materia.

Per quanto riguarda il trasferimento di dati negli U.S.A., il 26 luglio 2000 la Commissione europea ha adottato una decisione (n. 2000/520/CE in *G.U.C.E. n. L 215* del 25 agosto 2000) che constata che il dispositivo di *"Safe Harbor"* approntato dalla Commissione federale per il commercio degli Stati Uniti assicura un adeguato livello di protezione dei dati personali trasferiti dall'Unione europea.

Il *"Safe Harbor"* costituisce un insieme di principi a garanzia del trattamento dei dati personali uniti alla previsione di alcuni sistemi per assicurare il rispetto di tali principi. L'adesione al *"Safe Harbor"* è

facoltativa per le imprese americane, ma le regole in esso contenute vincolano le imprese aderenti; il loro rispetto è affidato alla *Federal Trade Commission* e, per le compagnie aeree, all'Amministrazione dei trasporti.

La decisione comunitaria è il frutto di due anni di intenso negoziato tra le parti volto ad evitare che il trasferimento di dati personali verso gli U.S.A. potesse essere limitato o sottratto a garanzie in seguito all'entrata in vigore della direttiva n. 95/46/CE. Nel corso di tale negoziato, ed in particolare nella fase finale, l'anno scorso, il Garante ha svolto una costante funzione di impulso in seno ai predetti organismi comunitari, per una soddisfacente soluzione dei punti critici, relativi all'effettività della tutela offerta dal *"Safe Harbor"* con riguardo non solo e non tanto ai livelli di protezione riconosciuti agli interessati, quanto alle forme per assicurare loro soddisfazione nel caso di violazione.

I cittadini dell'Unione europea che intendano reclamare per il trattamento effettuato da un partecipante al *"Safe Harbor"* possono rivolgersi ad un'istanza indipendente di composizione di controversie: ogni organismo statunitense aderente al *"Safe Harbor"* deve indicare l'istanza con la quale si impegna a collaborare. In vari casi è pure possibile agire davanti a giudici statunitensi, in base a norme di quell'ordinamento che non permettono "dichiarazioni false", quali appunto quelle di un'impresa che dichiari di aderire ad una certa politica di protezione dei dati personali successivamente non rispettata.

Con risoluzione del 5 luglio 2000 il Parlamento europeo ha indicato l'esigenza di migliorare il testo dell'accordo in particolare sul punto dei ricorsi degli interessati relativi alla violazione dei principi; la Commissione non ha negoziato tali modifiche ma ha trasmesso questa risoluzione alle autorità americane.

In questo quadro, nell'attuale fase di applicazione dell'accordo appare particolarmente importante la funzione di monitoraggio delle autorità nazionali di garanzia (che pure possono ricevere segnalazioni dagli interessati) per valutare nel corso del tempo l'opportunità di eventuali modifiche alla decisione comunitaria.

63. CLAUSOLE CONTRATTUALI

Il 27 marzo 2001 il Comitato previsto dall'art. 31 della direttiva ha infine espresso parere favorevole allo schema di decisione della Commissione sulle clausole contrattuali standard relative al trasferimento di dati personali in Paesi terzi.

L'apporto del Garante è stato particolarmente intenso anche dal punto di vista organizzativo, avendo peraltro formato oggetto della collaborazione offerta nel quadro di uno scambio di funzionari.

In prima approssimazione, con tali clausole, volte a facilitare il trasferimento dei dati, l'operatore che nel Paese terzo riceve i dati personali si impegna anzitutto nei confronti dell'operatore comunitario che glieli fornisce ad assicurare un grado minimo di protezione della riservatezza degli interessati. Il loro utilizzo non è necessario e la menzionata decisione non esclude che le diverse autorità garanti possano autorizzare contratti di diverso contenuto ai sensi dell'art. 26.2 della direttiva; tuttavia con la loro adozione gli Stati membri si obbligano a riconoscere come adeguata la protezione dei dati personali offerta da contratti che le contengono.

L'elaborazione di tali clausole è stata particolarmente complessa, da un lato poiché implicava l'analisi di delicate problematiche giuridiche anche in relazione alle differenze sostanziali tra gli ordinamenti comunitari dei diversi Stati membri, e dall'altro poiché essa si è svolta di pari passo con la definizione del *"Safe Harbor"*. Una sintesi di tali clausole sarebbe pertanto estremamente laboriosa e non facile, proprio perché l'intento di semplificare al massimo e di fornire agli operatori uno strumento agile ha necessariamente tenuto conto di tali complessità. Ci si limita quindi, di seguito, a dare cenno delle problematiche d'insieme che si sono poste.

In via preliminare si osserva che la determinazione di tali garanzie mediante clausole contrattuali affida all'autonomia delle parti forme di tutela che altrimenti dovrebbero essere sancite da laboriosi strumenti di diritto internazionale.

Anche in questo caso il principale problema che ha formato oggetto dei lavori del Comitato, e sul quale la componente italiana ed in particolare il Garante si sono fortemente impegnati, è stato l'effettività delle forme di tutela assicurate da tali clausole.

Infatti, per dati destinati all'esportazione in Paesi terzi, ivi compresi Paesi che non necessariamente offrono un sufficiente livello di salvaguardia dei dati personali, il problema è quello dell'effettività della tutela, sia con riferimento alla legge che regola il contratto tra "esportatore" comunitario dei dati ed "importatore" insediato nel Paese terzo, sia con riferimento al giudice chiamato a pronunciarsi su tale contratto; a quest'ultimo riguardo la legge regolatrice individuata nelle clausole è quella dello Stato membro nel quale è insediato l'esportatore dei dati.

Per quanto riguarda il giudice competente a decidere di controversie insorte tra le parti e l'interessato che non abbiano trovato una composizione amichevole, viene previsto uno standard minimo, e cioè la possibilità per l'interessato di deferire la composizione della disputa ad un terzo, che può essere, nei casi previsti, un'autorità nazionale di garanzia o il giudice di uno Stato membro. Sono inoltre ammesse, in ordinamenti che assicurino determinate garanzie in materia di esecuzione, decisioni arbitrali.

Dal punto di vista sostanziale appare particolarmente importante sottolineare che tali clausole, intercorrenti tra l'importatore e l'esportatore di dati, in realtà sono clausole in favore dei soggetti i cui dati sono oggetto di trattamento, perché consentono loro di agire a tutela dei propri dati personali.

Non diversamente dal *"Safe Harbor"* assume qui particolare rilievo, nella fase di applicazione, il ruolo delle autorità nazionali di garanzia, rientrando nelle loro attribuzioni sospendere o proibire nel caso concreto il trasferimento, in particolare quando un'autorità competente abbia stabilito che l'importatore dei dati non ha rispettato le clausole nonché, in primissima approssimazione, quando l'inosservanza delle clausole sia verosimile ed il protrarsi del trasferimento dei dati possa creare il rischio imminente di un grave pregiudizio agli interessati.

Spetterà poi alla Commissione, in relazione a quanto emergerà dalla fase di applicazione valutare l'opportunità di modificare la decisione relativa alle clausole.

I tre aspetti sin qui considerati, il *"Safe Harbor"*, le clausole contrattuali e le valutazioni sull'adeguatezza della protezione offerta dai diversi ordinamenti di Paesi terzi confermano la funzione centrale che le istituzioni comunitarie e le autorità garanti dei Paesi membri rivestono nella costruzione di un più generale quadro di garanzie per i dati personali, non suscettibile di essere elusa con la semplice "delocalizzazione" del trattamento in Paesi terzi.

Il Garante

La nuova composizione del Collegio

64. La continuità nell'attività dell'Autorità

Il 28 febbraio 2001 la Camera dei deputati e il Senato della Repubblica hanno eletto i quattro componenti del collegio del Garante, in vista del completamento del primo mandato quadriennale che aveva avuto inizio il 17 marzo 1997, subito dopo l'approvazione della legge n. 675/1996, con l'accettazione della nomina da parte dei componenti.

Il nuovo collegio si è insediato il 19 marzo 2001, alla presenza dei professori Stefano Rodotà e Giuseppe Santaniello (già componenti del collegio nel precedente quadriennio) e degli onorevoli Mauro Paissan e Gaetano Rasi, eletti nuovi componenti il 28 febbraio scorso.

Il 19 marzo 2001 il collegio del Garante ha eletto all'unanimità il prof. Stefano Rodotà e il prof. Giuseppe Santaniello, rispettivamente come Presidente e Vice presidente dell'Autorità, ed ha dato inizio al nuovo mandato ribadendo anche il carattere collegiale dell'organo nel lavoro interno ed esterno dell'istituzione, secondo le linee già affermatesi nel corso della precedente composizione della stessa Autorità.

Il rapporto con i cittadini

65. Le modalità di interpello dell'Autorità

Come già evidenziato nelle precedenti Relazioni annuali, il Garante ha mantenuto il contatto diretto con innumerevoli cittadini, uffici, imprese ed associazioni, assolvendo in vario modo al compito di favorire la piena conoscenza tra il pubblico delle molte disposizioni che regolano il trattamento dei dati personali nei diversi settori.

Anche nel corso del 2000 i contatti con l'Ufficio sono basati su grandi numeri e attraverso varie forme di interpello, basate anche su diversi quesiti e segnalazioni formulati direttamente dai cittadini per telefono, via *fax* o *e-mail*, o in occasione di incontri ed audizioni richiesti ai dipartimenti e servizi dell'Autorità.

Particolarmente utilizzato è risultato il servizio telefonico attivato dall'Autorità nelle ore antimeridiane, consultato incessantemente da molti interlocutori e in via di potenziamento con la prossima istituzione dell'Ufficio per le relazioni con il pubblico.

L'Autorità prosegue nella prassi di rispondere a quesiti cumulando, per quanto possibile, le questioni aventi analogo contenuto e privilegiando quelle che riguardano questioni di interesse generale, considerato il ridotto organico ancora a disposizione dell'Ufficio.

Lo strumento di interpello più utilizzato resta quello delle segnalazioni e dei reclami, per i quali, è bene ricordarlo, non sono stabilite particolari formalità e che non pongono specifici vincoli né nella

forma, né nei termini di presentazione (il procedimento è, poi, del tutto gratuito), come avviene invece per i "ricorsi" (nel senso stretto del termine) presentati ai sensi dell'art. 29 della legge n. 675/1996.

L'esame della parte della presente Relazione concernente i ricorsi permette di comprendere che il cittadino può avvalersi dello strumento-ricorso solo in particolari casi, risultando altrimenti inammissibile.

Diverse esigenze degli interessati possono essere facilmente risolte esercitando – anzitutto – i diritti garantiti dalla legge direttamente nei confronti del soggetto che detiene i dati personali per i quali si lamenta una violazione di legge o che sono inesatti, incompleti, ecc. A tal fine possono essere utilizzati anche i modelli fac-simile che l'Autorità ha messo a disposizione sul proprio sito *web* (*www.garanteprivacy.it*).

Fuori dei casi in cui sia opportuno presentare un formale ricorso ai sensi dell'art. 29 della legge (esaminato in trenta giorni), resta quindi consigliabile presentare una semplice segnalazione o reclamo, indicando però in modo circostanziato tutti gli elementi utili per esaminare meglio il caso e per semplificare gli eventuali accertamenti che l'Ufficio, a seconda dei casi, cura presso il titolare del trattamento, a volte anche attraverso visite ispettive.

LA TRATTAZIONE DEI RICORSI

66. PRINCIPALI PROBLEMI ESAMINATI

Se l'anno 1999 aveva rappresentato la fase di iniziale "rodaggio" della procedura (regolamentata dal d.P.R. n. 501/1998) relativa ai ricorsi proposti ai sensi dell'art. 29 della legge n. 675, l'anno 2000 può essere considerato come il primo anno di piena vigenza di questo nuovo meccanismo di tutela e, quindi, come il primo arco temporale al quale fare riferimento per individuarne problemi e prospettive.

Va anzitutto evidenziato come il numero dei ricorsi presentati sia andato progressivamente aumentando, a conferma di una più diffusa conoscenza della legge e degli strumenti di tutela dalla stessa apprestati.

Nel corso dell'anno solare 2000 sono pervenuti all'Ufficio 187 ricorsi, che sommati a quelli pervenuti nel 1999 ed a quelli presentati nei primi cinque mesi del corrente anno 2001 portano il totale dei ricorsi pervenuti alla data del 1° giugno 2001 a 381.

Tutti i ricorsi sono stati esaminati e decisi nel rispetto del termine di trenta giorni stabilito dall'art. 29, comma 4, della legge.

L'esame specifico dei ricorsi presentati e delle decisioni emesse fa però emergere come sia ancora frequente un uso improprio di questo strumento, talvolta erroneamente percepito come una sorta di "ultima spiaggia" da utilizzare dopo aver esperito ogni altro rimedio giudiziale o, al contrario, come mera "scorciatoia" per ottenere giustizia in modo estremamente veloce.

Inoltre, in diversi casi, sono stati presentati ricorsi che non facevano riferimento all'esercizio dei diritti dell'art. 13, ma avevano ad oggetto, più genericamente, lamentele relative ad altri profili che la legge n. 675 permette di affrontare, ma in altro modo, oppure casi nei quali venivano portate a conoscenza del Garante presunte violazioni di legge non coinvolgenti direttamente la posizione degli interessati, ma riferite invece a posizioni di terzi. Si tratta infatti di fattispecie spesso ugualmente meritevoli di attenzione che devono però essere portate all'attenzione del Garante non con lo strumento del ricorso ex art. 29, bensì con quello della "segnalazione" o del "reclamo" proposti ai sensi dell'art. 31, comma 1, lett. d), della legge n. 675 (*Provv.* del 29 febbraio 2000).

Va altresì ricordato che con lo strumento del ricorso (che è possibile presentare solo per far valere una delle posizioni giuridiche enumerate nell'art. 13, comma 1, della legge, e dopo un insoddisfacente interpello del titolare del trattamento) non è possibile proporre innanzi al Garante istanze (quali quelle di tipo risarcitorio) che restano di esclusiva competenza dell'autorità giudiziaria.

Un aiuto efficace ad una più corretta conoscenza del "meccanismo di funzionamento" dei ricorsi è venuta dall'utilizzo del sito Internet del Garante, sia grazie ad una apposita pagina contenente le istruzioni di base al riguardo, sia attraverso una sempre più ampia e tempestiva diffusione in rete delle più significative decisioni del Garante.

Particolarmente interessante è, poi, l'esame della tipologia dei ricorsi decisi dall'Autorità. Ne emerge infatti un'estrema varietà di temi trattati a conferma della trasversalità della disciplina sulla protezione dei dati personali. L'esperienza di questi due anni di vigenza delle norme in materia di ricorsi consente ora di richiamare l'attenzione sui temi che più frequentemente si sono presentati all'attenzione del Garante. Se ne propone di seguito una sintetica rassegna, rinviando per l'approfondimento delle singole questioni agli specifici paragrafi della presente Relazione.

Accesso ai dati personali dei lavoratori. Molti ricorsi hanno riguardato questa fattispecie, con particolare riferimento ai dati personali di tipo valutativo (sui quali il Garante si era pronunciato fin dal 2 giugno 1999) o comunque a giudizi, punteggi, indici di produttività del dipendente espressi dal datore di lavoro (vedi, ad es., il *Provv.* del 28 giugno 2000).

Dati personali contenuti nelle perizie medico legali. È il settore che ha visto la più alta incidenza di ricorsi proposti. Si tratta di richieste di accesso generalmente inserite in un più ampio contenzioso assicurativo e volte specificamente a conoscere le valutazioni ed i giudizi espressi dai medici di fiducia delle società di assicurazione in relazione ai danni fisici patiti dagli interessati in ordine ai sinistri denunciati (vedi, fra le più recenti, il *Provv.* dell'8 maggio 2001).

Telecomunicazioni. Numerose istanze di accesso, correzione o integrazione dei dati, nonché di cancellazione o di opposizione al trattamento sono state avanzate da utenti nei confronti dei gestori di servizi di telecomunicazione, specialmente delle società fornitrici di servizi telefonici. L'incalzante sviluppo tecnologico in materia ha portato ad applicare i predetti meccanismi di tutela anche alla realtà della rete, attraverso, ad esempio, la proposizione di ricorsi nei confronti di trattamenti di dati effettuati a mezzo siti Internet.

Dati trattati da banche, società finanziarie e centrali rischi private. È un altro dei fronti tradizionalmente "caldi" dove il trattamento dei dati personali si connette strettamente alle esigenze del corretto funzionamento del sistema economico, della sicurezza e dell'affidabilità degli operatori. Si tratta di un settore nel quale la questione affrontata in sede di ricorso ha portato talvolta a successivi ed autonomi approfondimenti, specie con riguardo all'informativa resa, alla raccolta del consenso e all'estensione delle ipotesi di comunicazione dei dati a terzi.

Dati sanitari. La delicatezza dei dati riguardanti lo stato di salute e la giustificata attenzione degli interessati al riguardo ha dato luogo alla presentazione di ricorsi anche in questo campo, sia con riguardo alla necessità dell'interessato di avere piena contezza dei dati – comuni e sensibili – raccolti sul proprio conto (in relazione a trattamenti sanitari svolti in strutture pubbliche o private), sia in relazione all'esigenza di verificare la liceità, la pertinenza e la non eccedenza dei trattamenti stessi (*Provv.* del 26 marzo 2001).

Trattamenti in ambito giornalistico. Una serie di ricorsi hanno riguardato questo settore con specifico riferimento al disposto dell'art. 25 della legge ed alle disposizioni di dettaglio previste dal c.d. codice deontologico dei giornalisti. All'interno di questo ambito si è segnalata come particolarmente delicata la casistica emersa in riferimento al trattamento dei dati personali di soggetti minori nel corso di trasmissioni televisive.

Casi diversi. Nell'ultimo periodo sono stati portati all'attenzione del Garante, con lo strumento del ricorso, alcuni temi rispetto ai quali emerge una diffusa sensibilità degli interessati. Basti ricordare al riguardo il trattamento dei dati in ambito condominiale o quello svolto da professionisti legali o da loro collaboratori e consulenti nell'ambito di procedimenti giudiziari.

67. ASPETTI PROCEDURALI

La legge n. 675 e le disposizioni del regolamento applicativo (artt. 18, 19 e 20 del d.P.R. n. 501/1998) hanno configurato il ricorso ex art. 29 come uno strumento estremamente veloce nella tempistica di decisione e sostanzialmente agevole nelle formalità procedurali. Purtuttavia, alcuni requisiti minimi devono essere osservati dal ricorrente che voglia correttamente utilizzare questo strumento.

In proposito vanno segnalati alcuni dei più frequenti "errori" nei quali sono incorsi i ricorrenti. Va anzitutto ricordato che la presentazione del ricorso può avvenire di regola solo a seguito di una previa istanza inoltrata, ai sensi dell'art. 13 della legge, al titolare o al responsabile del trattamento, qualora non sia pervenuta all'interessato alcuna risposta od il riscontro fornito sia ritenuto incompleto o inidoneo.

La legge ha peraltro previsto (art. 29, comma 2) un tempo per la risposta all'interessato estremamente breve (cinque giorni). Solo quando il decorso di tale pur breve termine può esporre "*taluno a pregiudizio imminente e irreparabile*" è possibile prescindere dal previo interpello del titolare del trattamento.

In alcuni casi, invece, sono stati presentati al Garante ricorsi che non erano stati preceduti dalla presentazione dell'istanza ex art. 13 (*Provv.* del 30 ottobre 2000), oppure ricorsi dei quali veniva evidenziata una generica urgenza non comprovata da utili riscontri.

Altri specifici profili procedurali sono emersi nel corso dell'ultimo anno. Fra questi si ricordano:

Autenticazione della firma del ricorrente. Il già citato d.P.R. n. 501 ha previsto che l'atto di ricorso debba recare la sottoscrizione del ricorrente autenticata a norma di legge (ossia dal legale, nel caso di procura rilasciata allo stesso, o da altri soggetti abilitati all'autenticazione della firma, nel caso di ricorso proposto direttamente senza assistenza di legale). Tale requisito è, come detto, espressamente richiesto dalle norme regolamentari concernenti i ricorsi (art. 18, comma 1, lettera e), d.P.R. n. 501/1998) e non può essere sostituito (come erroneamente ritenuto da altri ricorrenti) dall'autocertificazione della firma. La citata disposizione regolamentare costituisce, in effetti, una disciplina speciale, non abrogata dal d.P.R. 28 dicembre 2000, n. 445, che trova giustificazione nella peculiarità del procedimento attivato dal ricorso medesimo. Con tale strumento, infatti, gli interessati chiedono la tutela di propri diritti soggettivi in alternativa ad un'azione dinanzi all'autorità giudiziaria, e provocano l'adozione di un provvedimento che deve essere rispettato a pena di sanzione penale.

Verifica dell'identità del ricorrente. È stata eccepita da un titolare di trattamento l'inammissibilità di un ricorso, sostenendo che l'istanza di accesso ex art. 13 era stata presentata dall'interessato senza allegare un documento di riconoscimento. Tale eccezione è stata ritenuta infondata dal Garante (*Provv.* 14 marzo 2001). In effetti l'art. 17, comma 2, del d.P.R. n. 501/1998 precisa che "l'interessato deve dimostrare la propria identità, *anche* esibendo o allegando copia di un documento di riconoscimento". L'allegazione di un documento d'identità è, dunque, una delle possibili modalità di dimostrazione dell'identità personale, né esclusiva, né obbligatoria, essendo sufficiente appurare l'identità personale anche attraverso altre adeguate circostanze quale tra l'altro la conoscenza personale. Nel caso di specie, tra l'altro, risultava che il titolare stesso, sia in sede di prima risposta all'istanza ex art. 13, sia in sede di riscontro all'invito ad aderire alle richieste dell'interessato (formulato dall'Autorità nel quadro della procedura di ricorso), avesse comunque riscontrato le istanze dell'interessato senza sollevare obiezione alcuna.

Esercizio dei diritti e ricorso a mezzo di delega o procura a soggetto terzo. In proposito il Garante ha ricordato (*Provv.* 23 maggio 2001) che la legge n. 675 prevede la possibilità per l'interessato di esercitare i diritti di cui all'art. 13 della medesima legge personalmente o conferendo, per iscritto, delega o procura a persone fisiche o ad associazioni (art. 13, comma 4). Più specificamente l'art. 17, comma 2, del d.P.R. n. 501/1998 prevede che la persona che esercita i diritti di cui all'art. 13 su incarico dell'interessato, deve esibire o allegare al titolare stesso copia della procura o della delega recante sottoscrizione autenticata nelle forma di legge. In caso di successivo ricorso ex art. 29, che non sia presentato personalmente dall'interessato, il soggetto che lo sottoscrive per conto di quest'ultimo deve produrre la propria sottoscrizione autenticata nelle forme di legge ed allegare inoltre la procura speciale rilasciata (art. 18, commi 1, lett. e) e 2, d.P.R. n. 501/1998).

Alternatività del ricorso al Garante. L'art. 29, comma 1, ultimo periodo, della legge precisa che "*il ricorso al Garante non può essere proposto qualora, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'autorità giudiziaria*". Pertanto non è ad esempio possibile invocare con un ricorso la tutela del Garante (sulla base della legge sulla protezione dei dati personali), in riferimento a giudizi e a valutazioni espressi da un datore di lavoro nei confronti di un dipendente, quando l'atto che li contiene e che ha determinato la risoluzione del rapporto è stato già posto all'esame del giudice ordinario in funzione di giudice del lavoro con un'istanza di reintegrazione nelle funzioni lavorative basata anche sulla contestazione dei medesimi profili di *privacy* rappresentati poi al Garante.

Infine, esistono ambiti o tipi di trattamento rispetto ai quali non è possibile esercitare i diritti dell'art. 13 e conseguentemente proporre ricorso ex art. 29. In proposito si deve ad esempio citare la disposizione dell'art. 3 secondo la quale il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto – a date condizioni – all'applicazione della legge n. 675. Di conseguenza non è ipotizzabile la presentazione di ricorsi attinenti alla sfera dei rapporti interpersonali (*Provv.* 7 settembre 2000). Parimenti, non è al momento possibile proporre ricorsi in ordine ai trattamenti enumerati nell'art. 4, comma 1, della legge (trattamenti svolti da uffici giudiziari per ragioni di giustizia, trattamenti svolti per finalità di difesa dello Stato e per la prevenzione o la repressione dei reati, ecc.). In tale ambito specifico rientrano anche i trattamenti concernenti l'applicazione della legge n. 1423 del 1956 in tema di misure di prevenzione (*Provv.* 1° settembre 2000). Tali trattamenti non si collocano peraltro in una "zona franca" priva di alcuna tutela sotto il profilo della "*data protection*". È infatti possibile sollecitare, attraverso una richiesta o l'invio di una segnalazione o reclamo al Garante, la verifica della rispondenza dei trattamenti di dati ai requisiti stabiliti dalla legge e dai regolamenti (artt. 31, comma 1, lettera d) e 32). A tutti i trattamenti di cui al citato art. 4, comma 1, sono comunque applicabili le norme della legge n. 675 specificate nel comma 2 del medesimo art. 4.

IMPUGNAZIONE DEI PROVVEDIMENTI DELL'AUTORITÀ

68. CASI DI CONTENZIOSO E TIPOLOGIE DI ATTI IMPUGNATI

Il numero di provvedimenti del Garante che in questi primi anni di attività sono stati oggetto di impugnazione è piuttosto limitato. Si esamina qui brevemente questa casistica facendo riferimento alla tipologia degli atti impugnati.

Ricorsi ex art. 29. Dal febbraio 1999 (data di entrata in vigore delle norme regolamentari concernenti i ricorsi) al 31 maggio 2001 risultano essere stati impugnati davanti al competente tribunale ordinario, ai sensi dell'art. 29, comma 6, della legge, n. otto decisioni del Garante emesse in relazione a ricorsi (su un totale di 354 ricorsi già decisi). In tre dei casi citati, in presenza di decisioni del tribunale che hanno annullato il provvedimento del Garante precedentemente emesso, gli interessati hanno presentato ricorso per cassazione. Il Garante si è costituito in giudizio in sede di merito e di legittimità quando l'impugnazione è stata notificata all'Autorità o ne è giunta comunque notizia al Garante.

Uno dei "nodi" che si è posto al riguardo è quello concernente la legittimazione passiva del Garante e quindi la possibilità dello stesso di costituirsi, di regola tramite l'Avvocatura dello Stato, innanzi ai tribunali o alla Corte di cassazione per difendere le ragioni giuridiche dei provvedimenti opposti, limitatamente a questioni di interesse generale strettamente connessi ad una corretta applicazione della legge, anziché ad aspetti di merito legati a specifiche questioni.

Fin dal primo momento, sulla questione il Garante aveva chiesto il parere dell'Avvocatura generale dello Stato, che si è espressa sul delicato profilo con un parere del 29 ottobre 1999. In tale occasione, pur nella consapevolezza della novità e della peculiarità della fattispecie, è stato espresso un avviso favorevole alla costituzione dell'Autorità nei citati giudizi affinché il Garante possa far valere le proprie ragioni a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni. Ciò in quanto la determinazione del Garante, emessa appunto in relazione ad un ricorso presentato ai sensi dell'art. 29, non è solo decisione su un contrasto tra parti, ma pure espressione di una visione e valutazione dell'interesse pubblico generale, a tutela del quale l'Autorità è tenuta a svolgere le proprie funzioni.

L'Avvocatura ha peraltro sottolineato l'opportunità di limitare in concreto la costituzione in giudizio ai soli aspetti nei quali si presentino in maniera più specifica i profili attinenti all'interesse pubblico protetto.

A questo indirizzo il Garante si è attenuto costantemente in questi mesi, intervenendo a difesa di decisioni il cui rilievo, andando ben oltre il limitato caso di specie, aveva riflessi su un'ampia platea di interessati e coinvolgeva rilevanti profili interpretativi della disciplina sulla protezione dei dati personali (si pensi, ad esempio, alla questione se la legge sia applicabile ed in quale misura al settore giornalistico, anche quando il trattamento di dati non pertenga ad una "banca di dati").

Si segnalano in proposito gli atti con i quali alcuni titolari di trattamento hanno impugnato le decisioni con cui il Garante aveva riconosciuto a taluni dipendenti l'accesso a tutti i dati personali detenuti dal datore di lavoro, ivi compresi i giudizi e le valutazioni annuali, nonché l'impugnazione di un provvedimento con il quale era stato riconosciuto ad un danneggiato l'accesso integrale ad una perizia medico-legale redatta dal medico di fiducia di una società di assicurazione cui era stata presentata una richiesta di risarcimento del danno.

Si tratta di questioni di rilevante attualità per un vasto numero di interessati, specificamente approfondite nelle relative sezioni di questa relazione. In questa sede giova solo ricordare come al centro di entrambe le vicende vi sia il concetto stesso di "dato personale" che l'art. 1 della legge n. 675 e la direttiva comunitaria n. 95/46 descrivono in modo particolarmente ampio. È su questa definizione normativa che il Garante ha fatto leva per assumere e precisare, appunto, un'ampia conformazione del concetto di dato personale che, al di là degli elementi strettamente oggettivi o identificativi di un soggetto, ricomprende i giudizi e le valutazioni che parimenti offrono un contributo informativo su una determinata persona.

Vanno infine ricordati altri tre casi di opposizione a decisioni su ricorsi che hanno riguardato diversi aspetti della legge n. 675:

– l'opposizione alla decisione del Garante del 19 aprile 1999 (caso Valoti/Olcese–R.C.S. Editore S.p.a., oggetto anche di vari commenti in dottrina), con specifico riferimento ai limiti di applicabilità della legge n. 675 ai trattamenti in ambito giornalistico. Dopo l'annullamento della decisione del Garante da parte del Tribunale di Milano si è in attesa del deposito della recente decisione della Corte di cassazione;

– il decreto del Tribunale di Milano del 20 ottobre 2000 con il quale è stata rigettata l'opposizione proposta da RAI S.p.a. nei confronti della decisione del Garante del 31 maggio 2000, anch'essa relativa a trattamenti in ambito giornalistico;

– la decisione del Tribunale di Padova del 26 maggio 2000 che ha rigettato l'opposizione avverso il provvedimento del Garante del 9 settembre 1999 con il quale era stato rigettato il ricorso dell'interessato in merito al diniego di cancellazione dei propri dati personali dal registro dei battesimi della parrocchia nella quale era stato a suo tempo celebrato il sacramento.

Altri provvedimenti impugnati. In proposito si deve segnalare l'impugnazione di due decisioni adottate dal Garante sulla base di poteri e funzioni diversi da quelli di cui all'art. 29 della legge:

– l'impugnazione proposta dalla Congregazione cristiana dei Testimoni di Geova nei confronti del provvedimento del 29 settembre 1999 (autorizzazione generale n. 3/1999 al trattamento dei dati sensibili da parte degli organismi associativi e delle fondazioni) che è stata rigettata dal Tribunale di Roma il 5 luglio 2000;

– la recente impugnazione dinanzi al Tribunale di Roma, da parte dell'Associazione politica nazionale "Lista Marco Pannella", del provvedimento in data 11 gennaio 2001 relativo all'invio di messaggi politici tramite *e-mail.*

ATTIVITÀ ISPETTIVE E APPLICAZIONE DI SANZIONI AMMINISTRATIVE

69. LA PROGRAMMAZIONE DELLE ISPEZIONI E I RISULTATI

Nel corso del 2000 è proseguita l'attività di strutturazione e programmazione delle attività ispettive del Garante, intendendo per tali gli interventi esterni effettuati dall'Autorità nei luoghi dove si svolgono i trattamenti di dati.

Tali attività sono eseguite, di norma, da personale del Dipartimento vigilanza e controllo e possono essere classificate in cinque principali tipologie la cui scelta è determinata in ragione dello specifico fine istituzionale da raggiungere ed è informata a principi di proporzionalità, adeguatezza e gradualità.

Più in particolare, si distinguono sopralluoghi (con o senza preavviso), accessi alle banche di dati, collaborazioni, investigazioni e indagini conoscitive.

I *sopralluoghi con preavviso* sono effettuati sulla base del disposto dell'art. 32, comma 2, della legge, hanno natura collaborativa e consistono nell'invio di funzionari del Garante nei luoghi dove si svolge il trattamento per procedere, di concerto con il titolare o il responsabile, all'acquisizione diretta di informazioni e di documenti. Si tratta di una procedura utilizzata specie quando sono necessarie descrizioni analitiche alle quali gli interessati potrebbero avere difficoltà a rispondere in modo esaustivo. Un importante e riuscito sopralluogo con preavviso è stato ad esempio eseguito per controllare un particolare sistema di rilevazione di impronte digitali posto all'ingresso di un istituto bancario.

I *sopralluoghi senza preavviso* sono disposti, invece, anche in relazione a quanto previsto dall'art. 13, comma 1, della legge 24 novembre 1981, n. 689 e sono finalizzati al controllo dell'osservanza delle disposizioni per la cui violazione l'art. 39 della legge n. 675 prevede la sanzione amministrativa del pagamento di una somma di denaro. Si fa riferimento, ad esempio, alle ipotesi di mancata o infedele risposta alle richieste di informazioni e di esibizione di documenti (art. 32, comma 1) o di mancata o irregolare informativa (art. 10). In questi casi, i funzionari dell'Ufficio del Garante possono assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica. Tale tipologia d'intervento è stata utilizzata, tra l'altro, per verificare la legittimità di installazioni di impianti di videosorveglianza e di *webcam* in esercizi commerciali e in laboratori artigiani.

Gli *accessi alle banche dati* sono effettuati, invece, in base ai poteri dell'art. 32, comma 2, della legge. La norma fa riferimento anche ad "altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo". In tali casi, l'Ufficio dispone di poteri incisivi e l'intervento può essere in ipotesi eseguito anche contro la volontà degli interessati, previa autorizzazione del presidente del tribunale territorialmente competente (art. 32, comma 3, della legge), oppure dotandosi dell'assenso scritto ed informato del titolare o del responsabile del trat-

tamento (art. 15, comma 1, d.P.R. n. 501/1998). Simili accessi, ispezioni e verifiche sono state ad esempio eseguite nei confronti di due società di *direct marketing* che gestiscono grandi basi di dati personali a fini commerciali.

Ulteriori tipologie ispettive sono rappresentate dalle richieste di collaborazione che pervengono da autorità giudiziarie o di polizia e dalle investigazioni di polizia giudiziaria. Per queste ultime, la legge prevede che il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'art. 32 possa rivestire, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria (art. 33, comma 6-*bis*). Tale personale può effettuare indagini di propria iniziativa con i poteri di cui all'art. 347 ss. del codice di procedura penale.

Le *indagini conoscitive*, infine, sono interventi esterni a carattere collaborativo disposti per verificare lo stato di attuazione della legge in determinati settori che normalmente si concludono con delibere di portata applicativa generale nei confronti dei vari soggetti che svolgono trattamenti della specie considerata.

Le ispezioni sono state effettuate sulla base di un *programma periodico* che determina, per ciascuna tipologia, le priorità e i criteri informatori ai quali l'Ufficio deve attenersi. Sulla base di tali indicazioni, le attività ispettive dell'anno 2000 hanno tratto origine, per due terzi, da segnalazioni e reclami e, per la restante parte, da iniziative autonome del Garante. Nel settore privato i controlli hanno riguardato società di *direct marketing*, due editori, una banca, altre imprese del terziario e una ditta artigiana. Anche tre organismi pubblici (due comuni e un istituto ospedaliero) sono stati oggetto di accertamenti.

Metà dei controlli hanno avuto esito positivo con la constatazione di illegittimità riconducibili, almeno in parte, ad una ancora insufficiente conoscenza della normativa sulla protezione dei dati personali. Di conseguenza, sono stati emessi provvedimenti di blocco e di divieto e sono state applicate sanzioni amministrative. Nei casi più gravi sono state inviate segnalazioni all'autorità giudiziaria, una delle quali ha riguardato i responsabili di un soggetto pubblico per l'omessa adozione delle misure necessarie alla sicurezza dei dati (art. 36 della legge).

Particolare rilievo ha avuto un accertamento riguardante un vasto commercio di dati di minori venduti da una società di *direct marketing* ed utilizzati dalle imprese clienti per inviare sollecitazioni commerciali alle famiglie dei bambini. Gli accertamenti, effettuati anche in collaborazione con la Guardia di finanza e con la Polizia postale delle comunicazioni, sono stati estesi a editori e ad un'anagrafe comunale ed hanno portato all'emissione di un provvedimento di blocco dei trattamenti e di segnalazioni all'autorità giudiziaria per i reati di trattamento illecito di dati personali (art. 35 della legge) e di omessa e incompleta notificazione al Garante (art. 34) per i quali è prevista la reclusione fino a due anni.

L'analogo programma di ispezioni del primo semestre 2001 prevede che gli interventi vengano effettuati sulla base dei seguenti criteri: *a)* i sopralluoghi verranno di regola disposti quando, per acquisire gli elementi necessari, non sia ritenuto utile rivolgere una richiesta di informazioni o di esibizione di documenti; *b)* gli accessi alle banche dati verranno di regola disposti quando non sia ritenuto opportuno procedere alla richiesta di informazioni o di esibizione di documenti oppure quando le informazioni o i documenti richiesti o pervenuti siano ritenuti incompleti e non veritieri; *c)* le collaborazioni effettuate su richiesta della magistratura e delle forze di polizia verranno disposte dando priorità ai contesti dai quali emergono o potrebbero emergere notizie di reato.

L'Ufficio continuerà ad avvalersi della collaborazione di altri organi dello Stato quando ciò sia necessario per assicurare la speditezza e la completezza dei controlli, anche sulla base di eventuali protocolli d'intesa con le forze di polizia.

Quanto all'autorizzazione giudiziaria prevista dall'art. 32, comma 3, i primi accertamenti esterni svolti hanno evidenziato come tale procedura richieda, a volte, tempi di attesa non compatibili con le esigenze di rapidità dell'Ufficio. Con i successivi accertamenti è stata perciò sperimentata la procedura dell'assenso scritto e informato prevista dall'art. 15 del d.P.R. n. 501/1998 e i risultati sono stati decisamente positivi. L'assenso, infatti, è stato sempre concesso, gli accertamenti sono stati eseguiti dopo un brevissimo lasso di tempo dalle deliberazioni del Garante e sono stati acquisiti tutti gli elementi necessari per il prosieguo degli accertamenti. In futuro, pertanto, gli interventi dell'autorità giudiziaria saranno probabilmente limitati ai casi di maggiore complessità e gravità o quando l'assenso sia rifiutato o ritardato.

70. Il procedimento per l'applicazione di sanzioni

Nel corso del 2000 non sono emersi presso il Garante particolari problematiche applicative per quanto riguarda le sanzioni di carattere penale previste dalla legge n. 675/1996 (omessa o infedele noti-

ficazione – art. 34 –, raccolta e trattamento illecito dei dati – art. 35 –, omessa adozione delle misure minime di sicurezza – art. 36 –, inosservanza dei provvedimenti del Garante (art. 37)). Le doverose denunce di reato sono state trasmesse dall'Ufficio in conseguenza di ispezioni *in loco* o di un accertamento dei fatti nell'ambito di una deliberazione collegiale.

Si è proceduto invece a terminare la fase di rodaggio del procedimento amministrativo per l'applicazione delle sanzioni amministrative pecuniarie indicate nell'articolo 39 della legge.

Il comma 1 dell'art. 39 prevede infatti una sanzione applicabile a chiunque ometta di fornire le informazioni o di esibire i documenti richiesti dal Garante (pertanto tale richiesta può essere indirizzata indifferentemente al titolare, al responsabile, all'incaricato del trattamento, a terzi e, in ipotesi, allo stesso interessato).

La richiesta di informazioni o l'esibizione di documenti può essere formulata a seguito della presentazione di un ricorso (art. 29, comma 4) o in qualsiasi altro momento purché occorra ai fini dell'espletamento dei compiti del Garante (art. 32, comma 1).

L'illecito si configura allorché è decorso inutilmente il termine prefissato dal Garante. Nel caso appena indicato la sanzione è da lire un milione a lire sei milioni e in questo come nei successivi casi l'illecito può essere ovviamente definito con il pagamento in misura ridotta di lire due milioni, oltre alle spese del procedimento, come è avvenuto in un importante caso di mancata informativa circa la raccolta di impronte digitali all'ingresso di un istituto bancario (art. 16 l. n. 689/1981).

La sanzione è invece inferiore (da lire cinquecentomila a lire tre milioni: art. 39, comma 2) e può essere quindi oggetto di un pagamento in forma ridotta pari a lire un milione qualora l'illecito consista: *a)* nella mancata o incompleta o tardiva informativa diretta alla persona presso la quale sono raccolti i dati (art. 10, comma 1); *b)* nella mancata o incompleta o tardiva informativa all'interessato quando i dati sono stati raccolti presso terzi (art. 10, comma 3); *c)* nel mancato invio delle informative di cui ai commi 1 e 2 dell'art. 10 "giustificato" dall'improprio utilizzo delle eccezioni previste dall'art. 10, commi 2 e 4; *d)* nella comunicazione all'interessato dei dati idonei a rivelare lo stato di salute senza il tramite del medico scelto dall'interessato oppure, in mancanza di tale indicazione, dal titolare.

Come si diceva, l'Autorità ha ora definito compiutamente una procedura per applicare tali sanzioni.

Si procede previamente con la notificazione di una "contestazione di violazione amministrativa", che si concretizza di regola nell'invio dell'atto in copia conforme all'originale con plico raccomandato, dal ricevimento della quale decorrono i seguenti termini:

– uno di trenta giorni entro il quale la parte potrà far pervenire all'Autorità scritti difensivi, documenti e potrà chiedere di essere sentita;

– uno di sessanta giorni (art. 16 l. 24 novembre 1981, n. 689) entro il quale il titolare del trattamento è ammesso a pagare una somma in misura ridotta tramite versamento sul conto corrente postale intestato al Garante per la protezione dei dati personali.

In caso di pagamento deve darsi tempestiva comunicazione all'Ufficio, presentando o inviando copia della quietanza, al fine di evitare l'inoltro del rapporto per l'ordinanza-ingiunzione e l'applicazione della sanzione in misura intera trascorsi i sessanta giorni dalla notificazione.

Qualora non venga effettuato il pagamento in misura ridotta entro i sessanta giorni dalla notifica dell'atto, infatti, l'Ufficio predispone un rapporto e il Garante adotta i provvedimenti previsti all'articolo 18 della legge n. 689/1981 in relazione all'articolo 39 della legge n. 675/1996.

La destinazione dei proventi delle sanzioni tiene conto di quanto disposto dall'art. 14 del d.lg. 30 luglio 1999, n. 281, il quale, integrando il comma 3 dell'articolo 39 della legge n. 675/1996, ha stabilito che i proventi stessi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo che attende alle spese di funzionamento dell'Ufficio del Garante, per essere poi utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 31, comma 1, lett. i) (*"curare la conoscenza tra il pubblico delle norme che regolano la materia e le relative finalità, nonché delle misure di sicurezza"*) e 32 (*"accertamenti e controlli"*).

LA COLLABORAZIONE CON ALTRE AUTORITÀ INDIPENDENTI

71. LE PRINCIPALI ATTIVITÀ

L'art. 31, commi 5 e 6, della legge n. 675/1996, prevede una cooperazione tra il Garante ed altre autorità indipendenti nello svolgimento dei rispettivi compiti.

Anche nel corso del 2000 questa cooperazione si è sviluppata in diversi contatti ed anche attraverso quesiti, sia per le questioni di trattamento dei dati personali, sia per quanto riguarda il trattamento giuridico ed economico del personale.

Un piano di lavoro comune su alcuni punti è stato di recente convenuto in un positivo incontro tra il Garante e l'AIPA, che dovrebbe avere come primo sbocco un documento congiunto di linee-guida sulle basi di dati della pubblica amministrazione.

Quesiti e richieste di collaborazione vanno segnalate anche per quanto riguarda la Consob e l'Autorità per le garanzie nelle comunicazioni, da ultimo per quanto riguarda i diritti degli utenti riguardo alla formazione di elenchi per la telefonia mobile.

L'ATTIVITÀ DI INFORMAZIONE E COMUNICAZIONE

72. PROFILI GENERALI

Al forte consolidamento dell'attività del Garante e al pieno riconoscimento – da parte della società, del mondo delle imprese, della pubblica amministrazione e dei *media* – del ruolo di tutela svolto dall'Autorità, ha corrisposto uno sforzo di informazione, ancora più incisivo e puntuale, sui nuovi diritti introdotti dalla disciplina sulla protezione dei dati e sulla revisione dell'ordinamento giuridico oltre che delle prassi in vigore nel Paese.

L'impegno ad una comunicazione efficace e capillare risponde non solo all'esigenza di adempiere ai compiti affidati all'Autorità dalla legge sulla *privacy*, ma è frutto della consapevolezza che, anche grazie ad un costante, rigoroso e affidabile lavoro di chiarificazione e orientamento, può realizzarsi l'obiettivo di una crescita complessiva della società e la costruzione di quella cultura del rispetto che rappresenta un vero salto qualitativo, improntato alla trasparenza e al rigore, nei rapporti tra cittadini e le piccole e grandi banche dati presenti in Italia.

In questa direzione il Garante ha utilizzato diverse forme di comunicazione, da quelle più tradizionali a quelle a carattere multimediale, ipertertestuale e interattivo, diffondendo e rendendo accessibili le pubblicazioni *on-line* e servendosi, comunque, anche di supporti *off-line* quali ad esempio *CD Rom*.

L'attività di informazione del Garante ha privilegiato un linguaggio attento ad una funzione informativa e al tempo stesso esplicativa dei processi e delle ragioni alla base delle decisioni e delle iniziative poste in essere, nonché illustrativa delle innovazioni, in termini di procedure e prassi, che la legge sulla protezione dei dati ha determinato nei diversi ambiti organizzativi, sia sociali che economici. L'accento è stato posto dall'Autorità sulle novità introdotte dalle norme e sui diritti riconosciuti ai cittadini e agli utenti di scegliere liberamente e di controllare, anche attraverso un espresso consenso preventivo, l'ambito di circolazione dei dati.

La comunicazione dell'Autorità si è dunque connotata come fortemente tesa ad avviare procedure di riorganizzazione dei servizi pubblici e privati e a promuovere nuovi diritti dei cittadini (trasparenza, semplificazione, riservatezza, accesso). Comunicare, insomma, non ha mai rappresentato per un'istituzione come il Garante una funzione aggiuntiva ed estranea ai processi organizzativi interni, ma un elemento strategico irrinunciabile per avviare processi di trasformazione e per definire un nuovo sistema di relazioni tra istituzioni e cittadini.

In questo senso, la stessa previsione contenuta nell'art. 31, lettera i), della legge n. 675, che prevede tra i compiti del Garante quello di *"curare la conoscenza tra il pubblico delle norme che regolano la materia"*, risponde pienamente ai canoni fissati dalla innovativa legge n. 150 del 2000 con la quale la comunicazione pubblica viene definitivamente legittimata e diviene obbligo istituzionale.

Le tematiche che più hanno incontrato l'interesse della stampa riguardano la tutela dei consumatori (la protezione su Internet, le forme di raccolta di dati mediante tagliandi, l'utilizzo di dati sanitari nell'*e-commerce*, i rapporti con il sistema bancario, l'uso delle impronte digitali, il *direct marketing*); l'attività di ispezione svolta dal Garante direttamente presso le banche dati; il lavoro di indagine riguardo ai tracciamenti invisibili (Echelon, Internet); la sanità; le misure di sicurezza, i dati genetici, la videosorveglianza; i rapporti tra diritto di cronaca e tutela della riservatezza; le grandi reti della pubblica amministrazione; la propaganda elettorale; i controlli sui lavoratori; le grandi schedature di massa.

Nel periodo dal gennaio 2000 all'aprile 2001, le pagine dedicate alla *privacy* dai maggiori quotidiani e periodici nazionali sono state oltre 4000, delle quali circa 1700 dedicate specificamente all'attività del Garante. Le prime pagine sono state circa 650.

La tipologia dei prodotti informativi è stata, come si è detto, ampia e differenziata.

La *Newsletter* settimanale, al suo secondo anno di pubblicazione, ha svolto una funzione importante nella diffusione dell'attività dell'Ufficio. Illustrando gli interventi del Garante in chiave divulgativa, essa ha consentito di raggiungere un pubblico sempre più ampio, composto non più, come in un primo tempo, solo di giornalisti, amministratori pubblici e professionisti, ma anche di operatori del settore creditizio, industriale, di rappresentanti delle associazioni di categoria e di semplici cittadini. Affiancando la comunicazione tradizionale, realizzata attraverso comunicati stampa, con una di tipo più ampio e approfondito, la *Newsletter* si è rivelata oltre che uno strumento di comunicazione, anche una sorta di "archivio" di consultazione relativamente ai diversi ambiti di applicazione della legge n. 675 e ai variegati aspetti connessi con la tutela della riservatezza sui quali l'Autorità è intervenuta. La possibilità di consultare la *Newsletter on-line* ha facilitato la diffusione delle informazioni.

Le *Newsletter* diffuse nel periodo che va dal gennaio 2000 all'aprile 2001 sono state 55, mentre i comunicati-stampa 71.

È proseguita la realizzazione del *CD Rom*, giunto nel 2000 alla sua terza edizione: un archivio digitale ipertestuale che contiene la documentazione integrale, relativa all'attività del Garante, alla normativa nazionale ed internazionale di riferimento e alle pubblicazioni fin qui realizzate.

L'archivio digitale "*Cittadini e Società dell'informazione*" è distribuito su *CD Rom* multipiattaforma ed è realizzato in formato *Adobe Pdf*, scelto per la sua flessibilità nel gestire e riprodurre lunghi documenti di testo rispettandone i caratteri, l'impaginazione, le immagini e gli elementi grafici in maniera indipendente dalle applicazioni *software* e dall'*hardware* con cui sono stati generati. L'accesso alle informazioni è facilitato da un'interfaccia sobria, studiata per consentire di "navigare" attraverso le varie sezioni dell'archivio grazie ai controlli dinamici inseriti nelle pagine sotto forma di icone.

Un lavoro di catalogazione dei documenti consente infine, grazie agli strumenti messi a disposizione da *Acrobat*, di effettuare ricerche "*full text*" all'interno del *CD Rom*.

Il successo del *CD*, che viene inviato gratuitamente a chiunque ne faccia richiesta, è testimoniato dall'alto numero di richieste, oltre 6000 per la sola terza edizione, pervenute da amministrazioni pubbliche, dal settore privato, da liberi professionisti e da semplici cittadini.

Tra le attività di comunicazione va ricordata inoltre la pubblicazione, dapprima bi-trimestrale e dal 1° gennaio 2001 a cadenza mensile, del Bollettino "*Cittadini e Società dell'Informazione*" che ha raggiunto il numero 21 nel mese di giugno 2001 e che raccoglie i provvedimenti del Garante, la normativa in materia, i comunicati stampa ed altra documentazione sull'attività dell'Autorità.

Il rapporto con il pubblico, assicurato attraverso il menzionato servizio di *help desk*, ha mantenuto caratteristiche di informalità ed immediatezza, favorendo un flusso costante di informazione verso i cittadini e consentendo, nello stesso tempo, l'acquisizione di problematiche ed esigenze provenienti dalla società civile, dal mondo delle imprese, dalla ricerca e dalle pubbliche amministrazioni.

L'attenzione ad un rapporto diretto con la società riveste, del resto, un'importanza fondamentale, inserendosi in quel modello di istituzione aperta, non burocratica e attenta ai processi in atto e alle nuove prospettive, perseguito dall'Autorità fin dall'inizio della sua attività.

La prossima apertura dell'Ufficio per le relazioni con il pubblico attiverà forme di interazione ancora più efficaci e dirette con tutti i cittadini che avranno bisogno di informazioni e strumenti illustrativi e divulgativi sull'attività dell'Autorità.

73. SEMINARI, CONVEGNI ED ALTRE INIZIATIVE

La Conferenza internazionale organizzata a Venezia nel settembre del 2000 verrà menzionata nel par. 83. Qui vanno ricordati due convegni promossi ed organizzati anch'essi dal Garante, tenutisi

entrambi a Roma nel mese di luglio del 2000 e risultati assai utili ai fini del dibattito e dell'approfondimento su temi di particolare delicatezza.

Al primo, dedicato al tema dei dati genetici, ha fatto seguito la formulazione di un piano d'azione in sette punti, volto ad assicurare un utilizzo corretto dei dati genetici e ad evitare l'uso a fini economici, commerciali o discriminatori di questo genere di delicate informazioni personali.

Nel secondo, dedicato alla videosorveglianza, è stata presentata la prima indagine realizzata in Italia sulla presenza dei sistemi di videocontrollo installati in taluni luoghi pubblici e privati di tre grandi città (Roma, Milano e Napoli), nonché in una città di medie dimensioni (Verona). I dati emersi nella ricerca commissionata dal Garante, pur rappresentando una prima stima, hanno mostrato in maniera inequivocabile una crescente diffusione dell'uso di telecamere nel nostro Paese.

Un'altra importante occasione per approfondire il ruolo svolto dalla normativa sulla *privacy* nei confronti delle nuove frontiere della difesa dell'identità, della dignità e della libertà dell'individuo, è stata fornita dalla presentazione, svoltasi presso il Senato della Repubblica nel novembre 2000, del volume "*La tutela della riservatezza*" del "*Trattato di diritto amministrativo*" diretto dal prof. Giuseppe Santaniello, che ha ricostruito in modo organico ed aggiornato, anche sul piano internazionale, alcuni grandi temi della complessa tematica della protezione dei dati personali.

Con l'obiettivo di promuovere la conoscenza della legge e di diffonderla presso cittadini ed operatori pubblici e privati, il Garante ha partecipato ad altre importanti manifestazioni.

Il Forum P.A. edizione 2000, svoltosi a Roma dall'8 al 12 maggio, ha visto una rilevante partecipazione dell'Autorità. Il Forum ha infatti dedicato uno dei temi all'argomento "*Pubblica amministrazione e privacy*" riservando la presidenza di ben cinque convegni al Garante: "*Pubblica amministrazione e privacy: un nuovo rapporto con il cittadino*", presieduto dal prof. Stefano Rodotà; "*Privacy e giustizia*", presieduto dal prof. Giuseppe Santaniello; "*Privacy e dati sanitari*", presieduto dal prof. Ugo De Siervo; "*Privacy e nuove tecnologie*", presieduto dall'ing. Claudio Manganelli; "*Privacy ed efficienza della P.A.*", presieduto dal segretario generale, cons. Giovanni Buttarelli.

L'Autorità è stata anche presente al ComPA, Salone della comunicazione pubblica, svoltosi a Bologna dal 20 al 22 settembre 2000, e allo Smau di Milano, svoltosi dal 19 al 23 ottobre 2000.

Va ricordato, inoltre, che il 2000 ha registrato anche la costante presenza di rappresentanti del Garante e di funzionari dell'Ufficio in convegni, seminari ed incontri organizzati da università, comuni, associazioni di categoria ed organismi allo scopo di approfondire e discutere i diversi aspetti attuativi ed interpretativi della legge n. 675 del 1996.

Nell'aprile del 2001, infine, si è svolto a Napoli il "*Terzo Global Forum sulla Pubblica Amministrazione*" al quale è intervenuto il prof. Stefano Rodotà, che ha posto l'accento sui problemi di *privacy* che esistono anche per l'*e-government* e sulla necessità di assicurare l'autodeterminazione informativa da parte dei cittadini.

L'impegno per una comunicazione efficace e quanto più capillare deve, comunque, tener conto della ancora non completa penetrazione, in alcuni strati della società, della legge e degli strumenti di tutela da essa offerti. Un'indagine commissionata dal Garante sull'impatto determinato dalla legge sui cittadini italiani ha mostrato un buon livello di conoscenza della rete (67% degli intervistati) e ha indicato la televisione come canale preferenziale di acquisizione di notizie. Si è posta, quindi, l'esigenza da parte del Garante di un'azione di comunicazione sui *media* che utilizzi in maniera ancora più efficace questa fonte di conoscenza. In questo senso la collaborazione avviata con la Presidenza del Consiglio per una campagna di comunicazione istituzionale ha proprio l'intento di rispondere a questa esigenza strategica, per la quale è stata prevista anche la realizzazione di *depliant* divulgativi da distribuire al pubblico.

74. Il sito Internet dell'Autorità

Il 2000 è stato l'anno della definitiva attivazione, a partire da marzo, del sito *web* ufficiale del Garante, consultabile all'indirizzo *www.garanteprivacy.it* (oppure: *www.dataprotection.org*).

Dotandosi di uno strumento di comunicazione imprescindibile, quale appunto un sito Internet, l'Autorità è stata in grado di mettere a disposizione del pubblico un'ampia ed articolata quantità di documentazione riguardante la propria attività: provvedimenti, *Newsletter*, comunicati stampa, modulistica, normativa, ecc. e di dare tempestiva notizia sulle iniziative intraprese dall'Ufficio.

Il sito è caratterizzato da un facile accesso ed è basato su un primo progetto grafico che, pur sottolineando il carattere istituzionale dell'Autorità, è indirizzato ad una progressiva dinamicità e da un'im-

pronta comunicativa, e si propone inoltre come luogo di immediata percezione del "valore *privacy*", anche con apporti multimediali (video divulgativi, interviste audio e video), *link* a siti di autorità di altri Paesi e di organismi ed agenzie che si occupano di riservatezza.

Della data sua attivazione, il sito ha avuto una media di circa 10/12.000 pagine lette al giorno, con picchi di accesso fino ad oltre 40.000 pagine lette a seguito di interviste rilasciate da componenti dell'Autorità o dal segretario generale o a seguito di comunicati stampa e *newsletter* su aspetti rilevanti della tutela della riservatezza.

Superata la fase di sviluppo e completamento della prima infrastruttura *software*, la redazione del sito – che sarà potenziata nel prossimo futuro – si è dedicata alla cura dei contenuti inserendo il testo di vari provvedimenti adottati anche in passato dall'Autorità, dei comunicati stampa e delle *Newsletter*. Particolare cura è stata dedicata alla pubblicazione e all'aggiornamento dei testi normativi, costruendo la rete di *link* ipertestuali di correlazione tra provvedimenti, pareri, risposte ai quesiti e fonti normative nazionali ed internazionali.

In occasione della Conferenza internazionale "*One World One Privacy*" organizzata da questa Autorità dal 28 al 30 settembre 2000, cui hanno partecipato le altre autorità di Paesi europei ed extra europei nella splendida cornice veneziana della Fondazione Cini e di Palazzo Labia, il sito ha diffuso in diretta Internet multi lingua (italiano e traduzione simultanea in inglese, francese, tedesco, spagnolo) l'intervento di apertura del Presidente della Repubblica Carlo Azeglio Ciampi, in collegamento dal Quirinale e l'intervento da Palazzo Chigi del Presidente del Consiglio dei ministri Giuliano Amato (con traduzione simultanea).

Sono state diffuse in diretta anche la I[a] e la VI[a] sessione plenaria della Conferenza, mentre le altre due sessioni plenarie e le nove sessioni parallele, sempre con traduzione simultanea, sono state diffuse al termine dei lavori di ciascuna sessione. I materiali video sono tutt'ora fruibili, unitamente alla biografia dei relatori e ai testi degli interventi.

Gli accessi al sito, nel corso dell'anno 2000 e per la prima parte del 2001, sono cresciuti in modo esponenziale sino a giungere – nel periodo marzo/aprile/maggio 2001 – ad una media di 3.500/4000 utenti giornalieri. Nel grafico riportato in Figura 1, sono indicate le pagine visualizzate nel periodo indicato, oltre al volume raggiunto nei soli primi otto giorni del mese di giugno 2001.

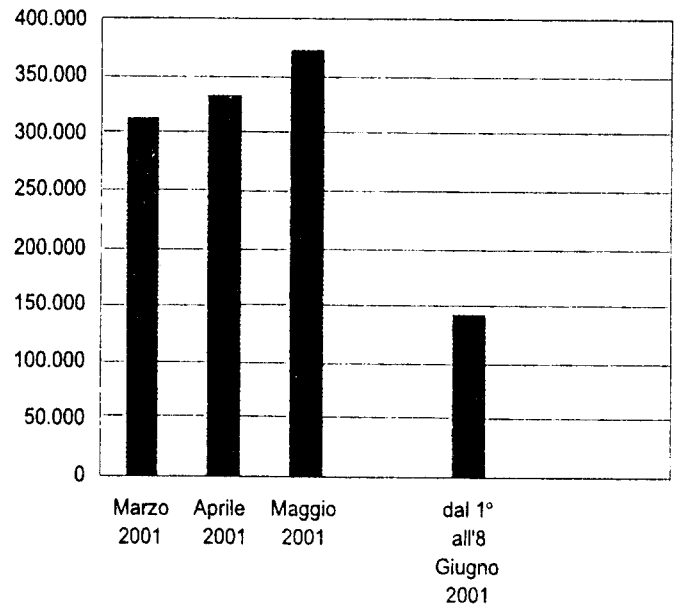


Figura 1

L'ulteriore analisi statistica degli accessi porta a considerare la ripartizione settimanale degli accessi, che si concentrano prevalentemente durante i primi giorni della settimana lavorativa. Si tratta verosimilmente di cittadini e professionisti che intendono mantenersi aggiornati sulle implicazioni orizzontali che la legge sul trattamento dei dati porta in ogni settore (Figura 2).

I crescenti bisogni di informazione hanno stimolato la redazione *web* ad impostare il progetto per una nuova piattaforma Internet che consenta un più rapido ed efficace reperimento delle informazioni anche attraverso la classificazione dei provvedimenti, un progetto grafico snello e in linea con l'evoluzione tecnologica e l'utilizzo delle più aggiornate tecniche di comunicazione multimediale. Il progetto, che si intende portare a compimento entro la fine del 2001, vuole anche adeguare i contenuti e la struttura progettuale alle *"linee guida per l'organizzazione, l'usabilità, e accessibilità dei siti web delle pubbliche amministrazioni"* (Presidenza del Consiglio dei ministri, Dipartimento della funzione pubblica – circolare 13 marzo 2001 n. 3), prevedendo in futuro progressivamente

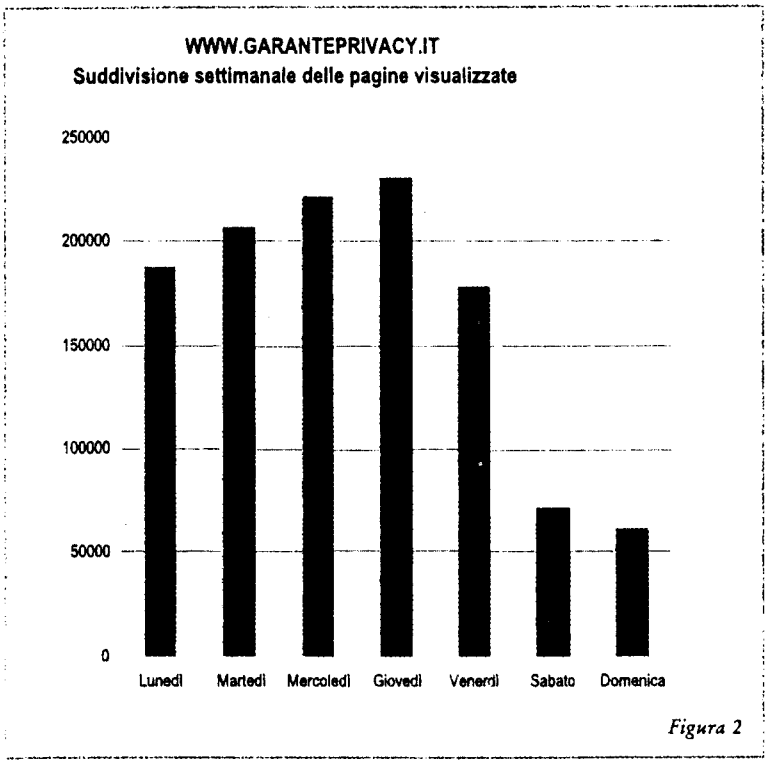


Figura 2

anche l'accessibilità alle informazioni a portatori di *handicap*, la creazione di percorsi guidati didattico/divulgativi per i giovani o più concretamente informativi per professionisti e imprenditori, la creazione di un avanzato motore di ricerca giuridico.

La medesima tecnologia *web* è stata utilizzata altresì per avviare una piattaforma Intranet, che potrà agevolare il flusso informativo interno; strutturare un più articolato *database* delle pronunce e dei pareri; offrire in tempo reale la visibilità – con accesso differenziato – dell'istruttoria di ricorsi, segnalazioni, pareri; riportare lo stato di avanzamento dei lavori di gruppi di studio o commissioni.

LA GESTIONE AMMINISTRATIVA DELL'UFFICIO

75. I REGOLAMENTI DEL GARANTE

Nella Relazione per il 1999 si è commentato positivamente l'intervento del d.lg. n. 51/1999 che ha delineato un nuovo e più stabile assetto organizzativo e funzionale per l'Ufficio del Garante.

L'aspetto più significativo previsto dal decreto legislativo ha riguardato anzitutto il riconoscimento al Garante del potere regolamentare di autodisciplinare il proprio funzionamento e l'organizzazione dell'Ufficio, potere dapprima esercitato dal Governo con il d.P.R. n. 501/1998.

In secondo luogo, il decreto legislativo ha previsto l'applicazione all'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge n. 241/1990 e del d.lg. n. 29/1993 e successive modificazioni, dei principi riguardanti la distinzione tra le funzioni di indirizzo attribuite agli organi di vertice e le funzioni di gestione attribuite ai dirigenti (art. 33, comma 1-*sexies*, legge n. 675).

Il logico corollario di queste scelte è stata, poi, l'attesa istituzione del ruolo organico del personale (dapprima collocato fuori ruolo da altre amministrazioni), la previsione di una disciplina dell'ordinamento delle relative carriere, del reclutamento, del trattamento giuridico ed economico e dell'inquadramento del personale già in servizio.

L'Autorità nel suo complesso si è quindi attivamente impegnata per porre allo studio, approfondire – anche con il contributo di esperti – e definire tre complessi regolamenti del Garante approvati il 28 giugno 2000 e pubblicati sulla *G.U.* il 13 luglio 2000 (reg. nn. 1/2000, 2/2000 e 3/2000), rispettivamente concernenti l'organizzazione e il funzionamento dell'Ufficio, il trattamento giuridico ed economico del personale, la gestione amministrativa e la contabilità.

Il primo e più importante dei tre regolamenti (il n. 1/2000) ha mutuato alcune valide disposizioni già contenute nel d.P.R. n. 501/1998, ma ne ha perfezionato ove necessario il contenuto, disciplinando in modo autonomo il funzionamento anzitutto del collegio del Garante (artt. 2-5), composto come è noto

da quattro componenti nominati direttamente dalle assemblee parlamentari, i quali eleggono al loro interno il presidente e il vice presidente del Garante.

Sono state nuovamente evidenziate le funzioni anche di rappresentanza del Garante esercitate dal presidente, il quale coordina l'attività dei componenti nei rapporti con il Parlamento e con gli altri organi costituzionali o di rilievo costituzionale, nell'attività di comunicazione pubblica e in altre relazioni istituzionali (art. 3).

Sono stati quindi dettati i principi generali che sorreggono l'attività dell'Ufficio (artt. 6-10), improntata al metodo della programmazione per funzioni-obiettivo, le funzioni del segretario generale (art. 7), che coordina l'attività di dipartimenti e servizi e dei dirigenti preposti a tali strutture di primo livello (art. 8).

Il regolamento individua direttamente i dipartimenti e i servizi, nonché le articolazioni interne della segreteria generale, demandando a successive deliberazioni l'individuazione dei compiti delle predette strutture e prevedendo altresì le modalità per istituire unità di secondo livello.

Dipartimenti, servizi e sottostanti unità potranno essere modificati, accorpati o soppressi a seconda delle necessità, a riprova della snellezza ed adattabilità della struttura.

È stata disciplinata la possibilità per i componenti di avvalersi di assistenti e di addetti di segreteria (art. 11) e sono state poste le basi per disciplinare la durata dei procedimenti amministrativi e l'accesso ai documenti amministrativi (art. 13).

Particolare attenzione è stata dedicata al procedimento di formazione dei provvedimenti che richiedono una deliberazione collegiale, rigorosamente ispirato ai principi della trasparenza, della partecipazione e del contraddittorio imposti dalla civiltà della legge generale sul procedimento amministrativo (l. n. 241 del 1990).

Detto procedimento ha inizio con l'assegnazione dell'affare, da parte del segretario generale, al dipartimento o al servizio competente, dove il dirigente procede, a sua volta, alla nomina del responsabile del procedimento. Quest'ultimo, dopo aver istruito e predisposto lo schema di provvedimento, provvede a trasmetterlo, attraverso la fattiva intermediazione del dirigente della struttura, al segretario generale che formula le proprie osservazioni. Lo schema di provvedimento, le osservazioni e la documentazione sono posti a disposizione del presidente e dei componenti anche attraverso strumenti informatici e telematici. Il presidente provvede alla designazione del relatore che introduce nella riunione la discussione e formula le proprie conclusioni nell'adunanza preventivamente fissata, secondo una cadenza almeno settimanale.

Come è facilmente intuibile, questa articolazione procedimentale tende a mutuare alcune caratteristiche del procedimento giurisdizionale. Una delle attività maggiormente qualificanti del Garante è, infatti, quella che si instaura a seguito della proposizione del ricorso alternativo a quello proponibile innanzi al giudice ordinario, che fornisce uno strumento per certi aspetti unico al cittadino che si ritenga leso da un trattamento di dati personali che lo riguardano, esaminato in un quadro di autonomia e di indipendenza di giudizio.

Le norme che disciplinavano la trattazione dei ricorsi nel d.P.R. n. 501/1998, a differenza di quelle concernenti l'organizzazione dell'Ufficio, sono rimaste applicabili anche sulla base di un espresso richiamo normativo.

76. La nuova organizzazione dell'Ufficio

Al di là di ogni enfasi si può affermare che la stesura dei predetti regolamenti ha impegnato per diversi mesi l'attività dell'Autorità. L'intero Ufficio ha vissuto la vicenda come uno dei momenti alti della gestione della legge n. 675 del 1996.

La gestazione dell'importante complesso normativo è avvenuta con la consapevolezza che esso fosse lo strumento sia per sanare la situazione di precarietà in cui si era trovato il personale, sia per avviare una struttura più forte, agile e funzionale e destinata a operare negli anni.

Alla fine di un percorso obiettivamente faticoso si è raggiunto l'effetto sperato di dare all'Ufficio un'organizzazione in linea con le moderne formule organizzatorie della pubblica amministrazione (tenendo conto dei disegni organizzativi delle altre autorità amministrative indipendenti), nonché una sistemazione definitiva del personale e un'avanzata gestione della contabilità e delle spese.

I regolamenti sono entrati in vigore il quindicesimo giorno successivo all'indicata data di pubblicazione. Il regolamento sull'organizzazione consta di venti articoli; quello sul trattamento giuridico ed economico del personale di sessantasette e quello concernente la gestione e contabilità di trentuno.

Non è questa la sede per riassumere il contenuto dell'intera normativa, pubblicata nella documentazione allegata. Non si può tuttavia sottacere il fatto che, per quanto concerne la sistemazione del personale, la normativa transitoria ha consentito alle persone che da qualche anno svolgevano la propria attività presso la struttura di entrare nel ruolo del personale dell'Autorità sulla base di una domanda e del non demerito, secondo un collaudato meccanismo di inquadramento pressoché automatico, fondato sulla qualifica corrispondente a quella posseduta presso l'amministrazione di provenienza.

Inoltre, al fine di valorizzare la qualità del lavoro svolto, sono stati banditi concorsi interni già interamente espletati, mediante i quali dipendenti già inquadrati a domanda hanno potuto transitare in una qualifica superiore. Rispetto ad alcune impugnative proposte dall'esterno e dall'interno, il competente tribunale amministrativo ha respinto l'istanza di sospensiva proposta.

È doveroso segnalare che solo la metà dei posti del nuovo ruolo organico è stato occupato dal personale comandato in precedenza. In relazione all'altra metà sono stati già banditi alcuni concorsi pubblici per varie qualifiche.

Per quanto riguarda lo stato giuridico ed economico, nonché per la gestione e la contabilità, si è adottato poi un regime analogo a quello osservato presso le altre autorità amministrative indipendenti di riferimento, orientato in modo equilibrato a giusti principi di informazione, concertazione e contrattazione con le rappresentanze sindacali.

L'Ufficio è, ora, alle soglie di un nuovo rilancio dell'efficienza e della produttività. L'abnegazione con cui il personale ha contribuito al raggiungimento di consistenti risultati nel primo quadriennio di attività del Garante, deve ora coniugarsi con nuove misure e razionalizzazioni amministrative che consentano all'Autorità di entrare definitivamente a regime e di abbreviare anche i tempi di risposta agli innumerevoli interpelli.

77. Il bilancio, gli impegni di spesa e l'attività contrattuale

L'esercizio finanziario 2000 è stato caratterizzato dal completamento del quadro istituzionale e gestionale interno con l'adozione dei citati regolamenti numeri 1/2000, 2/2000 e 3/2000. Tali regolamenti hanno iniziato a produrre effetti positivi con il nuovo anno, considerato che il personale in servizio in posizione di comando o di fuori ruolo è stato inquadrato, a domanda, dal 1° settembre 2000 e che il regolamento sulla amministrazione e la contabilità è stato applicato, per la parte gestionale del bilancio, dal 1° gennaio 2001.

Il dipartimento che si occupa della contabilità ha avvertito in modo incisivo gli effetti dell'adozione dei regolamenti, in quanto l'inquadramento del personale al 1° settembre ha avuto come conseguenza immediata l'apertura delle posizioni assicurative presso l'Inps del personale entrato in ruolo e la gestione della contabilità specifica per le buste paga, mentre fino alla data del 31 agosto il personale in servizio presso il Garante dipendeva giuridicamente ed economicamente, per il trattamento fondamentale, dalle rispettive amministrazioni pubbliche di provenienza.

Ciò ha comportato la regolarizzazione delle posizioni economiche, anche pregresse, dei dipendenti e l'attuazione della complessa gestione delle retribuzioni fisse e degli adempimenti di fine anno: conguagli fiscali, versamento delle ritenute, rilascio dei CUD, ecc..

A fini puramente statistici la spesa erogata sul capitolo degli oneri retributivi per il personale è passata da poco più di 1.100 milioni di lire del 1999 a 7.500 milioni di lire, di cui 2.600 provenienti da accantonamenti degli anni precedenti. Inoltre, per l'affidamento, sulla base di apposita convenzione, del servizio di cassa ad un istituto di credito, così come previsto dal regolamento n. 3/2000, si è proceduto alla scelta dell'istituto cassiere tra le banche che avevano offerto il servizio rispondendo all'avviso pubblicato su tre quotidiani alla fine di settembre. Infine, la predisposizione del bilancio di previsione 2001 e di tutti gli atti ad esso connessi è avvenuta nel rispetto di quanto previsto dagli articoli 4 ("Struttura del bilancio") e 5 ("Criteri di formazione del bilancio") del regolamento n. 3/2000.

Per il 2000 le risorse a disposizione del Garante sono state pari a lire 22.685.000.000. Di tale somma il contributo dello Stato di lire 22.045.000.000 ha rappresentato la quasi totalità delle risorse affluite sul fondo di contabilità speciale presso la Banca d'Italia, Tesoreria provinciale dello Stato. Per il 2000 sono affluite anche alcune ridotte risorse derivanti dalle quote di iscrizione dei partecipanti alla 22.ma Conferenza internazionale delle Autorità di protezione dei dati personali svoltasi a Venezia dal 28 al 30 settembre 2000.

La preparazione e lo svolgimento della Conferenza internazionale sono stati momenti di impegno che hanno rappresentato uno degli aspetti rilevanti della gestione del 2000. L'Autorità, infatti, si era impegnata a garantire la riuscita dell'evento contemperando l'esigenza di ottenere un elevato livello di rappresen-

tanza (in linea con le edizioni pregresse e future) con una razionalizzazione dei costi in un'ottica di economicità. Per tale motivo il Garante ha stabilito di aprire un c/c bancario sul quale sono confluite le quote di iscrizione dei partecipanti, che sono state graduate in modo tale da assicurarne la congruità. Il costo complessivo dell'evento è stato dell'ordine di circa 900 milioni di lire, IVA esclusa. Tenendo conto del fatto che le quote di iscrizione dei partecipanti hanno superato i 100 milioni di lire, il costo netto della manifestazione non ha superato gli 800 milioni di lire, IVA esclusa.

Altri aspetti rilevanti della gestione dell'esercizio 2000 sono stati:

Sede del Garante

Durante l'anno 2000 è stato completato il trasferimento degli uffici nella nuova sede di piazza di Monte Citorio ed è nel contempo continuata l'acquisizione di arredi per i locali: una serie di trattative private ha interessato l'acquisto di tendaggi e mobili d'ufficio. Si è proceduto quindi alla chiusura delle sedi di Largo del Teatro Valle e di Via della Chiesa Nuova.

Con la disponibilità del nuovo edificio si è reso necessario effettuare lavori per il collegamento in rete delle postazioni informatiche ubicate nell'immobile e per garantire la protezione elettrica ai sistemi della redazione *web* e del protocollo. I pagamenti effettuati per tali tipi di interventi sono risultati superiori a 400 milioni di lire; gli impegni contrattuali per la gestione del sito *web* e per l'acquisto di materiale informatico hanno superato i 500 milioni.

Formazione professionale

Nel corso dell'anno le iniziative concernenti l'aggiornamento e la formazione del personale sono state finalizzate prevalentemente alla conoscenza e all'approfondimento delle lingue straniere (inglese e francese). Gli interventi formativi sono stati diversificati in ragione del livello d'ingresso dei partecipanti e, in taluni casi, si sono caratterizzati per l'uso di metodi didattici innovativi. I dipendenti interessati sono stati quasi la metà del personale in servizio.

Convegni di studio e seminari di lavoro

Le iniziative promosse e coadiuvate dal Garante hanno riguardato, in particolare, la partecipazione al FORUM P.A. 2000 di Roma, al COMPA 2000 di Bologna e allo SMAU 2000 di Milano, nonché a numerosi convegni e dibattiti, in Italia e all'estero, per la promozione della legislazione sulla protezione dei dati personali. Della 22.ma Conferenza internazionale delle Autorità per la protezione dei dati personali si è già parlato.

Un cenno a parte merita il progetto "Attività di contrasto del crimine e tutela dei dati personali" detto "*PROGETTO Falcone*"che ha impegnato l'Ufficio in una serie di seminari tenuti a L'Aja e a Parigi, con incontro finale a Roma il 22 dicembre 2000, al quale hanno partecipato magistrati, funzionari di polizia ed esperti di vari Paesi europei. Il progetto è stato realizzato con il contributo economico della Commissione europea.

Attività contrattuale

Con l'adozione del regolamento n. 3/2000 l'attività negoziale, essendo tipica attività di gestione, è attribuita, a decorrere dall'entrata in vigore delle norme di cui al Capo V (luglio 2000) interamente ai dirigenti, nel rispetto rigoroso del principio della distinzione tra funzioni di indirizzo e controllo e di attuazione e gestione di cui all'art. 3 del decreto legislativo 3 febbraio 1993, n. 29 e successive modificazioni ed integrazioni e all'art. 33, comma 1-*sexies*, della legge 31 dicembre 1996, n. 675.

Nell'esercizio 2000 l'attività contrattuale del Garante è stata segnata da questo spartiacque, ma è stata comunque molteplice e con consistenti impegni di spesa.

Le attività negoziali più significative e complesse sono state:

– il rinnovo della convenzione con le Poste italiane per il servizio concernente la distribuzione e la spedizione dei modelli cartacei e dei dischetti per le notificazioni delle banche dati: costo lire 393.110.585;

– è stato esperito il bando di gara per la pulizia dei locali della sede di piazza di Monte Citorio. La gara indetta con procedura aperta a livello comunitario è stata aggiudicata secondo il criterio dell'offerta economicamente più vantaggiosa, per un biennio, dal 1° luglio 2000 al 30 giugno 2002 e per un costo complessivo di lire 178.272.000, IVA esclusa;

– altro bando di gara a livello comunitario è stato quello esperito per l'affidamento del servizio di trasporto di persone con autovettura di noleggio con conducente, poiché il vecchio contratto scadeva il 31 dicembre 2000. Il contratto, che ha validità biennale dal 1° gennaio 2001 al 31 dicembre 2002, prorogabile alle medesime condizioni per un altro anno, prevede un costo per il biennio di lire 611.728.940, IVA esclusa.

Il tribunale amministrativo investito della richiesta di sospensiva non ha accolto la richiesta stessa.

Del settore riguardante l'informatizzazione degli uffici ed il sito *web*, nonché le forniture per gli arredamenti della sede di piazza di Monte Citorio, si è parlato.

È invece da ricordare che in data 1° dicembre 2000 è stato sottoscritto, a seguito di trattativa privata, il contratto con un istituto autorizzato per la vigilanza della sede di piazza di Monte Citorio.

78. Il lavoro in rete e la sicurezza

Il trasferimento della sede del Garante nei nuovi locali di Piazza di Monte Citorio ha consentito di realizzare, come opera propedeutica a tutti i servizi informatici, una rete locale in cablaggio strutturato e a tecnologia Ethernet che già oggi permette la condivisione di risorse, la comunicazione interna, l'utilizzo di applicazioni *client-server* in rete e il collegamento a Internet.

Alla realizzazione di questa infrastruttura ha fatto seguito un adeguamento impiantistico dei locali tecnici per garantire che l'attività di elaborazione dei dati si possa svolgere nelle condizioni di massima protezione e sicurezza. In particolare, sono state predisposte misure per garantire la sicurezza fisica e logica degli impianti informatici e il controllo remoto degli apparati tecnologici.

Sono state poi portate a compimento iniziative di notevole importanza, come la messa in produzione del sito *web* del Garante, la totale informatizzazione dei posti di lavoro e l'avviamento sperimentale del sistema di *workflow* interno.

Diversi altri interventi sono stati progettati e sono correntemente in stato di realizzazione.

Tra questi, il nuovo sistema di *workflow* documentale che integrerà le funzionalità già disponibili di protocollo informatico; il sistema di gestione delle presenze del personale, totalmente funzionante con gli strumenti del *web*; i nuovi servizi Internet completamente autogestiti dal personale dell'Ufficio; il nuovo sistema di gestione della rassegna stampa, che sarà consultabile con avanzate funzionalità in rete; il sistema bibliotecario per la gestione della biblioteca, la pubblicazione del catalogo (OPAC); la gestione delle banche dati bibliografiche; la nuova rete LAN integrata ad alte prestazioni che consentirà anche la trasmissione di flussi isocroni e lo svolgimento di sedute di videoconferenza direttamente dai posti di lavoro (standard ITU H.323/H.320); i nuovi sistemi server del Garante che, proiettandosi nel mondo dei sistemi aperti e dell'*open source* consentiranno, oltre alla realizzazione di importanti servizi, anche di esplorare nuove tecnologie e tenere il passo con l'evoluzione dell'informatica negli ambiti connessi alla protezione dei dati personali (crittografia, firma digitale, certificazione, sicurezza).

Particolare impegno ha richiesto la stesura del documento programmatico sulla sicurezza secondo le disposizioni di cui al regolamento approvato con d.P.R. n. 318/1999. Il lavoro svolto nei primi mesi del 2000 e, successivamente, fino al 31 dicembre dello scorso anno, ha consentito di affinare le procedure verificandone l'effettiva rispondenza alle esigenze dell'Ufficio e costituendo un'occasione di revisione e di aggiornamento tecnico dei servizi informatici.

Con l'adozione del documento il Garante si è dotato anche di uno strumento che, grazie alla revisione periodica e alla flessibilità di impostazione, consentirà di recepire le innovazioni, adattandosi ai mutevoli scenari tecnologici. Inoltre il documento è lo strumento che consente di condensare tutte le iniziative rilevanti in tema di sicurezza informatica e fornisce al personale le linee-guida per una piena applicazione dei principi della legge 675/1996.

Nell'ambito del documento sono state individuate ed assegnate le responsabilità di amministrazione di sistema e di custodia delle parole chiave per gli elaboratori (tutti connessi a una rete locale a sua volta collegata, come tutte le moderne reti a tecnologia Internet, a una rete pubblica di telecomunicazione per l'integrazione nella Internet globale). Sono state inoltre codificate le procedure operative per la salvaguardia dei dati informatizzati, per la loro custodia e per la loro rimozione.

È stato inoltre previsto un piano di formazione che coinvolgerà il personale e che consentirà di implementare le politiche di sicurezza.

Correlato alla sicurezza dei dati è anche il potenziamento della protezione fisica degli impianti, dei locali e degli archivi tradizionali.

79. Biblioteca e centro di documentazione

La molteplicità delle problematiche culturali che riguardano la protezione dei dati richiede la messa in opera di una struttura di raccolta sistematica di una vastissima produzione di materiale bibliografico. Si è reso pertanto opportuno – anche in ragione del trasferimento dell'Autorità nella nuova sede e della disponibilità di ampi locali – dar vita a un progetto di costituzione di una grande biblioteca specializzata su base multidisciplinare, con l'obiettivo di disporre, in un arco temporale necessariamente breve, della totalità dei testi, italiani e stranieri, che abbiano riferimento alla *privacy*.

L'ampio spettro di campi nei quali il Garante si trova ad intervenire rende indispensabile, per il successo di questa iniziativa, una stabile cooperazione con l'esterno per il reperimento di testi e documenti. Particolare attenzione verrà quindi dedicata ai contatti con altre biblioteche pubbliche e private, con le istituzioni italiane e straniere e, naturalmente, con le altre autorità europee omologhe del Garante.

La principale funzione della biblioteca rimarrà quella di rispondere alle esigenze dell'attività del Garante: il suo nucleo principale avrà pertanto natura giuridica e riguarderà, in senso ampio, la sfera del diritto. Ma, accanto a questo compito primario, la biblioteca si proporrà di fornire un servizio alle altre istituzioni, agli istituti di ricerca italiani e stranieri, alle altre biblioteche, agli studiosi e ai singoli cittadini. In questa prospettiva, il progetto prevederà, fin dalla sua fase iniziale, di allargare l'orizzonte della raccolta di testi a tutti quei campi dove la *privacy* risulti collegata a tematiche di ordine più vasto e complesso, di tipo sociale, politico, storico, letterario, filosofico e religioso. Questo approccio multidisciplinare permetterà di evidenziare e di approfondire le coordinate culturali che indirizzano e orientano il lavoro dell'Autorità.

È stata prevista, a completamento del progetto, la creazione di un comitato scientifico composto da eminenti personalità soprattutto del mondo accademico che, sulla scorta dell'esempio di altre autorità, sappia individuare temi e problemi con i quali l'Ufficio sarà chiamato negli anni a venire a confrontarsi, segnatamente in ragione dei veloci cambiamenti della società dell'informazione.

Nella strutturazione del progetto di biblioteca, si è deciso anche di prestare particolare attenzione all'innovazione tecnologica. L'organizzazione e la gestione della biblioteca e delle sue infrastrutture disporrà in particolare dei seguenti elementi:

1. un sistema informatico bibliotecario per l'amministrazione del posseduto (schedatura, catalogazione, soggettazione, spoglio riviste), la pubblicazione *on line* del catalogo (OPAC), la gestione amministrativa e l'inventariazione del libro, la gestione del prestito, la catalogazione derivata;

2. un sistema ad alte prestazioni per la consultazione di *database* bibliografici (*abstract, full text* laddove disponibili) sui diversi temi di interesse del Garante, generalmente distribuiti in abbonamento su CD ROM;

3. un sito *web* per l'accesso ai servizi interni secondo percorsi guidati e personalizzabili;

4. un sito *web* specialistico per la consultazione del catalogo OPAC, la creazione di una *community* di utenti e la gestione di forum tematici di discussione;

5. una sala informatizzata per l'accesso locale ai servizi bibliotecari;

6. una sala di lettura provvista di connessioni di rete per il collegamento di computer portatili;

7. un sistema di controllo degli accessi interfacciato con il sistema di gestione bibliotecario e con il sottosistema prestiti.

L'obiettivo è quello di creare, nel centro di Roma, una biblioteca con servizi informatici di avanguardia dove i frequentatori potranno adoperare, tra l'altro, fino a sedici postazioni informatiche avanzate, tramite l'uso di una *smart card* personale. La tecnologia a *smart card* permetterà inoltre di gestire l'accesso, il prestito e le fotoriproduzioni con una soluzione integrata di autenticazione e *accounting*.

L'elemento essenziale e più importante riguarderà il sistema di gestione bibliotecario, tramite il quale gli addetti schederanno monografie e periodici, gestiranno il posseduto bibliotecario, i prestiti, gli acquisti ed effettueranno lo spoglio delle riviste. Tale sistema sarà basato su dispositivi che consentiranno ai visitatori e agli utenti occasionali, sia interni, sia esterni di consultare il catalogo OPAC con i comuni *browser web*, attraverso un percorso mediato dal sito *web* della biblioteca. Il sistema di gestione prevederà l'interconnessione con il circuito SBN (Sistema bibliotecario nazionale) e risponderà ai necessari requisiti di standardizzazione per le modalità di soggettazione e catalogazione.

Accanto al sistema di gestione bibliotecaria verrà sviluppata un'interfaccia per l'interrogazione via *web*, che andrà integrata in un sito appositamente predisposto per la biblioteca allo scopo di facilitare l'accesso ai servizi. Benché le funzioni più avanzate di catalogazione utilizzeranno una tradizionale interfaccia *client/server*, la visibilità al pubblico della biblioteca sarà di tipo *web oriented*.

80. IL PERSONALE E I COLLABORATORI ESTERNI

Con l'approvazione dei regolamenti del Garante, l'Autorità è, come si è detto, entrata in una fase nuova della sua vita istituzionale. In particolare, in conformità a quanto previsto dal regolamento n. 2/2000 del Garante, concernente il trattamento giuridico ed economico del personale dell'Ufficio (che ha previsto le modalità di inquadramento nel ruolo organico del contingente di personale utilizzato in sede di prima applicazione della legge n. 675/1996), il personale in posizione di fuori ruolo o di comando presso l'Ufficio alla data di entrata in vigore del regolamento è stato inquadrato, a domanda, nel ruolo organico con effetto dal 1° settembre 2000.

Su un totale di 45 unità in servizio alla predetta data, 42 hanno chiesto di essere inquadrate nel ruolo. Tre persone hanno optato per la permanenza in posizione di fuori ruolo.

Esaurita la fase del primo inquadramento del personale nel ruolo organico, l'Ufficio ha concentrato la sua attenzione sull'assetto organizzativo-funzionale e sulla definizione delle procedure per la copertura dei posti vacanti nel ruolo organico e per il reclutamento del personale a contratto.

Il primo aspetto ha comportato un duplice ordine di problemi. L'istituzione del ruolo organico e l'attuazione dell'ordinamento professionale previsto dal regolamento n. 2/2000 hanno posto l'esigenza di una valorizzazione delle esperienze e delle professionalità emerse nei primi due anni di vita dell'Autorità, al fine di garantire la continuità delle attività istituzionali dell'Ufficio. A tale fondamentale esigenza – come si è già evidenziato – si è ispirato il regolamento n. 2/2000, che ha previsto procedure concorsuali riservate al personale interno per una percentuale dei posti disponibili in organico non superiore al 50% (art. 65).

In attuazione di tale previsione regolamentare, il Garante ha indetto tre concorsi interni (pubblicati nella *G.U.* – IV serie speciale – del 22 agosto 2000) per l'accesso, rispettivamente, alle qualifiche di dirigente, funzionario e impiegato operativo, per una percentuale corrispondente al 50% della disponibilità organica nella qualifica di dirigente e per percentuali inferiori nelle altre due qualifiche. A conclusione delle procedure concorsuali, dei 14 posti messi a concorso, ne sono stati sono assegnati soltanto 12.

I concorsi sono stati oggetto di una interpellanza presentata alla Camera dei deputati dall'on. Chiappori ed altri (n. 2-02673) e di una interrogazione presentata al Senato dall'on. Gubert (n. 3-04172). In merito, il Garante si è adoperato, a richiesta del Governo, per chiarire la piena liceità e correttezza delle procedure concorsuali e la loro rispondenza ai parametri costituzionali e ai principi stabiliti dal decreto legislativo n. 29/1993 e successive modificazioni ed integrazioni.

La legittimità dei bandi e dell'operato dell'Autorità è stata oggetto anche di esame da parte del T.A.R. del Lazio, sezione I, il quale, in sede di valutazione della richiesta di sospensiva e di ammissione con riserva alle prove concorsuali presentata da alcuni aspiranti esterni, con ordinanza n. 9303/2000 dell'8 novembre 2000 ha rigettato l'istanza incidentale in quanto "il ricorso non appare assistito dal *fumus boni juris*". Analogo rigetto di istanza di sospensiva è stato successivamente pronunciato in relazione ad un ulteriore ricorso.

Le procedure concorsuali erano finalizzate al completamento e consolidamento dell'assetto organizzativo dell'Ufficio e avevano lo scopo di dotare lo stesso delle figure professionali indispensabili per le attività istituzionali dell'Autorità. Con l'attribuzione di alcuni incarichi di direzione di dipartimenti e servizi nel marzo di quest'anno, l'obiettivo può dirsi raggiunto.

L'adozione di tali atti di organizzazione è stato preceduto da alcuni fondamentali adempimenti previsti dal regolamento n. 1/2000: la definizione dei principali obiettivi delle unità organizzative e dell'Ufficio nel complesso delle sue articolazioni e l'individuazione dei compiti delle unità organizzative di primo livello (dipartimenti e servizi).

Contemporaneamente, sono state indette le procedure concorsuali per la copertura di una parte dei posti disponibili nel ruolo organico. I concorsi pubblici, a complessivi 21 posti, riguardano le varie posizioni professionali: 3 posti di dirigente (di cui uno per dirigente informatico), 10 di funzionario e 8 di impiegato operativo.

Contestualmente è stata definita la disciplina in tema di contratti a tempo determinato e di *stage* e sono state stabilite le relative modalità di selezione con la pubblicazione di due avvisi pubblici: il primo per il reclutamento di un massimo di 6 giovani laureati che non abbiano superato il trentacinquesimo anno di età da assumere con contratto di specializzazione a tempo determinato; il secondo finalizzato alla formazione di una graduatoria di giovani laureati di età non superiore a ventotto anni per la frequenza di periodi di tirocinio presso l'Ufficio.

Alla copertura dei posti che risulteranno vacanti a conclusione delle predette procedure, l'Autorità procederà con gradualità, sulla base delle esigenze via via emergenti.

Attualmente l'Ufficio dispone complessivamente di n. 57 unità, di cui n. 6 assunte con contratto a tempo determinato, come da prospetti allegati:

Personale di ruolo e fuori ruolo

Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	TOTALE	Posti vacanti
Dirigenti	26	15	4	19	7
Funzionari	40	18	3	21	19
Operativi	25	9	2	11	14
Esecutivi	9				9
TOTALE	100	42	9	51	49

Personale a contratto

Area	Posti disponibili	Personale in servizio
Dirigenti		1
Funzionari		3
Operativi		2
Esecutivi		6
TOTALE	20	

L'Autorità si avvale inoltre della collaborazione di quattro consulenti per attività di studio, ricerca e per i necessari approfondimenti in materia giuridica e per la comunicazione.

Nel corso del 2000, si sono conclusi diversi rapporti di consulenza instaurati per la redazione dei regolamenti del Garante, per esigenze contingenti o connesse ad eventi di carattere internazionale (XXII conferenza delle Autorità garanti, tenutasi a Venezia il 28/30 settembre 2000).

Agli inizi del 2001 hanno esaurito la loro opera le commissioni esaminatrici dei concorsi interni, presiedute da un consigliere di T.A.R. designato dal Consiglio di Presidenza del Consiglio di Stato e composte da tre docenti universitari e da un dirigente di prima fascia dello Stato.

IL REGISTRO DEI TRATTAMENTI

81. UTILIZZAZIONE DEL REGISTRO E ACCESSO

La notificazione al Garante, salvo i casi di esonero previsti dall'art. 7, comma 5 *ter*, della legge n. 675/1996, è obbligatoria per tutti i titolari che intendano iniziare o cessare un trattamento di dati personali o provvedere al loro trasferimento anche temporaneo all'estero (artt. 7, 16 e 28 legge n. 675/96).

Le notificazioni confluiscono nel registro generale dei trattamenti, previsto dall'art. 31, comma 1, lett. a) della l. 675/1996, che ne contiene circa 295.000.

Il registro è stato formalmente istituito dal Garante a decorrere dal primo febbraio 2000 con delibera n. 3 del 13/1/2000 che ne ha regolamentato le modalità di utilizzo. Il registro è consultabile da tutti gli interessati che intendono conoscere l'esistenza di trattamenti che possono riguardarlo ai sensi dell'art. 13, comma 1, del d.P.R. 31 marzo 1998, n. 501. Chiunque può accedervi, senza particolari formalità, presso l'Ufficio e mediante terminali che verranno dislocati su base almeno provinciale, sulla base di convenzioni *in itinere*, preferibilmente nell'ambito degli uffici per le relazioni con il pubblico presso le amministrazioni provinciali e di eventuali altre amministrazioni pubbliche (art. 13, comma 2, del d.P.R. 501/98 e comma 3, dell'art. 31 della legge).

Per il registro, prima della sua entrata in vigore a pieno regime, è stato previsto un periodo transitorio di sperimentazione durante il quale è stato utilizzato dall'Ufficio a fini di test e ricerche e come supporto per accertamenti ed ispezioni. La sperimentazione non ha impedito di soddisfare tutte le richie-

ste degli utenti in ordine, in particolare, al rilascio di copia della notificazione, come pure di richieste dell'autorità giudiziaria e di polizia.

Le notificazioni si sono incrementate nel corso del tempo, soprattutto per effetto delle modifiche alla prima notificazione – e in misura molto più contenuta, delle cessazioni del trattamento – ai sensi dell'art. 7, comma 2, della legge che prevede che le pertinenti modifiche intervenute debbano essere preventivamente notificate al Garante, al fine di tenere costantemente aggiornato il registro. Esse vengono effettuate utilizzando il modello standard o, in alternativa il *floppy disk*, distribuiti gratuitamente presso tutte le agenzie postali o attraverso convenzioni.

Gli importi dei diritti di segreteria sono rimasti invariati: £. 15.000 per chi effettua la notificazione mediante *floppy disk* e £. 25.000 per chi opta per il modello cartaceo.

I costi del servizio di notificazione non sono integralmente sostenuti con l'importo dei diritti di segreteria, anche in ragione dei costi legati alla capillare distribuzione dei modelli tramite Poste italiane S.p.a. D'altra parte, a fronte delle sanzioni penali comminate in caso di omessa notificazione, e in vista della futura notificazione per via telematica, è parso necessario sostenere tali oneri offrendo anche a coloro che non sono in grado di utilizzare strumenti informatici la possibilità di reperire agevolmente la modulistica nel luogo di residenza senza obbligarli a spostamenti sul territorio.

Il servizio di distribuzione si è rivelato funzionale. Si procederà comunque ad integrare i soggetti distributori anche per diminuire, ove possibile, i costi pur lasciando inalterata la qualità del servizio o addirittura migliorandola, offrendo agli utenti più possibilità per reperire il modello di notificazione.

Il modello, in attuazione dell'art. 12, comma 2, del d.P.R. n. 501/1998, è stato messo a disposizione del pubblico anche sul sito Internet del Garante all'indirizzo *www.garanteprivacy.it*, per cui tutti coloro che sono in grado di effettuare l'operazione possono scaricare sia il modello sia il programma. L'ulteriore possibilità di reperire il modello tramite negozi specializzati per uffici, all'uopo convenzionati, sembra essere stata meno utilizzata dagli utenti, mentre si è registrata una buona propensione all'acquisizione del modello direttamente dal sito del Garante o presso l'Ufficio.

Sempre sul sito, per agevolare l'utenza, oltre alla possibilità di rivolgere direttamente quesiti, sono state inserite le risposte ai dubbi posti circa la corretta compilazione del modello e l'interpretazione della legge (FAQ). Nel corso dell'anno, infatti, vi sono state numerose richieste per via telefonica, fax o *e-mail*, in ordine all'interpretazione delle norme e agli adempimenti concernenti la notificazione, che ha impegnato notevolmente gli uffici (a maggio 2001, circa 3.000 risposte telefoniche, via fax o Internet) seppure in misura attenuata rispetto all'anno precedente, il che sembra dimostrare una più estesa e migliore conoscenza della legge rispetto al passato.

L'attività di assistenza agli utenti, seppure talvolta faticosa, è stata comunque preziosissima per capire le difficoltà incontrate nella predisposizione della notificazione e per ipotizzare correttivi, semplificazioni e miglioramenti che in buona parte presuppongono interventi legislativi.

Le richieste d'accesso al registro sono state circa un centinaio nel corso dell'anno, provenienti da soggetti che avevano smarrito la propria copia, oppure dalla Guardia di finanza, dal Dipartimento vigilanza e controllo dell'Ufficio e, in misura minima, da coloro che intendevano sapere se erano oggetto di trattamento di dati da parte di talune ditte.

In ordine a quest'ultimo aspetto, l'Ufficio ha constatato che diversi soggetti ritengono tuttora, erroneamente, che dalla consultazione del registro sia possibile conoscere in quali banche dati è memorizzato il loro nominativo, ignorando che le notizie contenute nella notificazione sono invece di carattere generale e non nominative, ad eccezione di quelle relative al titolare e al responsabile del trattamento.

Molti quesiti posti (e notifiche errate) concernono i casi più complessi di fusione e di incorporazione di società, che hanno ingenerato dubbi sul tipo di notificazione da effettuare.

Nel corso dell'anno sono proseguite le attività di routine consistenti, essenzialmente, nella memorizzazione e nella regolarizzazione delle notificazioni irregolari o incomplete e di verifica del *database* per la sua normalizzazione.

Accanto ad esse sono state attivate fasi di monitoraggio e verifica che hanno permesso di pianificare gli interventi tesi al miglioramento del servizio.

Va sottolineato che, a seguito di tre anni di esperienze e sperimentazioni ci si è resi conto che anche il modello di notificazione e l'annesso *software* saranno oggetto di approfondimenti e, ove possibile, di semplificazioni, in maniera da renderli ancor più leggeri e "*user friendly*".

Tra l'altro, le convenzioni che si intendono stipulare con le camere di commercio, le province ed altri enti ed organismi, dovrebbero alleggerire l'attività di notificazione filtrandole *ab origine* in maniera da ridurre ulteriormente il numero delle notifiche irregolari che assorbono altrimenti risorse preziose. Il complesso di convenzioni da stipulare persegue l'ulteriore obiettivo di effettuare la notificazione per via telematica, ai sensi dell'art. 12, comma 2, del d.P.R. n. 501/1998.

La riflessione in corso sul modello e sul *database*, la sperimentazione che si vuole intraprendere circa i collegamenti telematici con le province, la stipula delle convenzioni *in itinere*, l'assestamento dell'attuale *database* e l'opportunità di utilizzare la firma digitale (legata alla possibilità di effettuare la notificazione per via telematica), impegneranno nei prossimi mesi ancor più l'Ufficio.

Il registro troverà a breve una più marcata efficienza e funzionalità, grazie anche al nuovo *software* e a misure amministrative che permetteranno di ovviare ad alcuni inconvenienti che pure sono stati registrati nella fase costituente del registro.

Il registro sarà altresì a breve consultabile anche presso l'istituendo Ufficio per le relazioni con il pubblico.

DATI STATISTICI

82. PROSPETTO ANALITICO

ATTI E PROVVEDIMENTI / ATTIVITA' GARANTE

Richieste di informazione e quesiti telefonici	9.000
Segnalazioni e reclami pervenuti	3.661
Quesiti pervenuti	1.569
Richieste di parere pervenute	170
Richieste di autorizzazione pervenute	191
Assistenza telefonica relativa alle notificazioni	3.000
Notificazioni dei trattamenti previste dagli articoli 7, 16 e 28 (*)	295.000
Comunicazioni previste dall'art. 27, comma 2	165
Comunicazioni in tema di dati sensibili e giudiziari previste dall'art. 41, comma 5	92
Autorizzazioni generali al trattamento dei dati sensibili (art. 22) rilasciate per categorie di titolari e di trattamenti (art. 41, comma 7)	7
Autorizzazioni rilasciate a singoli destinatari	2
Risposte a richieste di autorizzazione (art. 22)	20
Atti e provvedimenti a seguito di segnalazioni e reclami	687
Risposte a quesiti	118
Risposte a richieste di parere	44
Pareri rilasciati in base all'art. 31, comma 2	70
Altri provvedimenti di segnalazione del Garante	33
Provvedimenti istruttori ai sensi dell'art. 32 comma 1	95
Procedimenti contenziosi definiti sulla base di ricorsi (art. 29)	243
Elementi forniti per la risposta del Governo a interrogazioni parlamentari	10
Note e comunicazioni in materia di misure minime di sicurezza	537
Note e comunicazioni in materia di data certa ai fini dell'applicazione delle misure minime di sicurezza	341
Comunicati stampa e dichiarazioni alla stampa	71
Notiziari settimanali pubblicati dall'Ufficio Stampa (istituiti l'8 marzo)	55
Richieste di accesso e/o di verifica di dati esistenti nel Sistema Informativo Schengen (**)	122
Procedimenti relativi alle richieste di accesso e/o di verifica di dati esistenti nel Sistema Informativo Schengen già definiti (**)	42
Codici di deontologia promossi	6
Codici di deontologia pubblicati	1
Seminari e conferenze internazionali	4
Procedimenti ispettivi	20
Segnalazioni all'autorità giudiziaria	4

(*) n. compreso di quelle presenti negli anni precedenti

(**) periodo di riferimento della statistica: 11/04/2000 - 30/04/2001

SERVIZI ISPETTIVI

Ispezioni effettuate:		**20**
Sopralluoghi ex. Art. 32, comma 1	2	
Sopralluoghi ex. Art. 13 legge n. 689/1981	4	
Accessi alle banche dati con decreto dell'A.G.	5	
Accessi alle banche dati con assenso	8	
Collaborazioni con autorità giudiziarie	1	

Ispezioni effettuate nei confronti di:		**20**
Soggetti privati	17	
Soggetti pubblici	3	

Risultati ottenuti:		
Provvedimenti di divieto di trattamento ex. 31 comma 1, lettera	3	
Provvedimenti di blocco di trattamento ex. 31 comma 1, lettera	1	

Contestazione della sanzione amministrativa ex. Art. 39		**4**
Per violazione all'art. 10	2	
Per violazione all'art. 32, comma 1	1	
Pagamenti in misura ridotta della sanzione	1	

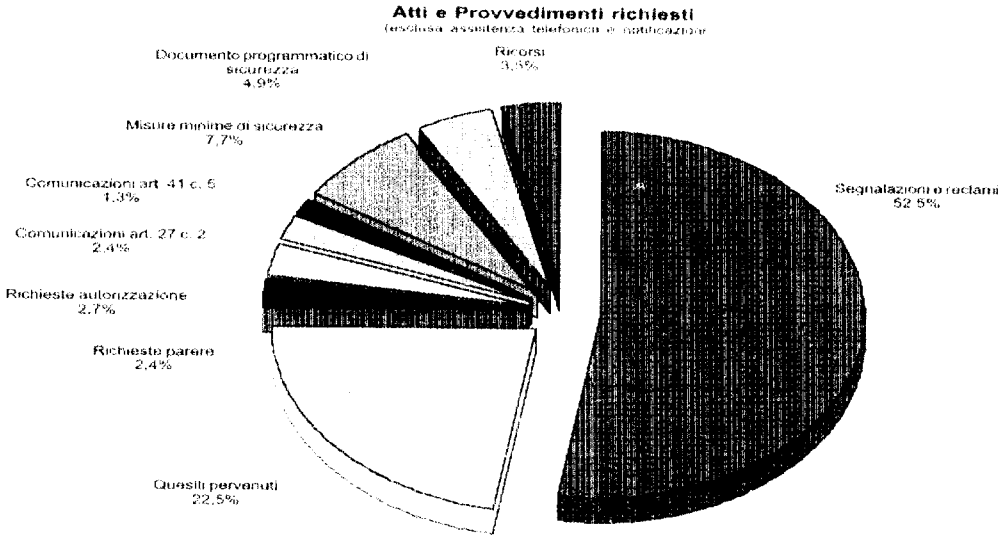
Persone segnalate all'autorità giudiziaria		**4**
Per omessa notificazione al Garante	2	
Per trattamento illecito (art. 35)	1	
Per omessa adozione misure minime di sicurezza (art. 36)	1	

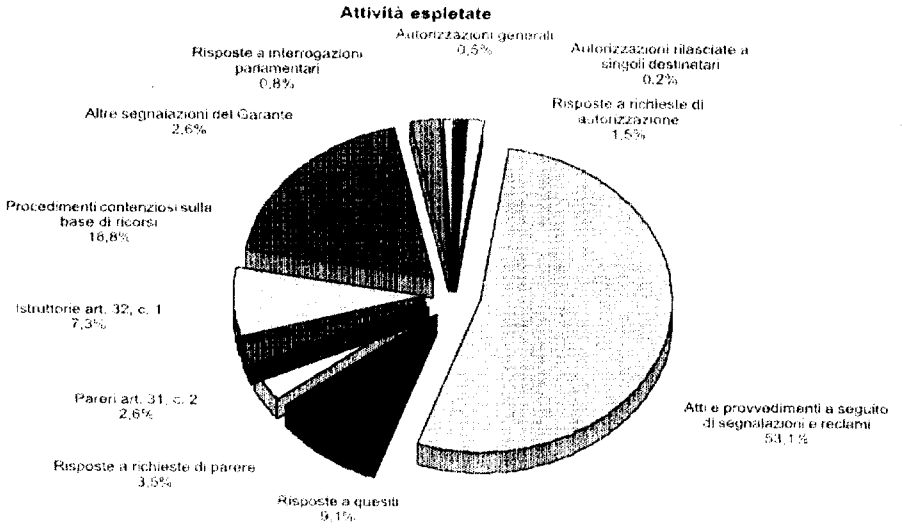
SERVIZIO RICORSI

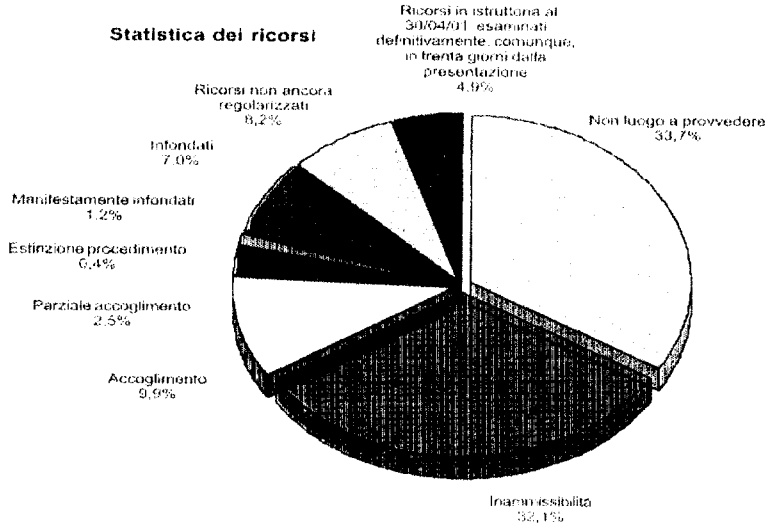
Pervenuti		**243**

Tipo di decisioni adottate:		**243**
Non luogo a provvedere	82	
Inammissibilità	78	
Accoglimento	24	
Parziale accoglimento	6	
Estinzione procedimento	1	
Manifestamente infondati	3	
Infondati	17	
Ricorsi non ancora regolarizzati	20	
Ricorsi in istruttoria alla data del 30 aprile 2001, esaminati definitivamente, comunque, in trenta giorni dalla presentazione	12	

Statistica di quelli pervenuti, dal 01/01/2000 al 30/04/2001


Atti e Provvedimenti richiesti
(esclusa assistenza telefonica e notificazioni)
Documento programmatico di sicurezza 4,9%
Ricorsi 3,5%
Misure minime di sicurezza 7,7%
Comunicazioni art. 41 c. 6 1,3%
Comunicazioni art. 27 c. 2 2,4%
Richieste autorizzazione 2,7%
Richieste parere 2,4%
Quesiti pervenuti 22,5%
Segnalazioni o reclami 52,5%


Attività espletate
Autorizzazioni generali 0,5%
Risposte a interrogazioni parlamentari 0,8%
Autorizzazioni rilasciate a singoli destinatari 0,2%
Altre segnalazioni del Garante 2,6%
Risposte a richieste di autorizzazione 1,5%
Procedimenti contenziosi sulla base di ricorsi 16,8%
Istruttorie art. 32, c. 1 7,3%
Pareri art. 31, c. 2 2,6%
Risposte a richieste di parere 3,5%
Risposte a quesiti 9,1%
Atti e provvedimenti a seguito di segnalazioni e reclami 53,1%


Statistica dei ricorsi
Ricorsi in istruttoria al 30/04/01 esaminati definitivamente, comunque, in trenta giorni dalla presentazione 4,9%
Ricorsi non ancora regolarizzati 8,2%
Non luogo a provvedere 33,7%
Infondati 7,0%
Manifestamente infondati 1,2%
Estinzione procedimento 0,4%
Parziale accoglimento 2,5%
Accoglimento 9,9%
Inammissibilità 32,1%

ATTIVITÀ COMUNITARIE E INTERNAZIONALI

LA CONFERENZA DI VENEZIA

83. IL BILANCIO DELL'INIZIATIVA E LA "CARTA" DI VENEZIA

Tra il 28 e il 30 settembre 2000 si è svolta per la prima volta in Italia, a Venezia, una Conferenza internazionale delle autorità garanti, dedicata ai diversi temi della *privacy* e della protezione dei dati personali.

L'iniziativa, giunta alla sua ventiduesima edizione, rappresenta un importante appuntamento annuale al quale prende parte un numero crescente di Autorità di garanzia istituite progressivamente in Paesi nel mondo.

Essa ha rappresentato, oltre che un notevole e riuscito sforzo organizzativo, il culmine dell'attività di evidenza internazionale svolta dal Garante nell'ultimo quadriennio ed ha ulteriormente consolidato, per i sentiti attestati di merito pervenuti da ogni parte all'indirizzo dell'Autorità (a soli quattro anni dalla sua costituzione), lo *standing* internazionale della stessa, già onorata in precedenza dalla elezione del prof. Stefano Rodotà quale Presidente del Gruppo dei garanti europei.

Principalmente, due tratti hanno contrassegnato la Conferenza: da un lato, l'apertura del convegno, non ristretto al mero contesto tecnico-giuridico, a sollecitazioni provenienti da ogni parte della società, come testimoniato dagli interventi non di mero saluto che hanno onorato le varie fasi dei lavori, provenienti dalle massime autorità istituzionali nazionali ed internazionali e per primo dal Presidente della Repubblica Carlo Azeglio Ciampi (oltre che dal Presidente del Consiglio dei ministri Giuliano Amato, dal Commissario europeo Vitorino e dal Ministro della funzione pubblica Franco Bassanini), dagli esponenti della cultura, del mondo accademico, dell'impresa e della società civile quali, tra gli altri, Umberto Eco, Spyros Simitis, André Vitalis, Yves Poullet, Joel Reidenberg, Lucio Stanca, Marc Rotemberg.

Dall'altro, è da rilevare la significativa partecipazione di Autorità di garanzia appartenenti a nuovi Paesi, segno inequivoco della progressiva estensione della disciplina a tutela dei dati personali a livello mondiale e indice della condivisa necessità di una progressiva armonizzazione ed omogeneizzazione dei principi fondamentali in materia.

I lavori della Conferenza, articolatisi in alcune sessioni plenarie e in numerose sessioni parallele (e svoltisi per larga parte presso la Fondazione Cini nonché, nell'ultima giornata, a Palazzo Labia), hanno visto alternarsi circa settanta autorevoli relatori provenienti da ogni parte del mondo.

Numerose relazioni, tempestivamente presentate dagli Autori, sono state già raccolte in anticipo nel volume "*One World, One Privacy*". 22nd International Conference on Privacy and Personal Data Protection. "*Toward an Electronic Citizenship. Reference Paper*", mentre è in fase di predisposizione una pubblicazione che seleziona i contributi più rilevanti.

Assai ampia è stata la selezione dei temi trattati nel corso delle giornate veneziane. All'interno delle sessioni plenarie la discussione è stata convogliata verso i seguenti temi: "*New Technologies, Security and Freedom*"; "*The State of Privacy*" e "*What Rules? Integrating Different Tools in a Global Perspective*".

Un'ulteriore e significativa parte dei lavori si è svolta in numerose sessioni parallele intitolate: "*Law Enforcement and Judicial Activities*" (presieduta dal prof. Giuseppe Santaniello); "*Contracts and Data*

Flows"; "*Privacy Costs and Software Solutions*"; "*Smart Cards and Centralized Data Banks*"; "*Intranets and Global Services*" (presieduta dall'ing. Claudio Manganelli); "*Privacy and the Media*" (introdotta dalla relazione del prof. Ugo De Siervo); "*E-transparency*" (presieduta dal dott. Giovanni Buttarelli); "*Genetic Data*" e "*New Challenges*".

Oltre alla valenza scientifica dei contributi presentati e degli scambi di opinioni emersi a margine dei lavori, la Conferenza ha offerto ulteriori frutti: il primo, di immediato rilievo per le Autorità di garanzia dei diversi Paesi, consiste nell'accordo raggiunto, sulla base di uno studio preliminare realizzato da Bruce Slane (*Data Protection Commisioner* in Nuova Zelanda), in ordine all'*iter* da seguire in futuro per l'approvazione di risoluzioni e documenti nelle successive Conferenze internazionali.

Ulteriore e più rilevante esito della Conferenza è stata poi la dichiarazione sottoscritta a conclusione dei lavori dalle Autorità di garanzia per la protezione dei dati personali dei ventisette Paesi presenti, ormai nota come "Carta" di Venezia: con essa, muovendo dal generale riconoscimento della *privacy* come diritto fondamentale della persona e quale elemento costitutivo della libertà del cittadino, si è ribadito il consenso intorno a principi e criteri comuni in materia di protezione dei dati già contenuti nelle Linee-guida dell'OCSE, nella Convenzione del Consiglio d'Europa n. 108/1981 e nelle direttive dell'Unione europea, oltre che nelle risoluzioni e raccomandazioni di organismi internazionali, atti sopranazionali contenenti il nucleo centrale dei principi generalmente condivisi in materia di protezione dei dati.

Peraltro si è convenuto che, lungi dal costituire un punto d'arrivo, questi testi normativi rappresentano un punto di partenza per un lavoro comune, preordinato alla loro diffusione nel panorama mondiale tenendo conto dei mutamenti tecnologici, sempre più rapidi e pervasivi, e all'incremento, su scala planetaria, della circolazione delle informazioni.

Più da vicino, gli obiettivi da perseguire dovrebbero articolarsi secondo tre direttici principali: il consolidamento del carattere vincolante dei principi generalmente condivisi, in particolare quelli relativi alle finalità della raccolta, alla lealtà e trasparenza del trattamento (con particolare riferimento ai c.d. trattamenti invisibili), alla proporzionalità, alla qualità dei dati, alla durata della conservazione, all'accesso e agli altri diritti degli interessati; la ricerca di un'accresciuta effettività della tutela attraverso un controllo indipendente dei trattamenti e la disponibilità di mezzi di ricorso facilmente utilizzabili; il rafforzamento delle garanzie per particolari tipologie di dati (come quelli genetici) o di trattamenti (si pensi alle diverse forme di sorveglianza elettronica).

Per tale via, infatti, si ritiene possibile assicurare universalmente un livello di garanzie adeguato, indipendentemente dal luogo in cui i dati sono trattati e dagli strumenti con i quali tali garanzie sono attuate a livello nazionale e internazionale.

IL RECEPIMENTO DELLE DIRETTIVE COMUNITARIE

84. LE DIRETTIVE SULLA PROTEZIONE DEI DATI, IL COMMERCIO ELETTRONICO E LA FIRMA ELETTRONICA

L'armonizzazione delle regole in materia di tutela delle persone riguardo al trattamento dei dati personali è stata raggiunta nell'Unione europea con l'adozione e la successiva entrata in vigore della direttiva 95/46/CE. I principi in essa contenuti, ispirati al rispetto ed alla pratica applicazione dell'articolo 8 della Convenzione europea dei diritti dell'uomo che, appunto, individua tra i diritti fondamentali quello alla riservatezza, sono poi stati estesi e specificati, con gli adattamenti resisi necessari, ad uno dei settori su cui maggiormente la rapida evoluzione della tecnica si coniuga con un parallelo se non addirittura esponenziale aumento dei rischi di violazione della *privacy*, quello delle telecomunicazioni, con la direttiva 97/66/CE.

Come già indicato nelle precedenti relazioni, l'Italia ha recepito molti aspetti della direttiva generale in materia di protezione dei dati con la legge n. 675 del 1996, mentre il decreto legislativo n. 171 del 1998 ha dato attuazione alla direttiva in materia di telecomunicazioni.

La trasposizione delle due direttive nel diritto interno degli Stati membri non è però, ad oltre due anni e mezzo dalla scadenza del termine fissato, stata ancora completata. Di seguito si accennerà alle nuove disposizioni introdotte in alcuni Paesi (segnatamente in Danimarca, Olanda ed in Germania riguardo alla direttiva 95/46/CE) e si traccerà un quadro aggiornato dello stato di attuazione delle direttive.

I principi introdotti dalle direttive non sono stati pensati come rivolti solo agli Stati membri. Essi costituiscono parte dell'*acquis* comunitario e dovranno pertanto essere integrati negli ordinamenti degli Stati candidati all'adesione. Il negoziato in corso per l'allargamento dell'Unione tiene in debita considerazione l'aspetto della protezione dei dati personali e l'Ufficio del Garante è presente alle riunioni di coordinamento che si svolgono periodicamente presso il Ministero degli affari esteri.

L'influenza della legislazione comunitaria in materia spiega anche effetti riguardo agli altri Paesi, come ben mostra l'esperienza del negoziato con gli Stati uniti per il trasferimento dei dati verso quel Paese ed il lungo e complesso lavoro svolto al riguardo dal Gruppo dei garanti dell'articolo 29 della direttiva, sotto la presidenza del Presidente del Garante italiano, prof. Stefano Rodotà.

È utile peraltro menzionare che anche le istituzioni e gli organismi comunitari sono tenuti all'applicazione dei principi delle direttive in materia di protezione dei dati personali, in base al disposto dell'articolo 286 del Trattato di Amsterdam e ad istituire un organo di controllo indipendente sui trattamenti di dati dagli stessi effettuati. Con il regolamento n. 45/2001 del 18 dicembre 2000 sono state dettate le disposizioni atte a costruire il necessario quadro giuridico di riferimento.

Stato di recepimento della direttiva 95/46/CE e della direttiva 97/66/CE (maggio 2001)

(Per una visione sinottica dello stato di recepimento delle due direttive si rimanda alla tabella riassuntiva al termine della presente sezione).

– Direttiva 95/46/CE

Nel corso del 2000 due stati dell'Unione europea hanno adottato disposizioni di trasposizione della direttiva generale in materia di protezione dei dati.

La Danimarca ha approvato la legge n. 429 del 31 maggio 2000 (Legge sul trattamento di dati personali), mentre nei Paesi Bassi è stata emanata dal Parlamento la legge 6 giugno 2000 sulla protezione dei dati personali, la cui entrata in vigore è prevista per l'estate del 2001. In entrambi i Paesi esisteva già una legge nazionale in materia di protezione dei dati, antecedente alla direttiva europea, e operavano già autorità nazionali di controllo. I nuovi testi legislativi, recependo i principi comunitari e allineando i poteri delle autorità di controllo a quelli delle autorità degli altri Paesi, si pongono come integralmente sostitutivi dei precedenti

La legge danese introduce anche alcune disposizioni dettagliate relative soprattutto al trattamento del "numero di registrazione nazionale", ai trattamenti per scopi di *marketing* o di valutazione della solvibilità (in particolare, le agenzie di *credit rating/reporting* devono chiedere l'autorizzazione dell'autorità nazionale di controllo prima di dare corso al trattamento).

I principi fondamentali fissati dalla direttiva (pertinenza, non eccedenza, esattezza, rispetto della finalità, correttezza, diritto di accesso e rettifica, informazione, consenso, ecc.) trovano pieno riconoscimento nel testo di legge danese.

L'articolo 2 della legge prescrive che nessuna disposizione può trovare applicazione se risulta in contrasto con l'articolo 10 della Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali.

I trattamenti effettuati per scopi esclusivamente di natura giornalistica sono esenti da varie disposizioni tranne quelle relative all'obbligo di adottare idonee misure di sicurezza e al risarcimento dei danni eventualmente causati all'interessato dal trattamento dei suoi dati personali. Sono inoltre esclusi dall'ambito di applicazione della legge i trattamenti effettuati dai servizi di informazione della polizia e della struttura di difesa nazionale.

Per quanto riguarda l'Autorità nazionale di controllo (*Datatilsynet*), essa si compone, in base alla nuova legge, di un Segretariato che svolge l'ordinaria attività e di un Consiglio che è costituito dal Ministro della giustizia e comprende 7 membri; il presidente del Consiglio deve essere un giudice abilitato allo svolgimento dell'attività giudiziaria.

L'articolo 61 prevede che non sia possibile ricorrere contro le decisioni dell'autorità di controllo dinanzi ad altre autorità amministrative.

La legge approvata dai Paesi Bassi al termine di un lungo *iter* legislativo prevede, per alcuni settori, l'emanazione di discipline più dettagliate attraverso appositi atti regolamentari (dei quali è prevista l'approvazione entro il 2001). Anch'essa segue nel complesso le disposizioni della direttiva comunitaria, soprattutto per quanto concerne i requisiti attinenti alla qualità dei dati ed alle condizioni per la liceità del trattamento (informativa, consenso, ecc.).

Strutturalmente è interessante rilevare che le circostanze nelle quali il trattamento di dati sensibili è consentito, oltre che in una disposizione generale (articolo 23) modellata sull'articolo 8(2) della direttiva, sono delineate in modo particolareggiato per le singole categorie di dati (relativi alla fede religiosa, alla razza, alle opinioni politiche, all'appartenenza sindacale, allo stato di salute) in rapporto a specifiche finalità e a singole categorie di titolari (articoli 17-22). L'articolo 21, in particolare, reca nel comma 4 il divieto di trattare dati di natura genetica se essi non riguardano direttamente l'interessato presso cui sono stati ottenuti, tranne che prevalga "un importante interesse di natura sanitaria" oppure il trattamento "sia necessario per scopi di ricerca scientifica o di statistica"; in quest'ultimo caso, poi, occorre il consenso espresso dell'interessato, dal quale si può tuttavia prescindere se il suo ottenimento "appare impossibile" o comporta "uno sforzo proporzionato" (purché siano previste garanzie sufficienti ad assicurare che il trattamento "non incida negativamente" sulla *privacy* dell'interessato).

In tema di notificazione dei trattamenti, la legge olandese prevede (oltre ai casi di esenzione sostanzialmente analoghi a quelli della legge italiana e di altre leggi nazionali) che essa non debba essere presentata se non si utilizzano strumenti automatizzati, a meno che il trattamento sia, per sua natura, soggetto ad "accertamento preliminare". Quest'ultimo è previsto dalla direttiva comunitaria (art. 20) e riguarda (artt. 31-32) i trattamenti concernenti il "numero personale di identificazione" per scopi diversi da quelli per cui esso è stato istituito, i trattamenti che consistono nella "registrazione di dati sulla base delle proprie osservazioni" effettuata "senza informarne gli interessati", ovvero trattamenti di dati di natura penale per finalità diverse da quelle previste nelle apposite licenze rilasciate alle agenzie investigative e di sicurezza private. In questi casi i titolari devono sempre notificare i trattamenti all'autorità di controllo e attenderne l'autorizzazione prima di procedere all'elaborazione dei dati.

Per quanto concerne i poteri dell'Autorità nazionale di protezione dati (*Registratiekamer*), va detto che in caso di mancato soddisfacimento da parte del titolare delle richieste di accesso o rettifica o cancellazione, o di mancata ottemperanza all'opposizione al trattamento di dati personali, l'interessato deve rivolgersi al tribunale territorialmente competente anziché all'autorità di controllo – eventualmente chiedendo a quest'ultima di fungere da mediatrice nel contenzioso oppure di esprimere il proprio parere sulla controversia con il titolare (artt. 46-47). L'Autorità può comunque eseguire accertamenti, d'ufficio o su segnalazione degli interessati, rispetto all'applicazione della normativa nazionale sulla protezione dei dati in determinati settori e, se del caso, imporre sanzioni amministrative pecuniarie o di natura restrittiva, nonché, in casi determinati (art. 75), di natura penale. L'Autorità è formata da un presidente e da due componenti, assistiti da un comitato consultivo e da un segretariato; in questo la struttura organizzativa è rimasta sostanzialmente immutata rispetto a quella prevista dalla legge precedentemente in vigore.

Per quanto riguarda gli altri Paesi dell'Unione europea, fino al maggio 2001 erano quattro (Francia, Germania, Irlanda, Lussemburgo) quelli ove la direttiva non era stata ancora recepita nel diritto nazionale.

In Germania il *Bundesrat* tedesco ha licenziato da poco in via definitiva (23 maggio 2001) il testo della nuova legge federale che modifica la Legge sulla protezione dati, già approvata dal *Bundestag* il 7 aprile scorso. La relativa proposta di legge era stata adottata il 14 giugno del 2000 dal Governo federale e successivamente presentata ai due rami del Parlamento.

La legge si applicherà ai soggetti pubblici della Federazione ed a quelli privati, mentre quella attuale regolamenta i trattamenti effettuati dai soggetti pubblici federali e dei *Länder* (se non esistono norme specifiche in materia nei singoli stati) e dai soggetti privati solo per quanto riguarda i dati contenuti o provenienti da archivi. Il testo consolidato della nuova normativa sarà pubblicato prossimamente sul *Bundesgesetzblatt* a cura del Ministero dell'interno. Essa introduce, in particolare, la definizione di dati "sensibili" ("categorie particolari di dati personali"), prevede la pseudonimizzazione o anonimizzazione dei dati, regolamenta l'impiego di sistemi di videosorveglianza in ambito pubblico (limitando l'utilizzazione delle immagini registrate agli scopi per cui i singoli dispositivi sono stati installati e prevedendo l'obbligo di informare gli interessati i cui dati siano stati raccolti, oltre all'indicazione dell'esistenza di dispositivi di sorveglianza in funzione), delimita i poteri del Garante federale per la protezione dei dati personali (che è competente a verificare il rispetto della normativa da parte dei soggetti pubblici che trattino dati personali).

A seguito degli emendamenti apportati, viene introdotto l'obbligo di nominare un "incaricato per la protezione dei dati" anche presso i soggetti pubblici – mentre in base alla legge precedente tale obbligo sussisteva soltanto per i trattamenti di dati personali effettuati da soggetti privati. La nuova legge federale ha quindi recepito in pieno l'indicazione della direttiva comunitaria, che non è ancora fatta propria in alcuni Paesi compresa l'Italia. La nuova articolazione legislativa sembra puntare dunque ad una maggiore armonizzazione nella configurazione del regime di protezione dati applicabile a soggetti pubblici e non pubblici.

Va rilevato che al controllo del Garante federale sui trattamenti effettuati dai soggetti pubblici si sottraggono soltanto i trattamenti di dati personali effettuati dalla *Deutsche Welle* (l'organismo che riuni-

sce le emittenti radiotelevisive pubbliche), presso la quale opera in modo autonomo un incaricato per la protezione dei dati.

La legge prevede, infine, che i trattamenti di dati iniziati prima della data di pubblicazione del testo della novella sulla Gazzetta ufficiale debbano essere resi conformi ad essa entro un termine di tre anni; le disposizioni di legge eventualmente non armonizzate con quelle della direttiva 95/46/CE potranno essere modificate in tal senso entro un termine di cinque anni. Va precisato che in sei *Länder* sono state adottate nel frattempo leggi sulla protezione dei dati che recepiscono la direttiva, applicabili ai soggetti pubblici di ciascun *Land* (Brandeburgo, Baden-Württemberg, Baviera, Assia, Renania settentrionale-Vestfalia, Schleswig-Holstein).

Negli altri Stati sopra menzionati (Francia, Irlanda, Lussemburgo) esiste già da tempo una legge nazionale applicabile ai trattamenti di dati personali. La Commissione europea ha avviato anche nei loro confronti una procedura di infrazione (gennaio 2000) per mancato recepimento della direttiva comunitaria, e tale procedura è ormai giunta alla terza fase – ossia, la citazione dinanzi alla Corte di giustizia delle Comunità europee. Di seguito si danno alcuni cenni sullo stato di avanzamento dell'iter legislativo nei Paesi in oggetto.

In Francia il Governo ha sottoposto nel mese di luglio 2000 un progetto preliminare di legge al parere dell'autorità nazionale di controllo (CNIL) che si è pronunciata; l'*iter* parlamentare per giungere alla promulgazione di una nuova legge (sostitutiva di quella attualmente in vigore, che risale al 1978) non si preannuncia breve;

In Irlanda il Governo deve approvare il progetto di legge in materia, che sarà successivamente presentato in Parlamento;

In Lussemburgo il testo della nuova Legge sulla protezione dei dati è stato presentato in Parlamento all'inizio del mese di ottobre 2000 e l'*iter* parlamentare è in corso.

Da segnalare infine l'approvazione della nuova legge islandese, sostitutiva della precedente e di una disciplina settoriale in Svezia per quanto riguarda i luoghi di lavoro. La *Grecia* ha emendato da ultimo l'articolo 9 della Costituzione in riferimento alla tutela della *privacy*, mentre in *Belgio* sono state adottate disposizioni che recepiscono la direttiva comunitaria con effetto dal 1° settembre 2001.

– Direttiva 97/66/CE

Lo stato di recepimento della direttiva specifica in materia di *privacy* e telecomunicazioni presenta una sostanziale novità rispetto all'anno precedente, ossia l'approvazione in Grecia della legge n. 2774 del 22 marzo 2000 sulla protezione dei dati nel settore delle telecomunicazioni, che attua la direttiva nel diritto nazionale. La vigilanza sull'applicazione di tale normativa è affidata congiuntamente all'ente greco per le telecomunicazioni (EETT) e all'autorità nazionale per la protezione dei dati.

Sono quindi due, attualmente, gli Stati membri dell'Unione europea in cui la direttiva non è stata ancora trasposta: Irlanda e Lussemburgo.

In Irlanda un progetto di legge è in via di definizione e dovrà essere approvato dal Ministro per le pubbliche imprese. In base alla normativa attualmente vigente, gli abbonati hanno già il diritto di ricevere fatturazioni non dettagliate, mentre alcuni dei requisiti fissati dalla direttiva (come l'identificazione della linea chiamante) sono già offerti da singoli gestori.

In Lussemburgo il Governo risulta aver messo a punto sinora soltanto il disegno di legge per recepire la direttiva 95/46 (v. sopra). Sono numerosi i problemi esistenti in Lussemburgo rispetto alla tutela della *privacy* nelle telecomunicazioni; si ricorda, in particolare, l'obbligo per i gestori di conservare i dati di traffico.

In diversi altri Paesi membri dell'UE il 2000 ha visto l'emanazione di disposizioni normative che hanno integrato le disposizioni di trasposizione della direttiva per le parti che (come già segnalato nella precedente Relazione) presentavano alcune lacune.

La Danimarca, in particolare, ha approvato la Legge n. 418 sulla concorrenza e le condizioni per il consumatore nel settore del marketing a distanza (31 maggio 2000), che ha modificato la legge generale sul *marketing* recependo l'articolo 12 della direttiva (chiamate indesiderate). È stata inoltre emanata una disciplina secondaria (due ordinanze, n. 569/2000 sulla fornitura di reti di telecomunicazione e servizi di telecomunicazione, e n. 665/2000 sulle basi di dati numerici) che prevedono l'obbligo per i fornitori di servizi di telecomunicazioni pubblici di adottare misure adeguate per garantire la sicurezza dei servizi. I dati di traffico devono essere cancellati o resi anonimi al termine di ciascuna chiamata, tranne per quanto riguarda dati specifici ai fini della fatturazione e dei pagamenti in caso di interconnessione (questi dati possono essere conservati e trattati fino al termine del periodo durante il quale "può essere legalmente contestata la fattura o preteso il pagamento": art. 6 direttiva).

In Germania la direttiva era già stata recepita attraverso la legge sulle telecomunicazioni (*Telekommunikationsgesetz*, *TKG* del 25 luglio 1996) e l'ordinanza sulla protezione dei dati per i servizi di telecomunicazione (*TDSV*, del 12 luglio 1996). Quest'ultima è stata però abrogata e sostituita nella

sua interezza da una nuova ordinanza (*Telekommunikations-Datenschutzverordnung*) del 18 dicembre 2000, che ha recepito anche le indicazioni della direttiva in materia di identificazione della linea chiamante (un punto rimasto in sospeso nella precedente normativa). In particolare, la nuova ordinanza prevede la possibilità per l'utente chiamato di rifiutare, gratuitamente, le chiamate provenienti da utenti che hanno eliminato la presentazione dell'identificativo della linea chiamante e di ottenere a sua volta l'eliminazione di quest'ultimo senza costi aggiuntivi. I dati relativi al traffico possono essere conservati per un massimo di sei mesi dopo il termine della comunicazione (contro gli ottanta giorni della precedente ordinanza), esclusivamente per verificare la correttezza degli importi fatturati; per il resto, essi devono essere cancellati non oltre il giorno successivo al termine della connessione.

In altri Stati membri, nonostante il recepimento della direttiva, la Commissione ha ritenuto non sufficiente o non corrispondente il livello di attuazione dei principi ed ha avviato procedimenti di infrazione.

I Paesi interessati sono l'Italia, il Belgio, il Lussemburgo ed il Regno Unito.

Nel caso dell'Italia, gli appunti mossi dalla Commissione con una lettera dell'ottobre 2000 riguardavano tuttavia due sole disposizioni non direttamente attinenti alla protezione dei dati, ovvero l'articolo 8(6) –informazione adeguata degli utenti sulle possibili modalità di gestione della CLI (*calling line identification,* l'identificazione della linea chiamante) – e l'articolo 9(1), lett. b) – possibilità di annullare la soppressione della CLI per i servizi che trattano chiamate di emergenza (compresi forze di polizia e servizi di ambulanza). La Commissione ha infatti ritenuto che le disposizioni contenute in merito nel decreto legislativo 171/98 non siano sufficienti a garantire il pieno recepimento delle due nome nel diritto italiano. Il Ministero delle comunicazioni e l'Ufficio del Garante sono stati richiesti di indicare soluzioni in proposito.

Va in conclusione rilevato che l'analisi complessiva riferita al settore delle TLC deve tenere conto degli sviluppi nel frattempo intercorsi a livello comunitario proprio in questi settori, e in modo particolare nella definizione da parte della Commissione europea di un quadro organico di riforma del settore delle comunicazioni elettroniche comprendente, fra l'altro, una proposta di direttiva che intende sostituire la direttiva 97/66.

Direttive sul commercio elettronico e sulla firma elettronica

La direttiva n. 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico), è stata adottata l'8 giugno 2000 al termine di un lungo e difficile negoziato, condotto anche con la partecipazione dell'Ufficio del Garante per gli aspetti più specificamente legati al rispetto dei diritti della persona riguardo al trattamento dei dati.

Come già ampiamente esposto nella precedente Relazione, finalità della direttiva era soprattutto quella di consentire lo sviluppo del commercio elettronico garantendo, attraverso la previsione di una cornice di regole armonizzate, che le attività legate alla Società dell'informazione possano svolgersi nel rispetto di principi comuni e condivisi, in modo da creare il necessario ed essenziale rapporto di fiducia rispetto agli utenti (consumatori e contraenti).

Un tassello fondamentale per l'instaurazione di un clima di fiducia rispetto alle transazioni in rete è, sicuramente, rappresentato da un livello elevato di tutela della riservatezza. Ed è proprio a tal fine che, grazie anche all'intervento nei lavori dell'Ufficio del Garante, si è riusciti ad evitare che si introducessero in questa direttiva principi e previsioni non in linea con le disposizioni dettate a tutela delle persone in relazione al trattamento di dati personali dalle direttive 95/46/CE e 97/66/CE.

Come ben evidenziato nel considerando 14 della direttiva "la protezione dei dati relativamente al trattamento dei dati personali è disciplinata unicamente dalla direttiva 95/46/CE ....e dalla direttiva 97/66/CE....che sono integralmente applicabili ai servizi della società dell'informazione. Dette direttive già istituiscono un quadro giuridico comunitario nel campo della protezione dei dati personali...". Di conseguenza ed a causa di ciò, le "questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46/CE e 97/66/CE" sono escluse dal campo di applicazione della direttiva sul commercio elettronico, come recita l'articolo 1, comma 5, lettera b).

Ciò nonostante sono presenti nella direttiva rischi di sovrapposizione e/o conflitto con taluni principi, ad esempio in relazione all'articolo 7 (comunicazione commerciale non sollecitata) ed agli articoli 12 a 14 che disciplinano la responsabilità dei prestatori intermediari rispetto al "trasporto", alla "memorizzazione temporanea" e all'"*hosting*" di informazioni, qualora queste contengano o attengano a dati personali.

Gli aspetti ora richiamati assumono grande interesse e richiedono ulteriore attenzione anche a causa delle proposte formulate dalla Commissione per definire il nuovo quadro delle comunicazioni elettroniche, inclusi i riflessi sulla vita privata.

Sarà pertanto cura dell'Autorità partecipare alla predisposizione del decreto attuativo della direttiva, previsto in allegato dalla legge comunitaria per il 2001.

La direttiva relativa ad un quadro comune sulle firme elettroniche, adottata il 13 dicembre 1999 (1999/ 93/CE), dovrà essere trasposta negli ordinamenti nazionali dei Paesi U.E. entro il 19 luglio 2001. La previsione dell'emanazione di un decreto attuativo è contenuta nella legge comunitaria per il 2000 (Legge 29 dicembre 2000, n. 422) entro un anno dalla data di entrata in vigore della legge stessa (gennaio 2002).

La direttiva, come già evidenziato nelle precedenti relazioni, è finalizzata ad introdurre una cornice di regole armonizzate tra i paesi membri delle Comunità europee per l'utilizzo delle firme elettroniche e, quindi, a favorire lo sviluppo del commercio elettronico.

Pur riferendosi prioritariamente all'adozione di strumenti utili al settore privato, la direttiva prende in considerazione anche l'uso delle firme elettroniche nei rapporti con il settore pubblico e la pubblica amministrazione, a fini di semplificazione. Essa detta quindi regole per garantire il riconoscimento giuridico delle firme elettroniche ed evitare qualsiasi forma di discriminazione di queste, consentendo, in presenza di precisi requisiti di sicurezza, che le firme elettroniche possano avere valore di prova delle transazioni ed essere considerate pienamente equivalenti alle firme apposte manualmente.

Durante la discussione, la delegazione italiana di cui faceva parte l'Ufficio del Garante, ha lungamente insistito per far introdurre nel testo principi di rigore riguardo alla fissazione dei requisiti necessari per identificare una firma elettronica e prevedere specifiche garanzie e sistemi di verifica nei casi in cui sulla stessa si volesse fondare una presunzione di equivalenza con le firme manoscritte.

Di particolare importanza per il Garante gli articoli 6 (relativo alla definizione delle responsabilità), l'articolo 7 che disciplina gli aspetti internazionali (equivalenza dei certificati rilasciati da prestatori di servizi di certificazione stabiliti in Paesi terzi) e l'articolo 8 (relativo alla protezione dei dati personali, incluso l'uso dello pseudonimo).

Anche in questo caso sarà cura dell'Autorità formulare tutti i contributi necessari alla predisposizione del decreto legislativo di attuazione.

LA MODIFICA DELLA DIRETTIVA SULLA *PRIVACY* NELLE TELECOMUNICAZIONI E LA CONVENZIONE *CYBERCRIME*

85 LE PROSPETTIVE PER I DIRITTI DEGLI INTERESSATI

Come richiamato in precedenza, l'analisi complessiva riferita al settore delle telecomunicazioni deve tenere conto degli sviluppi intercorsi nel settore a livello comunitario.

A seguito del riesame effettuato nel corso del 1999 del quadro normativo dei servizi di comunicazione elettronica, la Commissione europea ha predisposto sei proposte intese a ridisegnare la nuova disciplina delle reti e dei servizi di comunicazione elettronica.

Le proposte, presentate il 12 luglio 2000 al Consiglio ed al Parlamento, comprendono: una direttiva-quadro che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica; una direttiva relativa all'autorizzazione per le reti e i servizi, che armonizza le norme esistenti per la loro fornitura; una direttiva relativa all'accesso alle reti ed alla interconnessione; una direttiva relativa al servizio universale ed ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica; una direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; un regolamento sull'accesso disaggregato al circuito di utente (*local loop*).

Scopo del complessivo intervento è quello di emanare regole neutrali rispetto alla tecnologia, garantendo che i servizi vengano disciplinati secondo modalità equivalenti, indipendentemente, quindi, dai mezzi e dalle modalità con cui sono prestati.

La revisione della direttiva 97/66/CE in questo quadro doveva, a parere della Commissione, essere limitato a poche modifiche, consistenti per lo più nell'adeguamento della terminologia. Gli unici interventi di merito inizialmente previsti, fermo restando il principio del rispetto del livello di tutela garantito a livello europeo nel campo della tutela dei dati personali, riguardavano: definizioni (art. 2); dati relativi al traffico e alla fatturazione (art. 6); dati relativi all'ubicazione (art. 9); elenchi degli abbonati (art. 12); comunicazioni indesiderate (art. 13).

Per quanto riguarda le definizioni, oltre al riferimento a quelle, generali, contenute nella direttiva che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica nonché nella

direttiva 95/46/CE; la proposta prevede un'apposita disciplina per alcune ipotesi in cui si è ritenuto necessario chiarire i concetti utilizzati nel testo. Sono state, ad esempio, introdotte le definizioni di dati di traffico, di dati di localizzazione, di comunicazione e di chiamata (che resta per quanto si riferisce agli ordinari e tradizionali sistemi di telefonia vocale), di servizi a valore aggiunto e di posta elettronica.

La proposta di direttiva mantiene fermi i principi-cardine dell'obbligo di provvedere alla sicurezza della rete per i fornitori, della riservatezza delle comunicazioni (art. 5) e del divieto dell'uso dei dati di traffico, con conseguente necessità di cancellare o rendere anonimi dati relativi ad una comunicazione all'atto del completamento della stessa, fatte salve le eccezioni individuate dall'articolo 6.

L'articolo 9 contiene una nuova previsione che, tenendo conto della possibilità di fornire servizi a valore aggiunto basati sulla localizzazione degli utenti mobili, introduce misure di protezione della vita privata degli utenti e degli abbonati che richiedano la fornitura di tali servizi.

La proposta contiene novità anche riguardo agli elenchi degli abbonati, per i quali prevede che sia lasciata al singolo abbonato la scelta del se comparire o meno negli elenchi e, in caso affermativo, di decidere quali dati debbano figurare, previa in ogni caso un'ampia ed esaustiva informazione delle finalità perseguite e dei possibili usi e la possibilità di ritiro del consenso prestato e le comunicazioni indesiderate, per le quali vige lo stesso principio del consenso preliminare. Da notare che il testo proposto include la posta elettronica e gli sms.

Come vedremo al paragrafo 87 il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ha dedicato una considerevole parte delle attività svolte nel corso dell'anno 2000 all'analisi degli aspetti salienti per la tutela delle persone in relazione alla revisione del quadro giuridico delle telecomunicazioni (parere 2/2000) ed in particolare, alla proposta di direttiva, sia per condividere le scelte effettuate in ordine all'uso degli elenchi pubblici per i servizi di ricerca derivata (parere 5/2000), sia per sottolineare alcuni rischi e lacune del provvedimento (parere 7/2000). Un ampio lavoro è stato svolto da un gruppo specializzato, la *Internet task force*, per individuare gli aspetti tecnici necessari per garantire la protezione dei dati *on-line;* in questo studio si prendono in esame, anche criticamente, le scelte operate dalla Commissione nella proposta di direttiva. La scelta di ampliare il campo di applicazione rispetto alla vigente direttiva 97/66/CE, infatti, se da un lato certamente risponde alle esigenze di una realtà in rapida e continua evoluzione, dall'altro esige che il livello di tutela garantito ai singoli non sia attenuato. Questo implica un'attenta lettura delle disposizioni e dei principi della direttiva 97/66/CE proprio per verificare se essi mantengono o meno intatta la loro validità.

La discussione della direttiva è iniziata nell'aprile 2001, subito dopo che il Consiglio dei ministri telecomunicazioni aveva raggiunto un accordo politico sul testo delle tre direttive "centrali" (la direttiva quadro sui servizi e reti di comunicazione elettronica e le direttive su accesso ed interconnessione e sull'autorizzazione delle reti e dei servizi).

Nel gruppo di lavoro, in cui l'Ufficio del Garante era presente come delegazione italiana, è stato possibile superare difficoltà e preoccupazioni di talune delegazioni, in particolare rispetto: a) alla scelta di lasciare liberi gli abbonati se comparire o meno (e se sì con quali dati) negli elenchi elettronici o cartacei; b) all'inserimento della posta elettronica e degli sms nel generale divieto di invio di comunicazioni indesiderate (che ha richiesto un apposito considerando per evitare sovrapposizioni e conflitti con la previsione dell'articolo 7 della direttiva sul commercio elettronico); c) sugli aspetti legati alle definizioni dei dati di traffico e di localizzazione.

Perplessità e difficoltà non ancora superate si sono invece riscontrate in relazione ad una forte spinta veicolata da non sufficientemente specificate "esigenze della giustizia e delle forze dell'ordine" tese ad introdurre nel testo elementi di indebolimento dei diritti. In particolare tentativi sono stati rivolti ad attenuare sia il principio della riservatezza delle comunicazioni (articolo 5), attraverso l'introduzione di ulteriori fattispecie derogatorie, sia del divieto della conservazione dei dati di traffico, previsto all'articolo 6, attraverso l'eliminazione dello stesso principio che prescrive la cancellazione o l'anonimizzazione dei dati al termine della comunicazione, fatte salve ipotesi espressamente disciplinate.

La proposta è stata anche esaminata nel Consiglio dei ministri delle telecomunicazioni nella riunione del 27 giugno 2001.

Poiché lo sviluppo e la rapida trasformazione che coinvolge in particolare l'Europa verso la "Società dell'informazione" raggiungono e toccano ogni aspetto della vita umana, inclusi lavoro, educazione, formazione, tempo libero, la Commissione, come si è ricordato, ha lanciato nel dicembre 1999 un'iniziativa, denominata *"eEurope"* per fare in modo che il continente europeo possa pienamente trarre i benefici derivanti dalle tecnologie digitali. Questo progetto, adottato dal Consiglio europeo di Feira, prevede una serie di azioni che coprono il periodo fino alla fine del 2002. Nel piano di azione grande attenzione è rivolta alla sicurezza delle reti ed alla lotta contro la criminalità informatica (*cybercrime*).

Esso tende a individuare le modalità e i mezzi per lottare al fine di prevenire lo sviluppo di attività criminali, che possono assumere le forme più varie ed avere una valenza offensiva non riconducibile ai confini nazionali. Il Consiglio d'Europa ha da tempo intrapreso l'elaborazione di una Convenzione

contro la criminalità informatica. Sul progetto di testo il Consiglio dell'Unione ha adottato una posizione comune e diversi strumenti singoli volti a comporre una strategia più generale. Recentemente, il Gruppo dei garanti dell'articolo 29 della direttiva, ha adottato il parere 4/2001 relativo al citato progetto di Convenzione.

Nella Comunicazione del 26 gennaio 2001, intitolata alla "*creazione di una società dell'informazione più sicura attraverso il miglioramento della sicurezza delle infrastrutture e la lotta alla criminalità legata all'uso del computer*", la Commissione europea, svolta un'accurata indagine sui temi di maggior criticità, propone diverse misure. Per il breve periodo, l'adozione di norme armonizzate per combattere la pornografia infantile e lo sfruttamento sessuale dei bambini. Nel medio periodo, invece, la presentazione di altre iniziative di armonizzazione per migliorare le risposte in relazione ai crimini tecnologici (*hacking* ed altri) e ad azioni contro il razzismo e la xenofobia, oltre alla proposta di applicare il principio di mutuo riconoscimento alle ordinanze emesse dai giudici in relazione ad indagini associate alla criminalità informatica che coinvolgano più di uno Stato membro.

Da notare che un aspetto cruciale della comunicazione è relativo alla conservazione dei dati. La Commissione propone che la necessità di adottare misure sul tema, in particolare di natura legislativa, sia verificata in prosieguo dalla stessa Commissione in base ai risultati di consultazioni. A tal fine ipotizza un *forum* di discussione per le forze di polizia, la magistratura, gli operatori *Internet* e quelli delle telecomunicazioni, le organizzazioni di tutela dei diritti civili, i rappresentanti dei consumatori e le autorità di protezione dei dati, nella convinzione, condivisa, che qualunque tipo di soluzione sia fondata su solide basi (normative), oltre che proporzionata e bilanciata rispetto alle diverse esigenze rappresentate.

ALTRE NOVITÀ NEL DIRITTO COMUNITARIO E NEL SETTORE GIUSTIZIA-AFFARI INTERNI

86. PROFILI GENERALI

Il gruppo di lavoro protezione dei dati del Consiglio dell'Unione ha completato la discussione in relazione alla proposta di regolamento del Parlamento e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni e degli organi della Comunità europea.

La proposta, presentata dalla Commissione nel settembre 1999, era intesa a dare attuazione al dettato dell'art. 286 del Trattato di Amsterdam e, pertanto, ad introdurre all'interno delle istituzioni e degli organismi comunitari un livello di tutela dei dati personali corrispondente a quello assicurato in ciascuno degli Stati membri con la trasposizione delle direttive comunitarie 95/46/CE e 97/66/CE, conferendo alla nuova autorità di controllo indipendente il compito di sorvegliare i trattamenti effettuati da queste.

L'Ufficio del Garante ha preso parte attiva ai lavori del gruppo ed al complessivo *iter* che ha portato all'adozione il 18 dicembre 2000 del provvedimento, divenuto poi il regolamento 45/2001 riportato nella documentazione allegata alla presente Relazione.

I principi di protezione dei dati contenuti nella proposta di regolamento sono basati sulle norme comunitarie esistenti e li integrano dettando specifiche disposizioni laddove la direttiva-quadro 95/46/CE lasci margini attuativi agli Stati.

Oltre alle regole generali che riguardano l'oggetto, le definizioni e il campo di applicazione – limitato alle attività che rientrano in tutto o in parte nell'ambito riservato al diritto comunitario – il regolamento riprende i principi della direttiva in materia di qualità e di legittimazione al trattamento, includendo disposizioni specifiche e dettagliate sul cambiamento di finalità e sul loro trasferimento. I principi sono disciplinati in tre distinti articoli, a seconda che il trattamento avvenga all'interno delle istituzioni ed organismi comunitari, verso destinatari soggetti o non soggetti alla direttiva 95/46/CE.

Particolare attenzione è prestata alle condizioni che legittimano il trattamento dei dati sensibili (articolo 10), all'informazione e ai diritti dell'interessato (di accesso, rettifica, blocco, cancellazione), comprensivi della notifica a terzi degli interventi effettuati a seguito dell'esercizio del diritto di accesso.

Si prevede inoltre l'istituzione della figura del responsabile della protezione dati all'interno di ogni istituzione ed organismo comunitario e la specificazione dei suoi compiti e diritti (articoli 24-26); si disciplinano poi le ipotesi in cui è necessario il preventivo avviso del "Garante europeo" rispetto a trattamenti di dati personali che possono comportare rischi.

Un capo apposito, il IV, è dedicato alla protezione dei dati personali e alla tutela della riservatezza nell'ambito delle reti interne di telecomunicazione, ed è ispirato in larga misura ai principi dettati dalla direttiva 97/66/CE.

L'ultimo capo prevede l'istituzione dell'autorità di controllo indipendente, denominata Garante europeo della protezione dei dati: si tratta di un organismo importante, che si colloca a fianco degli organismi comunitari esistenti, con requisiti di indipendenza marcati, sia nelle procedure di scelta, sia nei poteri conferiti ed infine nella attribuzione di ampia autonomia finanziaria ed amministrativa, con la previsione di una linea di bilancio dedicata e di una struttura amministrativa collocata alle sue dipendenze.

Il Garante europeo, che dovrà essere nominato di comune accordo dal Parlamento europeo e dal Consiglio in base ad una lista predisposta dalla Commissione a seguito di un bando pubblico a presentare le candidature, resterà in carica cinque anni, con mandato rinnovabile, e sarà affiancato da un Garante aggiunto, scelto con la medesima procedura e per la stessa durata.

All'Autorità compete sovrintendere al rispetto dei diritti e delle libertà fondamentali delle persone fisiche, in particolare tutelando il diritto alla vita privata nei riguardi dei trattamenti di dati personali effettuati da istituzioni ed organismi comunitari, sorvegliando ed assicurando l'applicazione del regolamento e delle direttive comunitarie in materia, anche attraverso pareri ed indirizzi da rivolgere agli stessi organismi ed istituzioni.

Il Garante europeo della protezione dei dati collabora con le autorità nazionali di controllo in materia di protezione dei dati e con le autorità comuni di controllo istituite da convenzioni internazionali stipulate in base al titolo VI del Trattato (cooperazione in materia di affari interni e giustizia). Partecipa inoltre alle attività del Gruppo per la tutela delle persone istituito dall'articolo 29 della direttiva 95/46/CE.

Tra le funzioni più rilevanti a lui attribuite vi sono la possibilità di trattare reclami ed adottare decisioni (anche svolgendo indagini di propria iniziativa), di sorvegliare l'evoluzione delle tecnologie (in particolare dell'informazione e della comunicazione, per gli aspetti di interesse della protezione dei dati personali), di consigliare istituzioni ed organismi comunitari, di emettere provvedimenti ritenuti necessari al titolare e responsabile del trattamento; di accedere ai locali ove si svolgono i trattamenti se necessario per l'espletamento dei suoi compiti; di adire la Corte di giustizia e di intervenire nelle cause avanti a tale organo nel caso in cui le norme non prevedano la prima possibilità.

Il regolamento è entrato in vigore nel gennaio 2001 e la procedura per la nomina del Garante europeo e del garante aggiunto dovrebbe aver luogo nel breve periodo.

Per quanto concerne il settore giustizia-affari interni, per la parte seguita dal Garante, è opportuno segnalare che il gruppo "Sistemi di informazione e protezione dei dati" ha completato i lavori di predisposizione di una proposta di decisione per la costituzione di un segretariato comune, per fornire supporto alle autorità di controllo già previste ed istituite dalle convenzioni Schengen, Europol e Sistema doganale. La creazione di una struttura di tal genere era in particolare caldeggiata dall'Autorità Schengen, la quale, a seguito dell'incorporazione, con l'entrata in vigore del trattato di Amsterdam, delle strutture Schengen in quelle del Consiglio dell'Unione europea, era rimasta senza segretariato e con seri problemi di bilancio e di partecipazioni alle riunioni.

Questa struttura, collocata presso il Consiglio anche se in forma tale da garantire la sua autonomia, è ora costituita dal segretario protezione dati, nominato a seguito di una procedura di selezione aperta e dal personale assegnatogli per l'espletamento dei compiti previsti dai regolamenti interni di ciascuna delle autorità comuni. Per quanto attiene al supporto amministrativo, consistente in uffici e materiale necessario, incluse le sale riunioni ed il servizio di interpretazione, spetta al Consiglio assicurarle; al Consiglio sono imputate pure le spese amministrative generali.

La proposta è stata approvata dal Consiglio dei Ministri della giustizia e affari interni nella seduta del 17 ottobre. La decisione è stata pubblicata sulla Gazzetta ufficiale delle Comunità europee. L'operatività della decisione è fissata al 1° settembre 2001.

La concreta entrata in funzione del segretariato comune chiarirà se, come temuto da alcune delegazioni, il legame di dipendenza che viene a crearsi con il Consiglio su elementi fondanti dell'indipendenza quali la provvista di uomini, supporti strumentali e mezzi economici, sia tale da incidere sul necessario carattere di indipendenza ed autonomia delle autorità di controllo.

Come ricordato nelle precedenti relazioni, l'attività e la ricostituzione del gruppo di lavoro era scaturita da una richiesta formulata dall'Italia di avviare una riflessione sui numerosi strumenti elaborati od in corso di elaborazione nell'ambito del c.d. "terzo pilastro" del Trattato di Maastricht che istituiscono sistemi automatizzati di elaborazione e di scambi di dati con mezzi automatizzati e cartacei, onde poter valutare successivamente la congruità dell'approccio seguito nel regolare il rapporto tra la protezione dei dati e le diverse forme di cooperazione ed assistenza per esigenze di giustizia e di polizia, e formulare eventualmente nuove modalità operative.

Ciò per tener conto dell'esperienza ed evitare nei lavori successivi:
– un obiettivo sovraccarico dell'attività dei gruppi di lavoro incaricati in seno al Consiglio dell'Unione di portare avanti la cooperazione nelle materie contemplate dall'art. K1 del Trattato, considerata anche la particolarità e la tecnicità delle disposizioni attinenti alla protezione dei dati e alle connesse garanzie per le persone interessate;
– la previsione di modalità differenziate per lo scambio dei dati e per l'esercizio nei diversi Paesi dei diritti di accesso, rettifica, cancellazione, ecc. previsti in materia di protezione dei dati;
– il rischio di disarmonie e/o disparità di trattamento rispetto a situazioni pure omogenee;
– una duplicazione di mezzi e di fondi soprattutto per quel che riguarda il funzionamento delle strutture di supporto delle diverse autorità comuni di controllo.

Nei successivi lavori si è mostrata una sicura preferenza per un approccio pragmatico ai temi proposti attribuendo priorità all'ultimo dei punti appena evidenziati, vale a dire la razionalizzazione delle strutture di supporto delle autorità comuni di controllo, soddisfatta con la ricordata decisione del 17 ottobre 2000.

Non altrettanta attenzione e volontà è stata posta riguardo al tema della definizione dei principi e si è tentato di riprendere l'argomento solo con la presidenza portoghese. Da questa è stato infatti presentato un documento recante "principi generali concernenti la protezione dei dati nel terzo pilastro", documento che costituisce il frutto della riflessione sui principi comuni già esistenti in materia di protezione dei dati in quanto derivanti dalla Convenzione n. 108 del Consiglio d'Europa e dalla direttiva 95/46/CE e di quelli in applicazione nel terzo pilastro (come ad esempio la Raccomandazione 87(15) del Consiglio d'Europa sui trattamenti effettuati nel settore della polizia).

Anche in questo caso si è proceduto con varie difficoltà. Da parte della delegazione italiana, che includeva l'Ufficio del Garante, si è dichiarata una disponibilità a contribuire all'elaborazione del citato documento sull'elaborazione dei principi, pur preferendo che questa fosse preceduta da una adeguata ricognizione delle norme e delle prassi, sia a livello nazionale, sia di accordi bi-multilaterali definiti dai Paesi membri.

La richiesta italiana muoveva dalla necessità di verificare attentamente i singoli aspetti della cooperazione tra le forze di polizia, tra queste e la magistratura, nonchè l'impatto che le norme in materia di protezione dei dati avevano avuto ed hanno sulle attività da esse svolte.

La profonda convinzione che l'introduzione di norme specifiche in materia di protezione dei dati non costituisce un *vulnus* dell'attività di inquirenti e polizia nella prevenzione e repressione dei reati, ma, anzi, ne consentono una maggiore incisività e trasparenza, ha determinato il Garante a curare nell'ambito del programma Falcone, un progetto denominato *"Lotta alla criminalità organizzata e protezione dei dati"*, del quale si tratterà più ampiamente nel prosieguo.

Il gruppo, dopo aver ritenuto che l'iniziale mandato fosse troppo vago, ha ricevuto dal Co.re.per. un nuovo mandato per redigere un *"progetto di risoluzione sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea"*.

Il progetto di risoluzione (si tratta di un atto non vincolante) si applicherebbe a tutti gli strumenti adottati, dopo la sua entrata in vigore, in base alle procedure del titolo VI del trattato, concernenti la cooperazione giudiziaria e di polizia in materia penale.

Ciascuno di questi strumenti dovrebbe poi precisare quali principi individuati negli articoli successivi siano da prevedere nello strumento in questione e per quali tipi di trattamenti. Negli stessi strumenti possono essere fissate deroghe ed eccezioni ai principi ritenuti applicabili (elencati al titolo II) che si rendono necessarie tenendo conto dell'oggetto o delle specificità dello strumento. Il titolo III, unico articolo, prevede che il rispetto dei principi relativi alla protezione dei dati personali sia sorvegliato da una o più autorità di controllo indipendenti.

La cooperazione tra autorità garanti in Europa

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

Gli aspetti relativi alla tutela dei dati personali sono affrontati, come già indicato nella precedente relazione, dal "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" (organismo a carattere consultivo ed indipendente composto dai rappresentanti delle autorità di controllo nazionali, istituito dall'art. 29 della direttiva) e da un Comitato (previsto dall'art. 31 della stessa, che assiste la Commissione ed esprime il suo parere su progetti sottoposti dalla Commissione).

Nel corso dell'anno il Gruppo dei Garanti, presieduto dal prof. Stefano Rodotà, ha proseguito anzitutto i suoi interventi rispetto alla valutazione e delimitazione delle condizioni necessarie per giungere ad un'ipotesi di soluzione del negoziato con gli Stati Uniti e per definire le modalità attraverso le quali può essere consentito un trasferimento di dati personali verso o da quel Paese.

Il negoziato è stato assai intenso. Il testo finale dell'Accordo non recepisce tutte le indicazioni formulate dal Gruppo in diversi pareri, ma è comunque sensibilmente più attento ai diritti delle persone rispetto alle versioni originariamente discusse.

Oltre al negoziato con gli Stati Uniti, il Gruppo dei Garanti ha espresso propri pareri anche in ordine al progetto di decisione della Commissione sulle clausole contrattuali ai fini del trasferimento dei dati verso Paesi terzi (Parere 1/2001 del 26 gennaio 2001 WP 38), alla legge canadese in materia di informazioni personali e documenti elettronici (Parere 2/2001 del 26 gennaio 2001 WP 39) ed al livello di adeguatezza della legge australiana in materia di *privacy*, dettata per il settore privato (Parere 3/2001 del 26 gennaio 2001 WP 40).

Il Gruppo ha inoltre largamente concentrato i suoi lavori sulle sfide delle nuove tecnologie, in relazione alle quali è intervenuto adottando i pareri ricordati sopra al paragrafo 79.

È inoltre intervenuto, tra l'altro, su:

alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali (Parere 1/2000 doc. WP 28 adottato il 3 febbraio 2000);

problema del genoma (Parere 6/2000 doc. WP 34 adottato il 13 luglio 2000);

attuazione della direttiva 95/46/CE (Raccomandazione 1/2000 doc. WP 30 adottata il 3 febbraio 2000);

progetto di Convenzione del Consiglio d'Europa sulla criminalità informatica (Parere 4/2001 WP 41 adottato il 22 marzo 2001);

individuazione di alcuni requisiti minimi per la raccolta *on line* di dati personali nell'Unione europea (Raccomandazione 2/2001 doc. WP 43 adottata il 17 maggio 2001).

I documenti si trovano in allegato alla presente Relazione.

Da ultimo, il Gruppo ha approvato importanti documenti sulla protezione dei dati nel rapporto di lavoro e sul *panel* incaricato di seguire i casi applicativi del *Safe Harbor*. Ha costituito poi un gruppo di lavoro sull'uso delle tecnologie a fini di controllo sui luoghi di lavoro. Specifiche iniziative sono in atto per valorizzare gli atti adottati via Internet e attraverso pubblicazioni.

88. La partecipazione ad altri comitati e gruppi di lavoro

Il Garante, anche attraverso la partecipazione di funzionari dell'Ufficio, ha seguito attivamente ed attentamente gli sviluppi di alcune iniziative settoriali consistenti sia in gruppi di lavoro specifici costituiti in seno al Gruppo dell'articolo 29, sia scaturite da esigenze manifestatesi nel corso delle conferenze annuali dei Garanti europei.

Sotto il primo profilo, merita menzione il lavoro svolto presso la *Internet Task Force*, per brevità "ITF", nata nel 1999 con l'obiettivo di fornire un supporto conoscitivo integrato e sistematico alle attività del "*Data protection Working Party*" previsto dall'art. 29 della direttiva 95/46/EC, con particolare riguardo alla rete Internet ed in generale ai sistemi informativi *on-line*.

Nel corso degli ultimi due anni la "ITF" ha predisposto le bozze di alcuni documenti che sono poi stati adottati dal *Working Party*, per lo più sotto forma di raccomandazioni, allo scopo di migliorare la comprensione dei fenomeni per la tutela della *privacy* in rete.

Recentemente, con l'obiettivo di analizzare in maniera integrata quanto disposto dalle direttive 95/46/EC e 97/66/EC in merito alla protezione dei dati personali in generale e alla medesima tutela nello specifico settore delle telecomunicazioni, la *Internet Task Force* ha predisposto un voluminoso documento di lavoro, adottato il 21 novembre 2000 dal *Working Party*, dal titolo "*Privacy on the Internet – An integrated EU Approach to on-line Data Protection*".

Nel documento la "ITF", prevalentemente composta da esperti delle strutture nazionali per la protezione dei dati personali, compie una dettagliata analisi delle diverse tipologie dei servizi disponibili sulla rete Internet e una verifica delle norme applicabili in quanto tali, segnalando i rischi per ciascuna tipologia di servizio in relazione a carenze normative e/o tecnologiche.

Un ruolo importante hanno assunto nell'anno i seminari internazionali sulla trattazione dei ricorsi e delle segnalazioni ("*Complaints Handling Workshops*").

Facendo seguito ad un'esigenza manifestata nel corso della *Spring Conference of European Data Protection Commissioners* di Helsinki (aprile 1999), nel febbraio 2000 si è tenuto a Manchester il primo

seminario di una serie dedicata allo scambio di informazioni e alla definizione di un *modus operandi* comune per quanto concerne la trattazione dei ricorsi e delle segnalazioni presentate alle autorità nazionali per la protezione dei dati, con particolare riguardo ai casi che, per la loro rilevanza o per la natura delle parti interessate, travalicano l'ambito nazionale.

Al seminario, tenutosi il 7 e l'8 febbraio 2000, hanno partecipato i rappresentanti della quasi totalità delle autorità di garanzia nazionali dell'UE ed un rappresentante della Commissione. Le due giornate di studio sono servite a mettere a punto una sorta di decalogo per garantire un approccio comune alla trattazione dei ricorsi e delle segnalazioni con valenza "internazionale". Tale decalogo prevede, in particolare, l'opportunità di dare priorità ai ricorsi "internazionali" (caso per caso), di contattare l'autorità di protezione dati competente, di trasferire ogni elemento di prova utile alla valutazione del singolo caso (in conformità alle prassi nazionali), di garantire che le singole autorità si tengano reciprocamente informate. I risultati sono stati presentati alla Conferenza di primavera del 2000 tenutasi a Stoccolma, dove è stato deciso che, indicativamente, sarebbero stati due i seminari dedicati ogni anno al tema e che vi dovranno partecipare funzionari impegnati nel settore.

Su questa linea è proseguita l'attività durante il secondo seminario, svoltosi a L'Aja presso l'Autorità garante olandese (*Registratiekamer*) (26-27 ottobre 2000). Il seminario è stato organizzato in forma di *think tank*: le delegazioni partecipanti sono state invitate a presentare un caso significativo che illustrasse le modalità di trattazione dei *complaints*, possibilmente di ambito internazionale, e a riflettere sui possibili approcci comuni. Parallelamente è stato fatto circolare un questionario in cui si chiedeva a tutti i partecipanti di illustrare se e in che modo la singola autorità nazionale utilizzasse Internet per ricevere e/o rispondere a segnalazioni di singoli cittadini, o comunque per facilitare lo scambio di informazioni. L'autorità olandese ha illustrato il proprio modello di funzionamento, in cui un *front office* è deputato a gestire i casi (segnalazioni, richieste di parere, lamentele) risolvibili con maggiore facilità e secondo modelli già consolidati. Sono stati quindi illustrati vari casi nazionali, e per l'Italia, in particolare, il caso Gratistel (v. Relazione Annuale 1999), che aveva avuto un'eco a livello europeo come esempio di attività di tipo preventivo, non motivata da segnalazioni specifiche, bensì svolta prima dell'attivazione del servizio.

Durante l'ultima parte del seminario sono stati presentati i risultati del questionario relativo all'uso di Internet, dai quali è emerso che sostanzialmente tutte le autorità nazionali di protezione dati hanno un proprio sito *web* e lo utilizzano per scambiare informazioni con i cittadini. Tutte prevedono la possibilità di notificare i trattamenti per via informatica, con l'eccezione della Francia che esclude questa modalità in modo specifico (tranne per quanto concerne la notificazione dei siti *web*). Tutti hanno indicato l'opportunità di potenziare l'uso di Internet soprattutto quale strumento di sensibilizzazione del pubblico e dei titolari di trattamenti, oltre che di segnalazione di casi di interesse, anche se pochi (D-Berlino, Norvegia) prevedono espressamente invii e risposte via *e-mail*. È stata infine illustrata una proposta che, alla luce dei risultati di questo e del precedente seminario, prevede un sistema di scambio di informazioni relativo ai *complaints* "internazionali". Tale sistema si basa sull'utilizzo di moduli standard per sintetizzare i singoli casi, e sull'invio di questi moduli via Internet ad un punto centrale di coordinamento che provvede periodicamente (sempre via Internet) ad informare tutte le altre autorità sugli sviluppi e/o i problemi segnalati. Ciò al fine di facilitare e sviluppare la cooperazione tra le stesse autorità secondo quanto previsto dall'art. 28.6.§2 della direttiva 95/46/CE.

Gli sviluppi del seminario de L'Aja sono stati analizzati durante il successivo incontro, tenutosi ad Oslo il 29-30 marzo 2001. I rappresentanti della Commissione europea e dell'Autorità olandese hanno presentato il sito *web* denominato CIRCA (*Communication & Information Resource Center Administrator*), nel cui ambito è stato realizzato lo spazio virtuale che ospiterà il sistema di scambio di informazioni relativo a ricorsi, segnalazioni, reclami, ecc. che coinvolgano più autorità o abbiano comunque rilevanza internazionale. In proposito vi è un orientamento favorevole ad estendere la partecipazione anche alle autorità omologhe di altri Paesi europei con un adeguato livello di protezione dei dati, come la Svizzera e l'Ungheria. Si tratta di una *extranet* riservata alle autorità realizzata nel quadro del programma IDA della Commissione europea (e, quindi, gestita fisicamente mediante un *server* di quest'ultima), per il cui accesso sono previste opportune cautele. All'interno di tale spazio sono previste varie sezioni e, in particolare, una configurata più propriamente come "*newsgroup*", in cui sarà possibile presentare i procedimenti relativi a ricorsi e segnalazioni rispetto ai quali si intende scambiare informazioni con i colleghi delle altre autorità europee. Nella scheda-tipo da compilare per descrivere le caratteristiche dei singoli ricorsi non saranno riportate le generalità delle persone fisiche coinvolte, mentre si potranno indicare, se la legislazione nazionale lo consente, i nominativi di società o imprese, soprattutto quando il caso abbia risvolti internazionali. Ogni autorità ha provveduto ad individuare ed indicare i funzionari che fungeranno da tramite nazionale per il sito, con l'impegno di aggiornare tempestivamente le informazioni e trasmettere eventuali richieste di assistenza o chiarimento in materia di ricorsi (si è concordato che la lingua di lavoro sarà, salvo casi particolari, l'inglese). Il seminario si è suc-

cessivamente focalizzato sull'analisi di singoli casi di rilevanza internazionale, in particolare riguardo alla raccolta e all'utilizzazione di dati effettuata da siti Internet che si rivolgono a minori (come *"Kidlink"*). Le Autorità hanno deciso di condurre accertamenti in sede nazionale e di istituire un primo *newsgroup* all'interno del sito CIRCA dedicato appunto alla trattazione del caso *"Kidlink"* in modo da garantire un approccio quanto più possibile uniforme.

La delegazione italiana ha presentato un caso relativo al diritto di accesso dei dipendenti ai dati valutativi che li riguardano, il quale ha suscitato notevole interesse con riferimento alla nozione di "dato personale" e alle modalità di esercizio dei diritti dei lavoratori interessati (il Gruppo di lavoro ex art. 29 direttiva 95/46/CE ha infatti recentemente emanato una Raccomandazione su tale specifica materia). Si è concordato di istituire un secondo *newsgroup*, sempre all'interno del sito CIRCA, dedicato al problema della *privacy* sul luogo di lavoro con l'indicazione di approcci o materiali utili a sostenere le autorità nazionali nella trattazione di casi come quello italiano – allo scopo di fornire alle autorità giudiziarie nazionali eventualmente adite indicazioni sulla posizione comunitaria in ordine alla questione sottoposta ed un panorama complessivo della normativa e della giurisprudenza degli altri Paesi dell'UE.

L'AUTORITÀ COMUNE DI CONTROLLO SCHENGEN

89. IL RAPPORTO PER IL 1999-2000

L'Autorità comune di controllo (ACC) ha proseguito nel periodo in riferimento la sua attività istituzionale di verifica e controllo del funzionamento della parte centrale del Sistema di informazione Schengen.

La quarta relazione annuale di attività, relativa al periodo marzo 1999-febbraio 2000 è allegata alla presente Relazione; la quinta, relativa al periodo marzo 2000 - febbraio 2001, è in corso di predisposizione.

La relazione annuale dell'Autorità di controllo Schengen, forma oggetto, in uno spirito di trasparenza, di una presentazione pubblica anche per rendere conto ad un pubblico quanto più vasto possibile degli sforzi da essa compiuti al fine di difendere gli interessi dell'individuo nella tutela della vita privata.

L'ACC, anche basandosi su relazioni predisposte da gruppi di lavoro interni, ha formulato raccomandazioni, pareri, proposte e suggerimenti riguardanti sia il controllo della sicurezza del SIS, sia la tutela degli interessi dei singoli individui segnalati o, ancora, l'adempimento dell'obbligo d'informazione nei confronti del cittadino.

L'Autorità lamenta con decisione come, soprattutto a seguito dell'incorporazione di Schengen nelle strutture del Consiglio dell'Unione europea avvenuta con il Trattato di Amsterdam, il trattamento riservato alle sue proposte ed opinioni si è largamente deteriorato. L'ACC arriva a parlare di "trattamento ingeneroso riservato all'ACC, soprattutto per quanto concerne il debito rispetto della sua autonomia e rigorosa indipendenza e l'assegnazione delle risorse finanziarie necessarie per garantirle". Come già rilevato in precedenza è per questo che l'ACC ha salutato con favore la proposta di costituire un'unica struttura di supporto amministrativo per tutte le autorità operanti nel terzo pilastro e di cercare di prevedere effettivi riconoscimenti in termini di autonomia finanziaria ed organizzativa.

Tra i temi di maggior rilievo si segnalano:

Sicurezza degli uffici SIRENE

È proseguita l'opera di sensibilizzazione e di proposta. Sul punto della regolare verifica dei motivi di una interrogazione del SIS le autorità governative si sono dichiarate poco disponibili ad introdurre cambiamenti.

L'ACC, nel prendere atto della risposta, ha deciso di perseverare affinché la sicurezza degli uffici SIRENE sia migliorata e uniformata. Ha convenuto in particolare di stendere un questionario uniforme che permetta alle autorità nazionali di controllo per la protezione dei dati di effettuare le verifiche in modo armonizzato.

Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

Si tratta dell'interpretazione dell'articolo 102, paragrafo 1, della Convenzione, relativo alla conservazione dei documenti ad avvenuta cancellazione di una segnalazione, per il quale gli Stati membri agiscono in modo non uniforme: alcuni, infatti, conservano i documenti relativi alle segnalazioni dopo che queste sono state cancellate e li utilizzano per completare gli schedari di polizia. È in corso una valutazione da parte dei gruppi di lavoro in relazione alle osservazioni dell'ACC per verificare se occorra modificare il manuale SIRENE.

Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata

In caso di usurpazione d'identità alcuni Stati membri introducono nel SIS il nome del legittimo titolare dell'identità usurpata, mentre il bersaglio è piuttosto l'usurpatore.

Dopo un primo parere, cui hanno fatto seguito osservazioni e proposte, l'ACC, esaminate queste proposte nel dicembre 1999 e nel febbraio 2000, ha adottato un secondo parere, complementare al primo, nel marzo 2000. In esso si ribadisce il principio di proporzionalità, in virtù del quale non tutti i casi di usurpazione d'identità giustificano la segnalazione del nome del titolare legittimo e si sottolinea che l'elaborazione dei dati relativi alle persone la cui identità è stata usurpata potrà essere consentita solo previo libero ed esplicito accordo delle stesse o dietro loro richiesta. Nel parere si richiede anche che vengano previste altre misure, quali la possibilità di rilasciare al titolare legittimo dell'identità usurpata un documento supplementare, ad esempio integrativo al passaporto, che attesti che il titolare non è la persona che usurpa l'identità.

Controllo del C.SIS

Il gruppo tecnico appositamente creato dall'ACC costituito di esperti delle autorità di controllo nazionali, coordinato dal rappresentante lussemburghese, ha effettuato a suo tempo, su deliberazione dell'ACC, una visita di controllo. Dalla visita è emersa la possibilità di migliorare la sicurezza del sistema, per la quale sono state formulate specifiche raccomandazioni. Il livello di sicurezza è stato ritenuto globalmente soddisfacente. La relazione riservata sulla visita di controllo è stata approvata nel febbraio 2000 ed è stata trasmessa, corredata di una sintesi, al Comitato dell'articolo 36.

Campagna d'informazione sui diritti dei cittadini nei confronti del SIS

L'ACC ha valutato gli esiti della campagna di informazione svolta in quasi tutti i Paesi Schengen, ritenendola soddisfacente. Come risulta anche per l'Italia, l'efficacia della campagna informativa si può misurare considerando l'aumento delle richieste di verifica e, in generale, del ricorso alle autorità di protezione dei dati personali da parte di persone cui è stato in particolare negato un ingresso od un visto in relazione a dati personali contenuti nelle sezioni nazionali del SIS.

Va infine segnalato che dal 1° gennaio 2000 vi è stato un cambiamento ai vertici dell'ACC, del quale il segretario generale del Garante mantiene la vice presidenza. Il mandato del presidente e del vicepresidente è stato rinnovato per un anno nella riunione del 13 dicembre 2000.

EUROPOL

20. L'ATTIVITÀ DELL'AUTORITÀ COMUNE DI CONTROLLO E I PRIMI CASI DI CONTENZIOSO

L'Autorità comune di controllo sui trattamenti effettuati da Europol ha largamente concentrato i suoi lavori sulla valutazione dei progetti di apertura di archivi di analisi suggerendo, ove necessario, integrazioni e specificazioni alle Autorità Europol.

Ha inoltre espresso pareri informali con riguardo all'apertura delle trattative per la stipulazione di accordi con Stati ed organismi terzi ed Europol per lo scambio di dati ed informazioni e successivamente, per alcuni Stati, in relazione all'apertura dei negoziati.

L'Autorità ha inoltre affrontato temi legati a modi e forme con cui assicurare visibilità alla sua attività e agli atti adottati ed ha iniziato al riguardo una riflessione sui tipi di documenti per i quali può essere consentito l'accesso al pubblico.

Quanto al primo aspetto si sta lavorando per predisporre un documento di presentazione dell'Autorità e dei suoi compiti che sarà collocato nel formato elettronico nel sito di Europol ed in un opuscolo da distribuire.

Nel corso del 2001 è prevista la redazione della prima relazione di attività che, per l'Italia, sarà allegata, come quella dell'ACC Schengen, alla relazione annuale del Garante.

Al comitato ricorsi è stato sottoposto un primo caso, attualmente all'esame preliminare per valutarne l'ammissibilità.

IL CONTROLLO SUL SISTEMA INFORMATIVO DOGANALE

91. LA CREAZIONE DELL'AUTORITÀ DI CONTROLLO

L'Autorità di controllo non ha iniziato formalmente la propria attività poiché mancano ancora le designazioni di alcuni Stati membri, e la sua composizione non è al momento sufficiente per consentirne l'operatività.

Anche questa Autorità comunque potrà avvalersi del menzionato segretariato comune.

EURODAC

92. COLLABORAZIONE TRA STATI MEMBRI E GARANZIE PER GLI INTERESSATI

A seguito dell'entrata in vigore del regolamento istitutivo del Garante europeo, i compiti di supervisione e controllo sui trattamenti effettuati ai sensi del regolamento Eurodac saranno sottoposte a questa figura di garanzia.

CONSIGLIO D'EUROPA

93. LA CONVENZIONE SUL *CYBERCRIME*

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. Dopo l'adozione di una serie di provvedimenti settoriali, nel 1981 si è giunti come è noto 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 rappresenta il fondamento sul quale sono state costruite le successive regolamentazioni in ambito comunitario e nazionale.

L'attività del Consiglio d'Europa in materia non si è esaurita con l'approvazione della Convenzione, essendosi sviluppata in un'intensa attività di elaborazione della normativa di settore cristallizzata nelle note Raccomandazioni, nonché proseguendo con l'aggiornamento di quella preesistente.

Il Garante, sin dalla sua costituzione, ha continuato a prendere parte alle diverse attività del Consiglio d'Europa, contribuendo significativamente all'elaborazione dei diversi testi in discussione.

In particolare è continuato l'esame e l'approfondimento dello studio sulla Convenzione concernente il *cybercrime* per la lotta alla "criminalità informatica", vale a dire delle attività criminali realizzate attraverso l'impiego di strumenti telematici. La Convenzione mira a favorire la cooperazione internazionale nella lotta alla criminalità informatica attraverso l'armonizzazione delle procedure e il potenziamento dell'assistenza giudiziaria in questi settori. L'Assemblea Parlamentare del Consiglio d'Europa e ha espresso il 24 aprile 2001 un avviso che condivide le preoccupazioni dei Garanti europei.

Il testo predisposto ha destato infatti preoccupazioni nel Gruppo dell'articolo 29, che ha voluto esplicitare, nel parere 4/2001, i rischi che esso comporta sotto il profilo della protezione dei diritti umani fondamentali e della vita privata in particolare. Ulteriori note sono state poi inviate dal presidente del Gruppo.

Un punto esplicitamente e specificamente trattato, oramai divenuto un tema centrale su cui anche recentemente le autorità garanti europee si sono espresse negativamente con fermezza nelle Conferenze di Stoccolma ed Atene, concerne la conservazione più o meno generalizzata dei dati di traffico.

94. L'ATTIVITÀ DEI GRUPPI DI ESPERTI

È stato adottato dal gruppo CJ-PD che si occupa dell'elaborazione dei progetti di raccomandazione in materia di dati personali, il documento finale relativo al progetto di Raccomandazione che concerne la tutela dei dati personali raccolti e trattati a fini assicurativi, trasmesso per competenza, al Consiglio dei Ministri.

Altre iniziative hanno riguardato:

a) il parere del gruppo J-PD sul progetto di raccomandazione DH-S-AC per l'accesso ai documenti ufficiali;

b) la riorganizzazione degli organismi che hanno competenza in materia di protezione dati e le nuove metodologie di lavoro;

c) la celebrazione del ventesimo anniversario della Convenzione, anche in occasione della conferenza multilaterale di Varsavia sulla protezione dei dati promossa dal Consiglio d'Europa e dall'Autorità garante polacca il 19/20 novembre 2001;

È stato inoltre costituito un qualificato gruppo di lavoro, di cui fa parte anche il segretario generale del Garante, per approfondire, anche alla luce dei risultati del "Progetto Falcone", gli aspetti relativi all'applicazione dei principi di protezione dei dati all'attività di polizia (e giudiziaria) e per una valutazione della Raccomandazione 87/15 del Consiglio d'Europa.

95. LINEE-GUIDA IN MATERIA DI SORVEGLIANZA

In particolare, per le attività di videosorveglianza che presentano specifiche problematiche per la protezione dati, il Consiglio d'Europa ha conferito uno specifico incarico al segretario generale del Garante, per predisporre un dettagliato rapporto finalizzato alla ricerca di un corretto bilanciamento tra le esigenze di sicurezza e di controllo anticrimine e il diritto dei cittadini a difendere la loro sfera privata e la loro libertà.

Come è noto, il radicarsi di un fenomeno di espansione incontrollata del numero di impianti di videosorveglianza in luoghi pubblici e privati solleva non poche preoccupazioni nella società di oggi, attesa la loro invasività, specie in mancanza di una tutela diretta, salvo quella rappresentata, a livello embrionale, da una legge generale come la legge italiana n. 675/1996.

Il rapporto predisposto e pubblicato è volto, in particolare, alla protezione dei dati personali in relazione ai sistemi di videosorveglianza che ricadono, in senso lato, nell'ambito applicativo della Convenzione n. 108/1981 della Convenzione sulla tutela dei diritti dell'uomo e delle libertà fondamen-

tali, nonché di alcune Raccomandazioni del Consiglio d'Europa (in particolare, la N.R. (87) 15 in materia di trattamenti nell'ambito della pubblica sicurezza; la N.R. (89) 2 sulla protezione dei dati personali nel rapporto di lavoro e la N.R. (95) relativa alla protezione dei dati personali nel settore dei servizi di telecomunicazione, adottate in settori che pur non riferendosi espressamente alla tematica della videosorveglianza recano disposizioni e garanzie rilevanti sotto tale profilo).

In tale documento, presentato sotto forma di decalogo, sono state anche tracciate le prime linee-guida finalizzate alla piena garanzia e tutela del privato.

Le regole di base ivi enucleate si riportano di seguito sinteticamente:

– verificare che l'attività di sorveglianza si esplichi su base legale per fini leciti, espliciti e legittimi;

– adottare tutte le misure volte ad assicurare che l'attività sia conforme alla normativa in materia di protezione dei dati personali;

– ricorrere alla videosorveglianza solo quando non sia possibile utilizzare sistemi meno invasivi ed intrusivi della *privacy*;

– rispettare il principio di selettività e di proporzionalità in rapporto agli scopi perseguiti nei singoli casi, in modo da prevenire conseguenze irragionevoli sulle libertà e sui comportamenti degli interessati;

– rispettare il principio di pertinenza e di non eccedenza rispetto a immagini, suoni e dati biometrici raccolti, con particolare attenzione alle modalità di raccolta onde evitare che le informazioni raccolte siano registrate, indicizzate o conservate per lunghi periodi;

– evitare che l'attività di videosorveglianza possa determinare discriminazioni o possa essere disposta nei confronti di soggetti per il solo fatto di avere determinate opinioni, convinzioni o comportamenti di tipo sessuale;

– svolgere l'attività nel rispetto del principio di trasparenza e di pubblicità;

– assicurare maggiori garanzie in presenza di particolari rischi per gli interessati e di controllo;

– escludere, in linea di principio, la diffusione e la comunicazione dei dati personali a soggetti non interessati all'attività di sorveglianza;

– regolamentare il diritto di accesso, nonché gli altri diritti delle persone interessate;

– assicurare un'adeguata informativa ai lavoratori interessati e una possibile intesa con le organizzazioni sindacali per esigenze organizzative e/o produttive o per ragioni di sicurezza del lavoro che possano comportare un controllo a distanza.

Il rapporto e le linee-guida, dopo l'esame da parte del Gruppo, sono stati pubblicati, per un'ampia consultazione, sul sito web del Consiglio d'Europa. Quest'ultimo, dopo il parere favorevole del Gruppo di cui all'articolo 29 e un nuovo positivo esame da parte del CJ-PD-GC si accinge ad adottarlo formalmente.

O.C.S.E.

96. I RISULTATI CONSEGUITI NEL 2000

Il Garante, nel processo avviato dall'Organizzazione per la cooperazione e lo sviluppo economico, incentrato sui principi affermati nelle linee-guida sulla tutela della *privacy* per favorire la libera circolazione delle informazioni tra gli Stati membri, ha svolto, nel corso del 2000, un'intensa attività attraverso il Comitato ICCP (Comitato per la politica dell'informazione istituito all'interno della Direzione scienza, tecnologia e industria OCSE).

Tale attività è stata principalmente finalizzata a risolvere i problemi legati al commercio elettronico, alla sicurezza dell'informazione, alla protezione della *privacy* e all'infrastruttura della società dell'informazione.

Particolare valenza ha avuto la partecipazione del Garante alla riunione del sottogruppo WISP del Comitato ICCP, che espleta attività per la sicurezza dell'informazione e sulla *privacy*.

Nel corso della riunione indetta il 4- 5 maggio 2000 a Parigi sono state affrontate ed approfondite le principali tematiche relative:

– allo studio per la realizzazione e predisposizione a livello internazionale della Convenzione sui crimini informatici e, in ambito nazionale, la predisposizione di una specifica legge per combattere il c.d. *cybersquatting*;

– alla previsione dei criteri da utilizzare per la revisione delle linee guida sulla cifratura adottata dall'OCSE nel 1988;

– all'utilizzo del *software "generator"*, costituito da una serie di maschere da riempire con dati sensibili che vengono richiesti all'utente e che nel futuro formeranno oggetto di una raccolta di dati utilizzabile da organizzazioni che operano nel campo dell'*e-commerce*;

– alla predisposizione di un documento riguardante l'adozione di soluzioni contrattuali volte a consentire flussi transnazionali di dati TBDF (*Transborder data flow*) nel rispetto dei principi in tema di *privacy*.

Il gruppo si è adoperato, inoltre, per offrire strumenti metodologici e tecnici in relazione alle azioni da intraprendere ed indicando i tempi da rispettare per il raggiungimento dei suddetti importanti obiettivi.

ULTERIORI INIZIATIVE

97. IL "PROGRAMMA FALCONE" E LE ALTRE ATTIVITÀ

Il programma è stato avviato con il contributo finanziario delle istituzioni comunitarie per sostenere l'azione degli Stati membri volta ad intensificare la cooperazione in materia di giustizia ed affari interni.

Il Garante ha presentato nei primi mesi del 1999 una domanda per il cofinanziamento, nell'ambito del "Programma Falcone", di un progetto denominato "Attività di contrasto del crimine e tutela dei dati personali".

Per lo svolgimento dei seminari sono stati scelti due luoghi simbolicamente importanti: la sede di Europol a L'Aja per il primo (27 e 28 marzo 2000) e la Scuola nazionale della magistratura a Parigi per il secondo (6 e 7 luglio 2000).

Il progetto prevedeva una giornata conclusiva per presentare il lavoro svolto e formulare eventuali osservazioni e proposte, che si è svolta a Roma il 20 dicembre 2000; all'incontro, ospitato dalla Camera dei deputati, vi è stata un'ampia partecipazione e numerosi relatori.

Il progetto è stato indirizzato a magistrati, appartenenti alle forze di polizia e funzionari pubblici che nei Paesi membri dell'Unione svolgono prevalentemente la propria attività nel settore della prevenzione e contrasto della criminalità organizzata.

Al fine di individuare i soggetti dotati della competenza specifica per poter partecipare ai seminari dell'Aja e di Parigi, si è chiesta la collaborazione delle altre Autorità garanti in materia di protezione dei dati, nonché quella dei Ministeri della giustizia e dell'interno dei Paesi destinatari dell'azione. La finalità del progetto era quella di verificare gli aspetti dell'azione di polizia e giudiziaria legati alla raccolta, al trattamento, all'analisi dei dati, considerato l'intenso sviluppo di forme di collaborazione nelle attività di polizia e, più recentemente, giudiziarie in relazione al perseguimento dei compiti di prevenzione e repressione della criminalità, che determina un uso sempre maggiore di strumenti informativi e, talora, la creazione di veri e propri "sistemi". Attraverso lo stimolo della partecipazione attiva nei seminari si voleva ottenere un approccio "multidisciplinare", nel senso di confrontare le specifiche esperienze professionali con la normativa di tutela dei dati personali anche in linea con quanto suggerito dalla ricordata azione comune. In essa si fa infatti riferimento alla possibilità di definire norme e metodologie comuni al fine di facilitare l'individuazione del fenomeno e la raccolta dei dati da ottenere, però, tenendo conto della legislazione degli Stati membri in materia di protezione dei dati.

Gli approfondimenti condotti nei seminari e le risposte fornite ai questionari hanno evidenziato come su alcune questioni importanti i cittadini dei Paesi dell'Unione ricevono, nei rispettivi ordinamenti nazionali, trattamenti diversificati sotto il profilo dei diritti. In alcuni casi attività svolte dagli uffici di polizia non sono puntualmente o affatto disciplinate.

Ad esempio, per quanto riguarda la videosorveglianza non è risultato che vi sia una base giuridica uniforme: in alcuni Paesi si applicano i principi generali in materia di protezione dei dati personali, ma esistono poche norme specifiche che disciplinano i termini della conservazione delle immagini e registrazioni effettuate. Le osservazioni scaturite dal dibattito e la recente esperienza del Consiglio d'Europa sul tema costituiscono senza dubbio utili indicatori ai fini di un eventuale intervento armonizzatore.

Analogamente il problema si pone per i tempi e le modalità di conservazione dei dati relativi al traffico telefonico, per le modalità di accesso delle forze di polizia e dell'autorità giudiziaria agli elenchi degli abbonati di servizi telefonici, inclusi quelli di telefonia mobile. Per quanto concerne poi le carte telefoniche ricaricabili, varie soluzioni volte a consentire l'individuazione degli acquirenti sono basate solo sulla prassi e non su norme specifiche. L'esigenza di armonizzazione che sembra porsi anche in questo campo potrà forse essere considerata in occasione della discussione delle proposte di direttiva presentate recentemente dalla Commissione al Consiglio telecomunicazioni.

Anche riguardo alle modalità di raccolta e di trattamento dei dati genetici, l'utilizzo degli stessi, i tempi di conservazione ed i diritti delle persone cui si riferiscono mancano disposizioni adeguate nei sistemi processuali e certamente gli argomenti richiederanno un'ulteriore riflessione ed armonizzazione.

L'esperienza del Progetto ha mostrato come vi sia la crescente tendenza a prevedere obblighi, in via legislativa od anche amministrativa, di raccolta e conservazione di consistenti masse di informazioni. Rispettando la necessità di disporre, per l'azione di contrasto della criminalità, di un ampio materiale investigativo, manca un'armonizzazione o un indirizzo comune. Dall'analisi delle risposte ai questionari emerge senz'altro un problema rispetto alla rilevazione delle presenze alberghiere. L'Accordo di Schengen obbliga ad identificare i cittadini stranieri e comunitari, ma nei diritti nazionali variano le modalità di rilevazione (che in taluni casi riguardano i soli stranieri, in altri tutti i clienti, anche se cittadini del medesimo Paese). Sono diversi gli strumenti di rilevazione, in alcuni casi cartacei, in altri accessibili *on-line* per le forze di polizia e gli inquirenti. Variano ancora le modalità ed i tempi di conservazione, né sono noti i sistemi seguiti per la classificazione di queste informazioni (*files disgiunti* o creazione di un'unica banca dati).

La questione è però molto più ampia; andrà riproposto nel prossimo futuro il tema dell'imposizione a terzi, siano essi un *provider* per l'accesso ad Internet o singoli cittadini, dell'obbligo di consentire la raccolta o la conservazione di masse di informazioni.

Per quanto concerne le attività di competenza della magistratura penale, che recentemente ha iniziato a disporre di forme di supporto e cooperazione a livello europeo, si sono riscontrate maggiori difficoltà nell'accettazione delle disposizioni in materia di protezione dei dati, ritenendo alcuni che debba tenersi in maggior conto la speciale collocazione dell'ordine giudiziario nella disciplina dell'ambito di competenza delle autorità amministrative ed indipendenti di controllo.

Per il Garante, l'esperienza è stata di grande interesse ed utilità, sia per approfondire alcuni temi di rilevante attualità nel nostro Paese, sia per valutare la possibilità di operare suggerimenti per proseguire l'opera di individuazione e di definizione di norme specifiche per la tutela dei diritti nell'ambito delle attività di polizia e giustizia.

DOCUMENTAZIONE

TESTI

DISPOSIZIONI NORMATIVE

98

LEGGE N. 675 DEL 31 DICEMBRE 1996 - TUTELA DEL PERSONE E DI ALTRI SOGGETTI RISPETTO AL TRATTAMENTO DEI DATI PERSONALI (*)

Capo I – Principi generali

Art. 1. Finalità e definizioni

1. 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; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione.

2. Ai fini della presente legge si intende:

a) per "banca di dati", qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento;

b) per "trattamento", qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati;

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

d) per "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;

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

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

g) per "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

h) per "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) per "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

(*) Testo aggiornato in base ai seguenti decreti legislativi: n. 282 del 30 luglio 1999 - n. 281 del 30 luglio 1999 - n. 135 dell'11 maggio 1999 - n. 51 del 26 febbraio 1999 - n. 389 del 6 novembre 1998 - n. 171 del 13 maggio 1998 - n. 135 dell'8 maggio 1998 - n. 255 del 28 maggio 1997 - n. 123 del 9 maggio 1997.

l) per "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

m) per "Garante", l'autorità istituita ai sensi dell'articolo 30.

Art. 2. Ambito di applicazione

1. La presente legge si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato.

Art. 3. Trattamento di dati per fini esclusivamente personali

1. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali non è soggetto all'applicazione della presente legge, sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione.

2. Al trattamento di cui al comma 1 si applicano in ogni caso le disposizioni in tema di sicurezza dei dati di cui all'articolo 15, nonché le disposizioni di cui agli articoli 18 e 36.

Art. 4. Particolari trattamenti in ambito pubblico

1. La presente legge non si applica al trattamento di dati personali effettuato:

a) dal Centro elaborazione dati di cui all'articolo 8 della legge 1° aprile 1981, n. 121, come modificato dall'articolo 43, comma 1, della presente legge, ovvero sui dati destinati a confluirvi in base alla legge, nonché in virtù dell'accordo di adesione alla Convenzione di applicazione dell'Accordo di Schengen, reso esecutivo con legge 30 settembre 1993, n. 388;

b) dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge;

c) nell'ambito del servizio del casellario giudiziale di cui al titolo IV del libro decimo del codice di procedura penale e al regio decreto 18 giugno 1931, n. 778, e successive modificazioni, o, in base alla legge, nell'ambito del servizio dei carichi pendenti nella materia penale;

d) in attuazione dell'articolo 371-*bis*, comma 3, del codice di procedura penale o, per ragioni di giustizia, nell'ambito di uffici giudiziari, del Consiglio superiore della magistratura e del Ministero di grazia e giustizia;

e) da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento.

2. Ai trattamenti di cui al comma 1 si applicano in ogni caso le disposizioni di cui agli articoli 9, 15, 17, 18, 31, 32, commi 6 e 7 e 36, nonché, fatta eccezione per i trattamenti di cui alla lettera b) del comma 1, le disposizioni di cui agli articoli 7 e 34.

Art. 5. Trattamento di dati svolto senza l'ausilio di mezzi elettronici

1. Il trattamento di dati personali svolto senza l'ausilio di mezzi elettronici o comunque automatizzati è soggetto alla medesima disciplina prevista per il trattamento effettuato con l'ausilio di tali mezzi.

Art. 6. Trattamento di dati detenuti all'estero

1. Il trattamento nel territorio dello Stato di dati personali detenuti all'estero è soggetto alle disposizioni della presente legge.

2. Se il trattamento di cui al comma 1 consiste in un trasferimento di dati personali fuori dal territorio nazionale si applicano in ogni caso le disposizioni dell'articolo 28.

Capo II - Obblighi per il titolare del trattamento

Art. 7. Notificazione

1. Il titolare che intenda procedere ad un trattamento di dati personali soggetto al campo di applicazione della presente legge è tenuto a darne notificazione al Garante.

2. La notificazione è effettuata preventivamente ed una sola volta, a mezzo di lettera raccomandata ovvero con altro mezzo idoneo a certificarne la ricezione, a prescindere dal numero delle operazioni da svolgere, nonché dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta solo se muta taluno degli elementi indicati nel comma 4 e deve precedere l'effettuazione della variazione.

3. La notificazione è sottoscritta dal notificante e dal responsabile del trattamento.

4. La notificazione contiene:

a) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare;

b) le finalità e modalità del trattamento;

c) la natura dei dati, il luogo ove sono custoditi e le categorie di interessati cui i dati si riferiscono;

d) l'ambito di comunicazione e di diffusione dei dati;

e) i trasferimenti di dati previsti verso Paesi non appartenenti all'Unione europea o, qualora riguardino taluno dei dati di cui agli articoli 22 e 24, fuori del territorio nazionale;

f) una descrizione generale che permetta di valutare l'adeguatezza delle misure tecniche ed organizzative adottate per la sicurezza dei dati;

g) l'indicazione della banca di dati o delle banche di dati cui si riferisce il trattamento, nonché l'eventuale connessione con altri trattamenti o banche di dati, anche fuori del territorio nazionale;

h) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del responsabile; in mancanza di tale indicazione si considera responsabile il notificante;

i) la qualità e la legittimazione del notificante.

5. I soggetti tenuti ad iscriversi o che devono essere annotati nel registro delle imprese di cui all'articolo 2188 del codice civile, nonché coloro che devono fornire le informazioni di cui all'articolo 8, comma 8, lettera d), della legge 29 dicembre 1993, n. 580, alle camere di commercio, industria, artigianato e agricoltura, possono effettuare la notificazione per il tramite di queste ultime, secondo le modalità stabilite con il regolamento di cui all'articolo 33, comma 3. I piccoli imprenditori e gli artigiani possono effettuare la notificazione anche per il tramite delle rispettive rappresentanze di categoria; gli iscritti agli albi professionali anche per il tramite dei rispettivi ordini professionali. Resta in ogni caso ferma la disposizione di cui al comma 3.

5-*bis*. *(Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255)* La notificazione in forma semplificata può non contenere taluno degli elementi di cui al comma 4, lettere b), c), e) e g), individuati dal Garante ai sensi del regolamento di cui all'articolo 33, comma 3, quando il trattamento è effettuato:

a) da soggetti pubblici, esclusi gli enti pubblici economici, sulla base di espressa disposizione di legge ai sensi degli articoli 22, comma 3 e 24, ovvero del provvedimento di cui al medesimo articolo 24;

b) nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità, ovvero dai soggetti indicati nel comma 4-*bis* dell'articolo 25, nel rispetto del codice di deontologia di cui al medesimo articolo;

c) temporaneamente senza l'ausilio di mezzi elettronici o comunque automatizzati, ai soli fini e con le modalità strettamente collegate all'organizzazione interna dell'attività esercitata dal titolare, relativamente a dati non registrati in una banca di dati e diversi da quelli di cui agli articoli 22 e 24;

c-*bis*) *(Lettera inserita dall'art. 2, comma 1, lett. a), d.lg. 30 luglio 1999, n. 281)* per scopi storici, di ricerca scientifica e di statistica in conformità alle leggi, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

5-*ter*. *(Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255)* Fuori dei casi di cui all'articolo 4, il trattamento non è soggetto a notificazione quando:

a) è necessario per l'assolvimento di un compito previsto dalla legge, da un regolamento o dalla normativa comunitaria, relativamente a dati diversi da quelli indicati negli articoli 22 e 24;

b) riguarda dati contenuti o provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità di cui all'articolo 20, comma 1, lettera b);

c) è effettuato per esclusive finalità di gestione del protocollo, relativamente ai dati necessari per la classificazione della corrispondenza inviata per fini diversi da quelli di cui all'articolo 13, comma 1, lettera e), con particolare riferimento alle generalità e ai recapiti degli interessati, alla loro qualifica e all'organizzazione di appartenenza;

d) riguarda rubriche telefoniche o analoghe non destinate alla diffusione, utilizzate unicamente per ragioni d'ufficio e di lavoro e comunque per fini diversi da quelli di cui all'articolo 13, comma 1, lettera e);

e) è finalizzato unicamente all'adempimento di specifici obblighi contabili, retributivi, previdenziali, assistenziali e fiscali, ed è effettuato con riferimento alle sole categorie di dati, di interessati e di destinatari della comunicazione e diffusione strettamente collegate a tale adempimento, conservando i dati non oltre il periodo necessario all'adempimento medesimo;

f) è effettuato, salvo quanto previsto dal comma 5-*bis*, lettera b), da liberi professionisti iscritti in albi o elenchi professionali, per le sole finalità strettamente collegate all'adempimento di specifiche prestazioni e fermo restando il segreto professionale;

g) è effettuato dai piccoli imprenditori di cui all'articolo 2083 del codice civile per le sole finalità strettamente collegate allo svolgimento dell'attività professionale esercitata, e limitatamente alle categorie di dati, di interessati, di destinatari della comunicazione e diffusione e al periodo di conservazione dei dati necessari per il perseguimento delle finalità medesime;

h) è finalizzato alla tenuta di albi o elenchi professionali in conformità alle leggi e ai regolamenti;

i) è effettuato per esclusive finalità dell'ordinaria gestione di biblioteche, musei e mostre, in conformità alle leggi e ai regolamenti, ovvero per la organizzazione di iniziative culturali o sportive o per la formazione di cataloghi e bibliografie;

l) è effettuato da associazioni, fondazioni, comitati anche a carattere politico, filosofico, religioso o sindacale, ovvero da loro organismi rappresentativi, istituiti per scopi non di lucro e per il perseguimento di finalità lecite, relativamente a dati inerenti agli associati e ai soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, la fondazione, il comitato o l'organismo, fermi restando gli obblighi di informativa degli interessati e di acquisizione del consenso, ove necessario;

m) è effettuato dalle organizzazioni di volontariato di cui alla legge 11 agosto 1991, n. 266, nei limiti di cui alla lettera l) e nel rispetto delle autorizzazioni e delle prescrizioni di legge di cui agli articoli 22 e 23;

n) è effettuato temporaneamente ed è finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero, nel rispetto del codice di deontologia di cui all'articolo 25;

o) è effettuato, anche con mezzi elettronici o comunque automatizzati, per la redazione di periodici o pubblicazioni aventi finalità di informazione giuridica, relativamente a dati desunti da provvedimenti dell'autorità giudiziaria o di altre autorità;

p) è effettuato temporaneamente per esclusive finalità di raccolta di adesioni a proposte di legge d'iniziativa popolare, a richieste di referendum, a petizioni o ad appelli;

q) è finalizzato unicamente all'amministrazione dei condomini di cui all'articolo 1117 e seguenti del codice civile, limitatamente alle categorie di dati, di interessati e di destinatari della comunicazione necessarie per l'amministrazione dei beni comuni, conservando i dati non oltre il periodo necessario per la tutela dei corrispondenti diritti;

q-*bis*) *(Lettera inserita dall'art. 2, comma 1, lett. b), d.lg. 30 luglio 1999, n. 281)* è compreso nel programma statistico nazionale o in atti di programmazione statistica previsti dalla legge ed è effettuato in conformità alle leggi, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

5-*quater*. *(Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255.)* Il titolare si può avvalere della notificazione semplificata o dell'esonero di cui ai commi 5-*bis* e 5-*ter*, sempre che il trattamento riguardi unicamente le finalità, le categorie di dati, di interessati e di destinatari della comunicazione e diffusione, individuate, unitamente al periodo di conservazione dei dati, dai medesimi commi 5-*bis* e 5-*ter*, nonché:

a) nei casi di cui ai commi 5-*bis*, lettera a) e 5-*ter*, lettere a) e m), dalle disposizioni di legge o di regolamento o dalla normativa comunitaria ivi indicate;

b) nel caso di cui al comma 5-*bis*, lettera b), dal codice di deontologia ivi indicato;

c) nei casi residui, dal Garante con le autorizzazioni rilasciate con le modalità previste dall'articolo 41, comma 7, ovvero, per i dati diversi da quelli di cui agli articoli 22 e 24, con provvedimenti analoghi.

5-quinquies. *(Comma aggiunto dall'art. 1, comma 1, d.lg. 28 luglio 1997, n. 255)* Il titolare che si avvale dell'esonero di cui al comma 5-*ter* deve fornire gli elementi di cui al comma 4 a chiunque ne faccia richiesta.

Art. 8. Responsabile

1. Il responsabile, se designato, deve essere nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

2. Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.

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

4. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto.

5. Gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile.

Capo III - Trattamento dei dati personali

Sezione I - Raccolta e requisiti dei dati

Art. 9. Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento devono essere:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

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

1-*bis*. *(Comma aggiunto dall'art. 3, d.lg. 30 luglio 1999, n. 281)* Il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti o successivamente trattati e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi.

Art. 10. Informazioni rese al momento della raccolta

1. *(Comma così modificato dall'art. 1, d.lg. 9 maggio 1997, n. 123)* L'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

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

e) i diritti di cui all'articolo 13;

f) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile.

2. L'informativa di cui al comma 1 può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare l'espletamento di funzioni pubbliche ispettive o di controllo, svolte per il perseguimento delle finalità di cui agli articoli 4, comma 1, lettera e), e 14, comma 1, lettera d).

3. Quando i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1 è data al medesimo interessato all'atto della registrazione dei dati o, qualora sia prevista la loro comunicazione, non oltre la prima comunicazione.

4. La disposizione di cui al comma 3 non si applica quando l'informativa all'interessato comporta un impiego di mezzi che il Garante dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si rivela, a giudizio del Garante, impossibile, ovvero nel caso in cui i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. La medesima disposizione non si applica, altresì, quando i dati sono trattati 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, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

Sezione II - Diritti dell'interessato nel trattamento dei dati

Art. 11. Consenso

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

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

3. Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 10.

Art. 12. Casi di esclusione del consenso

1. Il consenso non è richiesto quando il trattamento:

a) riguarda dati raccolti e detenuti in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'acquisizione di informative precontrattuali attivate su richiesta di quest'ultimo, ovvero per l'adempimento di un obbligo legale;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

d) *(Lettera così sostituita dall'art. 4, comma 1, d.lg. 30 luglio 1999, n. 281)* è finalizzato unicamente a scopi di ricerca scientifica o di statistica ed è effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31;

e) *(Lettera così modificata dall'art. 12, comma 1, d.lg. 13 maggio 1998, n. 171)* è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. In tale caso, si applica il codice di deontologia di cui all'articolo 25;

f) riguarda dati relativi allo svolgimento di attività economiche raccolti anche ai fini indicati nell'articolo 13, comma 1, lettera e), nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) è necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere;

h) è necessario 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, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

Art. 13. Diritti dell'interessato

1. In relazione al trattamento di dati personali l'interessato ha diritto:

a) di conoscere, mediante accesso gratuito al registro di cui all'articolo 31, comma 1, lettera a), l'esistenza di trattamenti di dati che possono riguardarlo;

b) di essere informato su quanto indicato all'articolo 7, comma 4, lettere a), b) e h);

c) di ottenere, a cura del titolare o del responsabile, senza ritardo:

1) la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni;

2) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

3) l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;

4) l'attestazione che le operazioni di cui ai numeri 2) e 3) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

d) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

e) di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano, 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 e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto.

2. Per ciascuna richiesta di cui al comma 1, lettera c), numero 1), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati, secondo le modalità ed entro i limiti stabiliti dal regolamento di cui all'articolo 33, comma 3.

3. I diritti di cui al comma 1 riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia interesse.

4. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

5. Restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

Art. 14. Limiti all'esercizio dei diritti

1. I diritti di cui all'articolo 13, comma 1, lettere c) e d), non possono essere esercitati nei confronti dei trattamenti di dati personali raccolti:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni;

b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti la politica monetaria e valutaria, il sistema dei pagamenti, il controllo degli intermediari e dei mercati creditizi e finanziari nonché la tutela della loro stabilità;

e) ai sensi dell'articolo 12, comma 1, lettera h), limitatamente al periodo durante il quale potrebbe derivarne pregiudizio per lo svolgimento delle investigazioni o per l'esercizio del diritto di cui alla medesima lettera h).

2. Nei casi di cui al comma 1 il Garante, anche su segnalazione dell'interessato ai sensi dell'articolo 31, comma 1, lettera d), esegue i necessari accertamenti nei modi di cui all'articolo 32, commi 6 e 7, e indica le necessarie modificazioni ed integrazioni, verificandone l'attuazione.

Sezione III - Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento del danno

Art. 15. Sicurezza dei dati

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

2. Le misure minime di sicurezza da adottare in via preventiva sono individuate con regolamento emanato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400, entro centottanta giorni dalla data di entrata in vigore della presente legge, su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante.

3. Le misure di sicurezza di cui al comma 2 sono adeguate, entro due anni dalla data di entrata in vigore della presente legge e successivamente con cadenza almeno biennale, con successivi regolamenti emanati con le modalità di cui al medesimo comma 2, in relazione all'evoluzione tecnica del settore e all'esperienza maturata.

4. Le misure di sicurezza relative ai dati trattati dagli organismi di cui all'articolo 4, comma 1, lettera b), sono stabilite con decreto del Presidente del Consiglio dei ministri con l'osservanza delle norme che regolano la materia.

Art. 16. Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, del trattamento dei dati, il titolare deve notificare preventivamente al Garante la loro destinazione.

2. I dati possono essere:

a) distrutti;

b) ceduti ad altro titolare, purché destinati ad un trattamento per finalità analoghe agli scopi per i quali i dati sono raccolti;

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

c-*bis*) *(Lettera inserita dall'art. 5, d.lg. 30 luglio 1999, n. 281)* conservati o ceduti ad altro titolare, per scopi storici, di ricerca scientifica e di statistica, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

3. La cessione dei dati in violazione di quanto previsto dalla lettera b) del comma 2 o di altre disposizioni di legge in materia di trattamento dei dati personali è nulla ed è punita ai sensi dell'articolo 39, comma 1.

Art. 17. Limiti all'utilizzabilità di dati personali

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

2. L'interessato può opporsi ad ogni altro tipo di decisione adottata sulla base del trattamento di cui al comma 1 del presente articolo, ai sensi dell'articolo 13, comma 1, lettera d), salvo che la decisione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dalla legge.

Art. 18. Danni cagionati per effetto del trattamento di dati personali

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

Sezione IV - Comunicazione e diffusione dei dati

Art. 19. Incaricati del trattamento

1. Non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità.

Art. 20. Requisiti per la comunicazione e la diffusione dei dati

1. La comunicazione e la diffusione dei dati personali da parte di privati e di enti pubblici economici sono ammesse:

a) con il consenso espresso dell'interessato;

b) se i dati provengono da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi e i regolamenti stabiliscono per la loro conoscibilità e pubblicità;

c) in adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

d) *(Lettera così modificata dall'art. 12, comma 2, d.lg. 13 maggio 1998, n. 171)* nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. Restano fermi i limiti del diritto di cronaca posti a tutela della riservatezza ed in particolare dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Si applica inoltre il codice di deontologia di cui all'articolo 25;

e) se i dati sono relativi allo svolgimento di attività economiche, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) qualora siano necessarie per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere;

g) limitatamente alla comunicazione, qualora questa sia necessaria 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, o, comunque, per far valere o difendere un diritto in sede giudiziaria, nel rispetto della normativa di cui alla lettera e) del presente comma, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

h) limitatamente alla comunicazione, quando questa sia effettuata nell'ambito dei gruppi bancari di cui all'articolo 60 del testo unico delle leggi in materia bancaria e creditizia approvato con decreto legislativo 1° settembre 1993, n. 385, nonché tra società controllate e società collegate ai sensi dell'articolo 2359 del codice civile, i cui trattamenti con finalità correlate sono stati notificati ai sensi dell'articolo 7, comma 2, per il perseguimento delle medesime finalità per le quali i dati sono stati raccolti.

2. Alla comunicazione e alla diffusione dei dati personali da parte di soggetti pubblici, esclusi gli enti pubblici economici, si applicano le disposizioni dell'articolo 27.

Art. 21. Divieto di comunicazione e diffusione

1. Sono vietate la comunicazione e la diffusione di dati personali per finalità diverse da quelle indicate nella notificazione di cui all'articolo 7.

2. Sono altresì vietate la comunicazione e la diffusione di dati personali dei quali sia stata ordinata la cancellazione, ovvero quando sia decorso il periodo di tempo indicato nell'articolo 9, comma 1, lettera e).

3. Il Garante può vietare la diffusione di taluno dei dati relativi a singoli soggetti, od a categorie di soggetti, quando la diffusione si pone in contrasto con rilevanti interessi della collettività. Contro il divieto può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

4. La comunicazione e la diffusione dei dati sono comunque permesse:

a) *(Lettera così sostituita dall'art. 4, comma 2, d.lg. 30 luglio 1999, n. 281)* qualora siano necessarie per finalità di ricerca scientifica o di statistica e siano effettuate nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31;

b) quando siano richieste dai soggetti di cui all'articolo 4, comma 1, lettere b), d) ed e), per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia.

Capo IV - Trattamento di dati particolari

Art. 22. Dati sensibili

(Per quanto concerne il presente articolo, si richiama l'attenzione sul disposto dell'Articolo 17 ("Tutela della salute") del d.lg. 11 maggio 1999, n. 135, recante "Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici").

1. 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, possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.

1-*bis*. *(Comma inserito dall'art. 5, comma 1, d.lg. 11 maggio 1999, n. 135)* Il comma 1 non si applica ai dati relativi agli aderenti alle confessioni religiose i cui rapporti con lo Stato siano regolati da accordi o intese ai sensi degli articoli 7 e 8 della Costituzione, nonché relativi ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, che siano trattati dai relativi organi o enti civilmente riconosciuti, sempre che i dati non siano comunicati o diffusi fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati.

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

3. *(Comma così sostituito dall'art. 5, comma 2, d.lg. 11 maggio 1999, n. 135.)* Il trattamento dei dati indicati al comma 1 da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito solo se autorizzato da 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. In mancanza di espressa disposizione di legge, e fuori dai casi previsti dai decreti legislativi di modificazione ed integrazione della presente legge, emanati in attuazione della legge 31 dicembre 1996, n. 676, i soggetti pubblici possono richiedere al Garante, nelle more della specificazione legislativa, l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono rilevanti finalità di interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi del comma 2, il trattamento dei dati indicati al comma 1.

3-*bis*. *(Comma inserito dall'art. 5, comma 3, d.lg. 11 maggio 1999, n. 135)* Nei casi in cui è specificata, a norma del comma 3, la finalità di rilevante interesse pubblico, ma non sono specificati i tipi di dati e le operazioni eseguibili, i soggetti pubblici, in applicazione di quanto previsto dalla presente legge e dai decreti legislativi di attuazione della legge 31 dicembre 1996, n. 676, in materia di dati sensibili, identificano e rendono pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando tale identificazione periodicamente.

4. I dati personali idonei a rivelare lo stato di salute e la vita sessuale possono essere oggetto di trattamento previa autorizzazione del Garante, qualora il trattamento sia necessario 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, o, comunque, per far valere o difendere in sede giudiziaria un diritto di rango pari a quello del-

l'interessato, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Il Garante prescrive le misure e gli accorgimenti di cui al comma 2 e promuove la sottoscrizione di un apposito codice di deontologia e di buona condotta secondo le modalità di cui all'articolo 31, comma 1, lettera h). Resta fermo quanto previsto dall'articolo 43, comma 2.

Art. 23. Dati inerenti alla salute

(Si richiama l'attenzione sul disposto dell'art. 17 ("Tutela della salute") del d.lg. 11 maggio 1999, n. 135, recante "Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici".)

1. Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici possono, anche senza l'autorizzazione del Garante, trattare i dati personali idonei a rivelare lo stato di salute, limitatamente ai dati e alle operazioni indispensabili per il perseguimento di finalità di tutela dell'incolumità fisica e della salute dell'interessato. Se le medesime finalità riguardano un terzo o la collettività, in mancanza del consenso dell'interessato, il trattamento può avvenire previa autorizzazione del Garante.

1-*bis*. *(Comma inseriti dall'art. 2, comma 1, d.lg. 30 luglio 1999, n. 282.)* Con decreto del Ministro della sanità adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentiti la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano e il Garante, sono individuate modalità semplificate per le informative di cui all'articolo 10 e per la prestazione del consenso nei confronti di organismi sanitari pubblici, di organismi sanitari e di esercenti le professioni sanitarie convenzionati o accreditati dal Servizio sanitario nazionale, nonché per il trattamento dei dati da parte dei medesimi soggetti, sulla base dei seguenti criteri:

a) previsione di informative effettuate da un unico soggetto, in particolare da parte del medico di medicina generale scelto dall'interessato, per conto di più titolari di trattamento;

b) validità, nei confronti di più titolari di trattamento, del consenso prestato ai sensi dell'articolo 11, comma 3, per conto di più titolari di trattamento, anche con riguardo alla richiesta di prestazioni specialistiche, alla prescrizione di farmaci, alla raccolta di dati da parte del medico di medicina generale detenuti da altri titolari, e alla pluralità di prestazioni mediche effettuate da un medesimo titolare di trattamento;

c) identificazione dei casi di urgenza nei quali, anche per effetto delle situazioni indicate nel comma 1-*ter*, l'informativa e il consenso possono intervenire successivamente alla richiesta della prestazione;

d) previsione di modalità di applicazione del comma 2 del presente articolo ai professionisti sanitari, diversi dai medici, che intrattengono rapporti diretti con i pazienti;

e) previsione di misure volte ad assicurare che nell'organizzazione dei servizi e delle prestazioni sia garantito il rispetto dei diritti di cui all'articolo 1.

1-*ter*. *(Comma inseriti dall'art. 2, comma 1, d.lg. 30 luglio 1999, n. 282)* Il decreto di cui al comma 1 disciplina anche quanto previsto dall'articolo 22, comma 3-*bis*, della legge.

1-*quater*. *(Comma inseriti dall'art. 2, comma 1, d.lg. 30 luglio 1999, n. 282)* In caso di incapacità di agire, ovvero di impossibilità fisica o di incapacità di intendere o di volere, il consenso al trattamento dei dati idonei a rivelare lo stato di salute è validamente manifestato nei confronti di esercenti le professioni sanitarie e di organismi sanitari, rispettivamente, da chi esercita legalmente la potestà ovvero da un familiare, da un prossimo congiunto, da un convivente, o, in loro assenza, dal responsabile della struttura presso cui dimori.

2. *(Comma così modificato dall'art. 2, comma 2, d.lg. 30 luglio 1999, n. 282)* I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui al comma 1-*ter* solo per il tramite di un medico designato dall'interessato o dal titolare.

3. L'autorizzazione di cui al comma 1 è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità. È vietata la comunicazione dei dati ottenuti oltre i limiti fissati con l'autorizzazione.

4. La diffusione dei dati idonei a rivelare lo stato di salute è vietata, salvo nel caso in cui sia necessaria per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.

Art. 24. Dati relativi ai provvedimenti di cui all'articolo 686 del codice di procedura penale

1. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'articolo 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, è ammesso soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni autorizzate.

Art. 25. Trattamento di dati particolari nell'esercizio della professione di giornalista

1. *(Comma così sostituito dall'art. 12, comma 3, d.lg. 13 maggio 1998, n. 171)* Le disposizioni relative al consenso dell'interessato e all'autorizzazione del Garante, nonché il limite previsto dall'articolo 24, non si applicano quando il trattamento dei dati di cui agli articoli 22 e 24 è effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità. Il giornalista rispetta i limiti del diritto di cronaca, in particolare quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, ferma restando la possibilità di trattare i dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti in pubblico.

2. *(Comma così modificato dall'art. 12, comma 4, d.lg. 13 maggio 1998, n. 171)* Il Garante promuove, nei modi di cui all'articolo 31, comma 1, lettera h), l'adozione, da parte del Consiglio nazionale dell'ordine dei giornalisti, di un apposito codice di deontologia relativo al trattamento dei dati di cui al comma 1 del presente articolo effettuato nell'esercizio della professione di giornalista, che preveda misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli idonei a rivelare lo stato di salute e la vita sessuale. Nella fase di formazione del codice, ovvero successivamente, il Garante in cooperazione con il Consiglio, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire. Il Codice è pubblicato sulla Gazzetta Ufficiale a cura del Garante, e diviene efficace quindici giorni dopo la sua pubblicazione.

3. Ove entro sei mesi dalla proposta del Garante il codice di deontologia di cui al comma 2 non sia stato adottato dal Consiglio nazionale dell'Ordine dei giornalisti, esso è adottato in via sostitutiva dal Garante ed è efficace sino alla adozione di un diverso codice secondo la procedura di cui al comma 2. In caso di violazione delle prescrizioni contenute nel codice di deontologia, il Garante può vietare il trattamento ai sensi dell'articolo 31, comma 1, lettera l).

4. *(Comma così modificato dall'art. 2, comma 1, d.lg. 9 maggio 1997, n. 123)* Nel codice di cui ai commi 2 e 3 sono inserite, altresì, prescrizioni concernenti i dati personali diversi da quelli indicati negli articoli 22 e 24. Il codice può prevedere forme semplificate per le informative di cui all'articolo 10.

4-*bis*. *(Comma aggiunto dall'art. 2, comma 2, d.lg. 9 maggio 1997, n. 123)* Le disposizioni della presente legge che attengono all'esercizio della professione di giornalista si applicano anche ai trattamenti effettuati dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69, nonché ai trattamenti temporanei finalizzati esclusivamente alla pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero.

Art. 26. Dati concernenti persone giuridiche

1. Il trattamento nonché la cessazione del trattamento di dati concernenti persone giuridiche, enti o associazioni non sono soggetti a notificazione.

2. Ai dati riguardanti persone giuridiche, enti o associazioni non si applicano le disposizioni dell'articolo 28.

Capo V – Trattamenti soggetti a regime speciale

Art. 27. Trattamento da parte di soggetti pubblici

1. Salvo quanto previsto al comma 2, il trattamento di dati personali da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti.

2. La comunicazione e la diffusione a soggetti pubblici, esclusi gli enti pubblici economici, dei dati trattati sono ammesse quando siano previste da norme di legge o di regolamento, o risultino comunque necessarie per lo svolgimento delle funzioni istituzionali. In tale ultimo caso deve esserne data previa comunicazione nei modi di cui all'articolo 7, commi 2 e 3 al Garante che vieta, con provvedimento motivato, la comunicazione o la diffusione se risultano violate le disposizioni della presente legge.

3. La comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati o a enti pubblici economici sono ammesse solo se previste da norme di legge o di regolamento.

4. I criteri di organizzazione delle amministrazioni pubbliche di cui all'articolo 5 del decreto legislativo 3 febbraio 1993, n. 29, sono attuati nel pieno rispetto delle disposizioni della presente legge.

Art. 28. Trasferimento di dati personali all'estero

1. Il trasferimento anche temporaneo fuori del territorio nazionale, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento deve essere previamente notificato al Garante, qualora sia diretto verso un Paese non appartenente all'Unione europea o riguardi taluno dei dati di cui agli articoli 22 e 24.

2. Il trasferimento può avvenire soltanto dopo quindici giorni dalla data della notificazione; il termine è di venti giorni qualora il trasferimento riguardi taluno dei dati di cui agli articoli 22 e 24.

3. Il trasferimento è vietato qualora l'ordinamento dello Stato di destinazione o di transito dei dati non assicuri un livello di tutela delle persone adeguato ovvero, se si tratta dei dati di cui agli articoli 22 e 24, di grado pari a quello assicurato dall'ordinamento italiano. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

4. Il trasferimento è comunque consentito qualora:

a) l'interessato abbia manifestato il proprio consenso espresso ovvero, se il trasferimento riguarda taluno dei dati di cui agli articoli 22 e 24, in forma scritta;

b) sia necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per l'acquisizione di informative precontrattuali attivate su richiesta di quest'ultimo, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) sia necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento, ovvero specificato ai sensi degli articoli 22, comma 3 e 24, se il trasferimento riguarda taluno dei dati ivi previsti;

d) sia necessario 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, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

e) sia necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d'intendere o di volere;

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

g) sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto;

g-*bis*) *(Lettera inserita dall'art. 4, comma 3, d.lg. 30 luglio 1999, n. 281)* il trattamento sia finalizzato unicamente a scopi di ricerca scientifica o di statistica e sia effettuato nel rispetto dei codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 31.

5. Contro il divieto di cui al comma 3 del presente articolo può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

6. Le disposizioni del presente articolo non si applicano al trasferimento di dati personali effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità.

7. La notificazione di cui al comma 1 del presente articolo è effettuata ai sensi dell'articolo 7 ed è annotata in apposita sezione del registro previsto dall'articolo 31, comma 1, lettera a). La notificazione può essere effettuata con un unico atto unitamente a quella prevista dall'articolo 7.

Capo VI - Tutela amministrativa e giurisdizionale

Art. 29. Tutela

1. I diritti di cui all'articolo 13, comma 1, possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante. Il ricorso al Garante non può essere proposto qualora, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'autorità giudiziaria.

2. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che siano decorsi cinque giorni dalla richiesta avanzata sul medesimo oggetto al responsabile. La presentazione del ricorso rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

3. Nel procedimento dinanzi al Garante il titolare, il responsabile e l'interessato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. Il Garante può disporre, anche d'ufficio, l'espletamento di perizie.

4. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare e al responsabile, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. Il provvedimento è comunicato senza ritardo alle parti interessate, a cura dell'ufficio del Garante. La mancata pronuncia sul ricorso, decorsi trenta *(Parola così sostituita dall'art. 13, comma 1, lett. a), d.lg. 30 luglio 1999, n. 281)* giorni dalla data di presentazione, equivale a rigetto.

5. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento cessa di avere ogni effetto se, entro i successivi venti giorni, non è adottata la decisione di cui al comma 4 ed è impugnabile unitamente a tale decisione.

6. Avverso il provvedimento espresso o il rigetto tacito di cui al comma 4, il titolare o l'interessato possono proporre opposizione al tribunale del luogo ove risiede il titolare, entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. L'opposizione non sospende l'esecuzione del provvedimento.

6-*bis*. *(Comma inserito dall'art. 13, comma 1, lett. b)*, d.lg. 30 luglio 1999, n. 281) Il decorso dei termini previsti dai commi 4, 5 e 6 è sospeso di diritto dal 1° al 30 agosto di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Ove il decorso abbia inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussista il pregiudizio di cui al comma 2 e non preclude l'adozione dei provvedimenti di cui al comma 5.

7. Il tribunale provvede nei modi di cui agli articoli 737 e seguenti del codice di procedura civile, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), e può sospendere, a richiesta, l'esecuzione del provvedimento. Avverso il decreto del tribunale è ammesso unicamente il ricorso per cassazione.

8. Tutte le controversie, ivi comprese quelle inerenti il rilascio dell'autorizzazione di cui all'articolo 22, comma 1, o che riguardano, comunque, l'applicazione della presente legge, sono di competenza dell'autorità giudiziaria ordinaria.

9. Il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 9.

Capo VII - Garante per la protezione dei dati personli

(Denominazione così modificata dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123)

Art. 30. Istituzione del Garante

1. *(Comma così modificato dall'art. 3, comma 1, d.lg. 9 maggio 1997, n. 123)* È istituito il Garante per la protezione dei dati personali.

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

3. Il Garante è organo collegiale costituito da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. Essi eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. I membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

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

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

6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai membri compete un'indennità di funzione non eccedente, nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate, con il regolamento di cui all'articolo 33, comma 3, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

Art. 31. Compiti del Garante

1. Il Garante ha il compito di:

a) istituire e tenere un registro generale dei trattamenti sulla base delle notificazioni ricevute;

b) controllare se i trattamenti sono effettuati nel rispetto delle norme di legge e di regolamento e in conformità alla notificazione;

c) segnalare ai relativi titolari o responsabili le modificazioni opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;

d) ricevere le segnalazioni ed i reclami degli interessati o delle associazioni che li rappresentano, relativi ad inosservanze di legge o di regolamento, e provvedere sui ricorsi presentati ai sensi dell'articolo 29;

e) adottare i provvedimenti previsti dalla legge o dai regolamenti;

f) vigilare sui casi di cessazione, per qualsiasi causa, di un trattamento;

g) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle sue funzioni;

h) promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

i) curare la conoscenza tra il pubblico delle norme che regolano la materia e delle relative finalità, nonché delle misure di sicurezza dei dati di cui all'articolo 15;

l) vietare, in tutto o in parte, il trattamento dei dati o disporne il blocco quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;

m) segnalare al Governo l'opportunità di provvedimenti normativi richiesti dall'evoluzione del settore;

n) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione della presente legge, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce;

o) curare l'attività di assistenza indicata nel capitolo IV della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della Convenzione medesima;

p) esercitare il controllo sui trattamenti di cui all'articolo 4 e verificare, anche su richiesta dell'interessato, se rispondono ai requisiti stabiliti dalla legge o dai regolamenti.

2. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla presente legge.

3. Il registro di cui al comma 1, lettera a), del presente articolo, è tenuto nei modi di cui all'articolo 33, comma 5. Entro il termine di un anno dalla data della sua istituzione, il Garante promuove opportune intese con le province ed eventualmente con altre pubbliche amministrazioni al fine di assicurare la consultazione del registro mediante almeno un terminale dislocato su base provinciale, preferibilmente nell'ambito dell'ufficio per le relazioni con il pubblico di cui all'articolo 12 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni.

4. Contro il divieto di cui al comma 1, lettera l), del presente articolo, può essere proposta opposizione ai sensi dell'articolo 29, commi 6 e 7.

5. Il Garante e l'Autorità per l'informatica nella pubblica amministrazione cooperano tra loro nello svolgimento dei rispettivi compiti; a tal fine, invitano il presidente o un suo delegato membro dell'altro organo a partecipare alle riunioni prendendo parte alla discussione di argomenti di comune interesse iscritti all'ordine del giorno; possono richiedere, altresì, la collaborazione di personale specializzato addetto all'altro organo.

6. Le disposizioni del comma 5 si applicano anche nei rapporti tra il Garante e le autorità di vigilanza competenti per il settore creditizio, per le attività assicurative e per la radiodiffusione e l'editoria.

Art. 32. Accertamenti e controlli

1. Per l'espletamento dei propri compiti il Garante può richiedere al responsabile, al titolare, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

2. Il Garante, qualora ne ricorra la necessità ai fini del controllo del rispetto delle disposizioni in materia di trattamento dei dati personali, può disporre accessi alle banche di 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, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 2 sono disposti previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede senza ritardo sulla richiesta del Garante, con decreto motivato; le relative modalità di svolgimento sono individuate con il regolamento di cui all'articolo 33, comma 3.

4. I soggetti interessati agli accertamenti sono tenuti a farli eseguire.

5. Resta fermo quanto previsto dall'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

6. Per i trattamenti di cui agli articoli 4 e 14, comma 1, gli accertamenti sono effettuati per il tramite di un membro designato dal Garante. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, salvo che ricorrano i motivi di cui all'articolo 10, comma 4, della legge 1° aprile 1981, n. 121, come sostituito dall'articolo 42, comma 1, della presente legge, o motivi di difesa o di sicurezza dello Stato.

7. Gli accertamenti di cui al comma 6 non sono delegabili. Qualora risulti necessario in ragione della specificità della verifica, il membro designato può farsi assistere da personale specializzato che è tenuto al segreto ai sensi dell'articolo 33, comma 6. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai membri del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti al relativo ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 33, comma 3. Per gli accertamenti relativi agli organismi e ai dati di cui all'articolo 4, comma 1, lettera b), il membro designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

Art. 33. Ufficio del Garante

1. Alle dipendenze del Garante è posto un ufficio composto, in sede di prima applicazione della presente legge, *(Parole inserite dall'art. 1, comma 1, d.lg. 26 febbraio 1999, n. 51)* da dipendenti dello Stato e di altre amministrazioni pubbliche, collocati fuori ruolo nelle forme previste dai rispettivi ordinamenti, il cui servizio presso il medesimo ufficio è equiparato ad ogni effetto di legge a quello prestato nelle rispettive amministrazioni di provenienza. Il relativo contingente è determinato, in misura non superiore a quarantacinque unità, su proposta del Garante medesimo, con decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri del tesoro e per la funzione pubblica, entro novanta giorni dalla data di elezione del Garante. Il segretario generale può essere scelto anche tra magistrati ordinari o amministrativi. *(Parole aggiunte dall'art. 3, comma 2, d.lg. 9 maggio 1997, n. 123) (L'art. 3, comma 3 del decreto legislativo 9 maggio 1997, n. 123, prevede che "Il personale richiesto dal Garante per la protezione dei dati personali nella fase di costituzione del relativo ufficio, nelle more del perfezionamento del comando, del fuori ruolo o dell'aspettativa, può essere utilizzato dal Garante a decorrere dalla data indicata nella richiesta, sempre che tale data sia di almeno dieci giorni successiva a quella della richiesta, vi sia l'assenso dell'interessato e l'amministrazione o l'ente di appartenenza non si opponga.")*

1-*bis*. *(Comma aggiunto dall'art. 1, comma 2, d.lg. 26 febbraio 1999, n. 51)* È istituito il ruolo organico del personale dipendente del Garante. Con proprio regolamento il Garante definisce: a) l'ordinamento delle carriere e le modalità del reclutamento secondo le procedure previste dall'articolo 36 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni; b) le modalità dell'inquadramento in ruolo del personale in servizio alla data dell'entrata in vigore del regolamento; c) il trattamento giuridico ed economico del personale secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e, per gli incarichi di funzioni dirigenziali, dall'articolo 19, comma 6, del citato decreto legislativo n. 29, come sostituito dall'articolo 13 del decreto legislativo 31 marzo 1998, n. 80, tenuto conto delle specifiche esigenze funzionali e organizzative. Il regolamento è pubblicato nella Gazzetta ufficiale. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni. Per il periodo intercorrente tra l'8 maggio 1997 e la data di entrata in vigore del regolamento, resta ferma l'indennità di cui all'articolo 41 del decreto del Presidente della Repubblica 10 luglio 1991, n. 231, corrisposta al personale in servizio. Dal 1° gennaio 1998 e fino alla data di entrata in vigore del medesimo regolamento, è inoltre corrisposta la differenza tra il nuovo trattamento e la retribuzione già in godimento maggiorata della predetta indennità di funzione.

1-*ter*. *(Comma aggiunto dall'art. 1, comma 2, d.lg. 26 febbraio 1999, n. 51)* L'ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale di cui al presente comma è corrisposta una indennità pari alla eventuale differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al corrispondente personale di ruolo, e comunque non inferiore alla indennità di cui all'articolo 41 del citato decreto del Presidente della Repubblica n. 231.

1-*quater*. *(Comma aggiunto dall'art. 2, comma 1, d.lg. 26 febbraio 1999, n. 51)* Con proprio regolamento il Garante ripartisce l'organico, fissato nel limite di cento unità, tra il personale dei diversi livelli e quello delle qualifiche dirigenziali e disciplina l'organizzazione, il funzionamento dell'ufficio, la riscossione e la utilizzazione dei diritti di segreteria, ivi compresi quelli corrisposti dall'8 maggio 1997, e la gestione delle spese, anche in deroga alle norme sulla contabilità generale dello Stato. Il regolamento è pubblicato nella Gazzetta ufficiale.

1-quinquies. *(Comma aggiunto dall'art. 2, comma 1, d.lg. 26 febbraio 1999, n. 51)* In aggiunta al personale di ruolo, l'ufficio può assumere direttamente dipendenti con contratto a tempo determinato disciplinato dalle norme di diritto privato, in numero non superiore a venti unità, ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma 4.

1-sexies. *(Comma aggiunto dall'art. 2, comma 1, d.lg. 26 febbraio 1999, n. 51)* All'ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e quelli concernenti le funzioni di gestione attribuite ai dirigenti.

2. Le spese di funzionamento dell'ufficio del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero del tesoro. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

3. *(Comma così modificato dall'art. 2, comma 2, d.lg. 26 febbraio 1999, n. 51)* In sede di prima applicazione della presente legge, le norme concernenti l'organizzazione ed il funzionamento dell'ufficio del Garante, nonché quelle dirette a disciplinare la riscossione dei diritti di segreteria e la gestione delle spese, anche in deroga alle disposizioni sulla contabilità generale dello Stato, sono adottate con regolamento emanato con decreto del Presidente della Repubblica, entro tre mesi dalla data di entrata in vigore della presente legge, 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, e su parere conforme del Garante stesso. Nel medesimo regolamento sono determinate le indennità di cui all'articolo 30, comma 6, e altresì previste le norme concernenti il procedimento dinanzi al Garante di cui all'articolo 29, commi da 1 a 5, secondo modalità tali da assicurare, nella speditezza del procedimento medesimo, il pieno rispetto del contraddittorio tra le parti interessate, nonché le norme volte a precisare le modalità per l'esercizio dei diritti di cui all'articolo 13, nonché della notificazione di cui all'articolo 7, per via telematica o mediante supporto magnetico o lettera raccomandata con avviso di ricevimento o altro idoneo sistema. Il parere del Consiglio di Stato sullo schema di regolamento è reso entro trenta giorni dalla ricezione della richiesta; decorso tale termine il regolamento può comunque essere emanato. *(L'art. 5, comma 3, del decreto legislativo 9 maggio 1997, n. 123, prevede che "Fino alla data di entrata in vigore del decreto di cui all'articolo 33, comma 3, della legge 31 dicembre 1996, n. 675, per la gestione delle spese dell'ufficio del Garante per la protezione dei dati personali si osservano, in quanto compatibili, le disposizioni contenute nel regolamento per la gestione delle spese occorrenti per il funzionamento dell'Autorità per l'informatica nella pubblica amministrazione, approvate con decreto del Presidente del Consiglio dei Ministri 6 ottobre 1994, n. 769, pubblicato nella Gazzetta Ufficiale n. 78 del 2 aprile 1995.)"*

3-*bis*. *(Comma inserito dall'art. 2, comma 3, d.lg. 26 febbraio 1999, n. 51)* Con effetto dalla data di entrata in vigore del regolamento di cui al comma 1-*quater*, cessano di avere vigore le norme adottate ai sensi del comma 3, primo periodo.

4. Comma così modificato dall'art. 2, comma 4, d.lg. 26 febbraio 1999, n. 51) Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedano, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due volte.

5. Per l'espletamento dei propri compiti, l'ufficio del Garante può avvalersi di sistemi automatizzati ad elaborazione informatica e di strumenti telematici propri ovvero, salvaguardando le garanzie previste dalla presente legge, appartenenti all'Autorità per l'informatica nella pubblica amministrazione o, in caso di indisponibilità, ad enti pubblici convenzionati.

6. Il personale addetto all'ufficio del Garante ed i consulenti sono tenuti al segreto su tutto ciò di cui siano venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a banche di dati e ad operazioni di trattamento.

6-*bis*. *(Comma aggiunto dall'art. 2, comma 5, d.lg. 26 febbraio 1999, n. 51)* Il personale dell'ufficio del Garante addetto agli accertamenti di cui all'articolo 32 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

Capo VIII – Sanzioni

Art. 34. Omessa o infedele notificazione

1. Chiunque, essendovi tenuto, non provvede alle notificazioni prescritte dagli articoli 7 e 28, ovvero indica in esse notizie incomplete o non rispondenti al vero, è punito con la reclusione da tre mesi a due anni. Se il fatto concerne la notificazione prevista dall'articolo 16, comma 1, la pena è della reclusione sino ad anno.

Art. 35. Trattamento illecito di dati personali

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 11, 20 e 27, è punito con la reclusione sino a due anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, comunica o diffonde dati personali in violazione di quanto disposto dagli articoli 21, 22, 23 e 24, ovvero del divieto di cui all'articolo 28, comma 3, è punito con la reclusione da tre mesi a due anni.

3. Se dai fatti di cui ai commi 1 e 2 deriva nocumento, la reclusione è da uno a tre anni.

Art. 36. Omessa adozione di misure necessarie alla sicurezza dei dati

1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni.

2. Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino a un anno.

Art. 37. Inosservanza dei provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 22, comma 2, o dell'articolo 29, commi 4 e 5, è punito con la reclusione da tre mesi a due anni.

Art. 38. Pena accessoria

1. La condanna per uno dei delitti previsti dalla presente legge importa la pubblicazione della sentenza.

Art. 39. Sanzioni amministrative

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 29, comma 4, e 32, comma 1, è punito con la sanzione amministrativa del pagamento di una somma da lire un milione a lire sei milioni.

2. La violazione delle disposizioni di cui agli articoli 10 e 23, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da lire cinquecentomila a lire tre milioni.

3. *(Comma così modificato dall'art. 14, d.lg. 30 luglio 1999, n. 281)* L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente articolo è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 33, comma 2, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 31, comma 1, lettera i) e 32.

Capo IX - Disposizioni transitorie e finali ed abrogazioni

Art. 40. Comunicazioni al Garante

1. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dalla presente legge e dalla legge 23 dicembre 1993, n. 547, è trasmessa, a cura della cancelleria, al Garante.

Art. 41. Disposizioni transitorie

1. Fermo restando l'esercizio dei diritti di cui agli articoli 13 e 29, le disposizioni della presente legge che prescrivono il consenso dell'interessato non si applicano in riferimento ai dati personali raccolti precedentemente alla data di entrata in vigore della legge stessa, o il cui trattamento sia iniziato prima di tale data. Resta salva l'applicazione delle disposizioni relative alla comunicazione e alla diffusione dei dati previste dalla presente legge.

2. (Comma così sostituito dall'art. 2, d.lg. 28 luglio 1997, n. 255.) Per i trattamenti di dati personali iniziati prima del 1 gennaio 1998, le notificazioni prescritte dagli articoli 7 e 28 sono effettuate dal 1 gennaio 1998 al 31 marzo 1998 ovvero, per i trattamenti di cui all'articolo 5 riguardanti dati diversi da quelli di cui agli articoli 22 e 24, nonché per quelli di cui all'articolo 4, comma 1, lettere c), d) ed e), dal 1 aprile 1998 al 30 giugno 1998.

3. Le misure minime di sicurezza di cui all'articolo 15, comma 2, devono essere adottate entro il termine di sei mesi dalla data di entrata in vigore del regolamento ivi previsto. Fino al decorso di tale termine, i dati personali devono essere custoditi in maniera tale da evitare un incremento dei rischi di cui all'articolo 15, comma 1.

4. Le misure di cui all'articolo 15, comma 3, devono essere adottate entro il termine di sei mesi dalla data di entrata in vigore dei regolamenti ivi previsti.

5. *(Comma da ultimo così modificato dall'art. 1, comma 1, d.lg. 6 novembre 1998, n. 389).* Nei ventiquattro mesi successivi alla data di entrata in vigore della presente legge, i trattamenti dei dati di cui all'articolo 22, comma 3, ad opera di soggetti pubblici, esclusi gli enti pubblici economici, e all'articolo 24, possono essere proseguiti anche in assenza delle disposizioni di legge ivi indicate, previa comunicazione al Garante.

6. In sede di prima applicazione della presente legge, fino alla elezione del Garante ai sensi dell'articolo 30, le funzioni del Garante sono svolte dal presidente dell'Autorità per l'informatica nella pubblica amministrazione, fatta eccezione per l'esame dei ricorsi di cui all'articolo 29.

7. *(Comma così sostituito dall'art. 4, comma 1, d.lg. 9 maggio 1997, n. 123)* Le disposizioni della presente legge che prevedono un'autorizzazione del Garante si applicano limitatamente alla medesima autorizzazione e fatta eccezione per la disposizione di cui all'articolo 28, comma 4, lettera g), a decorrere dal 30 novembre 1997. Le medesime disposizioni possono essere applicate dal Garante anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti.

7-*bis*. *(Comma aggiunto dall'art. 4, comma 2, d.lg. 9 maggio 1997, n. 123)* In sede di prima applicazione della presente legge, le informative e le comunicazioni di cui agli articoli 10, comma 3, e 27, comma 2, possono essere date entro il 30 novembre 1997.

Art. 42. Modifiche a disposizioni vigenti

1. L'articolo 10 della legge 1° aprile 1981, n. 121, è sostituito dal seguente:
"Art. 10. - (Controlli).
1. *(Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123)* Il controllo sul Centro elaborazione dati è esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.

2. *(Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123)* I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità procedente ne dà notizia al Garante per la protezione dei dati personali.

3. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera a) del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intelligibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

4. *(Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123)* Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre venti giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali.

5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi. Il tribunale provvede nei modi di cui agli articoli 737 e seguenti del codice di procedura civile.".

2. Il comma 1 dell'articolo 4 del decreto legislativo 12 febbraio 1993, n. 39, è sostituito dal seguente: "1. È istituita l'Autorità per l'informatica nella pubblica amministrazione, denominata Autorità ai fini del presente decreto; tale Autorità opera in piena autonomia e con indipendenza di giudizio e di valutazione.".

3. Il comma 1 dell'articolo 5 del decreto legislativo 12 febbraio 1993, n. 39, è sostituito dal seguente: "1. Le norme concernenti l'organizzazione ed il funzionamento dell'Autorità, l'istituzione del ruolo del personale, il relativo trattamento giuridico ed economico e l'ordinamento delle carriere, nonché la gestione delle spese nei limiti previsti dal presente decreto, anche in deroga alle disposizioni sulla contabilità generale dello Stato, sono adottate con regolamento 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 il Ministro del tesoro e su parere conforme dell'Autorità medesima. Il parere del Consiglio di Stato sullo schema di regolamento è reso entro trenta giorni dalla ricezione della richiesta, decorsi i quali il regolamento può comunque essere emanato. Si applica il trattamento economico previsto per il personale del Garante per l'editoria e la radiodiffusione ovvero dell'organismo che dovesse subentrare nelle relative funzioni, fermo restando il limite massimo complessivo di centocinquanta unità. Restano altresì fermi gli stanziamenti dei capitoli di cui al comma 2, così come determinati per il 1995 e tenendo conto dei limiti di incremento previsti per la categoria IV per il triennio 1996-1998.".

4. *(Commi così modificati dall'art. 5, comma 1, d.lg. 9 maggio 1997, n. 123)* Negli articoli 9, comma 2 e 10, comma 2, della legge 30 settembre 1993, n. 388, le parole: "Garante per la protezione dei dati" sono sostituite dalle seguenti: "Garante per la protezione dei dati personali".

Art. 43. Abrogazioni

1. Sono abrogate le disposizioni di legge o di regolamento incompatibili con la presente legge e, in particolare, il quarto comma dell'articolo 8 ed il quarto comma dell'articolo 9 della legge 1° aprile 1981, n. 121. Entro sei mesi dalla data di emanazione del decreto di cui all'articolo 33, comma 1, della presente legge, il Ministro dell'interno trasferisce all'ufficio del Garante il materiale informativo raccolto a tale data in attuazione del citato articolo 8 della legge n. 121 del 1981.

2. Restano ferme le disposizioni della legge 20 maggio 1970, n. 300, e successive modificazioni, nonché, in quanto compatibili, le disposizioni della legge 5 giugno 1990, n. 135, e successive modificazioni, del decreto legislativo 6 settembre 1989, n. 322, nonché le vigenti norme in materia di accesso ai documenti amministrativi ed agli archivi di Stato. Restano altresì ferme le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

3. Per i trattamenti di cui all'articolo 4, comma 1, lettera e), della presente legge, resta fermo l'obbligo di conferimento di dati ed informazioni di cui all'articolo 6, primo comma, lettera a), della legge 1° aprile 1981, n. 121.

Capo X - Copertura finanziaria ed entrata in vigore

Art. 44. Copertura finanziaria

1. All'onere derivante dall'attuazione della presente legge, valutato in lire 8.029 milioni per il 1997 ed in lire 12.045 milioni a decorrere dal 1998, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 1997-1999, al capitolo 6856 dello stato di previsione del Ministero del tesoro per l'anno 1997, all'uopo utilizzando per il 1997, quanto a lire 4.553 milioni, l'accantonamento riguardante il Ministero degli affari esteri e, quanto a lire 3.476 milioni, l'accantonamento riguardante la Presidenza del Consiglio dei ministri e, per gli anni 1998 e 1999, quanto a lire 6.830 milioni, le proiezioni per gli stessi anni dell'accantonamento riguardante il Ministero degli affari esteri e, quanto a lire 5.215 milioni, le proiezioni per gli stessi anni dell'accantonamento riguardante la Presidenza del Consiglio dei ministri.

2. Il Ministro del tesoro è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 45. Entrata in vigore

1. La presente legge entra in vigore centoventi giorni dopo la sua pubblicazione nella Gazzetta Ufficiale. Per i trattamenti svolti senza l'ausilio di mezzi elettronici o comunque automatizzati che non riguardano taluno dei dati di cui agli articoli 22 e 24, le disposizioni della presente legge si applicano a decorrere dal 1° gennaio 1998. Fermo restando quanto previsto dall'articolo 9, comma 2, della legge 30 settembre 1993, n. 388, la presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale, limitatamente ai trattamenti di dati effettuati in esecuzione dell'accordo di cui all'articolo 4, comma 1, lettera a) e alla nomina del Garante.

99 LEGGE N. 676 DEL 31 DICEMBRE 1996 - DELEGA AL GOVERNO IN MATERIA DI TUTELA DELLE PERSONE E DI ALTRI SOGGETTI RISPETTO AL TRATTAMENTO DEI DATI PERSONALI

Preambolo

La Camera dei deputati ed il Senato della Repubblica

hanno approvato;

Il Presidente della Repubblica

Promulga la seguente legge:

Art. 1. Delega per l'emanazione di disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali

1. Il Governo della Repubblica è delegato ad emanare, entro diciotto mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti disposizioni integrative della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, con l'osservanza dei seguenti principi e criteri direttivi:

a) specificare le modalità di trattamento dei dati personali utilizzati a fini storici, di ricerca e di statistica, tenendo conto dei principi contenuti nella Raccomandazione n. R (83) 10, adottata il 23 settem-

bre 1983 dal Consiglio d'Europa, e successive modificazioni, con particolare riferimento alla durata della loro conservazione ed alle garanzie adeguate prescritte dalla normativa comunitaria riguardo ai dati raccolti per scopi diversi da quelli statistici, storici o scientifici e successivamente conservati per tali, diverse, finalità;

b) garantire la piena attuazione dei principi previsti dalla legislazione in materia di dati personali nell'ambito dei diversi settori di attività, nel rispetto dei criteri direttivi e dei principi della normativa comunitaria e delle seguenti raccomandazioni adottate dal Consiglio d'Europa:

1) n. R. (81) 1, del 23 gennaio 1981, in materia di dati sanitari, e successive modificazioni;
2) n. R. (85) 20, del 25 ottobre 1985, sui dati utilizzati per fini di direct marketing;
3) n. R. (86) 1, del 23 gennaio 1986, sui dati impiegati per scopi di sicurezza sociale;
4) n. R. (89) 2, del 18 gennaio 1989, sui dati utilizzati per finalità di lavoro;
5) n. R. (90) 19, del 13 settembre 1990, in materia di dati personali utilizzati per finalità di pagamento e di altre operazioni connesse;
6) n. R. (91) 10, del 9 settembre 1991, sulla comunicazione a terzi dei dati personali detenuti da organi pubblici;
7) n. R. (95) 4, del 7 febbraio 1995, sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici;

c) razionalizzare il trattamento economico del personale del Garante per la protezione dei dati personali in relazione a quello previsto dall'ordinamento per ogni altra Autorità di garanzia secondo il tendenziale criterio dell'uniformità a parità di responsabilità costituzionale;

d) individuare i presupposti per l'attribuzione di un numero di identificazione personale, ivi compreso il codice fiscale, e per il trattamento del medesimo e delle informazioni ad esso connesse, nonché per il collegamento con altri dati, sentita l'Autorità per l'informatica nella pubblica amministrazione, prevedendo adeguate garanzie con riferimento ai numeri di identificazione personale connessi a dati di carattere sensibile o idonei a rivelare i provvedimenti di cui all'articolo 686, commi 1, lettere a) e d), 2 e 3 del codice di procedura penale;

e) stabilire le modalità e i termini per l'aggiornamento, per la rettificazione e per le altre modificazioni dei dati effettuati in conseguenza dell'esercizio dei diritti dell'interessato o di un provvedimento del Garante per la protezione dei dati personali, quando i dati personali sono riprodotti su disco ottico;

f) prevedere forme semplificate di notificazione del trattamento dei dati personali e del loro trasferimento all'estero, con particolare riguardo ai trattamenti non automatizzati di dati diversi da quelli sensibili e da quelli di cui all'articolo 686 del codice di procedura penale, ed ulteriori casi di esonero dal relativo obbligo per trattamenti da individuare preventivamente che, in ragione delle relative modalità o della natura dei dati personali, non presentino rischi di un danno all'interessato, ferma restando l'applicabilità delle altre disposizioni di legge;

g) prevedere forme di semplificazione degli adempimenti a carico delle piccole imprese e di coloro che esercitano imprese artigiane;

h) estendere l'applicazione delle disposizioni relative al trattamento dei dati da parte di chi esercita la professione di giornalista, ad eccezione delle disposizioni concernenti i dati sensibili, ai soggetti che esercitano con carattere di continuità l'attività di pubblicista o di praticante giornalistica iscritti, rispettivamente, negli elenchi di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69;

i) adattare, ai trattamenti in ambito pubblico esclusi dall'applicazione della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, i principi desumibili dalla medesima legislazione, sulla base dei seguenti criteri:

1) pieno recepimento dei principi medesimi;
2) rispetto dei principi stabiliti dalla Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, nonché della normativa comunitaria, tenendo conto dei criteri di cui alla raccomandazione n. R. (87) 15, adottata il 17 settembre 1987 dal Consiglio d'Europa;
3) ricognizione puntuale dei soggetti pubblici titolari dei trattamenti esclusi, nonché dei medesimi trattamenti;
4) introduzione degli adattamenti resi indispensabili dalla specificità degli interessi perseguiti dai suddetti trattamenti in ambito pubblico;

5) particolare considerazione per i trattamenti di dati che implichino maggiori rischi di un danno all'interessato;

6) specificazione delle modalità attraverso le quali si svolge il controllo sul rispetto delle disposizioni di legge che presiedono ai suddetti trattamenti in ambito pubblico;

l) prevedere norme che favoriscano lo sviluppo dell'informatica giuridica e le modalità di collegamento, per l'autorità giudiziaria e per l'autorità di pubblica sicurezza, con le banche dati della pubblica amministrazione;

m) mantenere il raccordo tra le attività del Garante per la protezione dei dati personali e quelle dell'Autorità per l'informatica nella pubblica amministrazione, anche modificando le disposizioni della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e del decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni, nonché l'armonizzazione dello stato giuridico del relativo personale;

n) stabilire le modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari del trattamento di dati inerenti i servizi accessibili al pubblico e la corrispondenza privata, nonché i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale;

o) individuare i casi in cui, all'atto della comunicazione o della diffusione di dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da pubbliche amministrazioni, debba essere indicata la fonte di acquisizione dei dati.

Art. 2. Delega per l'emanazione di disposizioni correttive della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

1. Il Governo della Repubblica è delegato ad emanare, entro diciotto mesi dalla data di entrata in vigore della presente legge, uno o più decreti legislativi recanti disposizioni correttive della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, con l'osservanza dei seguenti principi e criteri direttivi:

a) rispetto dei principi e della impostazione sistematica della legislazione in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

b) introduzione delle sole correzioni a tale legislazione che, dopo il primo periodo di applicazione della medesima, sentiti il Garante per la protezione dei dati personali e nelle materie di sua competenza l'Autorità per l'informatica nella pubblica amministrazione, si dimostrino necessarie per realizzarne pienamente i principi o per assicurarne la migliore attuazione o per adeguarla all'evoluzione tecnica del settore.

Art. 3. Esercizio della delega

1. I decreti legislativi di cui agli articoli 1 e 2 sono adottati ai sensi dell'articolo 14 della legge 23 agosto 1988, n. 400.

100. LEGGE 24 MARZO 2001, N. 127 - DIFFERIMENTO DEL TERMINE PER L'ESERCIZIO DELLA DELEGA PREVISTA DALLA LEGGE 31 DICEMBRE 1996, N. 676, IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI (*)

Art.1.

1. I decreti legislativi di cui all'articolo 1, comma 1, lettere b), numeri 2), 3), 4), 5) e 6), c), d), e), i), l), n), ed o), e all'articolo 2 della legge 31 dicembre 1996, n. 676, e successive modificazioni, in materia

(*) *Pubblicata in G.U. Serie generale del 19 aprile 2001, n. 91.*

di trattamento dei dati personali, sono emanati entro il 31 dicembre 2001, sulla base dei principi e dei criteri direttivi indicati nella medesima legge.

2. I decreti legislativi di cui al comma 1, sono emanati previo parere delle Commissioni permanenti del Senato della Repubblica e della Camera dei deputati competenti per materia. Il parere è espresso entro trenta giorni dalla richiesta, indicando specificamente le eventuali disposizioni non ritenute corrispondenti ai principi e ai criteri direttivi contenuti nella legge di delegazione.

3. Il Governo procede comunque alla emanazione dei decreti legislativi qualora il parere non sia espresso entro trenta giorni dalla richiesta.

4. Il Governo emana, entro dodici mesi dallo scadere del termine di cui al comma 1 e previa acquisizione dei pareri previsti nel comma 2, da esprimersi entro sessanta giorni dalla richiesta, un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse, coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurarne la migliore attuazione.

5. Il Governo procede comunque alla emanazione del testo unico qualora il parere non sia espresso entro sessanta giorni dalla richiesta.

Art. 2.

1. La presente legge entra in vigore il giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

101. LEGGE N. 325 DEL 3 NOVEMBRE 2000 - DISPOSIZIONI INERENTI ALL'ADOZIONE DELLE MISURE MINIME DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI PREVISTE DALL'ARTICOLO 15 DELLA LEGGE 31 DICEMBRE 1996, N. 675 (*)

Art. 1 - Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge 31 dicembre 1996, n. 675

1. In sede di prima applicazione della disciplina contenuta nell'articolo 15 della legge 31 dicembre 1996, n. 675, le misure di sicurezza di cui al decreto del Presidente della Repubblica 28 luglio 1999, n. 318, possono essere adottate entro il 31 dicembre 2000 dai soggetti che documentino per iscritto le particolari esigenze tecniche e organizzative che rendono necessario avvalersi di un termine più ampio di quello previsto dall'articolo 41, comma 3, della medesima legge n. 675 del 1996.

2. Il documento di cui al comma 1 deve essere redatto entro un mese dalla data di entrata in vigore della presente legge con atto avente data certa e deve contenere una esposizione sintetica delle informazioni necessarie, da cui risultino:

a) gli accorgimenti da adottare o già adottati e gli elementi che caratterizzano il programma di adeguamento, nonché le singole fasi in cui esso è eventualmente ripartito;

b) le linee-guida previste per dare piena attuazione alle misure minime di sicurezza, la cui inosservanza è sanzionata ai sensi dell'articolo 36 della legge 31 dicembre 1996, n. 675, nonché alle più ampie misure di sicurezza previste dal comma 1 dell'articolo 15 della medesima legge n. 675 del 1996.

(*) Pubblicata nella Gazzetta Ufficiale n. 262 del 9 novembre 2000.

3. Il documento di cui ai commi 1 e 2 deve essere conservato presso di sé a cura del soggetto interessato.

4. La violazione di uno degli obblighi di cui ai commi 2 e 3 comporta l'inapplicabilità di quanto previsto al comma 1.

Art. 2 - Entrata in vigore

La presente legge entra in vigore, il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale.

PROVVEDIMENTI DEL GARANTE

REGOLAMENTO N. 1 DEL 28 GIUGNO 2000 SULL'ORGANIZZAZIONE E IL FUNZIONAMENTO DELL'UFFICIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (ART. 33, LEGGE 31 DICEMBRE 1996, N.675) (*)

Deliberazione del 28 giugno 2000

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo de Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, con la quale è stato istituito il Garante per la protezione dei dati personali;

Visto l'art. 33, comma 1-*bis* [1], della suddetta legge n. 675/1996, introdotto dall'art. 1, comma 2, del decreto legislativo 26 febbraio 1999, n. 51, il quale prevede che il Garante, con proprio regolamento, definisca:

a) l'ordinamento delle carriere e le modalità di reclutamento del personale;
b) le modalità dell'inquadramento in ruolo del personale in servizio alla data di entrata in vigore del regolamento;
c) il trattamento giuridico ed economico del personale;

Visto, altresì, il comma 1-*quater* del medesimo art. 33, introdotto dall'art. 2, comma 1, del decreto legislativo 26 febbraio 1999, n. 51, il quale demanda ad un regolamento del Garante la ripartizione dell'organico, fissato nel limite di cento unità, tra il personale dei diversi livelli e quello delle qualifiche dirigenziali, nonché la disciplina dell'organizzazione e del funzionamento dell'ufficio, della riscossione ed utilizzazione dei diritti di segreteria, anche in deroga alle norme sulla contabilità generale dello Stato;

Considerato che, in attuazione delle disposizioni sopra citate, la definizione delle previsioni regolamentari, per motivi di omogeneità, chiarezza e completezza, è stata opportunamente articolata in tre regolamenti attinenti, rispettivamente, all'organizzazione e al funzionamento dell'ufficio del Garante, al trattamento giuridico ed economico del personale, e alla gestione amministrativa e contabilità;

Visti gli atti d'ufficio propedeutici alla redazione dei predetti schemi di regolamento e considerato che il personale addetto all'ufficio ha potuto esprimere suggerimenti e proposte al riguardo;

Ritenuto di procedere, in conformità all'art. 33 della citata legge n. 675/1996 ed ai criteri sistematici sopra richiamati, all'adozione di tre distinti regolamenti concernenti le materie prima richiamate;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Giuseppe Santaniello;

(*) *Pubblicato in G.U. Serie generale n. 162 del 13 luglio 2000.*

Delibera:

1. Sono adottati i seguenti regolamenti numeri 1/2000, 2/2000 e 3/2000, rispettivamente concernenti:

a) l'organizzazione e il funzionamento dell'ufficio del Garante;
b) il trattamento giuridico ed economico del personale;
c) la gestione amministrativa e la contabilità.

2. I regolamenti di cui al punto 1 e le unite tabelle, di cui è richiesta la pubblicazione nella Gazzetta Ufficiale, ai sensi dell'art. 33, comma 1-bis, della legge 31 dicembre 1996, n. 675 e successive modificazioni ed integrazioni, sono rispettivamente riportati negli allegati A, B e C alla presente delibera di cui costituiscono parte integrante.

Roma, 28 giugno 2001

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

Capo I – Principi generali

Art. 1. Definizione

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675, di seguito denominata "legge". Ai medesimi fini, si intende altresì:

a) per "Garante", l'organo collegiale istituito ai sensi dell'art. 30 della legge;
b) per "presidente", il presidente del Garante;
c) per "componenti", i componenti del Garante;
d) per "ufficio", l'ufficio del Garante.

Art. 2. Il Garante

1. Il Garante:

a) determina gli indirizzi e i criteri generali della propria attività;
b) nomina, su proposta del presidente, il segretario generale e conferisce l'incarico ai dirigenti delle unità organizzative di primo livello;
c) definisce gli obiettivi e i programmi da realizzare, indica le priorità, emana le direttive generali per l'azione amministrativa e la gestione e ne verifica l'attuazione, in conformità ai principi di cui all'art. 3 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni;
d) approva il documento programmatico, il bilancio di previsione ed il bilancio consuntivo;
e) richiede pareri al Consiglio di Stato e ad altri organi consultivi;
f) adotta il codice etico dell'ufficio e assolve ad ogni altro compito previsto dalle leggi e dai regolamenti.

Art. 3. Presidente e componenti

1. Il presidente è eletto dai componenti a scrutinio segreto con il voto di almeno tre componenti. Se tale maggioranza non è raggiunta dopo la terza votazione, è eletto presidente il componente che consegue il maggior numero di voti e, a parità di voti, il più anziano di età.

2. Il presidente:

a) rappresenta il Garante;
b) convoca le riunioni del Garante, ne stabilisce l'ordine del giorno, designa i relatori e dirige i lavori;
c) promuove le liti e vi resiste relativamente agli atti di competenza propria o del collegio, ed ha il potere di conciliare e transigere;
d) coordina l'attività dei componenti nei rapporti con il Parlamento e con gli altri organi costituzionali o di rilievo costituzionale, nell'attività di comunicazione pubblica, nonché nelle relazioni con le autorità indipendenti e di vigilanza, con le pubbliche amministrazioni, con le autorità di controllo degli altri Paesi, con gli organi dell'Unione europea e del Consiglio d'Europa e con gli altri organismi internazionali.

3. Il Garante elegge un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. I componenti possono essere incaricati di svolgere compiti specifici o di trattare questioni determinate.

Art. 4. Insediamento dell'organo e cessazione dei componenti

1. I componenti dichiarano formalmente, all'atto dell'accettazione della nomina, di non trovarsi in alcuna delle situazioni di cui all'art. 30, comma 4, della legge.

2. Se ricorre in ogni tempo taluna delle situazioni di incompatibilità di cui all'art. 30, comma 4, della legge, il Garante stabilisce un termine entro il quale l'interessato deve far cessare la situazione di incompatibilità. La deliberazione è adottata con l'astensione dell'interessato.

3. Decorso il termine di cui al comma 2, ove non sia cessata la situazione di incompatibilità, il Garante dichiara la decadenza del componente ai sensi dell'art.30, comma 4, della legge.

4. La durata in carica del componente decorre dalla data di accettazione della nomina.

5. I componenti cessano dalla carica, oltre che nell'ipotesi di cui al comma 3, per dimissioni volontarie o per impossibilità a svolgere la propria attività a causa di un impedimento di natura permanente o comunque superiore a sei mesi.

6. Le dimissioni dei componenti hanno effetto dalla data di comunicazione della loro accettazione da parte del Garante. L'impedimento permanente di cui al comma 5 è accertato dal Garante.

7. Nei casi di cui ai commi 3 e 5, il presidente o chi ne fa le veci informa immediatamente i Presidenti della Camera dei deputati e del Senato della Repubblica per l'elezione del nuovo componente.

Art. 5. Riunioni

1. Il Garante ha sede in Roma e può stabilire proprie forme di rappresentanza presso l'Unione europea e Organismi internazionali.

2. Il Garante si riunisce nel luogo indicato nell'atto di convocazione. Le riunioni possono essere tenute in videoconferenza o con altre idonee tecniche audiovisive e vengono fissate dal presidente anche in base a eventuali calendari di lavoro stabiliti, di regola, con cadenza settimanale a giorno fisso.

3. L'ordine del giorno è comunicato ai componenti entro il terzo giorno che precede la riunione. Nei casi d'urgenza, la convocazione può essere immediata. Durante le riunioni, l'ordine del giorno può essere integrato, previa comunicazione immediata agli assenti, se nessuno dei presenti si oppone.

4. Ciascun componente, indicandone le ragioni, può chiedere la convocazione del Garante e l'iscrizione di un argomento all'ordine del giorno. Se la richiesta proviene da almeno due componenti, il presidente la accoglie in ogni caso.

5. Per la validità delle riunioni del Garante è necessaria la presenza del presidente e di due componenti, ovvero di tre componenti. Le deliberazioni sono adottate a maggioranza dei votanti. Il voto è sempre palese, salvo nel caso di deliberazioni concernenti il presidente o i componenti, le persone addette all'ufficio o i consulenti.

6. Il segretario generale svolge le funzioni di segretario. In caso di assenza o impedimento temporaneo, ovvero qualora il Garante lo reputi opportuno, le funzioni di segretario possono essere svolte da un dipendente designato dal Garante o dal componente più giovane.

7. Le deliberazioni sono sottoscritte dal presidente, dal relatore e dal segretario generale.

8. Nei casi di particolare urgenza e di indifferibilità che non permettono la convocazione in tempo utile del Garante, il presidente può adottare i provvedimenti di competenza dell'organo, i quali cessano di avere efficacia sin dal momento della loro adozione se non sono ratificati dal Garante nella prima riunione utile, da convocarsi non oltre il trentesimo giorno.

9. La disposizione di cui al comma 8 non si applica in caso di esame dei ricorsi, di applicazione di sanzioni amministrative o di adozione dei divieti di cui agli articoli 21, comma 3, e 31, comma 1, lettera l), della legge, di approvazione del documento programmatico, del bilancio preventivo e del bilancio consuntivo, ovvero allorché occorre disporre accertamenti relativamente ai trattamenti di cui all'art. 4 della legge.

Capo II - L'ufficio

Art. 6. Attività dell'Ufficio

1. L'attività dell'Ufficio è improntata al metodo della programmazione per funzioni-obiettivo, nel rispetto del principio della distinzione tra funzioni di indirizzo e controllo e di attuazione e gestione di

cui all'art. 3 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni e all'art. 33, comma 1-*sexies*, della legge 31 dicembre 1996, n. 675. A tal fine il Garante, contestualmente all'approvazione del bilancio preventivo, definisce i principali obiettivi e risultati da realizzare in relazione alle risorse umane, tecnologiche e finanziarie assegnate, le priorità e i principali indicatori di parametri di misurazione e valutazione, specificando gli eventuali obiettivi di miglioramento, progetti speciali e scadenze intermedie. Il segretario generale e i responsabili dei dipartimenti e dei servizi rispondono, nell'ambito di competenza, del risultato dell'attività dell'Ufficio e delle sue articolazioni.

2. Il Garante verifica i risultati dell'attività dell'Ufficio anche sulla base delle notizie di cui all'art. 9, comma 4, lettera e), e si avvale a tal fine del servizio di controllo interno.

Art. 7. Il segretario generale

1. Il segretario generale è nominato per la durata del mandato del Garante e rimane in carica per un periodo non superiore a trenta giorni dalla data di insediamento del nuovo collegio. La nomina può essere rinnovata alla scadenza.

2. Il segretario generale coordina l'attività dei dipartimenti e dei servizi. A tal fine:

a) cura l'esecuzione delle deliberazioni e l'attuazione dei programmi, degli obiettivi e delle direttive generali di cui all'art. 2, coordinando l'attività dei dirigenti dei dipartimenti e dei servizi e degli altri titolari di incarichi di responsabilità, indirizzandone l'attività anche attraverso riunioni periodiche e specifici progetti e sostituendosi ad essi in caso di inerzia o di inottemperanza;
b) promuove la più ampia partecipazione del personale alla realizzazione degli obiettivi e dei programmi, e l'informazione interna sull'attività svolta o in programma, anche mediante l'utilizzazione di strumenti informatici e telematici su cui deve basarsi, di regola, l'attività dell'ufficio, nonché attraverso riunioni periodiche e gruppi di lavoro;
c) è sentito dal Garante e può formulare ad esso proposte in relazione agli obiettivi, ai programmi, alle priorità e alle direttive generali di cui all'art. 2;
d) esercita i poteri delegati dal Garante o dal presidente;
e) esercita i poteri di spesa e contrattuali nell'ambito degli stanziamenti di bilancio ed assegna le risorse ai dipartimenti e ai servizi in conformità al regolamento di contabilità;
f) richiede pareri nell'ambito di competenza e risponde ai rilievi degli organi di controllo sugli atti di competenza dell'ufficio;
g) promuove le liti e vi resiste relativamente agli atti non di competenza del Garante o del presidente e può conciliare e transigere;
h) esercita le attribuzioni di cui all'art. 16 del decreto legislativo 3 febbraio 1993, n. 29 e successive modificazioni e integrazioni.

3. Il segretario generale assicura al Garante una completa e tempestiva informazione sulla propria attività e su quella dell'ufficio.

4. Il trattamento economico del segretario generale è determinato dal Garante sulla base dei criteri previsti dall'art.27 del regolamento concernente il trattamento giuridico ed economico del personale del Garante, nonché dall'art. 19, comma 6, del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni.

Art. 8. Organizzazione generale dell'ufficio

1. L'organizzazione dell'ufficio è ispirata ai seguenti principi:

a) efficienza, efficacia, trasparenza ed economicità dell'attività amministrativa;
b) determinazione delle competenze secondo organicità e omogeneità, tenendo conto del criterio dell'articolazione per funzioni delle attività strumentali amministrative e tecnologiche e dell'articolazione per materie o tematiche delle altre attività specie in ambito giuridico;
c) previsione di servizi stabili nel quadro di una organizzazione flessibile e adattabile a mutate esigenze;
d) integrazione e piena cooperazione tra i servizi;
e) incentivi alla formazione del personale anche attraverso avvicendamenti periodici negli incarichi;

f) possibilità di istituire unità temporanee di primo e secondo livello per svolgere specifici compiti o perseguire obiettivi nel breve periodo, anche mediante l'utilizzazione di professionalità esterne nei modi di cui all'art.33, comma 4, della legge;

g) utilizzazione di personale compreso nel ruolo organico o collocato fuori ruolo in conformità al rispettivo ordinamento, ovvero assunto con contratto a tempo determinato anche per favorire la specializzazione di giovani laureati, in conformità al regolamento sul trattamento giuridico ed economico del personale dell'ufficio.

2. L'ufficio è articolato in unità organizzative di primo e di secondo livello.

3. Le unità organizzative di primo livello sono i dipartimenti e i servizi.

4. Le unità organizzative di secondo livello sono le ulteriori strutture di cui si compongono i dipartimenti e i servizi.

5. Presso il Garante sono istituiti i seguenti servizi:

a) servizio di segreteria del collegio;
b) servizio relazioni istituzionali;
c) servizio relazioni comunitarie e internazionali;
d) servizio relazioni con i mezzi di informazione;
e) servizio studi e documentazione.

Con successiva deliberazione è istituito presso il Garante il servizio di controllo interno.

Presso la segreteria generale sono istituiti un ufficio di segreteria, la segreteria di sicurezza, l'ufficio archivio e protocollo e l'ufficio per le relazioni con il pubblico.

Sono istituiti i seguenti dipartimenti:

a) dipartimento affari giuridici "A";
b) dipartimento affari giuridici "B";
c) dipartimento affari giuridici "C";
d) dipartimento risorse umane;
e) dipartimento amministrazione e contabilità;
f) dipartimento contratti e risorse finanziarie;
g) dipartimento vigilanza e controllo e registro dei trattamenti;
h) dipartimento risorse tecnologiche.

6. Il Garante individua, su proposta del segretario generale, i compiti dei servizi e dei dipartimenti e istituisce le unità temporanee di primo livello di cui al comma 1, lettera f).

7. Il Garante si avvale anche dell'opera di consulenti ed esperti, nonché di dirigenti non preposti ad unità organizzative di primo livello.

Art. 9. Nomina dei dirigenti delle strutture di primo livello

1. Il Garante individua i dipartimenti e i servizi e procede all'eventuale graduazione delle funzioni dirigenziali sulla base della natura e della rilevanza dei compiti attribuiti a ciascuna unità organizzativa. Il Garante individua anche le funzioni dirigenziali che non comportano la responsabilità di unità organizzative e procede alla relativa graduazione.

2. Il Garante conferisce gli incarichi di direzione delle unità organizzative di primo livello di regola a personale compreso nel ruolo organico, per la durata non superiore al biennio e rinnovabile.

3. Gli incarichi di cui al comma 2 possono essere conferiti anche a personale non compreso nel ruolo organico, assunto con contratto a tempo determinato o collocato fuori ruolo in conformità ai rispettivi ordinamenti, ivi compresi magistrati ordinari e amministrativi, avvocati dello Stato, consiglieri parlamentari, docenti universitari e dirigenti di pubbliche amministrazioni.

4. I dirigenti:

a) dirigono, coordinano e controllano le unità organizzative cui sono preposti e i processi che da essi dipendono, curano l'attuazione dei rispettivi compiti e obiettivi secondo le direttive stabilite e adottano gli atti e i provvedimenti amministrativi, di spesa e di acquisizione delle entrate ad essi delegati;

b) rispondono della gestione delle risorse assegnate;

c) assegnano la trattazione degli affari di competenza alle unità organizzative di secondo livello o nell'ambito del dipartimento o del servizio;

d) curano le valutazioni del personale in conformità al regolamento sul trattamento giuridico ed economico del personale;

e) assicurano, anche attraverso strumenti informatici e telematici, una tempestiva informazione interna sull'attività anche contrattuale di competenza, e predispongono una relazione di sintesi sulle attività svolte nei mesi di maggio e di ottobre di ciascun anno, trasmettendola al segretario generale che informa il Garante;

f) formulano proposte ed esprimono pareri al segretario generale e, d'intesa con lui, al Garante anche nell'ambito delle relative riunioni, ove richiesto;

g) esercitano le funzioni di cui all'art. 17 del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni.

5. Il segretario generale, su proposta del dirigente competente, individua con propria determinazione le eventuali unità di secondo livello e ne conferisce la responsabilità al personale con qualifica di funzionario.

Art. 10. Reggenza delle unità organizzative

1. In caso di protratta assenza o di impedimento del dirigente preposto all'unità organizzativa, il Garante può attribuire, sentito il segretario generale, la responsabilità dell'unità ad un altro dirigente o a un funzionario di provata esperienza.

2. In caso di protratta assenza o impedimento del funzionario preposto ad una unità organizzativa di secondo livello, la sostituzione è disposta dal segretario generale su proposta del dirigente competente.

Art. 11. Assistenti dei componenti

1. Con deliberazione del Garante, sono assegnati al presidente e a ciascun componente, su loro designazione, fino a due assistenti e un addetto di segreteria, scelti anche fra magistrati ordinari o amministrativi, avvocati dello Stato, consiglieri parlamentari, docenti e ricercatori universitari, dirigenti o dipendenti di pubbliche amministrazioni, ovvero tra il personale dipendente in servizio presso l'ufficio o assunto con contratto a tempo determinato.

2. Al personale di cui al comma 1 è attribuito un trattamento economico corrispondente a quello spettante in base alla qualifica.

3. Gli assistenti possono svolgere altre funzioni presso l'ufficio, secondo modalità prestabilite d'intesa tra il componente cui sono assegnati e il segretario generale.

Art. 12. Custodia degli atti riservati

1. Con provvedimento del Garante è istituita una segreteria di sicurezza presso la quale sono conservati gli atti e i documenti acquisiti ai sensi dell'art. 32, commi 6 e 7, della legge. Alla segreteria è preposto il segretario generale e un numero di addetti dell'ufficio non superiore a cinque unità, assegnati tenendo conto del profilo professionale e delle specifiche attitudini. L'accesso agli atti e ai documenti relativi ai trattamenti di cui all'art. 4, comma 1 lettera b), della legge è regolato dal Garante in conformità ai criteri osservati per le segreterie di sicurezza presso le amministrazioni dello Stato.

Capo III - Procedimenti

Art. 13. Trasparenza partecipazione e contraddittorio

1. L'ufficio ispira la propria attività ai principi della trasparenza, della partecipazione e del contraddittorio stabiliti dalla legge 7 agosto 1990, n. 241.

2. Con successivi regolamenti il Garante determina la durata dei procedimenti amministrativi di competenza, non individuata da leggi o altri regolamenti, e detta disposizioni in materia di accesso ai documenti amministrativi formati e detenuti dall'ufficio.

Art. 14. Assegnazione degli affari e responsabile del procedimento

1. Il segretario generale assegna l'affare al dipartimento o al servizio competente o individua il dipartimento o servizio competente relativamente agli affari di competenza di più unità organizzative. Il relativo dirigente assegna la competenza del procedimento all'unità organizzativa di secondo livello, se esistente, ovvero a sé o ad altro dipendente.

2. Le generalità del responsabile del procedimento sono indicate nella comunicazione dell'avvio del procedimento.

3. Il responsabile del procedimento provvede agli adempimenti necessari per lo svolgimento dell'attività preliminare e istruttoria e per la definizione del procedimento, in conformità alle norme applicabili e alle istruzioni impartite.

Art. 15. Relatore

1. Per gli atti per i quali si provvede con deliberazione del Garante, la competente unità organizzativa verifica la completezza della documentazione utile, predispone lo schema dell'atto o provvedimento e delle osservazioni e li sottopone al segretario generale entro il sesto giorno antecedente la riunione, affinché formuli, ove necessario, le osservazioni. Lo schema, le osservazioni e la documentazione sono formati e posti a disposizione del presidente e dei componenti, anche mediante strumenti informatici e telematici, senza ritardo e comunque entro il terzo giorno antecedente la riunione. Sono posti a disposizione senza ritardo anche gli eventuali aggiornamenti necessari.

2. Il presidente designa il relatore tra i componenti o svolge personalmente tale funzione.

3. Sulla base del materiale di cui al comma 1, il relatore introduce la discussione e formula le proprie conclusioni.

4. Quando la natura del procedimento lo richiede, il relatore può essere designato anche prima del terzo giorno antecedente alla riunione, affinché possa seguire la trattazione.

5. Per lo svolgimento dei propri compiti, il presidente e i componenti possono chiedere alla competente struttura di fornire la documentazione utile e avvalersi della consultazione diretta di atti e documenti del protocollo e dell'archivio.

Capo IV – Disposizioni varie

Art. 16. Bollettino

1. Il Garante promuove la pubblicazione di un bollettino nel quale sono riportati i provvedimenti più significativi, gli atti e i documenti di cui si ritiene opportuna la pubblicità e le risposte di interesse generale date ai quesiti pervenuti. Su richiesta dell'interessato o qualora risulti comunque opportuno, possono essere omesse le relative generalità.

2. Il Bollettino è edito anche attraverso strumenti telematici.

3. Il Garante cura la catalogazione dei provvedimenti di cui all'art. 40 della legge, in particolare mediante il bollettino, e ne agevola la consultazione anche da parte degli uffici giudiziari.

Art. 17. Rappresentanza e difesa

1. Fermo restando quanto previsto dall'art. 23 della legge 24 novembre 1981, n. 689, la rappresentanza e la difesa in giudizio del Garante è assunta dall'Avvocatura dello Stato ai sensi dell'art. 43 del regio

decreto 30 settembre 1933, n. 1611, e successive modificazioni ed integrazioni, recante il testo unico delle leggi e delle norme giuridiche sulla rappresentanza e difesa in giudizio dello Stato e sull'ordinamento dell'Avvocatura dello Stato.

Art. 18. Diritti di segreteria

1. Il Garante stabilisce con proprio provvedimento l'ammontare dei diritti di segreteria inerenti, in particolare, ai ricorsi, alle richieste di autorizzazione e alle notificazioni, tenendo eventualmente conto anche dei relativi costi di gestione, nonché le modalità del loro pagamento. Per la riscossione coattiva si applicano le disposizioni di cui al regio decreto 14 aprile 1910, n. 639, e successive modificazioni ed integrazioni.

Capo V – Disposizioni finali

Art. 19. Disposizioni regolamentari in vigore

1. Ai sensi dell'art. 33, comma 3-*bis*, della legge 31 dicembre 1996, n. 675, introdotto dall'art. 2, comma 4, del decreto legislativo 26 febbraio 1999, n. 51, rimangono in vigore le disposizioni contenute negli articoli 1, 6, 12, commi da 1 a 6, 13, 14, 15, 16, 17, 18, 19 e 20 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501.

Art. 20. Entrata in vigore

1. Il presente regolamento entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica.

103 REGOLAMENTO N. 2 DEL 28 GIUGNO 2000 CONCERNENTE IL TRATAMENTO GIURIDICO ED ECONOMICO DEL PERSONALE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (*)

Deliberazione del 28 giugno 2000

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo de Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, con la quale è stato istituito il Garante per la protezione dei dati personali;

Visto l'art. 33, comma 1-*bis*, della suddetta legge n. 675/1996, introdotto dall'art. 1, comma 2, del decreto legislativo 26 febbraio 1999, n. 51, il quale prevede che il Garante, con proprio regolamento, definisca:

a) l'ordinamento delle carriere e le modalità di reclutamento del personale;
b) le modalità dell'inquadramento in ruolo del personale in servizio alla data di entrata in vigore del regolamento;
c) il trattamento giuridico ed economico del personale;

(*) Pubblicato in G.U. Serie generale n. 162 del 13 luglio 2000.

Visto, altresì, il comma 1-*quater* del medesimo art. 33, introdotto dall'art. 2, comma 1, del decreto legislativo 26 febbraio 1999, n. 51, il quale demanda ad un regolamento del Garante la ripartizione dell'organico, fissato nel limite di cento unità, tra il personale dei diversi livelli e quello delle qualifiche dirigenziali, nonché la disciplina dell'organizzazione e del funzionamento dell'ufficio, della riscossione ed utilizzazione dei diritti di segreteria, anche in deroga alle norme sulla contabilità generale dello Stato;

Considerato che, in attuazione delle disposizioni sopra citate, la definizione delle previsioni regolamentari, per motivi di omogeneità, chiarezza e completezza, è stata opportunamente articolata in tre regolamenti attinenti, rispettivamente, all'organizzazione e al funzionamento dell'ufficio del Garante, al trattamento giuridico ed economico del personale, e alla gestione amministrativa e contabilità;

Visti gli atti d'ufficio propedeutici alla redazione dei predetti schemi di regolamento e considerato che il personale addetto all'ufficio ha potuto esprimere suggerimenti e proposte al riguardo;

Ritenuto di procedere, in conformità all'art. 33 della citata legge n. 675/1996 ed ai criteri sistematici sopra richiamati, all'adozione di tre distinti regolamenti concernenti le materie prima richiamate;

Viste le osservazioni dell'ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a), del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Giuseppe Santaniello;

Delibera:

1. Sono adottati i seguenti regolamenti numeri 1/2000, 2/2000 e 3/2000, rispettivamente concernenti:

a) l'organizzazione e il funzionamento dell'ufficio del Garante;
b) il trattamento giuridico ed economico del personale;
c) la gestione amministrativa e la contabilità.

2. I regolamenti di cui al punto 1 e le unite tabelle, di cui è richiesta la pubblicazione nella Gazzetta Ufficiale, ai sensi dell'art. 33, comma 1-*bis*, della legge 31 dicembre 1996, n. 675 e successive modificazioni ed integrazioni, sono rispettivamente riportati negli allegati A, B e C alla presente delibera di cui costituiscono parte integrante.

Roma, 28 giugno 2001

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

TITOLO I - Stato giuridico e trattamento economico

Capo I – Principi generali

Art. 1. Principi generali e definizioni

1. Le disposizioni del presente regolamento si applicano ai dipendenti di ruolo dell'Autorità, nonché, ove compatibili, al personale collocato fuori ruolo, comandato o distaccato da altre amministrazioni pubbliche o enti pubblici, ovvero assunto con contratto di lavoro a tempo determinato per quanto non previsto da clausole negoziali.

2. Ai fini del presente regolamento si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675, di seguito denominata "legge". Ai medesimi fini, si intende altresì:

a) per "Garante", l'organo collegiale istituito ai sensi dell'art. 30 della legge;
b) per "presidente", il presidente del Garante;
c) per "componenti", i componenti del Garante;
d) per "Ufficio", l'Ufficio del Garante.

Art. 2. Rinvio ad altre disposizioni

1. Per quanto non previsto dal presente regolamento si applicano, in quanto compatibili, le disposizioni sullo stato giuridico ed economico dei dipendenti dell'Autorità per le garanzie nelle comunicazioni, e, in via residuale, quelle che disciplinano il rapporto di lavoro privato.

2. Il trattamento giuridico ed economico del personale è stabilito in base ai criteri fissati dal regolamento in vigore per i dipendenti dell'Autorità per le garanzie nelle comunicazioni tenuto conto delle specifiche esigenze funzionali ed organizzative dell'ufficio, in conformità a quanto previsto dall'art.33, comma 1-*bis*, della legge 31 dicembre 1996, n. 675, introdotto dall'art.1, comma 2, del decreto legislativo 26 febbraio 1999, n. 51.

Art. 3. Adeguamento

1. Il presente regolamento è adeguato periodicamente alle modifiche intervenute, riguardo al trattamento giuridico ed economico del personale, nelle disposizioni di cui all'art.2.

Capo II – Stato giuridico del personale

Art. 4. Stato giuridico del personale

1. Il personale di ruolo è inquadrato nelle aree dirigenziale, direttiva, operativa ed esecutiva secondo la professionalità, il livello di responsabilità, l'autonomia della funzione svolta e la complessità delle mansioni attribuite.

2. L'area dirigenziale comprende la qualifica di dirigente.

3. L'area direttiva comprende la qualifica di funzionario.

4. L'area operativa comprende la qualifica di impiegato che è articolata nelle seguenti fasce retributive:
a) fascia A;
b) fascia B;
c) fascia C;
d) fascia D.

5. L'area esecutiva comprende la qualifica di commesso che è articolata nelle seguenti fasce retributive:
a) fascia A;
b) fascia B;
c) fascia C;
d) fascia D.

Art. 5. Reclutamento del personale: criteri generali

1. L'assunzione del personale avviene tramite le procedure di reclutamento di cui all'art. 36 e all'art. 28, in quanto compatibile, del decreto legislativo 3 febbraio 1993, n. 29 e successive modificazioni e integrazioni, fermo restando quanto previsto dalla legge 12 marzo 1999, n. 68 e dall'art. 16 della legge 28 febbraio 1987, n. 56. Nell'accesso alle diverse qualifiche e nello sviluppo professionale, è garantita pari opportunità tra uomini e donne.

2. Nell'espletamento delle procedure di reclutamento, l'Autorità assicura adeguata pubblicità e adotta modalità di svolgimento che garantiscano l'imparzialità, la celerità e l'economicità delle procedure, ricorrendo, ove opportuno, all'ausilio di sistemi automatizzati, diretti anche a realizzare forme di preselezione.

3. L'Autorità determina, di volta in volta, i posti da mettere a concorso, secondo le concrete esigenze.

4. I bandi di concorso sono emanati, su deliberazione del Garante, dal Presidente e pubblicati nella Gazzetta Ufficiale della Repubblica italiana e sul Bollettino ufficiale dell'Autorità.

5. Nella composizione delle commissioni di esame l'Autorità si adegua ai principi di cui all'art.36, comma 3, lettera e) del decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni ed integrazioni.

Art. 6. Requisiti generali

1. Possono partecipare alle procedure di cui all'art. 5, coloro che siano in possesso dei seguenti requisiti generali:
a) essere cittadino italiano o cittadino italiano non appartenente alla Repubblica o cittadino appartenente ad un Paese dell'Unione europea;
b) idoneità fisica all'impiego, da accertarsi da parte di istituzioni sanitarie pubbliche;
c) età non inferiore agli anni diciotto.

2. I concorsi per l'inquadramento nel ruolo organico delle varie qualifiche e fasce retributive del personale sono banditi, di regola, per il livello iniziale di ciascuna qualifica.

3. I criteri di svolgimento dei concorsi e la composizione delle commissioni di esami sono precisati nei relativi bandi.

4. I requisiti di cui al presente articolo devono essere posseduti all'atto dell'assunzione in ruolo, ad eccezione del requisito dell'età che deve essere posseduto alla data di scadenza stabilita dal bando di concorso per la presentazione delle domande.

Art. 7. Assunzione e periodo di prova

1. I candidati dichiarati vincitori al termine delle procedure selettive sono assunti con contratto individuale di lavoro subordinato.

2. Il periodo di prova, computato come servizio di ruolo effettivo se concluso favorevolmente, ha la durata di sei mesi per il personale appartenente all'area direttiva e di tre mesi per il personale appartenente alle aree operativa ed esecutiva, a decorrere dal giorno di effettivo inizio del servizio.

3. Il periodo di prova è prolungato per un periodo di tempo uguale a quello di assenza dal servizio a qualunque titolo.

4. Entro trenta giorni dal termine del periodo di prova, ove questo sia giudicato favorevolmente dal segretario generale sulla base di una relazione presentata dal responsabile del dipartimento o del servizio di appartenenza, i vincitori sono confermati in ruolo secondo l'ordine della graduatoria del concorso o della procedura selettiva approvata dall'Autorità. In caso di esito sfavorevole, viene dichiarata dall'Autorità la risoluzione del rapporto di lavoro e il dipendente ha titolo ad una indennità di liquida-

zione ragguagliata ad un dodicesimo degli emolumenti retributivi annui previsti, rilevanti per il trattamento di quiescenza.

5. Il personale collocato fuori ruolo presso l'Autorità o assunto con contratto di diritto privato a tempo determinato o comandato, che ha partecipato al concorso o alla procedura selettiva risultandone vincitore può essere esentato dal periodo di prova, sempre che il servizio prestato presso l'Autorità sia stato di durata superiore al periodo di prova stesso.

6. In caso di assenza per malattia durante il periodo di prova, il dipendente ha diritto all'intera retribuzione per i primi trenta giorni di assenza, alla metà per i successivi sessanta giorni; trascorsi tali periodi, e perdurando l'assenza, il dipendente è collocato in aspettativa, senza retribuzione, per altri novanta giorni.

7. Qualora la malattia dipenda da causa di servizio, al dipendente spetta la retribuzione integrale per il periodo di un anno; l'Autorità ha diritto di recuperare quanto eventualmente erogato dall'INAIL per il periodo d'assenza.

8. Trascorsi i periodi di assenza di cui sopra, qualora il dipendente non sia in grado di riprendere servizio, è dichiarata la cessazione del rapporto, attribuendosi al dipendente stesso il trattamento economico di cui al comma 4.

Capo III – Doveri

Art. 8. Obblighi

1. Il dipendente deve prestare la propria attività con lealtà, diligenza e spirito di collaborazione, in conformità alle leggi, ai regolamenti, alle disposizioni interne e al codice etico, nell'interesse esclusivo dell'Autorità.

2. Il dipendente deve osservare l'orario di lavoro, mantenere il segreto di ufficio in conformità alle leggi ed assolvere tempestivamente i compiti attribuitigli attenendosi alle direttive di indirizzo generale e particolare e alle altre istruzioni impartite.

3. Nell'assolvimento dei propri compiti il dipendente deve attuare le misure disposte e le istruzioni impartite dall'amministrazione in materia di igiene e di sicurezza del lavoro di cui è destinatario; deve inoltre promuoverne la conoscenza e vigilare sulla loro corretta applicazione da parte del personale subordinato.

Art. 9. Divieti e incompatibilità

1. Il personale in servizio presso l'Autorità deve osservare i divieti e le incompatibilità stabiliti dalle leggi, dai regolamenti e dal codice etico approvato dal Garante.

Art. 10. Responsabilità civile

1. Il dipendente è responsabile, per dolo o colpa grave, dei danni arrecati all'Autorità o a terzi.

2. L'Autorità può in via cautelare assoggettare a ritenuta la retribuzione del dipendente ovvero quanto possa a lui competere in caso di cessazione dal servizio, qualora il dipendente ammetta la propria responsabilità per il danno subito dall'Autorità. Resta salva la facoltà dell'Autorità di proporre ogni altra azione per la tutela del proprio credito.

Capo IV - Orario di lavoro

Art. 11. Orario di lavoro

1. L'orario settimanale ordinario di lavoro è di 37 ore e 30 minuti primi articolato su cinque giorni lavorativi e decorre, di norma, dal lunedì al venerdì. Le modalità di applicazione dell'orario di lavoro sono stabilite con ordine di servizio.

2. L'Autorità può instaurare rapporti di lavoro a tempo parziale in riferimento a particolari esigenze funzionali, ai quali si applicano, per quanto non previsto dal presente regolamento o con successivi atti dell'Autorità, le disposizioni vigenti nel pubblico impiego.

3. L'Autorità può sperimentare forme di lavoro a distanza anche in applicazione delle disposizioni di legge o di regolamento vigenti in materia.

4. In relazione a comprovate esigenze dei dipendenti o a motivate necessità funzionali dell'ufficio, l'orario di lavoro può essere modificato per alcuni dipendenti, anche richiedendone la reperibilità nei giorni non lavorativi.

5. Nei limiti della flessibilità dell'orario di lavoro giornaliero, il dipendente può chiedere di fruire di permessi brevi per esigenze personali, da compensare con prestazioni aggiuntive rese nel medesimo o in altri giorni lavorativi.

Art. 12. Riposo settimanale

1. Il personale ha diritto ad un giorno di riposo settimanale, che di regola coincide con la domenica o con altro giorno indicato a seconda della confessione religiosa d'appartenenza, e non presta di regola servizio negli altri giorni festivi.

2. Il personale, ove sia chiamato in via eccezionale a fornire prestazioni eccedenti le quattro ore nel corso della giornata destinata al proprio riposo settimanale o in altro giorno festivo, ha titolo ad usufruire del riposo non goduto in una delle giornate lavorative immediatamente successive.

3. Le prestazioni di cui al comma 2, di durata pari o inferiore alle quattro ore, danno titolo ad un permesso orario di durata corrispondente da fruire all'inizio o al termine dell'orario di lavoro di una delle giornate lavorative immediatamente successive.

4. Per le prestazioni rese ai sensi dei precedenti commi 2 e 3, il dipendente ha diritto alla remunerazione prevista per il lavoro straordinario.

Art. 13. Festività e giornate semifestive o feriali non lavorative

1. Sono considerati giorni festivi quelli previsti dalla legge e il 29 giugno, festività patronale di Roma. Al dipendente che svolge attività lavorativa in tali giornate spetta il compenso previsto dall'art. 14, comma 4. Qualora il giorno festivo coincida con il giorno di riposo settimanale, trova applicazione il regime relativo alle prestazioni rese nel giorno di riposo settimanale di cui all'art. 12.

2. Sono considerati semifestivi il 14 agosto, il 24 dicembre e il 31 dicembre. In tali giorni, fermi restando i termini di inizio dell'orario di lavoro, la durata del normale orario di lavoro giornaliero è ridotta a cinque ore. Al personale che in dette giornate svolga attività lavorativa oltre le cinque ore spetta il compenso previsto dall'art. 14, comma 3.

3. Sono considerate giornate feriali non lavorative le giornate in cui, in particolare il sabato, il personale non è normalmente tenuto a prestare servizio in dipendenza della concentrazione dell'orario settimanale in cinque giorni, ai sensi dell'art. 11. Al personale che svolga attività lavorativa in tali giornate è riconosciuto il trattamento previsto dall'art. 14, comma 4.

Art. 14. Lavoro straordinario e riposi compensativi

1. I dipendenti operativi ed esecutivi sono tenuti a svolgere prestazioni eccedenti l'orario di lavoro ordinario previsto nel contratto, qualora ricorrano eccezionali e comprovate esigenze di servizio.

2. Le ore di lavoro straordinario, compreso quello festivo infrasettimanale e notturno, sono retribuite secondo le modalità previste per il personale dell'Autorità per le garanzie nelle comunicazioni.

3. Le ore eccedenti l'orario di lavoro, a richiesta del dipendente e previa autorizzazione del responsabile dell'unità organizzativa nella quale operano, possono essere compensate con un numero di ore libere corrispondenti da fruire di norma, compatibilmente con le esigenze di servizio, non oltre il mese successivo.

4. Le prestazioni effettuate dai funzionari in giorni feriali non lavorativi sono recuperate, previa autorizzazione del responsabile dell'unità organizzativa nella quale operano, con un numero di ore libere corrispondenti da fruire, di norma, non oltre il mese successivo, oppure sono remunerate con i compensi previsti per il lavoro straordinario.

5. Il personale che fornisca prestazioni eccedenti il normale orario giornaliero di lavoro nell'arco di tempo compreso fra le ore 0.00 e le ore 6.00 di una giornata lavorativa, ha titolo ad un riposo di pari durata, da fruire di norma all'inizio della prestazione lavorativa di detta giornata.

6. In considerazione delle esigenze connesse all'espletamento dei servizi d'istituto, il segretario generale, sentiti i dirigenti dei dipartimenti e dei servizi, determina annualmente il numero di ore di lavoro straordinario che può essere effettuato dal personale dell'area operativa ed esecutiva. Il numero complessivo delle ore di lavoro straordinario effettuabile da ciascun dipendente non può superare le seicento ore annue. Per comprovate ed eccezionali esigenze d'ufficio relative a singoli casi, il limite può essere elevato.

7. Le prestazioni lavorative eventualmente rese oltre il monte ore assegnato a ciascun dipendente danno diritto a riposi compensativi.

8. Il responsabile di ciascuna unità organizzativa provvede mensilmente a programmare le prestazioni di lavoro straordinario del personale assegnato, in relazione agli obiettivi da raggiungere.

Capo V - Congedi ed aspettative

Art. 15. Ferie e festività soppresse

1. Nel corso di ciascun anno solare i dipendenti hanno diritto a periodi di ferie nelle seguenti misure:

a) durante l'anno solare in cui è avvenuta l'assunzione, due giorni lavorativi per ogni mese intercorrente tra la data di inizio del servizio ed il 31 dicembre successivo, con eventuale arrotondamento dell'unità superiore, fino ad un massimo annuo di ventitre giorni;
b) per gli anni successivi:

- ventitre giorni lavorativi, per anzianità di servizio fino a quattro anni;
- ventisei giorni lavorativi, per anzianità di servizio oltre i quattro e fino a dodici anni;
- trenta giorni lavorativi, per anzianità di servizio superiore a dodici anni.

2. Ai fini dell'applicazione del presente articolo, nel computo dell'anzianità di servizio si considera anche quella maturata in pubbliche amministrazioni anteriormente all'inquadramento nel ruolo organico.

3. I dipendenti hanno inoltre diritto nell'arco dell'anno a sei giorni di permesso retribuito ai sensi della legge 23 dicembre 1977, n. 937, due dei quali possono essere fruiti anche frazionatamente mediante permessi orari.

4. Le ferie sono sospese da malattie debitamente documentate e tempestivamente comunicate all'Autorità, qualora abbiano dato luogo a ricovero ospedaliero o si siano protratte per più di un giorno.

5. Le ferie si riducono nei soli casi previsti da disposizioni di legge, ad eccezione dei permessi di cui all'art. 33, comma 3, della legge 5 febbraio 1992, n. 104.

6. Per eccezionali esigenze di servizio le ferie possono essere rinviate o anche interrotte, fermo il diritto da parte del dipendente di fruirne o di completarne il godimento nello stesso anno cui si riferiscono e comunque entro il termine tassativo del 30 settembre dell'anno successivo. In tali casi si ha diritto al rimborso delle eventuali spese che si dimostri di avere sostenuto nella circostanza.

7. Per i dipendenti che cessino dal servizio per qualsiasi causa senza aver potuto fruire delle ferie spettanti al momento della cessazione, è riconosciuta una indennità commisurata ai giorni di ferie spettanti e non goduti.

8. Ai fini del calcolo di cui ai commi 1 e 7, le frazioni di mese superiori a quindici giorni sono considerate mese intero.

Art. 16. Permessi straordinari retribuiti

1. Oltre alle ferie, ai dipendenti sono riconosciuti, a domanda, i seguenti periodi di permesso straordinario retribuito:

a) fino a dieci giorni di calendario complessivi nell'arco dell'anno solare per giustificati motivi personali o familiari;
b) quindici giorni continuativi di calendario in occasione di matrimonio;
c) i giorni strettamente occorrenti per comparire in giudizio, per rispondere a chiamate di pubbliche autorità o per l'esercizio del diritto di voto nelle elezioni politiche ed amministrative, per il Parlamento Europeo e nei referendum popolari di cui alla legge 25 maggio 1970, n. 352, ovvero per osservare periodi di contumaciali in relazione a malattie infettive di familiari, per partecipare a concorsi o per donazione di sangue, nonché in tutti gli altri casi previsti da disposizione di legge o di regolamento o per i quali siano emanate dall'Autorità speciali disposizioni.

2. I permessi straordinari di cui al comma 1, lettera a), qualora non sia necessaria un'assenza dal servizio per l'intera giornata, possono essere fruiti mediante permessi orari retribuiti, di durata compresa tra una e cinque ore giornaliere (tre ore in occasione di semifestività) entro il limite annuo di due giornate ovvero di cinque giornate nel caso di documentate malattie di lunga durata o con decorso cronico che richiedano trattamenti terapeutici continuativi o periodici presso strutture sanitarie. In ogni caso, i permessi orari a valere sui permessi straordinari di cui al comma 1, lettera a) non possono eccedere complessivamente le cinque giornate all'anno.

Art. 17. Aspettativa per motivi personali o di famiglia

1. Per particolari motivi personali o di famiglia il dipendente può, a domanda, essere collocato in aspettativa fino al massimo di un anno.

2. L'Autorità provvede sulla domanda entro trenta giorni e può non accoglierla qualora la ritenga non adeguatamente giustificata, ovvero, per motivate ragioni di servizio, rinviarne l'accoglimento o ridurre la durata dell'aspettativa richiesta.

3. Durante l'aspettativa il dipendente non ha diritto alla retribuzione.

Art. 18. Permessi e aspettativa per motivi di studio e di lavoro

1. I dipendenti che seguono regolari corsi di studio in Italia ovvero all'estero, presso università o altri istituti pareggiati o legalmente riconosciuti o comunque abilitati al rilascio di titoli legali, ovvero presso altri istituti, possono essere esentati, limitatamente alla durata del corso, dall'obbligo di fornire prestazione eccedenti l'orario ordinario di lavoro ed hanno titolo a fruire di permesso straordinario retribuito per i giorni in cui debbano sostenere prove di esame e per il tempo necessario per il viaggio.

2. Il dipendente che intenda frequentare corsi di studio o attività di formazione all'estero, ovvero sia assegnatario di borse di studio all'estero che comportino la frequenza ai corsi per i quali sussista un rilevante interesse per l'amministrazione, può, a domanda, sempre che non vi ostino ragioni di servizio, essere autorizzato a fruire di un periodo di astensione dal servizio fino ad un massimo di due anni.

3. Durante il periodo di astensione dal servizio di cui al comma 2 il dipendente non ha diritto alla retribuzione, salva l'eventuale possibilità di usufruire della concessione di un contributo secondo le modalità e la misura definita dall'Autorità.

Art. 19. Assenze per malattia e aspettativa per motivi di salute

1. Il dipendente che, per accertate ragioni di salute, sia nell'impossibilità di prestare servizio, ha diritto alla retribuzione per un periodo che non può superare complessivamente novanta giorni nel corso di dodici mesi. Ai fini del computo di tale periodo si sommano tutti i giorni di assenza per malattia o aspettativa per motivi di salute verificatisi nel corso degli anzidetti dodici mesi.

2. Esaurito il periodo di assenza per malattia di cui al comma 1, il dipendente che non sia in condizioni di riprendere il servizio è collocato in aspettativa.

3. L'aspettativa ha termine col cessare della causa per la quale è stata disposta e, comunque, non può protrarsi per un periodo superiore a due anni.

4. Agli effetti della determinazione della durata massima del periodo di aspettativa e del conseguente trattamento economico, due o più periodi di aspettativa per motivi di salute si sommano nell'arco di un quinquennio quando tra essi intercorra un periodo di servizio attivo inferiore a novanta giorni.

5. Il dipendente che per ragioni di salute sia impossibilitato a prestare servizio deve segnalare tale circostanza all'Autorità senza ritardo, fornendo tutte le indicazioni utili per effettuare eventuali visite mediche domiciliari. Le visite di controllo delle assenze per malattia o infermità del dipendente sono disposte a mezzo dei servizi sanitari previsti dalla normativa in materia. Ai sensi e per gli effetti delle disposizioni vigenti in materia, durante le fasce orarie di reperibilità, fissate dalle ore 10.00 alle ore 12.00 e dalle ore 17.00 alle ore 19.00 di tutti i giorni, compresi quelli festivi e le domeniche, il dipendente deve farsi trovare nel domicilio comunicato all'Autorità per consentire l'effettuazione delle visite di controllo.

6. In tutti i casi in cui l'infermità derivante da infortunio non sul lavoro sia causata da responsabilità di terzi, il dipendente deve darne comunicazione all'Autorità, la quale ha diritto a recuperare dal terzo responsabile le retribuzioni da essa corrisposte durante il periodo di assenza, compresi gli oneri riflessi inerenti.

Art. 20. Tutela della maternità e della paternità

1. Al personale si applicano le disposizioni della legge 30 dicembre 1971, n. 1204, come modificata dalla legge 9 dicembre 1977, n. 903 e dalla legge 8 marzo 2000, n. 53.

2. Alle lavoratrici madri in astensione obbligatoria dal lavoro, ai sensi degli articoli 4 e 5 della citata legge n. 1204 del 1971, nonché agli altri soggetti di cui agli articoli 6 e 7 della citata legge n. 903 del 1977, spetta l'intera retribuzione.

3. Nell'ambito del periodo di astensione facoltativa dal lavoro di cui all'art. 7, comma 1, della citata legge n. 1204 del 1971, i primi trenta giorni di assenza sono considerati permessi straordinari retribuiti. Per il restante periodo di astensione facoltativa, alle lavoratrici madri o, in alternativa, ai lavoratori padri, spetta la retribuzione ridotta al trenta per cento.

4. Nei casi previsti dall'art. 7, comma 4, della medesima legge n. 1204, i predetti soggetti hanno diritto ad astenersi dal lavoro per malattia del bambino di età inferiore a otto anni ovvero di età compresa fra tre e otto anni, in quest'ultimo caso nel limite di cinque giorni lavorativi all'anno, con le modalità di cui al citato art. 7, commi 4 e 5, della legge n. 1204.

Art. 21. Validità dei periodi di aspettativa

1. I periodi di aspettativa per motivi di salute sono computati per intero ai fini della progressione economica, di carriera e del trattamento di quiescenza e non riducono le ferie. I periodi di aspettativa per servizio militare, ovvero per la frequenza di corsi di studio all'estero di cui all'art.18, comma 2, sono computati per intero ai fini della progressione economica, di carriera e del trattamento di quiescenza, ma non ai fini della maturazione delle ferie.

Capo VI - Missioni e comandi

Art. 22. Missioni

1. Ai fini dello svolgimento di particolari compiti di istituto, i dipendenti possono essere inviati in missione in località italiane ed estere.

2. Le missioni non possono superare complessivamente il periodo di tre mesi nel corso di un anno, salvo, per periodi superiori e in relazione a particolari incarichi, il consenso espresso dell'interessato.

3. Al personale in missione si applica il trattamento economico individuato con successiva deliberazione del Garante in conformità a quanto previsto dall'art. 2. Per specifiche esigenze che non permettono l'uso di altri mezzi di trasporto, ovvero per altre particolari situazioni oggetto di preventiva autorizzazione, i rimborsi spese possono comprendere spese sostenute per l'uso di taxi o di noleggio auto.

4. Al personale inviato all'estero per periodi superiori ad un mese, per motivi di studio o di formazione professionale, è riconosciuto, in sostituzione del trattamento di missione, un contributo forfettario nella misura determinata dall'Autorità.

Art. 23. Comandi

1. In casi particolari di interesse dell'Autorità, i dipendenti possono essere comandati presso amministrazioni o enti pubblici, presso altre autorità indipendenti, presso istituzioni comunitarie o internazionali, ovvero presso autorità di garanzia in materia di protezione dei dati personali operanti in altri Paesi.

2. Il comando può avere la durata sino ad un anno ed è prorogabile qualora permanga l'interesse che lo giustifica.

3. Il provvedimento stabilisce le relative modalità di attuazione anche in relazione al trattamento economico. Durante il comando, i dipendenti sono considerati in ogni caso in servizio.

Capo VII - Sanzioni disciplinari e procedimento

Art. 24. Sanzioni disciplinari

1. Per la violazione dei suoi doveri, il dipendente è soggetto alle seguenti sanzioni disciplinari:

a) note di censura per l'inosservanza di disposizioni di legge o di ordini di servizio;
b) multe inflitte anche per assenze ingiustificate dal lavoro, che comportano la mancata corresponsione della retribuzione da quattro ore all'intero trattamento giornaliero;
c) sospensione dal servizio e della retribuzione fino ad un anno;
d) licenziamento.

2. I richiami verbali o scritti in caso di mancanze lievi non costituiscono sanzioni disciplinari ai fini dell'applicazione del presente capo e sono adottati dal segretario generale o dal dirigente del dipartimento o del servizio presso il quale il dipendente presta servizio.

3. In caso di mancanze gravi, le note di censura sono adottate per i dirigenti dal Garante su proposta del segretario generale e per il rimanente personale dal segretario generale su proposta del dirigente presso cui presta servizio il dipendente, sentito il dirigente del Dipartimento risorse umane.

4. La sospensione dal servizio e dalla relativa retribuzione fino ad un anno è inflitta per gravi violazioni delle norme di condotta applicabili al personale. Il licenziamento è inflitto per fatti di particolare gravità e tali da non consentire la prosecuzione del rapporto di lavoro.

5. Al dipendente sospeso dal servizio e dalla retribuzione è riconosciuto un assegno alimentare di misura pari a quello corrispondentemente previsto dal regolamento del personale dell'Autorità per le

garanzie nelle comunicazioni. L'applicazione della predetta sanzione comporta l'impossibilità della presa in esame dell'interessato ai fini di eventuali promozioni per i successivi tre anni, nonché la sospensione dello scatto di anzianità per i successivi due anni.

Art. 25. Procedimento disciplinare

1. Gli addebiti suscettibili di configurarsi come infrazione disciplinare diversa dalla nota di censura sono comunicati per iscritto al dipendente, entro cinque giorni dalla loro formale conoscenza, dal dirigente del Dipartimento risorse umane, il quale effettua senza indugio gli accertamenti del caso, sentito anche l'interessato, direttamente o mediante un funzionario delegato.

2. Qualora non si pervenga alla loro immediata archiviazione, gli addebiti sono contestati all'interessato per iscritto entro venti giorni dalla ricezione della comunicazione di cui al comma 1. L'interessato ha accesso agli atti e ai documenti relativi agli accertamenti che lo riguardano e può ulteriormente sviluppare la sua difesa nei successivi venti giorni.

3. Entro ulteriori dieci giorni, il dirigente del Dipartimento risorse umane può ordinare l'archiviazione degli atti o disporre ulteriori accertamenti da svolgersi entro il medesimo termine ovvero trasmettere gli atti al segretario generale proponendo l'applicazione della sanzione disciplinare della censura. Qualora ritenga invece applicabile una più grave sanzione, deferisce il dipendente al Consiglio di disciplina proponendo la relativa sanzione.

4. Il Consiglio di disciplina è composto dal segretario generale e da due dirigenti o equiparati estratti a sorte tra quelli in servizio presso il Garante, fatta eccezione del dirigente del Dipartimento risorse umane e del dirigente della struttura presso cui presta servizio il dipendente interessato. Per i casi relativi al personale dirigente, il consiglio di disciplina è composto da due componenti del Garante e dal segretario generale.

5. Il Consiglio acquisisce gli atti e la relazione che li accompagna e decide sulle sanzioni disciplinari proposte con la partecipazione del dipendente interessato, eventualmente assistito da persona di sua fiducia o da una organizzazione dallo stesso indicata, nel termine di trenta giorni prorogabile per una sola volta per un periodo corrispondente. Il Consiglio può chiedere chiarimenti al dirigente o al funzionario istruttore e a testimoni. Se necessario, può svolgere ulteriori accertamenti anche tramite eventuali perizie.

6. I provvedimenti relativi alle sanzioni inflitte sono comunicati al dipendente nel testo integrale.

7. Durante il procedimento disciplinare, il dipendente può, a titolo cautelativo e per gravi motivi, essere sospeso dal servizio e, limitatamente ad un terzo, anche dalla retribuzione.

8. Non si tiene conto ad alcun effetto delle sanzioni disciplinari di cui all'art. 24, comma 1, lettere a) e b).

Art. 26. Termini

1. I termini relativi al procedimento disciplinare sono perentori. Per il loro computo non si tiene conto dei giorni non lavorativi.

2. Il procedimento estinto per decorrenza dei termini non può essere rinnovato.

3. Il procedimento disciplinare non può essere instaurato se per il fatto contestato ha avuto inizio un procedimento penale mediante richiesta di rinvio a giudizio e, se già instaurato, è sospeso fino al termine del giudizio di primo grado. Valutate le circostanze, si può comunque procedere alla sospensione cautelare del dipendente.

Capo VIII - Trattamento economico

Art. 27. Trattamento economico. Criterio generale

1. Il trattamento economico del personale dipendente è stabilito nella misura prevista dall'art. 33, comma 1-*bis*, della legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, tenuto conto delle specifiche funzioni espletate, secondo le tabelle allegate al presente regolamento.

2. Il trattamento economico del personale assunto nel corso dell'anno decorre dal giorno di effettivo inizio delle prestazioni.

3. In nessun caso al dipendente di ruolo che muti qualifica è corrisposta una retribuzione complessiva inferiore a quella precedentemente percepita. Qualora il livello del trattamento economico spettante risulti inferiore a quello precedentemente percepito, al dipendente è attribuito un assegno *ad personam* pensionabile e riassorbibile pari alla differenza tra il trattamento economico in godimento all'atto del passaggio e quello spettante nella nuova posizione.

4. L'Autorità può stipulare polizze sanitarie integrative delle prestazioni del servizio sanitario nazionale, nonché per la copertura dei rischi di premorienza e per i danni causati a terzi dal personale in servizio nell'esercizio o a causa delle proprie funzioni, salvo che il fatto derivi da comportamento doloso.

5. Al personale, compreso quello avente qualifica dirigenziale, è riconosciuto un buono pasto. Il buono pasto è attribuito per la singola giornata lavorativa nella quale il dipendente protrae l'attività di servizio nelle ore pomeridiane, con l'effettuazione di un intervallo di almeno mezzora. Nelle more dell'espletamento delle procedure per l'acquisizione dei buoni pasto, al personale è corrisposto l'equivalente in denaro di ciascun buono pasto con le modalità previste dall'art. 3, comma 7, della legge 23 dicembre 1996, n. 662.

TITOLO II - Ordinamento del personale

Capo I – Dirigenza

Sezione I - Funzioni

Art. 28. Dirigenti

1. I dirigenti, nell'ambito delle funzioni loro attribuite dalla legge e dal regolamento di organizzazione e funzionamento dell'ufficio, assicurano il rispetto degli indirizzi dell'Autorità e l'attuazione delle deliberazioni e delle decisioni adottate.

2. I dirigenti possono essere preposti ai dipartimenti e ai servizi. Quando non sia affidata loro la direzione di un dipartimento o un servizio, svolgono funzioni di studio, di consulenza, di ricerca ed analisi o eventuali altre assegnate direttamente dall'Autorità.

3. I dirigenti sono responsabili, in via esclusiva, della gestione e dei risultati dei procedimenti in ordine ai quali organizzano le risorse umane e materiali disponendo dei relativi poteri di coordinamento e di controllo, anche in collaborazione tra più unità organizzative.

Sezione II - Concorsi

Art. 29. Concorsi pubblici per l'accesso alla qualifica di dirigente. Requisiti

1. I concorsi per dirigente sono, di norma, banditi per il livello iniziale della relativa scala stipendiale.

2. Possono partecipare al concorso per la posizione iniziale della qualifica dirigenziale coloro che, muniti del diploma di laurea indicato nel bando di concorso, risultino in possesso di almeno uno dei seguenti requisiti, oltre a quelli di carattere generale di cui all'art. 6:

a) abbiano un'esperienza di almeno tre anni in campi di interesse per l'attività istituzionale dell'Autorità:
- come dirigenti o equiparati in enti ovvero istituzioni o imprese di notevole rilievo nazionale, comunitario o internazionale, in amministrazioni dello Stato o altre pubbliche amministrazioni con competenza nei predetti campi;
- in istituti di istruzione universitaria con qualifica non inferiore a ricercatore;

b) abbiano conseguito uno dei seguenti titoli: diploma di specializzazione, dottorato di ricerca o altro titolo post-universitario conseguito mediante uno o più corsi di durata complessiva almeno biennale presso istituti italiani o stranieri;

c) abbiano svolto presso l'ufficio, per un periodo non inferiore a due anni, funzioni di dirigente in posizione di collocamento fuori ruolo, di comando, di aspettativa o di contrattista, ovvero funzioni di collaborazione continuativa in base a contratto a tempo determinato o a rapporto di consulenza;

d) abbiano prestato servizio nel ruolo del personale dell'Autorità con la qualifica di funzionario e siano collocati almeno al 21 livello della scala stipendiale.

3. L'Autorità può bandire eccezionalmente concorsi per dirigente anche a livelli di progressione di carriera diversi da quello iniziale, qualora le competenze richieste non possano essere individuate tra il personale dell'Autorità. I requisiti di partecipazione saranno individuati nei relativi bandi di concorso.

Art. 30. Concorsi per dirigenti. Titoli ed esami

1. I concorsi per dirigenti si svolgono per titoli ed esami.

2. I titoli sono costituiti:

a) dagli attestati relativi alle attività di cui all'art. 29, limitatamente al periodo eccedente quello minimo necessario per l'ammissione al concorso;

b) da ogni altro titolo accademico, professionale o di studio, attinente all'attività istituzionale dell'Autorità;

c) da pubblicazioni di carattere giuridico o tecnico in campi di interesse per l'attività istituzionale dell'Autorità;

d) dalla conoscenza approfondita di almeno una lingua straniera.

I criteri di valutazione dei titoli saranno specificati nel bando di concorso.

3. Gli esami sono scritti ed orali. La prova scritta, a contenuto teorico-pratico, è diretta ad accertare, anche attraverso l'analisi di questioni concrete, l'attitudine dei concorrenti alla corretta soluzione, sotto il profilo della legittimità e dell'efficienza, di questioni e problemi attinenti a materie ed attività istituzionali dell'Autorità. La prova orale consiste in un colloquio finalizzato ad un'adeguata valutazione della personalità del candidato, della sua preparazione e capacità professionali, avuto riguardo alle attività ed alle funzioni a concorso. Le materie oggetto del colloquio sono specificate nel bando di concorso.

4. I concorsi per livelli stipendiali superiori al decimo si svolgono per titoli e colloquio con le modalità di cui alla prova orale prevista al comma 3.

5. Valgono, in quanto applicabili, i titoli di preferenza previsti dalle leggi relative agli impiegati dello Stato.

Sezione III - Valutazione e progressione economica

Art. 31. Rapporto valutativo annuale

1. Per ciascun dirigente è effettuata ogni anno una valutazione che tiene conto della qualità del lavoro prestato, dei risultati raggiunti, della preparazione, dell'osservanza dei doveri d'ufficio, dell'attitudine ad assumere maggiori responsabilità, nonché delle competenze dimostrate.

2. La valutazione si svolge attraverso la compilazione di un rapporto nel quale sono riportati analiticamente gli elementi concernenti ciascun fattore di valutazione, unitamente al giudizio conclusivo e al punteggio finale.

3. La valutazione dei dirigenti è svolta dai responsabili dei dipartimenti e dei servizi sulla base dei criteri definiti annualmente con deliberazione del Garante, su proposta del segretario generale.

4. Il comitato di valutazione è composto dai responsabili dei dipartimenti e dei servizi ed è presieduto dal segretario generale, eventualmente assistito da un consulente esterno; svolge funzioni di segretario il responsabile del Dipartimento risorse umane.

5. Il rapporto, previa verifica da parte del comitato della conformità ai criteri di valutazione, è comunicato dal valutatore al dirigente interessato, che lo controfirma per presa d'atto apponendovi eventuali note ed osservazioni.

6. Il comitato, sulla base dei rapporti e tenuto conto delle eventuali osservazioni degli interessati, predispone la graduatoria del personale dirigente sulla base del punteggio ottenuto.

7. Il rapporto per gli assistenti dei componenti è redatto da ciascun componente e trasmesso al Comitato.

8. La valutazione dei responsabili dei dipartimenti e dei servizi è effettuata da un collegio composto da un componente del Garante, dal segretario generale e da un consulente esterno.

9. La valutazione dei dirigenti non ha luogo se il periodo di lavoro complessivamente prestato nell'arco dell'anno solare è inferiore a sei mesi, anche non continuativi, sempre che l'assenza non sia dovuta ad astensione obbligatoria o facoltativa dal lavoro per maternità. Qualora gli elementi non siano sufficienti per formulare la valutazione, i dirigenti interessati conseguono comunque uno scatto nella progressione di carriera. I dipendenti in posizione di distacco o comando presso altre amministrazioni sono valutati sulla base degli elementi forniti dall'amministrazione presso cui il dipendente presta servizio.

10. Annualmente l'Autorità redige un elenco del personale dirigenziale con l'indicazione della posizione attribuita nella progressione di carriera.

Art. 32. Progressione economica dei dirigenti

1. La progressione del personale dirigente si effettua mediante scatti annuali secondo le tabelle allegate, salvo giudizio di insufficienza.

2. Il personale dirigente è valutato ogni anno. Con cadenza biennale nel mese di luglio ha luogo un procedimento di valutazione per l'attribuzione di progressioni sino ad un massimo di tre scatti per non oltre il 50% del personale dirigente in servizio. Le progressioni sono conferite, ai fini normativi ed economici, con decorrenza dal 1° agosto successivo. Le progressioni sono attribuite in relazione alle disponibilità di bilancio.

Sezione IV - Trattamento economico

Art. 33. Trattamento economico dei dirigenti

1. Il trattamento economico del personale dirigente è composto dalle seguenti voci:

a) retribuzione di livello;
b) retribuzione di risultato;
c) retribuzione di posizione, per i dirigenti di dipartimenti e servizi e per i dirigenti di cui all'art. 8, comma 6, del regolamento sull'organizzazione e il funzionamento dell'ufficio;
d) eventuale assegno *ad personam* di cui al comma 5.

2. La retribuzione di livello è determinata secondo l'allegata tabella 1.

3. La retribuzione di risultato di cui al comma 1, lettera b), è attribuita sulla base dei risultati raggiunti dal dirigente a fronte degli obiettivi programmati in ciascun anno.

4. È istituito un fondo per la qualità della prestazione individuale. Il fondo può essere incrementato dall'Autorità, tenuto conto delle disponibilità di bilancio. La misura e le modalità di erogazione della retribuzione di risultato sono stabilite annualmente con deliberazione del Garante.
5. I dirigenti cui sia affidata la responsabilità di dipartimenti e servizi o cui siano attribuite particolari funzioni godono, per la durata dell'incarico, di una retribuzione di posizione, determinata con deliberazione del Garante, nel limite del 15% della retribuzione tabellare prevista per il relativo livello, in relazione all'effettiva responsabilità e alla natura e complessità della funzione svolta.

6. Nel caso di conseguimento della qualifica di dirigente da parte di funzionari con trattamento economico superiore a quello spettante nella nuova posizione è attribuito un assegno *ad personam* pensionabile e riassorbibile pari alla differenza tra il trattamento economico in godimento all'atto del passaggio e quello spettante nella nuova posizione.

Capo II - Area direttiva

Sezione I - Funzioni

Art. 34. Funzionari

1. I funzionari svolgono compiti connessi con l'attività procedimentale di pertinenza dell'Autorità; effettuano attività di studio e di ricerca; provvedono ad adempimenti amministrativi, contabili e tecnici ed esercitano le altre attribuzioni loro affidate dai dirigenti. Ai funzionari possono essere assegnati compiti di coordinamento, integrazione e controllo in relazione a particolari progetti od attività.

2. Nell'ambito dei dipartimenti e dei servizi, i funzionari possono assumere la responsabilità delle relative articolazioni interne secondo quanto previsto dall'art. 9, comma 5, del regolamento sull'organizzazione e il funzionamento dell'ufficio.

3. I funzionari possono assumere funzioni di reggenza ai sensi dell'art. 10 del regolamento sull'organizzazione e il funzionamento dell'ufficio.

Sezione II - Concorsi

Art. 35. Concorsi per funzionari. Requisiti

1. I concorsi per funzionario sono, di norma, banditi per il livello iniziale.

2. Possono partecipare al concorso per l'assunzione al livello iniziale della qualifica di funzionario coloro che, muniti del diploma di laurea e con la votazione specificati nel bando di concorso, siano in possesso di uno dei seguenti requisiti, oltre a quelli di carattere generale di cui all'art.6:

a) abbiano un'esperienza di almeno due anni in campi di interesse per l'attività istituzionale dell'Autorità:
- in significative e continuative esperienze di studio e ricerca in istituzioni di ricerca e universitarie, effettuate a seguito di superamento di prova concorsuale, ovvero in enti, istituti o imprese di rilievo nazionale, comunitario o internazionale;
- nella carriera direttiva di enti, istituzioni, imprese di notevole rilievo nazionale, comunitario o internazionale, o di pubbliche amministrazioni, aventi attribuzioni in materie che interessano l'Autorità;
- nell'attività professionale presso studi legali o commerciali, in qualità di libero professionista abilitato;

b) abbiano prestato servizio, in qualità di funzionario, presso l'Autorità, per un periodo non inferiore ad un anno, anche con contratto a tempo determinato ovvero in posizione di comando, di collocamento fuori ruolo, di aspettativa o con rapporto di collaborazione continuativa e coordinata;

c) per il personale operativo costituisce requisito di partecipazione alle procedure selettive per il livello iniziale della qualifica di funzionario, il possesso di un diploma di laurea in materie attinenti all'attività istituzionale, come precisato nel bando di selezione, e l'avere prestato servizio nell'area operativa da almeno tre anni.

3. Al fine del calcolo dell'anzianità di servizio, il periodo di svolgimento delle predette attività può essere cumulato.

4. L'Autorità può bandire concorsi per funzionario anche a livelli di progressione di carriera diversi da quello iniziale, qualora le competenze richieste non possano essere individuate tra il personale dell'Autorità. I requisiti di partecipazione saranno individuati nei relativi bandi di concorso.

Art. 36. Concorsi per funzionari. Titoli ed esami

1. I concorsi per funzionari si svolgono per titoli ed esami.

2. I titoli sono costituiti:

a) dagli attestati relativi alle attività di cui all'art. 35, limitatamente al periodo eccedente quello minimo necessario per l'ammissione al concorso;
b) da ogni altro titolo accademico, professionale o di studio, attinente all'attività istituzionale dell'Autorità;
c) da pubblicazioni di carattere giuridico o tecnico in campi di interesse per l'attività istituzionale dell'Autorità;
d) dalla conoscenza approfondita di almeno una lingua straniera.
I criteri di valutazione dei titoli sono specificati nel bando di concorso.

3. Gli esami sono scritti ed orali. La prova teorico-pratica è diretta ad accertare, anche attraverso l'analisi di questioni concrete, l'attitudine dei concorrenti alla corretta soluzione, sotto il profilo della legittimità e dell'efficienza, di questioni e problemi attinenti a materie ed attività istituzionali dell'Autorità. La prova orale consiste in un colloquio finalizzato ad un'adeguata valutazione della personalità del candidato, della sua preparazione e capacità professionali, avuto riguardo alle attività ed alle funzioni a concorso. Le materie oggetto del colloquio sono specificate nel bando di concorso.

4. Valgono, in quanto applicabili, i titoli di preferenza previsti dalle leggi relative agli impiegati dello Stato.

Art. 37. Concorsi per posizioni di carattere tecnico o amministrativo

1. In relazione a specifiche posizioni concernenti attività di natura tecnica ed amministrativa, necessarie al funzionamento dell'Autorità, ma non rientranti nella sua ordinaria attività istituzionale, possono essere banditi concorsi per funzionari con particolari requisiti di ammissione, da individuare in relazione alle attività da svolgere ed alle posizioni da ricoprire.
2. I requisiti di partecipazione sono individuati nel bando di concorso avuto riguardo, per quanto concerne le anzianità di servizio, a quelle previste nell'art. 35. Nel bando sono indicati il tipo di laurea richiesto, le categorie dei titoli da valutare e la ripartizione dei punteggi fra i titoli e le prove previste.

3. I concorsi si svolgono per titoli ed esami. Le prove consistono in:

a) una prova scritta nelle materie individuate nel bando di concorso;
b) una prova pratica diretta ad accertare l'attitudine dei concorrenti alla corretta soluzione, sotto il profilo della legittimità e dell'efficienza, di questioni e problemi attinenti alle materie relative alla specifica posizione a concorso, in relazione alle esigenze organizzative connesse all'attività istituzionale dell'Autorità;
c) una prova orale consistente in un colloquio finalizzato ad un'adeguata valutazione della personalità del candidato, della sua preparazione e capacità professionali, avuto riguardo alle attività ed alle funzioni a concorso. Le materie oggetto del colloquio sono specificate nel bando di concorso. Tra i titoli rivestono carattere preferenziale le esperienze professionali svolte in relazione all'attività richiesta.

4. Valgono, in quanto applicabili, i titoli di preferenza previsti dalle leggi relative agli impiegati dello Stato.

Sezione III - Valutazione e progressione economica

Art. 38. Rapporto valutativo annuale

1. Per ciascun dipendente è effettuata ogni anno una valutazione che tiene conto della qualità del lavoro prestato, dei risultati raggiunti, della preparazione, dell'osservanza dei doveri d'ufficio, dell'attitudine ad assumere maggiori responsabilità, nonché delle competenze dimostrate nell'espletamento degli incarichi conferiti.

2. La valutazione si svolge con le modalità previste all'art. 31.

Art. 39. Progressione economica del personale direttivo

1. La progressione del personale direttivo si effettua mediante scatti annuali secondo le tabelle allegate, salvo giudizio di insufficienza.

2. Il personale direttivo è valutato ogni anno. Con cadenza biennale nel mese di luglio ha luogo un procedimento di valutazione per l'attribuzione di progressioni sino ad un massimo di tre scatti per il 50% dei funzionari in servizio. Le progressioni sono conferite, ai fini normativi ed economici, con decorrenza dal 1° agosto successivo. Le progressioni sono attribuite in relazione alle disponibilità di bilancio.

Sezione IV - Trattamento economico

Art. 40. Trattamento economico del personale direttivo

1. Il trattamento economico del personale direttivo è composto dalle seguenti voci:
a) retribuzione di livello;
b) retribuzione di risultato;
c) retribuzione di posizione, per i responsabili di articolazioni interne ai dipartimenti ed ai servizi e di particolari posizioni organizzative;
d) eventuale assegno *ad personam* di cui al comma 6.

2. La retribuzione di livello è determinata secondo l'allegata tabella 2.

3. La retribuzione di risultato di cui al comma 1, lettera b), è attribuita sulla base dei risultati raggiunti dal funzionario a fronte degli obiettivi programmati in ciascun anno.

4. È istituito un fondo per la qualità della prestazione individuale. Il fondo può essere incrementato dall'Autorità, tenuto conto delle disponibilità di bilancio. La misura e le modalità di erogazione della retribuzione di risultato sono stabilite annualmente con deliberazione del Garante.

5. I funzionari cui sia affidata la responsabilità di articolazioni interne ai dipartimenti e ai servizi o cui siano attribuite particolari funzioni, godono, per la durata dell'incarico, di una retribuzione di posizione, determinata con deliberazione del Garante, nel limite del 15% della retribuzione tabellare prevista per il relativo livello, in relazione all'effettiva responsabilità e alla natura e complessità della funzione svolta.

6. Nel caso di conseguimento della qualifica di funzionario da parte di personale operativo con trattamento economico superiore a quello spettante nella nuova posizione è attribuito un assegno *ad personam* pensionabile e riassorbibile pari alla differenza tra il trattamento economico in godimento all'atto del passaggio e quello spettante nella nuova posizione.

Capo III - Area operativa

Sezione I - Funzioni

Art. 41. Personale operativo

1. Il personale operativo:

a) svolge compiti amministrativi e di segreteria, di analisi, programmazione ed amministrazione di dati, specie su supporti magnetici, di gestione del sistema informativo e della biblioteca;
b) disimpegna altresì compiti di classificazione, archiviazione, protocollo, registrazione, copia, dattilografia e stenografia;
c) svolge altri compiti ad esso specificamente assegnati.
2. Il personale operativo può coadiuvare nell'attività di verbalizzazione e far parte, con funzioni tecniche o in qualità di segretario, di commissioni e di comitati.

3. Il personale operativo può collaborare ad adempimenti operativi connessi ad attività di studio, ricerca e di elaborazione dei dati.

Sezione II - Procedure selettive

Art. 42. Procedure selettive per l'area operativa. Requisiti

1. Possono partecipare alle procedure selettive per l'area operativa coloro i quali siano in possesso, oltre che dei requisiti generali per l'ammissione alle procedure di reclutamento previsti nell'art. 6, di diploma di scuola secondaria di secondo grado e di almeno uno dei seguenti requisiti:

a) abbiano svolto per almeno tre anni attività in posizioni corrispondenti a quelle per le quali è bandito il concorso in uffici pubblici o privati;

b) abbiano prestato servizio presso l'Autorità con analoghe funzioni per almeno due anni con contratto a tempo determinato, ovvero in posizione di comando o di collocamento fuori ruolo;

c) per il personale della carriera esecutiva costituisce requisito di partecipazione alla procedura selettiva, per il livello iniziale della carriera operativa, il possesso, da almeno quattro anni, di un diploma di scuola secondaria di secondo grado congiuntamente all'aver prestato servizio nel ruolo da almeno sei anni.

2. Le procedure selettive per l'area operativa sono indette, di norma, per il livello stipendiale iniziale della fascia "D" della corrispondente tabella allegata. L'Autorità può bandire procedure selettive per la carriera operativa anche per fasce e/o livelli diversi dall'iniziale, qualora le competenze richieste non possano essere individuate fra il personale dell'Autorità. I requisiti di partecipazione sono individuati nei relativi bandi di concorso.

Art. 43. Procedure selettive per l'area operativa: titoli ed esami

1. Le procedure selettive per il livello iniziale della fascia "D" della carriera operativa si svolgono per titoli, una prova pratica, una prova scritta ed un colloquio valutativo vertente sulle discipline concernenti le attribuzioni dell'Autorità.

2. I titoli sono costituiti dal voto del diploma di scuola secondaria di secondo grado, dall'eventuale diploma di laurea e dalla relativa votazione.

3. Il contenuto delle prove pratica e scritta è stabilito nel bando di selezione. Il colloquio è diretto alla valutazione della preparazione del candidato in ordine all'espletamento dei compiti previsti nel bando di concorso e del grado di conoscenza di almeno una lingua straniera.

4. La valutazione dei titoli precede le prove d'esame. La procedura preselettiva, ove prevista, precede la valutazione dei titoli e le prove di esame.

Sezione III - Trattamento economico

Art. 44. Trattamento economico del personale operativo

1. Il trattamento economico del personale operativo è composto dalle seguenti voci:

a) retribuzione stipendiale;
b) premio annuale individuale.

2. Il trattamento economico è articolato in quattro fasce retributive suddivise in livelli stipendiali, secondo l'allegata tabella.

3. La retribuzione corrispondente al livello iniziale di ogni fascia e le relative progressioni retributive sono determinate secondo l'allegata tabella 3.

4. È istituito un fondo per il premio individuale annuale nella misura stabilita annualmente con deliberazione del Garante.

Sezione IV - Valutazione e progressione economica

Art. 45. Rapporto valutativo annuale

1. Per ciascun dipendente è effettuata ogni anno una valutazione che tiene conto della qualità del lavoro prestato, dei risultati ottenuti, della preparazione, dell'osservanza dei doveri d'ufficio, nonché della possibilità di utilizzo in altre unità organizzative.

2. La valutazione si svolge con le modalità previste all'art. 31.

Art. 46. Progressione economica

1. La progressione economica avviene da un livello all'altro di ciascuna fascia retributiva ed attraverso il passaggio alla fascia superiore.

2. La progressione da un livello all'altro avviene in ragione dell'attribuzione di un livello per ciascun anno di servizio. I dipendenti pervenuti al terzo livello di una fascia retributiva e che sulla base della valutazione relativa agli ultimi due anni si collochino nel primo 20% della graduatoria del personale dell'area, non interessato dai passaggi e dalle progressioni di cui ai commi 3 e 5 del presente articolo, possono ottenere la progressione al quinto livello della fascia di appartenenza.

3. I passaggi alle fasce retributive superiori hanno luogo, a seguito di scrutinio per valutazione comparativa, tra i dipendenti collocati almeno al sesto livello della fascia retributiva di appartenenza; i passaggi sono disposti, ogni anno, in misura non eccedente il 20% dei dipendenti sottoposti allo scrutinio. I dipendenti scrutinati, con esito positivo, per il passaggio alla fascia superiore, sono collocati nel livello stipendiale immediatamente più elevato rispetto alla retribuzione in godimento all'atto del passaggio.

4. Il personale pervenuto all'ultimo livello di una fascia è collocato al livello stipendiale della fascia superiore immediatamente più elevato rispetto alla retribuzione in godimento.

5. I dipendenti dell'ultima fascia retributiva, pervenuti al sesto livello e che sulla base della valutazione relativa agli ultimi due periodi, si collochino nel primo 20% della graduatoria del personale della carriera, possono ottenere la progressione di due livelli. Ulteriori progressioni di due livelli possono essere disposte, al termine di ogni quinquennio di servizio, in relazione al suddetto esito della valutazione.

6. Gli scrutini per valutazione comparativa sono basati sui rapporti valutativi annuali di cui all'art. 45.

7. Le progressioni economiche sono conferite dal Garante, su proposta del segretario generale e sentito il dirigente competente, tenuto conto delle disponibilità di bilancio. Esse decorrono, ai fini giuridici ed economici, dal 1 luglio dell'anno successivo a quello oggetto di valutazione e di scrutinio.

8. I dipendenti cui sia stato attribuito un motivato giudizio di insufficienza nell'ultimo rapporto valutativo, non conseguono avanzamenti.

Capo IV - Area esecutiva

Sezione I - Compiti e assunzioni

Art. 47. Personale esecutivo

1. Il personale esecutivo svolge compiti sussidiari connessi al funzionamento degli uffici; provvede all'apertura ed alla chiusura degli stessi, svolge mansioni di operatore al centralino telefonico, provvede al funzionamento dei telefoni, telefax e telex, delle fotocopiatrici e delle apparecchiature informatiche e telematiche e svolge, all'occorrenza, compiti di anticamera; se munito delle necessarie abilitazioni può essere destinato alla guida degli eventuali veicoli dell'ufficio. è addetto inoltre al presidio di impianti ed apparecchiature di sicurezza. Svolge altri compiti che gli sono specificamente assegnati.

2. Il personale esecutivo, inoltre:

a) collabora alla gestione del magazzino di cancelleria ed al funzionamento della biblioteca;
b) svolge incarichi connessi alla spedizione della corrispondenza, inclusa l'affrancatura, e cura la ricezione della corrispondenza stessa, anche di quella raccomandata ed assicurata;
c) svolge compiti di manutenzione e riparazione di impianti e strutture delle sedi dell'ufficio.

Art. 48. Assunzione nella carriera esecutiva

1. L'assunzione del personale della carriera esecutiva avviene in base all'art.16 della legge 28 febbraio 1987, n. 56, e successive modificazioni ed integrazioni.

2. Il Garante, con propria deliberazione, stabilisce le modalità di svolgimento delle procedure di selezione del personale.

Sezione II - Trattamento economico

Art. 49. Trattamento economico del personale esecutivo

1. Il trattamento economico del personale esecutivo è composto dalle seguenti voci:

a) retribuzione stipendiale;
b) premio annuale individuale.

2. Il trattamento economico è articolato in quattro fasce retributive suddivise in livelli stipendiali come riportato nella tabella allegata.

3. La retribuzione corrispondente al livello iniziale di ciascuna fascia e le relative progressioni retributive sono determinate secondo l'allegata tabella 4.

4. È istituito un fondo per il premio annuale individuale nella misura stabilita annualmente con deliberazione del Garante.

Sezione III - Valutazione e progressione economica

Art. 50. Rapporto valutativo annuale

1. Per ciascun dipendente è effettuata ogni anno una valutazione che tiene conto della qualità del lavoro prestato, dei risultati ottenuti, della preparazione, dell'osservanza dei doveri d'ufficio, nonché della possibilità di utilizzo in altre unità organizzative.

2. Il procedimento per la valutazione si svolge con le modalità previste all'art. 31.

Art. 51. Progressione del personale esecutivo

1. La progressione del personale esecutivo avviene da un livello all'altro di ciascuna fascia retributiva ed attraverso il passaggio alla fascia superiore.

2. La progressione da un livello all'altro avviene in ragione dell'attribuzione di un livello per ciascun anno di servizio. I dipendenti pervenuti al terzo livello di una fascia retributiva e che sulla base della valutazione relativa agli ultimi due anni, si collochino nel primo 20% della graduatoria del personale dell'area, possono ottenere la progressione al quinto livello della fascia di appartenenza.
3. I passaggi alle fasce retributive superiori hanno luogo, a seguito di scrutinio per valutazione comparativa, tra i dipendenti collocati almeno al sesto livello della fascia retributiva di appartenenza; i passaggi sono disposti, ogni anno, in misura non eccedente il 20% dei dipendenti sottoposti allo scrutinio. I dipendenti scrutinati con esito positivo, per il passaggio alla fascia superiore, sono collocati nel livello

stipendiale immediatamente più elevato rispetto alla retribuzione in godimento all'atto del passaggio.

4. Il personale pervenuto all'ultimo livello di una fascia è collocato al livello stipendiale della fascia superiore immediatamente più elevato rispetto alla retribuzione in godimento.

5. I dipendenti dell'ultima fascia retributiva, pervenuti al sesto livello e che sulla base della valutazione relativa agli ultimi due periodi, si collochino nel primo 20% della graduatoria del personale dell'area, possono ottenere la progressione di due livelli.
Ulteriori progressioni di due livelli possono essere disposte, al termine di ogni quinquennio di servizio, in relazione al suddetto esito della valutazione.

6. Gli scrutini per valutazione comparativa sono basati sui rapporti valutativi annuali di cui all'art. 50.

7. Le progressioni economiche sono conferite dal Garante, su proposta del segretario generale e sentito il dirigente competente, tenuto conto delle disponibilità di bilancio. Esse decorrono, ai fini giuridici ed economici, dal 1 luglio dell'anno successivo a quello oggetto di valutazione e di scrutinio. Ai dipendenti cui è stato attribuito un motivato giudizio di insufficienza nell'ultimo rapporto valutativo, non sono riconosciuti avanzamenti.

TITOLO III - Personale non di ruolo

Capo I - Personale a contratto

Art. 52. Personale a contratto

1. L'Autorità si avvale di personale a contratto per consentire la specializzazione di giovani laureati nei settori di interesse dell'Autorità, ovvero per acquisire particolari esperienze o competenze anche in relazione a specifici settori o campi di attività individuati dal Garante con propria deliberazione, con la quale si provvede anche a definire il trattamento giuridico ed economico del predetto personale e le condizioni della sua utilizzazione.

2. Salvo quanto previsto all'art. 54, la durata massima dei rapporti di lavoro a tempo determinato è stabilita in due anni, rinnovabili per non più di due volte.

3. All'atto della cessazione del rapporto, a qualunque titolo, è corrisposto al personale a contratto un numero di mensilità pari agli anni di servizio prestato, o frazione di anno superiore ai sei mesi.

4. Non si applicano al personale a contratto le disposizioni concernenti la retribuzione di risultato ed i premi annuali individuali, nonché quelle sulle progressioni economiche. Al predetto personale compete, in base all'area di appartenenza, uno scatto ovvero un livello per ciascun anno di servizio, qualora non sia stato attribuito un motivato giudizio di insufficienza nell'ultimo rapporto valutativo.

Capo II - Personale fuori ruolo, esperti e tirocinio

Art. 53. Disciplina economica e destinazione del personale comandato e fuori ruolo

1. Ai dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici in posizione di fuori ruolo, ovvero in aspettativa ai sensi dell'art.13 del decreto del Presidente della Repubblica 11 luglio 1980 n. 382, e successive modificazioni ed integrazioni, o al personale comunque comandato presso l'Autorità è corrisposta una indennità pari al 50% della retribuzione in godimento, con esclusione dell'indennità integrativa speciale; qualora detto trattamento economico risulti inferiore a quello spettante al corrispondente personale di ruolo è corrisposta una ulteriore indennità perequativa in conformità a quanto previsto dall'art.33, comma 1-bis, della legge 31 dicembre 1996, n. 675, introdotto dall'art.1, comma 2, del decreto legislativo 26 febbraio 1999, n. 51.

Art. 54. Nomina di esperti e collaboratori esterni

1. In applicazione dell'art.33, comma 4, della legge 31 dicembre 1996, n. 675, come modificato dall'art.2, comma 4, del decreto legislativo 26 febbraio 1999, n. 51, l'Autorità può avvalersi di liberi professionisti, di dipendenti pubblici o di esperti di qualificata esperienza nei limiti e alle condizioni previsti dalle rispettive norme di stato giuridico, nonché di persone giuridiche pubbliche e private e di associazioni. Tali incarichi, della durata massima di due anni, possono essere rinnovati per non più di due volte. Per le prestazioni professionali non a carattere continuativo provvede il segretario generale.

2. I compensi per i consulenti iscritti ad albi professionali sono corrisposti, anche nei modi previsti per i servizi in economia, sulla base delle tariffe minime stabilite per le relative categorie professionali, mentre per gli altri professionisti o per i dipendenti pubblici i compensi sono stabiliti di volta in volta dal segretario generale, in rapporto alla durata e alla rilevanza delle prestazioni, secondo i criteri stabiliti nell'apposito tariffario preventivamente approvato dal Garante, da richiamarsi nel relativo disciplinare.

3. L'Autorità può avvalersi dell'opera di consulenti assunti con contratto a tempo determinato, di durata non superiore a due anni, rinnovabile per non più di due volte, nel quale è stabilita la durata della prestazione e l'ammontare del compenso, sulla base dei criteri di cui al comma 2.

Art. 55. Disciplina del tirocinio

1. L'Autorità può avvalersi della collaborazione di giovani laureati per una esperienza temporanea di stage non superiore ad un anno nelle discipline attinenti alle materie di interesse dell'Autorità, anche sulla base di apposite convenzioni con università, enti ed istituti di ricerca.

2. Il periodo di tirocinio è gratuito e non rappresenta titolo di servizio per la partecipazione ai concorsi indetti dall'Autorità.

TITOLO IV - Cessazione del rapporto d'impiego

Capo I - Disposizioni generali

Art. 56. Cessazione dal servizio

1. Il personale che cessa dal servizio ha titolo al trattamento spettante fino al giorno della effettiva cessazione; il trattamento precedentemente goduto dal dipendente deceduto viene corrisposto integralmente per l'ultimo mese e per quello successivo a favore del coniuge e dei figli minori.

Art. 57. Trattamento di quiescenza e previdenza

1. Il trattamento di quiescenza e previdenza è definito dal relativo regolamento, approvato dall'Autorità, in base ai criteri fissati dal contratto collettivo di lavoro in vigore per il personale dipendente dall'Autorità per le garanzie nelle comunicazioni.

Capo II - Cause estintive

Art. 58. Cause estintive del rapporto d'impiego

1. Il rapporto d'impiego, oltre che per le cause indicate nei titoli precedenti, si estingue per:

a) collocamento in quiescenza;
b) dimissioni volontarie;
c) inabilità riconosciuta a domanda;
d) dispensa dal servizio;
e) licenziamento.

Art. 59. Collocamento a riposo d'ufficio

1. Il dipendente che abbia compiuto 65 anni di età è collocato a riposo d'ufficio, qualora non presenti istanza per permanere in servizio per un ulteriore biennio.

2. I provvedimenti di collocamento a riposo sono adottati dall'Autorità e hanno effetto dal giorno del raggiungimento del limite di età o di servizio.

Art. 60. Dimissioni volontarie

1. Le dimissioni volontarie debbono essere presentate per iscritto alla Autorità, la quale provvede in merito entro trenta giorni. Il dipendente è tenuto a rimanere in servizio sino a quando non gli sia stata comunicata l'accettazione delle dimissioni stesse.

2. L'accettazione può essere ritardata, per gravi motivi di servizio, per un periodo non superiore a trenta giorni.

Art. 61. Cessazione a domanda per inabilità

1. Il dipendente che per infermità, difetti fisici o altri motivi di salute, non sia più in grado di adempiere ai propri compiti può chiedere di cessare dal servizio per inabilità.

2. L'accertamento delle condizioni anzidette è effettuato secondo le modalità previste, a norma di legge, per gli impiegati civili dello Stato.

3. I dipendenti cessati dal servizio, perché riconosciuti inabili, possono essere riammessi in servizio, a domanda, qualora venga accertata la cessazione della causa che ne aveva determinato il collocamento a riposo. La riammissione in servizio dà diritto alla normale retribuzione, restando assorbita ogni altra indennità relativa alla cessazione del servizio già percepita; ai restanti effetti il periodo di lavoro anteriore e quello successivo alla cessazione sono unificati.

Art. 62. Dispensa dal servizio

1. Con delibera dell'Autorità, sentito il segretario generale, è dispensato dal servizio il dipendente che:

a) trascorso il termine massimo riguardante l'aspettativa per motivi di salute, non sia riconosciuto idoneo a riprendere servizio a seguito degli accertamenti sanitari disposti a norma di legge;
b) abbia riportato un giudizio di insufficienza negli ultimi due rapporti valutativi annuali.

Art. 63. Licenziamento

1. Con delibera dell'Autorità, sentito il segretario generale, è licenziato, sulla base del procedimento di cui all'art. 25, il dipendente che:

a) abbia compiuto un'azione di gravità tale da non consentire la prosecuzione del rapporto di lavoro;
b) abbia dimostrato grave negligenza nell'assolvimento dei propri compiti in modo reiterato o continuo ovvero abbia violato i doveri prescritti nei precedenti articoli 8 e 9.

2. Il dipendente che abbia riportato condanna penale può essere licenziato solo al termine del procedimento di cui all'art. 9, comma 2, della legge 7 febbraio 1990, n. 19.

TITOLO V - Disposizioni transitorie e inquadramento del personale

Art. 64. Inquadramento nel ruolo organico

1. Il ruolo organico dell'Ufficio è articolato secondo quanto previsto nella tabella 5.

2. In sede di prima applicazione del presente regolamento, il personale in posizione di fuori ruolo o di comando dalle amministrazioni di appartenenza in servizio alla data di entrata in vigore della presente

disposizione e che non abbia demeritato, è inquadrato, a domanda, con immediato trasferimento nel ruolo organico sulla base dell'allegata tabella di corrispondenza n. 6. La domanda deve pervenire entro quindici giorni dalla medesima data e l'inquadramento è effettuato dal Garante su proposta del segretario generale, non oltre i trenta giorni successivi. L'inquadramento è modificato in caso di mutamento, con riferimento al momento dell'inquadramento stesso, delle situazioni giuridiche riconosciute all'interessato nella amministrazione di appartenenza.

3. Coloro che non presentano la domanda di cui al comma 1 rimangono in servizio temporaneamente, compatibilmente con le esigenze dell'ufficio, fermi restando gli incarichi di cui all'art.11 del regolamento sull'organizzazione e il funzionamento dell'Ufficio.

4. In sede di inquadramento in ruolo, si procede all'attribuzione al personale che non abbia demeritato di un numero di scatti o livelli corrispondenti agli anni o frazione di anno pari o superiore a sei mesi di servizio prestato presso l'ufficio.

5. Ai soli fini dell'applicazione del presente articolo, in sede di inquadramento in ruolo, a riconoscimento della professionalità maturata, oltre a quanto previsto dal comma 4, si procede all'attribuzione al personale che non abbia demeritato di uno scatto per ciascun quadriennio, o frazione di esso pari o superiore al biennio, di anzianità maturata presso amministrazioni pubbliche prima del collocamento fuori ruolo o del comando presso l'ufficio, nelle qualifiche della carriera corrispondente a quella considerata per l'inquadramento.

Art. 65. Accesso alle aree

1. In sede di prima applicazione del presente regolamento, allo scopo di consentire la continuità delle attività istituzionali del Garante, l'accesso alle aree è disciplinato nel modo seguente:

a) entro trenta giorni dall'inquadramento in ruolo ai sensi dell'art. 64, il Garante bandisce, per la copertura della metà dei posti vacanti della qualifica di dirigente, un concorso per titoli di servizio professionali e di cultura integrato da una prova individuata nel bando. Al concorso sono ammessi a partecipare i dipendenti, provenienti dalla ex carriera direttiva o comunque dall'area "c" individuata dal contratto collettivo nazionale di lavoro del comparto ministeri del 16 febbraio 1999, pubblicata nella Gazzetta Ufficiale, supplemento ordinario, del 25 febbraio 1999, n. 46 e in possesso di diploma di laurea che abbiano maturato un'anzianità di almeno quattro anni nella carriera medesima, di cui almeno uno maturato presso l'Autorità, e che non abbiano demeritato. Il bando definisce la composizione della commissione esaminatrice e determina i criteri per la valutazione dei titoli preferenziali e le materie d'esame;

b) entro trenta giorni dall'inquadramento in ruolo ai sensi dell'art. 64, il Garante bandisce, per la copertura fino al limite massimo della metà dei posti vacanti delle qualifiche di funzionario e di impiegato operativo, un concorso per titoli di servizio professionali e di cultura integrato da una prova individuata nel bando. Al concorso sono ammessi a partecipare i dipendenti in possesso dei titoli di studio prescritti agli articoli 35 e 42 che abbiano maturato un'anzianità di almeno tre anni nelle qualifiche corrispondenti a quella immediatamente inferiore, di cui almeno uno presso l'Autorità, e che non abbiano demeritato. Il bando definisce la composizione della commissione esaminatrice e determina i criteri per la valutazione dei titoli e le materie d'esame. Nel bando possono essere altresì individuati particolari profili professionali per i quali sono ammessi a partecipare dipendenti anche non in possesso dei predetti titoli e che abbiano maturato un'anzianità di almeno venti anni nelle citate qualifiche.

2. Ai vincitori dei concorsi di cui al comma 1, è riconosciuto un numero di scatti o livelli corrispondenti a quelli attribuiti ai sensi dell'art. 64, comma 4.

Art. 66. Relazioni sindacali

1. Entro novanta giorni dalla data di entrata in vigore del presente regolamento, il Garante concorda con le organizzazioni sindacali del personale un protocollo per le relazioni collettive che, in applicazione dei principi e delle norme vigenti in materia, disciplini l'informazione e la consultazione delle organizzazioni rappresentative del personale in tema di rapporto di lavoro, di trattamento giuridico ed economico del personale anche per quanto riguarda la progressione economica e di carriera, e di eventuali modifiche del presente regolamento nelle parti corrispondenti.

Art. 67. Entrata in vigore

Il presente regolamento entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica. Le disposizioni del presente titolo V entrano in vigore il giorno successivo alla data della medesima pubblicazione.

REGOLAMENTO N. 3 DEL 28 GIUGNO 2000 - CONCERNENTE LA GESTIONE AMMINISTRATIVA E LA CONTABILITÀ (*)

104

Deliberazione del 28 giugno 2000

Capo I - Definizioni e principi generali

Art. 1. Definizioni

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675, di seguito denominata "legge". Ai medesimi fini, si intende altresì:
a) per "Garante", l'organo collegiale istituito ai sensi dell'art. 30 della legge;
b) per "presidente", il presidente del Garante;
c) per "componenti", i componenti del Garante;
d) per "Ufficio", l'Ufficio del Garante.

Art. 2. Principi generali

1. La gestione dell'Ufficio è informata ai principi generali della contabilità finanziaria, economica e patrimoniale e risponde ai requisiti della veridicità, pubblicità e trasparenza, nonché del pareggio, dell'universalità, annualità, continuità, prudenza e unità.

2. L'attività finanziaria dell'Ufficio si realizza sulla base della programmazione della spesa e della prudente valutazione delle entrate, attraverso distinte funzioni-obiettivo corrispondenti a unità organizzative per la gestione delle risorse assegnate, le quali possono essere ulteriormente articolate in centri di costo.

Capo II - Bilancio

Art. 3. Esercizio finanziario e bilancio di previsione

1. L'esercizio finanziario ha la durata di un anno e coincide con l'anno solare.

2. La gestione finanziaria si svolge in base al bilancio annuale di previsione, redatto in termini di competenza.

3. Lo schema del bilancio e del documento programmatico che lo accompagna sono predisposti dal dipartimento amministrazione e contabilità entro il 15 ottobre e sono sottoposti al Garante per l'approvazione entro il 31 ottobre.

4. In caso di ritardo nell'approvazione, il Garante può deliberare l'esercizio provvisorio fino ad un massimo di quattro mesi, sulla base di un dodicesimo per mese degli stanziamenti previsti nello schema predisposto o, in mancanza, nel bilancio del precedente esercizio.

Art. 4. - Struttura del bilancio

1. Il bilancio di previsione è costituito:
a) dal preventivo finanziario delle entrate per provenienza e delle spese per destinazione ripartite per funzioni istituzionali;

(*) Pubblicato in G.U. Serie generale n. 162 del 13 luglio 2000.

b) dal prospetto di ripartizione delle entrate e delle spese, articolato in titoli, categorie e capitoli.
2. Il bilancio di previsione è accompagnato dai seguenti allegati:

a) dal documento programmatico;
b) dalla tabella dimostrativa dell'avanzo o disavanzo di amministrazione presunto;
c) da una relazione che indica i criteri seguiti per la predisposizione del bilancio ed altre notizie utili sulla gestione.

Art. 5. Criteri di formazione del bilancio

1. Il bilancio di previsione è formulato in termini di competenza. Entro il 15 settembre dell'esercizio precedente, i dirigenti rappresentano le esigenze funzionali dei dipartimenti e dei servizi al segretario generale, che ne valuta preliminarmente la compatibilità in rapporto agli obiettivi e ai programmi da realizzare, indicati dal Garante per l'anno di riferimento.

2. Nelle entrate confluiscono le somme percepite a titolo di pagamento dei diritti di segreteria ai sensi dell'art. 33, commi 1-*quater* e 3 della legge 31 dicembre 1996, n. 675, nonché le somme pari al cinquanta per cento dei proventi delle sanzioni amministrative ai sensi dell'art. 39, comma 3, della medesima legge, o percepite a qualunque altro titolo in base alle leggi e ai regolamenti.

3. Nel bilancio di previsione è iscritto come posta a sé stante, rispettivamente, delle entrate o delle spese, l'avanzo o il disavanzo di amministrazione presunto al 31 dicembre dell'esercizio precedente a quello al quale il bilancio si riferisce. L'avanzo può essere utilizzato per il raggiungimento del pareggio del bilancio. Il disavanzo è iscritto come prima posta delle uscite per il relativo riassorbimento.

Art. 6. Variazioni di bilancio, assestamento e fondo di riserva

1. Nell'ambito della medesima funzione istituzionale le variazioni compensative tra i capitoli assegnati vengono disposte dal dirigente del dipartimento o servizio e comunicate al dipartimento amministrazione e contabilità.

2. Le altre variazioni di bilancio sono deliberate dal Garante, di regola entro il 31 ottobre dell'anno cui il bilancio si riferisce.

3. I provvedimenti di variazione sono riportati in un quadro riepilogativo sintetico.

4. Nel bilancio di previsione è iscritto un fondo di riserva per le spese impreviste, il cui ammontare non può superare il tre per cento delle spese correnti previste. Su detto fondo non possono essere assunti impegni ed emessi mandati di pagamento.

5. Contestualmente all'approvazione del conto consuntivo il Garante delibera l'assestamento del bilancio per l'esercizio in corso.

6. Le variazioni per nuove e maggiori spese possono essere proposte solo se è assicurata la necessaria copertura finanziaria.

Art. 7. Bilancio consuntivo

1. Il bilancio consuntivo si compone del rendiconto finanziario, della situazione patrimoniale e del conto economico.

2. Il bilancio consuntivo è predisposto dal dipartimento amministrazione e contabilità ed è accompagnato da una relazione del segretario generale che evidenzia i risultati della gestione finanziaria. Il segretario generale presenta il bilancio consuntivo al Garante entro il 31 marzo dell'anno successivo all'esercizio finanziario, per la sua approvazione entro il 30 aprile.

3. Il bilancio consuntivo è trasmesso nei successivi trenta giorni alla Corte dei conti, ai sensi dell'art. 33, comma 2 della legge.

Capo III - Entrate

Art. 8. Accertamento e riscossione delle entrate

1. L'entrata è accertata quando il segretario generale, appurata la ragione del credito ed il soggetto debitore, iscrive l'ammontare del credito come competenza dell'esercizio finanziario o di altro successivo, a seconda della sua scadenza.

2. L'accertamento di entrata dà luogo ad annotazione nelle scritture con imputazione al competente capitolo di entrata.

3. Le entrate sono riscosse dall'istituto di credito che gestisce il servizio di cassa, sulla base di apposita convenzione, mediante reversali di incasso firmate dal segretario generale o, su sua delega, dal dirigente del dipartimento amministrazione e contabilità, e contenenti le seguenti indicazioni: esercizio finanziario, capitolo, nome e cognome o ragione sociale del debitore, causale, importo in cifre e in lettere, data di emissione.

Art. 9. Gestione delle spese

1. La gestione delle spese segue le fasi dell'assunzione degli impegni, della liquidazione e del pagamento.

2. L'impegno determina, sulla base di obbligazioni giuridicamente perfezionate, l'importo della spesa, il destinatario e l'imputazione di bilancio. Per le spese pluriennali possono essere presi impegni di spesa sugli esercizi successivi.

3. Gli impegni di spesa sono assunti dal segretario generale e dai responsabili delle funzioni-obiettivo nei limiti di spesa ad essi assegnati.

4. Tutti gli impegni di spesa sono trasmessi senza ritardo al dipartimento amministrazione e contabilità e da questo registrati progressivamente, previa verifica della relativa regolarità amministrativa e contabile, in particolare per quanto riguarda l'assunzione dell'impegno di spesa da parte del competente dirigente, la corretta imputazione al capitolo di spesa dell'esercizio di pertinenza e la disponibilità finanziaria.

5. Le spese per l'affidamento di studi, ricerche, consulenza e prestazioni professionali, di cui all'art. 54 del regolamento concernente il trattamento giuridico ed economico del personale, se a carattere continuativo, sono impegnate dal Garante, negli altri casi dal segretario generale.

6. Con l'approvazione del bilancio e delle successive variazioni, si costituisce automaticamente l'impegno sui relativi stanziamenti per le seguenti spese:

a) per le indennità spettanti al presidente e ai componenti, per il trattamento economico fondamentale e accessorio del segretario generale e del personale dipendente, nonché per i relativi oneri riflessi;
b) per i trattamenti di quiescenza e previdenza;
c) per i canoni anche di locazione e per le imposte;
d) per le spese puntualmente determinate, dovute in base a contratti o a disposizioni di legge o di regolamento.

7. La liquidazione della spesa, consistente nella determinazione dell'esatto ammontare dovuto e del soggetto creditore, e l'emissione dell'ordine di pagamento sono effettuate dal dipartimento amministrazione e contabilità, previo accertamento della regolarità della fornitura o della prestazione e della sua rispondenza ai termini e alle condizioni pattuite effettuata a cura del dirigente del dipartimento o del servizio interessato e del dirigente del dipartimento contratti e risorse finanziarie.

8. Il dispositivo di liquidazione con i documenti giustificativi di spesa deve essere allegato al mandato di pagamento estinto dall'istituto cassiere.

9. I mandati di pagamento devono contenere almeno i seguenti elementi:
a) dati anagrafici del creditore;
b) importo dovuto in cifre e lettere, data di emissione e eventuale data di valuta;

c) modalità di pagamento del titolo che su richiesta del creditore può essere estinto mediante accreditamento in c/c bancario o postale, mediante vaglia postale ed assegno circolare non trasferibile.

10. Gli ordini di pagamento, previa verifica della regolarità della spesa, sono firmati dal segretario generale, ovvero dal responsabile del dipartimento amministrazione e contabilità o da un suo delegato.

Art. 10. Spese di rappresentanza

1. Sono spese di rappresentanza quelle fondate sulla esigenza del Garante e dell'ufficio di manifestarsi all'esterno e di intrattenere pubbliche relazioni con soggetti ad esso estranei in rapporto ai propri fini istituzionali. Le spese di rappresentanza sono disposte dal presidente e dal segretario generale e sono a carico dell'apposito capitolo di bilancio. Sono da considerare comunque spese di rappresentanza:

a) colazioni e consumazioni in occasione di particolari riunioni, convegni, seminari o incontri di lavoro con personalità o autorità estranee al Garante o in occasione di visite;
b) omaggi floreali, biglietti augurali, inviti o altre forme di partecipazione ad eventi significativi, organizzazione di cerimonie;
c) cerimonie di apertura di nuove sedi (stampa di inviti, affitto locali, addobbi ed impianti vari, servizi fotografici, eventuali rinfreschi);
d) piccoli doni, quali targhe, medaglie, libri, coppe, oggetti simbolici ad autorità, personalità o esperti italiani o stranieri o a membri di delegazioni straniere in visita al Garante oppure in occasione di visite e riunioni all'estero compiute da rappresentanti o delegazioni ufficiali del Garante e dell'ufficio;
e) servizi fotografici e stampe in occasione di relazioni pubbliche.

Capo IV - Rilevazione dei risultati della gestione finanziaria

Art. 11. Rilevazioni delle economie di bilancio e dei residui attivi e passivi alla chiusura dell'esercizio

1. Le somme iscritte tra le entrate di competenza e non accertate entro il termine dell'esercizio costituiscono minori accertamenti rispetto alle previsioni.

2. La differenza tra le somme stanziate e quelle impegnate costituisce economia di bilancio. Costituiscono economie, altresì, le minori spese sostenute rispetto all'impegno assunto, verificate con la conclusione della fase di ultima liquidazione.

3. Le entrate accertate e non riscosse costituiscono residui attivi, i quali sono compresi tra le attività patrimoniali.

4. Le spese impegnate e non pagate entro il termine dell'esercizio costituiscono residui passivi, i quali sono compresi tra le passività patrimoniali.

Art. 12. Eliminazione dei residui attivi e passivi

1. Annualmente è compilata alla chiusura dell'esercizio la situazione dei residui attivi e passivi distintamente per esercizio di provenienza e per capitolo.

2. I residui attivi possono essere ridotti o eliminati dopo che siano stati esperiti tutti gli atti per ottenerne la riscossione, salvo che il relativo costo non superi l'importo da recuperare e, comunque, per somme inferiori a lire 100.000 (euro 51,64).

3. I residui passivi sono eliminati per insussistenza del titolo giuridico.

Art. 13. Determinazione del risultato economico dell'esercizio

1. Ai fini della determinazione del risultato economico dell'esercizio si tiene conto dei seguenti elementi:
a) la determinazione delle quote di ammortamento dei beni di cui all'art. 18;
b) la rilevazione della quota di accantonamento del trattamento di fine rapporto;

c) la rilevazione delle eventuali quote di accantonamento dei fondi rischi;
d) gli accantonamenti per svalutazione dei crediti;
e) il calcolo dei ratei e risconti attivi e passivi;
f) le variazioni intervenute nelle rimanenze.

Art. 14. Fondo interno di cassa

1. Il Garante può deliberare la costituzione di un fondo di cassa interno, di entità non superiore a venti milioni, reintegrabile durante l'esercizio finanziario.

2. Con il fondo si può provvedere al pagamento delle spese minute di ufficio, postali, relative a piccole acquisizioni, riparazioni e manutenzioni di mobili, locali, apparati, attrezzature e altre dotazioni anche informatiche e telematiche ivi comprese carte telefoniche, per l'utilizzazione di veicoli, per i trasporti e le spedizioni, per l'acquisto di giornali e pubblicazioni periodiche, per acconti di spese di viaggio e di missione, per spese di rappresentanza o necessarie per la pubblicazione di bandi od altri avvisi sulle pubblicazioni ufficiali, sulla stampa quotidiana o periodica, o su altri bollettini. Nei casi di urgenza, ove non sia possibile provvedere con gli ordinari ordinativi di pagamento, possono sostenersi altre spese comunque connesse con l'ordinaria gestione dell'ufficio.

3. Il dirigente del dipartimento amministrazione e contabilità può autorizzare il cassiere ad anticipare somme in contanti per l'espletamento di compiti d'ufficio. Il beneficiario delle anticipazioni deve presentare apposita rendicontazione. Ai medesimi fini possono essere acquisite e utilizzate anche carte di credito. Il cassiere imputa le spese sostenute ai diversi stanziamenti di bilancio, sulla base dei rendiconti o degli estratti conto.

4. Il cassiere, nominato dal segretario generale per un biennio rinnovabile fra i dipendenti di ruolo del Garante, con qualifica non inferiore a quella di funzionario, è responsabile delle operazioni di cassa ed accerta la regolarità formale delle determinazioni di pagamento prima di effettuare i pagamenti. Nessun pagamento di importo superiore ad un milione di lire, può essere effettuato senza il visto del responsabile del dipartimento amministrazione e contabilità.

5. Il cassiere presenta ogni trimestre al responsabile del dipartimento amministrazione e contabilità un apposito rendiconto, con i relativi documenti giustificativi, salva la possibilità di autocertificazioni per le spese minute.

Art. 15. Scritture contabili

1. Le scritture finanziarie devono consentire di rilevare la situazione degli accertamenti e degli impegni a fronte delle relative previsioni, nonché delle somme riscosse e pagate e di quelle rimaste da riscuotere e da pagare.

2. Le scritture patrimoniali devono consentire la dimostrazione del valore del patrimonio all'inizio dell'esercizio, le variazioni intervenute nel corso dell'esercizio per effetto della gestione del bilancio, nonché la consistenza del patrimonio alla chiusura dell'esercizio.

3. Le scritture economiche devono consentire la determinazione a consuntivo del risultato economico dell'esercizio.

4. I registri contabili e gli schemi di bilancio sono determinati con deliberazione del Garante.

Art. 16. Gestione patrimoniale

1. Il responsabile del dipartimento amministrazione e contabilità cura la redazione e l'aggiornamento dell'inventario generale e dell'inventario del patrimonio librario, assegna, conserva e garantisce l'uso dei beni, assicura la vigilanza sui soggetti di cui al comma 2.

2. Il dirigente di ciascun dipartimento o servizio o chi ne svolge le funzioni in caso di reggenza, svolge la funzione di conservare i beni mobili dati in dotazione alle unità organizzative.

Art. 17. Criteri di valutazione dei beni patrimoniali

1. Gli immobili sono iscritti nello stato patrimoniale al valore determinato ai sensi dell'art. 52, comma 4, del decreto del Presidente della Repubblica 26 aprile 1986, n. 131, e successive modificazioni o al prezzo di acquisto se maggiore, ivi compresi gli oneri di diretta imputazione.

2. I mobili, gli impianti e i macchinari sono valutati al prezzo di acquisto, ovvero di stima o di mercato se trattasi di oggetti pervenuti ad altro titolo, ivi compresi gli oneri di diretta imputazione.

3. Le immobilizzazioni immateriali sono valutate sulla base dei costi effettivamente sostenuti.

4. Le quote ordinarie di ammortamento sono calcolate in relazione alle aliquote fissate dalla normativa tributaria.

5. I titoli di Stato o garantiti dallo Stato o equiparati per legge sono valutati al valore d'acquisto.

6. I crediti sono valutati sulla base del presumibile valore di realizzo.

7. I debiti sono valutati secondo il valore di estinzione.

8. Le rimanenze sono valutate al costo d'acquisto.

Art. 18. Classificazione dei beni

1. I beni immobili e mobili sono classificati secondo la denominazione attribuita alle immobilizzazioni materiali nello schema di situazione patrimoniale.

2. I singoli beni sono annotati sui registri contabili di cui all'art. 15.

3. Il materiale bibliografico è annotato in apposito registro tenuto a cura del responsabile della biblioteca.

4. La cancellazione dagli inventari dei beni per fuori uso, perdita e cessione è disposta previa acquisizione del verbale di dismissione redatta da una apposita commissione.

Capo V - Attività negoziale

Art. 19. Principi in materia di attività negoziale

1. Ai lavori, agli acquisti, alle alienazioni, alle permute, alle forniture, alle locazioni, comprese quelle finanziarie ed ai servizi in genere, si provvede mediante contratti da stipularsi secondo le norme del presente regolamento, salvo quanto previsto dalla normativa comunitaria e dalla corrispondente normativa nazionale di recepimento, nonché dalla legislazione nazionale sui lavori pubblici.

2. Ai lavori, agli acquisti, alle alienazioni, alle permute, alle forniture, alle locazioni, comprese quelle finanziarie, ed ai servizi in genere si provvede con contratti da stipularsi secondo le procedure e le norme contenute nel presente regolamento.

3. I contratti devono avere termine e durata certi e non possono comunque superare i nove anni salvo i casi di assoluta necessità o di convenienza, da indicare nel relativo atto di decisione a contrattare. Per il medesimo oggetto non possono essere stipulati più contratti, se non per comprovate ragioni di necessità o di convenienza, da indicare nell'atto di decisione a contrattare.

4. La decisione a contrattare da parte del segretario generale o del dirigente deve evidenziare il fine pubblico che si intende perseguire con il contratto, l'oggetto e le clausole essenziali, la procedura prescelta per la scelta del contraente e i criteri di aggiudicazione.

5. Nei contratti sono previste adeguate penalità per inadempienze e ritardi nell'esecuzione dei lavori o delle prestazioni convenute. A garanzia dell'esecuzione dei contratti, le imprese devono prestare

idonea cauzione o fideiussione, nella misura determinata dal contratto. Nei contratti a durata pluriennale o ad esecuzione continuata o periodica, e salvo che nei casi disciplinati espressamente per legge, l'Ufficio può riservarsi la facoltà di rinegoziare i costi a proprio favore, al verificarsi di condizioni od eventi contrattualmente predeterminati. Tale clausola è comunque prevista per l'ipotesi in cui l'originaria congruità dei prezzi, per qualsiasi motivo, venga meno.

6. Fermo restando quanto previsto per legge, l'aggiudicazione o l'affidamento di lavori di particolare complessità sono effettuati sulla base di un progetto esecutivo recante la precisa indicazione del costo complessivo dei lavori. Il costo così definito può essere aumentato solo per causa di forza maggiore o per motivate ragioni tecniche, sempre che detti eventi fossero imprevedibili all'atto della progettazione. In tal caso non possono essere effettuati lavori nuovi o diversi senza il preventivo assenso scritto da parte degli organi competenti all'approvazione dei contratti ai sensi dell'art. 20, comma 1. In ogni caso, l'eventuale incremento dei costi, compresa la revisione dei prezzi, è disciplinato dalle norme vigenti in materia per le amministrazioni dello Stato.

7. Oltre alle anticipazioni consentite per legge, sono ammessi pagamenti in acconto in ragione delle parti di opere realizzate, dei beni forniti e delle prestazioni eseguite. è vietata la corresponsione di interessi e provvigioni a favore dell'appaltatore o dei fornitori sulle somme eventualmente anticipate per l'esecuzione del contratto.

8. È garantito il rispetto del principio della non discriminazione in base alla nazionalità nei confronti dei fornitori appartenenti agli Stati membri dell'Unione europea.

Art. 20. Approvazione e stipulazione dei contratti

1. I contratti sono approvati e sottoscritti dal dirigente responsabile del dipartimento o del servizio per importi inferiori a lire duecento milioni e per importi superiori dal segretario generale su proposta del dirigente stesso.

2. Salvo quanto diversamente disposto per legge, la valutazione della congruità dei prezzi è effettuata dai soggetti competenti all'approvazione dei contratti sulla base del riscontro dei prezzi correnti di mercato. Nei casi di particolare complessità o qualora risulti comunque opportuno, può esser chiesto il parere ad organi tecnici specializzati della pubblica amministrazione o può essere costituita dal segretario generale un'apposita commissione formata da personale interno ed esterno. Il parere di congruità non è richiesto per l'affidamento di studi, ricerche e consulenze. Per i contratti di importo non superiore ai 100 milioni di lire, il parere può essere fornito anche da una commissione permanente composta da personale interno. Ai soli componenti esterni, se presenti, possono essere corrisposti compensi determinati di volta in volta in rapporto alla durata e alla rilevanza delle prestazioni.

3. I contratti sono stipulati di regola nelle forme del diritto privato, anche mediante scambio di corrispondenza secondo l'uso del commercio. La forma dei contratti è in ogni caso quella scritta. Per i contratti stipulati con procedura aperta e procedura ristretta è richiesta la forma pubblica amministrativa, con l'intervento dell'ufficiale rogante designato dal segretario generale fra il personale di ruolo.

Art. 21. Procedure contrattuali

1. Le procedure contrattuali possono essere "aperte" (pubblico incanto), "ristrette" (licitazione privata e appalto concorso) e "negoziate" (trattativa privata).

2. Le gare si svolgono seguendo, di norma, la procedura "ristretta", salvo che si ritenga più vantaggioso il ricorso alla procedura "aperta".

3. Nei casi previsti dall'art. 26 si può procedere mediante il sistema delle spese in economia.

Art. 22. Procedura aperta

1. Nella procedura "aperta" (pubblico incanto) possono presentare offerta tutti i soggetti interessati.

2. I concorrenti devono documentare di possedere i requisiti di partecipazione richiesti dal bando di gara.

Art. 23. Procedura ristretta

1. Nella procedura "ristretta" (licitazione privata e appalto concorso) sono invitati a presentare la propria offerta solo i concorrenti che, avendo presentato domanda di partecipazione alla gara, abbiano dimostrato la propria capacità tecnica, economica e finanziaria ad effettuare la prestazione richiesta. Il bando può prevedere che alcuni requisiti siano comprovati mediante autocertificazione, fermo restando l'obbligo di produrre la relativa documentazione prima dell'eventuale aggiudicazione.

2. La selezione dei concorrenti da invitare alla gara, nell'ambito di coloro che hanno presentato domanda di partecipazione, è effettuata da una commissione nominata all'uopo dal segretario generale. All'esito della selezione è comunque assicurata una partecipazione che consenta un'adeguata concorrenza. Il bando può inoltre stabilire il numero massimo di concorrenti da invitare.

3. Qualora sia ritenuto opportuno avvalersi di particolari competenze tecniche o di esperienze specifiche, ai concorrenti invitati alla procedura ristretta può essere richiesta la redazione di un progetto sulla base di un piano di massima predisposto dall'Ufficio e di indicare le condizioni alle quali intendono eseguirlo.

4. Ai concorrenti selezionati è inviata la lettera di invito a presentare, entro termini specificati, la propria offerta tecnico-economica. Alla lettera sono allegati il capitolato tecnico e lo schema di contratto che regola il rapporto con l'aggiudicatario.

5. Per lo svolgimento della procedura ristretta è necessaria la presenza di almeno due offerte valide.

Art. 24. Criteri di aggiudicazione

1. Nel bando di gara sono specificati i criteri di aggiudicazione seguiti che sono, alternativamente, i seguenti:

a) in caso di pubblico incanto, al prezzo più alto se si tratta di contratti attivi, ovvero al prezzo più basso se si tratta di contratti passivi;
b) in caso di licitazione privata, al prezzo più basso qualora il capitolato tecnico sia molto particolareggiato e, comunque, tale da identificare inequivocabilmente la prestazione che l'Ufficio intende ricevere;
c) in caso di licitazione privata e di appalto concorso, all'offerta più vantaggiosa sotto il profilo tecnico-economico, qualora nel capitolato tecnico siano contenute solo prescrizioni di massima e si ritenga conveniente, quindi, avvalersi della collaborazione e dell'apporto di competenza tecnica ed esperienza specifica da parte dell'offerente per l'elaborazione del progetto definitivo. In tal caso nel bando di gara sono indicati, in ordine decrescente di importanza, gli elementi presi in considerazione per la valutazione comparativa.

Art. 25. Procedura negoziata

1. È ammessa la procedura negoziata (trattativa privata) nei seguenti casi:

a) quando, a seguito di esperimento di gara, per qualsiasi motivo, l'aggiudicazione non abbia avuto luogo;
b) per la fornitura di beni, la prestazione di servizi, ivi compresi quelli di tipo informatico e telematico, e l'esecuzione di lavori che una sola impresa può fornire od eseguire con i requisiti tecnici ed il grado di perfezione richiesti, nonché quando l'acquisto riguardi beni la cui produzione è garantita da privativa industriale;
c) per la locazione d'immobili;
d) quando l'urgenza, adeguatamente motivata, dei lavori, degli acquisti e delle forniture dei beni e servizi dovuta a circostanze imprevedibili, o quando la particolare natura e le caratteristiche dell'oggetto e delle prestazioni anche in relazione ad esigenze di sicurezza o di segretezza, ovvero quando la necessità di far eseguire le prestazioni a spese e a rischio degli imprenditori inadempienti, non consentano l'indugio della gara;

e) per lavori complementari non considerati nel contratto originario o che siano resi necessari da circostanze imprevedibili all'atto dell'affidamento del contratto, a condizione che siano affidati allo stesso contraente, non siano tecnicamente o economicamente separabili dalla prestazione principale, ovvero, benché separabili, siano strettamente necessari per il completamento dei lavori o della fornitura originaria e il loro ammontare non superi il 50% dell'importo originario;

f) per l'affidamento al medesimo contraente di forniture destinate al completamento, al rinnovo parziale, o all'ampliamento di quelle esistenti, qualora il ricorso ad altri fornitori costringa ad acquistare materiale di tecnica differente, il cui impiego o la cui manutenzione comporti notevoli difficoltà o incompatibilità tecniche. La durata di tali contratti non può superare, come norma generale, i tre anni;

g) per l'acquisizione di beni o prodotti soggetti a prezzi amministrati o sorvegliati;

h) quando trattasi di contratti di importo non superiore a 200 milioni di lire, con esclusione dei casi in cui detti contratti costituiscano ripetizione, frazionamento o completamento di precedenti lavori o forniture;

i) quando trattasi di contratti di assicurazione.

2. Nei casi indicati alle lettere a), d), h) ed i) del comma 1 devono essere interpellate più imprese o ditte, persone od enti e, comunque, non inferiori a tre.

Art. 26. Servizi in economia

1. Possono essere eseguite in economia, senza l'adozione della delibera a contrattare, forniture di beni e servizi che non superano singolarmente la somma di lire 20 milioni (euro 10329,13) IVA esclusa, dando atto delle indagini di mercato ed eventuali trattative svolte. Si può procedere sulla base di un solo preventivo nei casi di indifferibilità, urgenza, o di specificità della fornitura, ovvero quando l'importo complessivo della spesa non supera lire 5 milioni (euro 2582,28) IVA esclusa.

2. Per la definizione delle transazioni di importo superiore a lire 100 milioni è richiesto il parere preventivo dell'Avvocatura generale dello Stato.

Art. 27. Collaudi e verifiche

1. Quando il collaudo di lavori e forniture è richiesto dall'oggetto del contratto, quest'ultimo ne stabilisce le forme. Possono essere previsti collaudi parziali e in corso d'opera.

2. Il collaudo è effettuato in forma individuale e collegiale dal personale dell'Ufficio in possesso della competenza tecnica necessaria, ovvero, qualora se ne ravvisi la necessità, da consulenti appositamente incaricati. La nomina dei collaudatori è effettuata dal segretario generale.

3. Il collaudo non può essere effettuato da chi abbia progettato, diretto o sorvegliato i lavori, ovvero da chi abbia partecipato all'aggiudicazione del contratto o alle relative forniture.

4. Nel caso in cui l'importo dei lavori o delle forniture non superi i duecento milioni di lire, l'atto formale di collaudo può essere sostituito da un certificato di regolare esecuzione rilasciato dal dirigente del dipartimento contratti e risorse finanziarie o da altro dipendente appositamente incaricato.

5. Per l'acquisizione di beni e servizi diversi dai lavori e dalle forniture di cui ai commi precedenti, relativamente ai quali non sia possibile procedere al collaudo secondo le modalità e i criteri ivi previsti, il funzionario cui viene effettuata la consegna procede ad una verifica della regolarità e della corrispondenza dei beni e dei servizi acquistati con quelli ordinati. Di tale corrispondenza e regolarità è redatta apposita attestazione.

Art. 28. Aggiornamenti

1. I limiti di spesa e di somma indicati nei precedenti articoli possono essere aggiornati annualmente in base alle variazioni dell'indice ISTAT dei prezzi al consumo.

Capo VI - Disposizioni transitorie e finali

Art. 29. Rapporti contrattuali in corso

1. I rapporti contrattuali già costituiti e le gare in corso di svolgimento alla data di entrata in vigore del presente regolamento restano regolati dalle norme vigenti all'atto della stipula dei contratti o dell'indizione delle gare.

Art. 30. Bilanci

1. I nuovi schemi di bilancio di previsione e consuntivi e le relative disposizioni attuative si applicano a decorrere dall'esercizio finanziario 2001.

2. Il segretario generale può apportare eventuali modifiche tecniche ai predetti schemi entro un anno dalla data della loro utilizzazione.

Art. 31. Entrata in vigore

1. Il presente regolamento entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica.

105 # *PROVVEDIMENTO N. 1/P/2000 DEL 30 DICEMBRE 1999 - 13 GENNAIO 2000 INDIVIDUAZIONE DI ATTIVITÀ CHE PERSEGUONO RILEVANTI FINALITÀ DI INTERESSE PUBBLICO PER LE QUALI È AUTORIZZATO IL TRATTAMENTO DEI DATI SENSIBILI DA PARTE DEI SOGGETTI PUBBLICI (*)*

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nelle sedute del 30 dicembre 1999 e del 13 gennaio 2000, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Visto 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;

Visto, in particolare, l'articolo 22, comma 3, della medesima legge, come modificato dall'articolo 5 del decreto legislativo 11 maggio 1999, n. 135, che ammette il trattamento dei dati "sensibili" da parte dei soggetti pubblici, esclusi gli enti pubblici economici, solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite;

Considerato che per i trattamenti non autorizzati da una espressa disposizione di legge avente tali caratteristiche, i soggetti pubblici possono chiedere al Garante per la protezione dei dati personali di individuare, tra le attività ad essi demandate dalla legge, quelle che perseguono rilevanti finalità di interesse pubblico e per le quali il trattamento dei dati "sensibili" è conseguentemente autorizzato nelle more di una specificazione legislativa;

Considerato che diverse amministrazioni pubbliche tra cui, in particolare, enti locali, aziende sanitarie locali e uffici periferici dell'amministrazione statale, hanno chiesto al Garante di individuare alcune attività, tra quelle ad esse attribuite dalla legge, che perseguono rilevanti finalità di interesse pubblico;

Considerato che il termine per la decisione del Garante, limitatamente alle richieste presentate entro il 31 dicembre 1999, è di novanta giorni durante i quali il trattamento dei dati può essere proseguito sino alla decisione (articolo 5, comma 4, d.lg. n. 135/1999);

Considerato che il capo I del decreto legislativo n. 135/1999 individua alcuni principi generali in materia di trattamento di dati sensibili e di carattere giudiziario da parte dei soggetti pubblici;

Visto l'articolo 22, comma 3-bis, della legge n. 675/1996, introdotto dall'articolo 5, comma 3, del d.lg. n. 135/1999, secondo cui, nei casi in cui la rilevante finalità di interesse pubblico è specificata per legge o con provvedimento del Garante, ma non sono specificati i tipi di dati e le operazioni eseguibili, i soggetti pubblici dovranno identificare e rendere pubblici, secondo i rispettivi ordinamenti, i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite nei singoli casi, aggiornando tale identificazione periodicamente;

(*) *Pubblicato in G.U. 2 febbraio 2000, n. 26, p. 31.*

Considerato che il citato articolo 22, comma 3, della legge può essere applicato dal Garante anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti cui si riferiscono le richieste presentate (cfr. articoli 22, comma 3, ultimo periodo e 41, comma 7, della legge n. 675/1996, come modificato dall'articolo 4, comma 1, del d.lg. 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante n. 7/1999 del 29 settembre 1999, relativa al trattamento di dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici;

Visti gli atti d'ufficio e le richieste di soggetti pubblici sinora pervenute;

Considerato che alcune richieste non devono essere prese in considerazione in quanto si riferiscono, in tutto o in parte, a rilevanti finalità di interesse pubblico menzionate nel capo II del citato decreto legislativo n. 135/1999, per le quali il trattamento dei dati "sensibili" e di carattere giudiziario è già consentito (articolo 5, comma 5-bis, d.lg. n. 135/1999);

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'articolo 7, comma 2, lett. a) del D.P.R. 31 marzo 1998, n. 501;

Relatore il prof. Ugo De Siervo;

TUTTO CIÒ PREMESSO IL GARANTE:

1) nelle more di una specificazione legislativa e ai sensi dell'articolo 22, comma 3, della legge n. 675/1996, individua, tra le attività che le leggi demandano a soggetti pubblici, le seguenti attività che perseguono rilevanti finalità di interesse pubblico:

a) attività socio-assistenziali, con particolare riferimento a -interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;

- interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
- assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;
- indagini psico-sociali relative all'adozione di provvedimenti di adozione anche internazionale;
- compiti di vigilanza per affidamenti temporanei;
- iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;
- interventi in tema di barriere architettoniche;

b) attività relative alla gestione di asili nido;

c) attività concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico;

d) attività ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;

e) attività finalizzate all'assegnazione di alloggi di edilizia residenziale pubblica;

f) attività relative alla leva militare;

g) attività di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente;

h) attività degli uffici per le relazioni con il pubblico;

i) attività in materia di protezione civile;

j) attività di supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;

k) attività dei difensori civici regionali e locali, con particolare riferimento alla trattazione di petizioni e segnalazioni;

2) dichiara conseguentemente autorizzato il trattamento dei dati sensibili di cui all'articolo 22, comma 1, della legge n. 675/1996, da parte dei soggetti pubblici, anche diversi da quelli che hanno presentato richiesta, cui le leggi demandano le attività indicate nel precedente punto 1), nel rispetto dei principi generali di cui agli articoli 2, 3 e 4 del decreto legislativo 11 maggio 1999, n. 135, e in relazione ai tipi di dati e di operazioni che saranno identificati e resi pubblici dalle amministrazioni ai sensi del comma 3-bis del medesimo articolo 22, secondo i rispettivi ordinamenti;

3) dichiara non luogo a provvedere sulle richieste riconducibili a finalità menzionate nel capo II del decreto legislativo 11 maggio 1999, n. 135.

Roma, 30 dicembre 1999 - 13 gennaio 2000

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

AUTORIZZAZIONI GENERALI 2000 (*)

AUTORIZZAZIONE N. 1/2000 AL TRATTAMENTO DEI DATI SENSIBILI NEI RAPPORTI DI LAVORO

106

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 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;

Visto l'art. 22, comma 3 e comma 3 bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, n. 135;

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;

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 (art. 41, comma 7, legge n. 675/1996, come sostituito dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 29 settembre 1999 relativa al trattamento dei dati "sensibili" nei rapporti di lavoro, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 2 ottobre 1999 e avente efficacia fino al 30 settembre 2000;

Visti i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli 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, alla luce dell'esperienza maturata;

Ritenuto opportuno che tali nuove autorizzazioni provvisorie siano a tempo determinato, in conformità anche a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità emanato con d. P. R. 31 marzo 1998, n. 501;

(*) *Pubblicate in Gazzetta Ufficiale n. 229 del 30 settembre 2000.*

Ritenuta la necessità che anche le nuove 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni adottate in materia dal Consiglio d'Europa;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato ai fini dell'adempimento di obblighi contabili, retributivi, previdenziali, assistenziali, fiscali e assicurativi nell'ambito dei rapporti di lavoro, e che è pertanto necessario che tali trattamenti formino oggetto di un'autorizzazione generale ai sensi dell'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d. P. R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il prof. Stefano Rodotà;

Autorizza

il trattamento dei dati sensibili di cui all'art. 22, comma 1, della legge n. 675/1996, finalizzato alla gestione dei rapporti di lavoro, alle condizioni di seguito indicate.

1) Ambito di applicazione.

La presente autorizzazione è rilasciata 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, 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 dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi anche aziendali.

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 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;

- a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatari;

- 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);

- a candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti;

- a persone fisiche che ricoprono cariche sociali nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto 1);

- a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui alle precedenti lettere.

3) Finalità del trattamento.

Il trattamento dei dati sensibili deve essere necessario:

- per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi anche aziendali, in particolare ai fini 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;

- 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;

- per il perseguimento delle finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;

- per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, 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;

- per l'esercizio del diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;

- per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;

- per garantire le pari opportunità.

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:

- 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;

- 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;

- nell'ambito dei dati idonei a rivelare lo stato di salute, i dati raccolti in riferimento a malattie anche professionali, invalidità, infermità, gravidanza, puerperio o allattamento, 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 e dal d. P.R. n. 318/1999, 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).

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato, in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia.

Restano inoltre fermi gli obblighi di 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'art. 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.

I dati sensibili possono essere comunicati e, ove necessario diffusi, nei limiti strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), a soggetti pubblici o privati, ivi compresi organismi sanitari, casse e fondi di previdenza ed assistenza sanitaria integrativa anche aziendale, agenzie di intermediazione, associazioni di datori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

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.

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.

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:

- nell'art. 8 della legge 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

- nell'art. 6 della legge 5 giugno 1990, n. 135, che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività;

- nelle norme in materia di pari opportunità o volte a prevenire discriminazioni.

Efficacia temporale

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.
La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

AUTORIZZAZIONE N. 2/2000 AL TRATTAMENTO DEI DATI IDONEI A RIVELARE LO STATO DI SALUTE E LA VITA SESSUALE

107

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 22, comma 1, della legge n. 675/1996, il quale individua come "sensibili", tra l'altro, i dati personali idonei a rivelare lo stato di salute o la vita sessuale;

Visto l'art. 23 della legge n. 675/1996, come modificato dall'art. 2 del decreto legislativo 30 luglio 1999, n. 282;

Visto l'art. 22, comma 3 e comma 3-bis, della legge n. 675/1996, rispettivamente modificato ed introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, n. 135;

Visto l'art. 17 del decreto legislativo 11 maggio 1999, n. 135 e successive modificazioni ed integrazioni, nonché il provvedimento del Garante n. 1/P/2000 del 30 dicembre 1999 - 13 gennaio 2000, pubblicato sulla Gazzetta Ufficiale n. 26 del 2 febbraio 2000, con il quale sono state individuate le rilevanti finalità di interesse pubblico di cui all'art. 22 comma 3 della legge n. 657/1996;

Visto l'art. 23, comma 1-bis, della legge n. 675/1996 che prevede "modalità semplificate per le informative di cui all'articolo 10 della medesima legge e per la prestazione del consenso nei confronti di organismi sanitari pubblici, di organismi sanitari e di esercenti le professioni sanitarie convenzionati o accreditati dal Servizio sanitario nazionale, nonché per il trattamento dei dati da parte dei medesimi soggetti"; considerato che analoghe modalità semplificate sono previste dall'art. 17, comma 3, del decreto legislativo n. 135/1999;

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 (art. 41, comma 7, della legge n. 675/1996, modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 29 settembre 1999 relativa al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, pubblicata sulla Gazzetta Ufficiale della Repubblica italiana il 2 ottobre 1999 e avente efficacia fino al 30 settembre 2000;

Visti i risultati positivi conseguiti con le autorizzazioni generali nn. 2/1997, 2/1998 e 2/1999 che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli 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, alla luce dell'esperienza maturata;

Visto l'art. 17, comma 5, del decreto legislativo 11 maggio 1999, n. 135, (come integrato e modificato dall'art. 16 del d.lg. 30 luglio 1999, n. 281, secondo cui il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione da rilasciare entro dodici mesi dalla data di entrata in vigore della citata normativa integrativa; considerato che il trattamento dei dati genetici può essere proseguito nei limiti di quanto disposto dalla presente autorizzazione fino al rilascio della predetta autorizzazione;

Vista la legge 5 febbraio 1999, n. 25 che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria n. 95/46/CE e ritenuto pertanto opportuno rilasciare nuove autorizzazioni provvisorie a tempo determinato, in conformità anche a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità emanato con il d. P. R. 31 marzo 1998, n. 501;

Ritenuta la necessità che le nuove autorizzazioni prendano anch'esse 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni adottate in materia di dati sanitari dal Consiglio d'Europa ed in particolare dalla Raccomandazione N.R (97) 5 in base alla quale i dati sanitari devono essere trattati, di regola, solo nell'ambito dell'assistenza sanitaria o sulla base di regole di segretezza di efficacia pari a quelle previste in tale ambito;

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'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lett. a) del d.P.R. 31 marzo 1998, n. 501;

Relatore il Prof. Ugo De Siervo;

Autorizza:

- 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 il consenso non sia prestato o non possa essere prestato per effettiva irreperibilità;

- gli organismi e le case di cura private, nonché ogni altro soggetto privato, a trattare con il consenso i dati idonei a rivelare lo stato di salute e la vita sessuale;

- gli organismi sanitari pubblici, istituiti anche presso università, ivi compresi i soggetti pubblici allorché agiscano nella qualità di autorità sanitarie, a trattare i dati idonei a rivelare lo stato di salute, anche per il perseguimento delle finalità di rilevante interesse pubblico individuate dall'art. 17, comma 1, del decreto legislativo n. 135/1999 o dal provvedimento del Garante n. 1/P/2000 del 30 dicembre 1999 - 13 gennaio 2000, o da altro provvedimento di questa Autorità parimenti adottato ai sensi dell'art. 22, comma 3 bis, della legge n. 675/1996, qualora ricorrano contemporaneamente le seguenti condizioni:

- il trattamento sia finalizzato alla tutela dell'incolumità fisica e della salute di un terzo o della collettività;

- manchi il consenso (articolo 23, comma 1, ultimo periodo, legge n. 675/1996), in quanto non sia prestato o non possa essere prestato per effettiva irreperibilità;

- il trattamento non sia previsto da una disposizione di legge che specifichi, ai sensi dell'art. 22, comma 3, della legge n. 675/1996, come modificato dall'art. 5 del decreto legislativo n. 135/1999, i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Il consenso, ove previsto, è acquisito in conformità anche a quanto previsto dall'art. 23, commi 1-bis e 1-quater, della legge n. 675/1996 e dall'art. 17, comma 3, del decreto legislativo n. 135/1999, e successive modificazioni ed integrazioni.

Ambito di applicazione e finalità del trattamento

1.1. L'autorizzazione è rilasciata, anche senza richiesta:

- ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi;

- al personale sanitario infermieristico, tecnico e della riabilitazione che esercita l'attività in regime di libera professione;

- 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, dalla normativa comunitaria o da regolamenti, in particolare in materia di igiene e di sanità pubblica, di prevenzione delle malattie professionali e degli infortuni, di diagnosi e cura, ivi compresi i trapianti di organi e tessuti, di riabilitazione degli stati di invalidità e di inabilità fisica e psichica, di profilassi delle malattie infettive e diffusive, di tutela della salute mentale, di assistenza farmaceutica e di assistenza sanitaria alle attività sportive o di accertamento, in conformità alla legge, degli illeciti previsti dall'ordinamento sportivo. Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario, ovvero di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini 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 inca-

ricati del trattamento preposti a tali compiti osservino le stesse regole di segretezza alle quali sono sottoposti i medesimi destinatari della presente autorizzazione, nel rispetto di quanto previsto dall'art. 17, comma 3, del decreto legislativo n. 135/1999.

1.2. L'autorizzazione è rilasciata, altresì, ai seguenti soggetti:

- 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'art. 23, comma 1, ultimo periodo, della legge n. 675/1996 e dall'art. 5, comma 1, del decreto legislativo 30 luglio 1999, n. 282), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima. Resta fermo quanto previsto dai decreti legislativi 30 luglio 1999, nn. 281 e 282 in materia di ricerca scientifica e di ricerca medica ed epidemiologica;

- 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;

- 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;

- 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, salvo quanto previsto dall'art. 22, comma 1-bis, della legge n. 675/1996;

- 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;

- 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;

- alle persone fisiche e giuridiche e ad altri organismi, limitatamente ai dati dei beneficiari e dei donatori e alle operazioni indispensabili all'effettuazione di trapianti di organi e tessuti, nonché di donazioni di sangue.

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:

- ai fini dello svolgimento delle investigazioni di cui all'art. 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;

- per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, 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:

- 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;

- 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 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 in cui sarà efficace l'apposita autorizzazione per il trattamento dei dati genetici prevista dall'art. 17, comma 5, del decreto n. 135/1999, e successive modificazioni ed integrazioni, 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 articoli 9, 15 e 17 della legge n. 675/1996 e dal d.P.R. n. 318/1999, 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 sopra elencati.

Restano inoltre fermi gli obblighi di acquisire il consenso dell'interessato e di informarlo in conformità a quanto previsto dagli articoli 10, 22 e 23 della legge n. 675/1996. Per le informazioni relative ai nascituri, il consenso è prestato dalla gestante.

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 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 deve essere verificata periodicamente la stretta pertinenza e la non eccedenza dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati.

5) 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, 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:

- dall'art. 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;

- dall'art. 11 della legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare al medico provinciale competente per territorio una dichiarazione che non faccia menzione dell'identità della donna;

- dall'art. 734-bis del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal Codice di deontologia medica adottato il 3 ottobre 1998 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.

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.
La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

108 AUTORIZZAZIONE N. 3/2000 AL TRATTAMENTO DEI DATI SENSIBILI DA PARTE DEGLI ORGANISMI DI TIPO ASSOCIATIVO E DELLE FONDAZIONI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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;

Visto l'art. 22, comma 3 e comma 3 bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, n. 135;

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;

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);

Vista l'autorizzazione del Garante rilasciata il 29 settembre 1999 relativa al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 2 ottobre 1999 e avente efficacia fino al 30 settembre 2000;

Visti i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli 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, alla luce dell'esperienza maturata;

Vista la legge 5 febbraio 1999, n. 25 che stabilisce il termine del 27 febbraio 2000 per l'emanazione di alcuni decreti legislativi finalizzati a completare la disciplina sulla protezione dei dati personali in attuazione della direttiva comunitaria n. 95/46/CE e ritenuto pertanto opportuno che tali nuove autorizzazioni provvisorie siano a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità emanato con d. P. R. 31 marzo 1998, n. 501;

Ritenuta, tuttavia, la necessità che anche le nuove autorizzazioni prendano anch'esse 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 di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni adottate in materia dal 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 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;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d. P. R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il Prof. Ugo De Siervo;

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, alle condizioni di seguito indicate.

Ambito di applicazione e finalità del trattamento

1) La presente autorizzazione è rilasciata senza richiesta:

- alle associazioni anche non riconosciute, ivi comprese le confessioni religiose e le comunità religiose, salvo quanto previsto dall'art. 22, comma 1 bis, come introdotto dall'art. 5, comma 1 del decreto legislativo n. 135/1999, 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;

- 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);

- alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818.

L'autorizzazione è rilasciata altresì agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per l'applicazione dell'articolo 310 del decreto legislativo 16 aprile 1994, n. 297.

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.

La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi, sempre che il diritto da far valere o difendere sia di rango pari a quello dell'interessato, e i dati siano trattati esclusivamente per tale finalità e per il periodo strettamente necessario per il suo perseguimento.

La presente autorizzazione è rilasciata inoltre per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.

Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi 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:

- agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;

- 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;

- ai soggetti che ricoprono cariche sociali o onorifiche;

- 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;

- agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;

- ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

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. 2/1999.

Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 22, comma 1, della legge 31 dicembre 1996, n. 675, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi.

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 e dal d.P.R. n. 318/1999, 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 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 dalla normativa comunitaria, da norme di legge o di regolamento che stabiliscono divieti o limiti in materia di trattamento di dati personali.

Restano inoltre ferme le norme volte a prevenire discriminazioni, e in particolare le disposizioni contenute nel decreto-legge 26 aprile 1993, n. 122, convertito, con modificazioni, dalla legge 25 giugno 1993, n. 205, in materia di discriminazione per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio.

9) Efficacia temporale.

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

109 AUTORIZZAZIONE N. 4/2000 AL TRATTAMENTO DEI DATI SENSIBILI DA PARTE DEI LIBERI PROFESSIONISTI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 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;

Visto l'art. 22, comma 3 e comma 3 bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, n. 135;

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;

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 (art. 41, comma 7, legge n. 675/1996, come sostituito dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 29 settembre 1999 relativa al trattamento dei dati "sensibili" nei rapporti di lavoro, pubblicata sulla Gazzetta Ufficiale della Repubblica italiana il 2 ottobre 1999 e avente efficacia fino al 30 settembre 2000;

Visti i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli 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, alla luce dell'esperienza maturata;

Ritenuto opportuno che tali nuove autorizzazioni provvisorie siano a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità emanato con d. P. R. 31 marzo 1998, n. 501;

Ritenuta la necessità che anche le nuove 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni adottate in materia dal 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'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d. P. R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il Prof. Giuseppe Santaniello;

Autorizza

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 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'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza.

Sono equiparati ai liberi professionisti i soggetti iscritti nei corrispondenti albi o elenchi speciali istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato.

L'autorizzazione è rilasciata anche ai sostituti e agli ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, ai praticanti e ai tirocinanti presso il libero professionista, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

Il presente provvedimento non si applica al trattamento dei dati sensibili effettuato:

- dagli esercenti la professione sanitaria e dagli psicologi, dal personale sanitario infermieristico, tecnico e della riabilitazione, ai quali si riferisce l'autorizzazione generale n. 2/2000;

- 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. 1/2000;

- 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. 2/2000.

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:

- 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;

- per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi;

- 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;

- per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.

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 e dal d. P.R. n. 318/1999, 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:

- di informare l'interessato ai sensi dell'art. 10, commi 1 e 3, della legge n. 675/1996, anche quando i dati sono raccolti presso terzi;

- 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 trat-

tati 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'art. 9, comma 1, lett. e) della legge n. 675/1996, i dati sensibili possono essere conservati, per il periodo di tempo previsto da leggi, dalla normativa comunitaria o da regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per adempiere agli incarichi conferiti.

A tal fine deve essere verificata 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 (art. 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 dalla normativa comunitaria o da regolamenti 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.

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.
La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

110 AUTORIZZAZIONE N. 5/2000 AL TRATTAMENTO DEI DATI SENSIBILI DA PARTE DI DIVERSE CATEGORIE DI TITOLARI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 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;

Visto l'art. 22, comma 3 e comma 3 bis, della medesima legge, rispettivamente modificato e introdotto dall'art. 5 del decreto legislativo 11 maggio 1999, n. 135;

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;

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 (art. 41, comma 7, della legge n. 675/1996, modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Vista l'autorizzazione del Garante adottata il 29 settembre 1999 relativa al trattamento dei dati sensibili da parte di diverse categorie di titolari, pubblicata nella Gazzetta Ufficiale della Repubblica italiana il 2 ottobre 1999 e avente efficacia fino al 30 settembre 2000;

Visti i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli 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, alla luce dell'esperienza maturata;

Ritenuto opportuno che tali nuove autorizzazioni provvisorie siano a tempo determinato, in conformità a quanto previsto dal regolamento concernente l'organizzazione e il funzionamento dell'Ufficio di questa Autorità emanato con d. P. R. 31 marzo 1998, n. 501;

Ritenuta la necessità che anche le nuove 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 (art. 7, comma 5-quater);

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale, principi valutati anche sulla base delle raccomandazioni adottate in materia dal 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'art. 41, comma 7, della legge n. 675/1996;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d.P.R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore l'Ing. Claudio Manganelli;

Autorizza

- il trattamento dei dati sensibili di cui all'art. 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, creditizie, assicurative, di gestione di fondi, del settore turistico, del trasporto.

1) Soggetti ai quali è rilasciata l'autorizzazione:

- imprese autorizzate all'esercizio dell'attività bancaria e creditizia o assicurativa ed organismi che le riuniscono, anche se in stato di liquidazione coatta amministrativa;

- società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;

- società ed altri organismi di intermediazione finanziaria, in particolare per la gestione o l'intermediazione di fondi comuni di investimento o di valori mobiliari;

- società ed altri organismi che emettono carte di credito o altri mezzi di pagamento, o che ne gestiscono le relative operazioni;

- 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;

- imprese che operano nel settore turistico o alberghiero o del trasporto, le agenzie di viaggio e gli operatori turistici.

2) Finalità del trattamento.

La presente autorizzazione è rilasciata, anche senza richiesta, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti di cui al punto 1) assumono, nel proprio settore di attività, al fine di fornire specifici beni, prestazioni o servizi richiesti dall'interessato.

L'autorizzazione è rilasciata anche per adempiere o per esigere l'adempimento ad obblighi previsti, anche in materia fiscale, dalla normativa comunitaria, dalla legge, dai regolamenti, o dai contratti collettivi, o prescritti da autorità od organi di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.

Il trattamento avente tali finalità può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

3) Interessati ai quali i dati si riferiscono e categorie di dati trattati.

Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

4) Comunicazione e diffusione dei dati.

I dati sensibili possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società controllate e collegate ai sensi dell'art. 2359 del codice civile, nonché, ove necessario, ai familiari dell'interessato.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 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.

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.

Prescrizioni applicabili.

Il trattamento è regolato dalle autorizzazioni:

- n. 1/2000, rilasciata il 20 settembre 2000, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione;

- n. 4/2000, rilasciata il 20 settembre 2000, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati, qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Capo IV - Attività di selezione del personale.

1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento.

La presente autorizzazione è rilasciata, anche senza richiesta, alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di 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 e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la loro raccolta è giustificata da scopi determinati e legittimi ed è strettamente indispensabile per instaurare tale rapporto.

Il trattamento dei dati idonei a rivelare lo stato di salute dei familiari o dei conviventi dei candidati è consentito con il consenso scritto degli interessati e qualora sia finalizzato al riconoscimento di uno specifico beneficio in favore dei candidati, in particolare ai fini di un'assunzione obbligatoria o del riconoscimento di un titolo derivante da invalidità o infermità, da eventi bellici o da ragioni di servizio.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Il trattamento deve riguardare le sole informazioni strettamente pertinenti a tale finalità, sia in caso di risposta a questionari inviati anche per via telematica, sia nel caso in cui i candidati forniscano dati di propria iniziativa, in particolare attraverso l'invio di curricula.

Non è consentito il trattamento dei dati:

- 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;

- inerenti a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;

- 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 sensibili non possono essere diffusi.

Capo V - Mediazione a fini matrimoniali.

1) Soggetti ai quali è rilasciata l'autorizzazione.

La presente 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 trattamento.

Il trattamento può riguardare i soli dati e le sole operazioni che risultino indispensabili in relazione allo specifico profilo o alla personalità descritto o richiesto dalle persone interessate al matrimonio o alla convivenza.

I dati devono essere forniti personalmente dai medesimi interessati.

L'informativa preliminare al consenso scritto deve porre in particolare evidenza le categorie di dati trattati e le modalità della loro comunicazione a terzi.

Comunicazione dei dati.

I dati possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 13, comma 1, lettera c), n. 4), della 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.

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

1) Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

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. 2/2000, rilasciata il 20 settembre 2000.

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 e dal d.P.R. n. 318/1999, 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'art. 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, 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 dalla normativa comunitaria, da norme di legge o di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

- dalla legge 20 maggio 1970, n. 300;

- 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.

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.
La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
Manganelli

IL SEGRETARIO GENERALE
Buttarelli

111 AUTORIZZAZIONE N. 6/2000 AL TRATTAMENTO DI ALCUNI DATI SENSIBILI DA PARTE DEGLI INVESTIGATORI PRIVATI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 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 (art. 22, comma 1, legge n. 675/1996);

Considerato che una speciale disposizione (art. 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;

Vista l'autorizzazione del Garante adottata il 29 settembre 1999 relativa al trattamento di alcuni dati sensibili da parte degli investigatori privati, pubblicata sulla Gazzetta ufficiale della Repubblica italiana il 2 ottobre 1999 e avente efficacia fino al 30 settembre 2000;

Visti i risultati positivi conseguiti con le autorizzazioni generali rilasciate negli anni precedenti, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto, pertanto, opportuno rilasciare nuove autorizzazioni generali anche al fine di proseguire la semplificazione degli 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, alla luce dell'esperienza maturata;

Considerato che il Garante ha rilasciato un'autorizzazione di ordine generale relativa ai dati idonei a rivelare lo stato di salute e la vita sessuale (n. 2/2000, rilasciata il 20 settembre 2000), 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. 2/2000 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. 2/2000 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 in via di emanazione (art. 22, comma 4, legge n. 675/1996);

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d. P. R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore l'Ing. Claudio Manganelli;

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.

La presente autorizzazione è rilasciata, anche senza richiesta, alle persone fisiche e giuridiche, agli istituti, agli enti, alle associazioni e agli organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni).

Il trattamento può essere effettuato unicamente:

- 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 ed inviolabile;

- 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:

- nell'ambito dei rapporti di lavoro (autorizzazione n. 1/2000, rilasciata il 20 settembre 2000);

- relativamente ai dati idonei a rivelare lo stato di salute e la vita sessuale (autorizzazione generale n. 2/1999, rilasciata il 20 settembre 2000);

- da parte degli organismi di tipo associativo e delle fondazioni (autorizzazione generale n. 3/2000, rilasciata il 20settembre 2000);

- da parte dei liberi professionisti iscritti in albi o elenchi professionali, ivi inclusi i difensori e i relativi sostituti ed ausiliari (autorizzazione generale n. 4/2000, rilasciata il 20 settembre 2000);

- relativamente ai dati di carattere giudiziario (autorizzazione generale n. 7/2000, rilasciata il 20 settembre 2000).

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 entro cui questa deve essere conclusa.

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'art. 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 nell'autorizzazione generale n. 2/2000, 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, in via di emanazione ai sensi degli articoli 22, comma 4 e 31, comma 1, lettera h), della legge n. 675/1996.

4) Conservazione dei dati.

Nel quadro del rispetto dell'obbligo previsto dall'art. 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 (art. 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 dalla normativa comunitaria, ovvero da norme di legge o di regolamento, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare:

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;

- dalla legge 5 giugno 1990, n. 135, in materia di sieropositività e di infezione da HIV;

- dalle norme processuali o volte a prevenire discriminazioni;

- dall'art. 734-bis del codice penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano fermi gli obblighi previsti dagli articoli 9, 15, 17 e 28 della legge n. 675/1996 e dal d. P.R. n. 318/1999 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).

Efficacia temporale.

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.
La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
Manganelli

IL SEGRETARIO GENERALE
Buttarelli

112

AUTORIZZAZIONE N. 7/2000 AL TRATTAMENTO DI DATI A CARATTERE GIUDIZIARIO DA PARTE DI PRIVATI, DI ENTI PUBBLICI ECONOMICI E DI SOGGETTI PUBBLICI

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 24, comma 1, della medesima legge, che ammette il trattamento di dati personali idonei a rivelare i provvedimenti giudiziari indicati nell'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, da parte di soggetti pubblici e privati e di enti pubblici economici, "soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e le precise operazioni autorizzate";

Constatata la necessità di evitare che diversi soggetti privati ed enti pubblici economici debbano interrompere alcuni trattamenti di dati che risultano giustificati da una finalità di rilevante interesse pubblico in ragione della loro natura e degli scopi ai quali essi sono strumentali;

Considerato che diversi trattamenti dei predetti dati da parte di soggetti pubblici sono disciplinati nel decreto legislativo 11 maggio 1999, n. 135, nonché nel provvedimento del Garante n. 1/P/2000 del 30 dicembre 1999 - 13 gennaio 2000, pubblicato sulla Gazzetta Ufficiale n. 26 del 26 febbraio 2000;

Considerato che i trattamenti dei medesimi dati giudiziari da parte dei soggetti pubblici, per finalità non previste nel capo II del decreto legislativo 11 maggio 1999, n. 135, devono essere autorizzati dal Garante ai sensi dell'art. 24 della legge 31 dicembre 1996, n. 675;

Ritenuta la necessità di autorizzare i soggetti pubblici al trattamento dei dati di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, e ciò al fine di consentire l'accertamento dell'assenza di alcune situazioni che la normativa in materia di appalti pubblici considera quali cause di esclusione dalla partecipazione a gare d'appalto, in modo che, per esigenze di buon andamento e impar-

zialità dell'azione amministrativa, i soggetti operanti in materia presentino i requisiti previsti di professionalità e correttezza;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio, nei confronti di singoli titolari oppure, con provvedimenti generali, di determinate categorie di titolari o di trattamenti (art. 41, comma 7, della legge n. 675/1996, come modificato dall'art. 4, comma 1, del decreto legislativo 9 maggio 1997, n. 123);

Visti i risultati positivi conseguiti con le autorizzazioni al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e soggetti pubblici rilasciate il 10 maggio 1999, come integrata con provvedimenti del 3 giugno 1999 e del 9 settembre 1999 e 29 settembre 1999, che sono risultate uno strumento idoneo per prescrivere ed uniformare le misure e gli accorgimenti a garanzia degli interessati, tenendo conto dei diritti e degli interessi meritevoli di tutela degli operatori che verrebbero penalizzati dalla necessaria richiesta di singoli provvedimenti autorizzatori;

Ritenuto opportuno rilasciare una nuova autorizzazione generale in ordine ai dati di carattere giudiziario citati in premessa, al fine di semplificare gli adempimenti previsti dalla legge n. 675/1996, di armonizzare le prescrizioni da impartire ad una ampia categoria di titolari del trattamento e di favorire altresì la funzionalità dell'Ufficio del Garante, alla luce dell'esperienza maturata;

Considerato che l'art. 8, par. 5, della direttiva 95/46/CE prevede specifiche garanzie per i dati sopraindicati e per altre categorie di dati a carattere giudiziario, in quanto ammette il trattamento dei dati relativi alla più ampia categoria delle "infrazioni, ... condanne penali o ... misure di sicurezza" "...solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che possono essere fissate dallo Stato membro in base ad una disposizione nazionale che preveda garanzie appropriate e specifiche", sempreché un "registro completo" delle condanne penali sia tenuto "solo sotto il controllo dell'autorità pubblica";

Ritenuto che in vista della completa attuazione legislativa di tale disciplina comunitaria è opportuno che la presente autorizzazione generale non rechi disposizioni particolarmente dettagliate, in modo da evitare che l'attività dei titolari dei trattamenti sia soggetta a modifiche sostanziali nel corso di un breve periodo di tempo, ferme restando alcune garanzie per gli interessati;

Ritenuta la necessità di favorire la prosecuzione dell'attività di documentazione, studio e ricerca in campo giuridico, in particolare per quanto riguarda la diffusione di dati relativi a precedenti giurisprudenziali, in ragione sia dell'affinità che tali attività presentano con quelle di manifestazione del pensiero già disciplinate dagli articoli 12, 20 e 25 della legge n. 675/1996, sia della possibile adozione di norme volte a favorire lo sviluppo dell'informatica giuridica;

Ritenuto, tuttavia, opportuno che la presente autorizzazione prenda comunque in considerazione le finalità dei trattamenti, le categorie di interessati e di destinatari della comunicazione e della diffusione, nonché il periodo di conservazione dei dati, 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 (art. 7, comma 5-quater);

Considerata la necessità che sia garantito, anche nell'attuale fase transitoria, il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, specie per quanto riguarda la riservatezza e l'identità personale;

Visto l'art. 35 della legge n. 675/1996 che sanziona penalmente la violazione delle prescrizioni della presente autorizzazione;

Visto il regolamento recante norme sulle misure minime di sicurezza previsto dall'art. 15, comma 2, della legge n. 675/1996 e adottato con d. P. R. 28 luglio 1999, n. 318;

Visto l'art. 14 del d. P. R. 31 marzo 1998, n. 501;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il Prof. Giuseppe Santaniello;

Autorizza

i trattamenti di dati personali idonei a rivelare i provvedimenti di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale, per le rilevanti finalità di interesse pubblico di seguito specificate ai sensi dell'art. 24 della legge n. 675/1996 e secondo le seguenti prescrizioni:

Capo I - Rapporti di lavoro

1) Ambito di applicazione e finalità del trattamento.

L'autorizzazione è rilasciata, anche senza richiesta di parte, a persone fisiche e giuridiche, enti, associazioni ed organismi che:

- sono parte di un rapporto di lavoro;

- utilizzano prestazioni lavorative anche atipiche, parziali o temporanee ai sensi della legge 24 giugno 1997, n. 196 (in materia di prestazioni di lavoro temporaneo);

- conferiscono un incarico professionale a consulenti, liberi professionisti, agenti, rappresentanti e mandatari.

Il trattamento deve essere strettamente necessario per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro, anche autonomo o non retribuito od onorario.

L'autorizzazione è altresì rilasciata a soggetti che in relazione ad un'attività di composizione di controversie esercitata in conformità alla legge svolgono un trattamento strettamente necessario al medesimo fine.

2) Interessati ai quali i dati si riferiscono.

Il trattamento può riguardare dati attinenti a soggetti che hanno assunto o intendono assumere la qualità di:

- lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione lavoro, ovvero di associati anche in compartecipazione o di titolari di borse di lavoro e di rapporti analoghi;

- amministratori o membri di organi esecutivi o di controllo;

- consulenti e liberi professionisti, agenti, rappresentanti e mandatari.

Capo II - Organismi di tipo associativo e fondazioni

1) Ambito di applicazione e finalità del trattamento.

L'autorizzazione è rilasciata anche senza richiesta:

- ad associazioni anche non riconosciute, ivi compresi partiti e movimenti politici, associazioni ed organizzazioni sindacali, patronati, associazioni a scopo assistenziale o di volontariato, a fondazioni, comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché a cooperative sociali e società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818;

- ad enti ed associazioni anche non riconosciute che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi.

Il trattamento deve essere strettamente necessario per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo.

2) Interessati ai quali i dati si riferiscono.

Il trattamento può riguardare dati attinenti:

- ad associati, soci e aderenti, nonché, nei casi in cui l'utilizzazione dei dati sia prevista dall'atto costitutivo o dallo statuto, a soggetti che presentano richiesta di ammissione o di adesione;

- a beneficiari, assistiti e fruitori delle attività o dei servizi prestati dall'associazione, dall'ente o dal diverso organismo.

Capo III - Liberi professionisti

1) Ambito di applicazione e finalità del trattamento.

L'autorizzazione è rilasciata anche senza richiesta ai:

- liberi professionisti, anche associati, 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'art. 24, comma 2, della legge 7 agosto 1997, n. 266, in tema di attività di assistenza e consulenza;

- soggetti iscritti nei corrispondenti albi o elenchi speciali, istituiti anche ai sensi dell'art. 34 del regio decreto-legge 27 novembre 1933, n. 1578 e successive modificazioni e integrazioni, recante l'ordinamento della professione di avvocato;

- sostituti e ausiliari che collaborano con il libero professionista ai sensi dell'art. 2232 del codice civile, praticanti e tirocinanti, qualora tali soggetti siano titolari di un autonomo trattamento o siano contitolari del trattamento effettuato dal libero professionista.

2) Interessati ai quali i dati si riferiscono.

Il trattamento può riguardare dati attinenti ai clienti.

I dati relativi ai terzi possono essere trattati solo ove ciò sia strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi determinati e legittimi.

Capo IV - Imprese bancarie ed assicurative ed altri trattamenti

1) Ambito di applicazione e finalità del trattamento.

L'autorizzazione è rilasciata, anche senza richiesta:

- ad imprese autorizzate o che intendono essere autorizzate all'esercizio dell'attività bancaria e creditizia, assicurativa o dei fondi pensione, anche se in stato di liquidazione coatta amministrativa, ai fini:

1) dell'accertamento, nei casi previsti dalle leggi e dai regolamenti, del requisito di onorabilità nei confronti di soci e titolari di cariche direttive o elettive;
2) dell'accertamento, nei soli casi espressamente previsti dalla legge, di requisiti soggettivi e di presupposti interdittivi in particolare ai sensi del regio decreto 21 dicembre 1933, n. 1736, sull'assegno bancario;
3) dell'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana;
4) dell'accertamento di situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, in relazione ad illeciti direttamente connessi con la medesima attività. Per questi ultimi casi, limitatamente ai trattamenti di dati registrati in una specifica banca di dati ai sensi dell'art. 1, comma 2, lett. a) della legge 675/1996, il titolare deve inviare al Garante una dettagliata relazione sulle modalità del trattamento.

- a soggetti titolari di un trattamento di dati svolto nell'ambito di un'attività di richiesta, acquisizione e consegna di atti e documenti presso i competenti uffici pubblici, effettuata su incarico degli interessati;

- alle società di intermediazione mobiliare, alle società di investimento a capitale variabile, e alle società di gestione del risparmio e dei fondi pensione, ai fini dell'accertamento dei requisiti di onorabilità in applicazione dei decreti legislativi 24 febbraio 1998, n. 58 e 21 aprile 1993, n. 124, dei decreti ministeriali 11 novembre 1998, n. 468 e 14 gennaio 1997, n. 211 e di eventuali altre norme di legge o di regolamento.

2) Ulteriori trattamenti.

L'autorizzazione è rilasciata altresì:

- a chiunque, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempreché il diritto da far valere o difendere 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 suo perseguimento;

- a chiunque, per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;

- a persone fisiche e giuridiche, istituti, enti ed organismi che esercitano un'attività di investigazione privata autorizzata con licenza prefettizia (art. 134 del regio decreto 18 giugno 1931, n. 773, e successive modificazioni e integrazioni). Il trattamento deve essere necessario: 1) per permettere a chi conferisce uno specifico incarico di far valere o difendere in sede giudiziaria un proprio diritto di rango pari a quello del soggetto al quale si riferiscono i dati, ovvero di un diritto della personalità o di un altro diritto fondamentale ed inviolabile; 2) su incarico di un difensore 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);

- a chiunque, per adempiere ad obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale, contenute anche nella legge 19 marzo 1990, n. 55, e successive modificazioni ed integrazioni, o per poter produrre la documentazione prescritta dalla legge per partecipare a gare d'appalto.

- ai soggetti pubblici, ai fini dell'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gara d'appalto, come previsto dalla normativa in materia di appalti pubblici, e, in particolare, dall'art. 11 del decreto legislativo 24 luglio 1992, n. 358, come da ultimo modificato dall'art. 9 del decreto legislativo 20 ottobre 1998, n. 402.

Capo V - Documentazione giuridica

Ambito di applicazione e finalità del trattamento.

L'autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati per finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali.

Capo VI - Prescrizioni comuni a tutti i trattamenti

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

1) Dati trattati.

Possono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

2) Modalità di trattamento.

Il trattamento dei dati deve essere effettuato unicamente con logiche e mediante forme di organizzazione dei dati strettamente correlate agli obblighi, ai compiti o alle finalità precedentemente indicati.

Fuori dei casi previsti dai Capi IV, punto 2 e V, o nei quali la notizia è acquisita da fonti accessibili a chiunque, i dati devono essere forniti dagli interessati, nel rispetto della disciplina prevista dall'art. 689 del codice di procedura penale in tema di richiesta di certificati, salvo quanto previsto dall'art. 688 del medesimo codice per ciò che riguarda l'acquisizione di certificati del casellario giudiziale da parte di amministrazioni pubbliche e di enti incaricati di pubblici servizi.

3) Conservazione dei dati.

Con riferimento all'obbligo previsto dall'art. 9, comma 1, lett. e) della legge n. 675/1996, i dati possono essere conservati per il periodo di tempo previsto da leggi o regolamenti e, comunque, per un periodo non superiore a quello strettamente necessario per le finalità perseguite.

Ai sensi dell'art. 9, comma 1, lett. c), d) ed e) della legge, i soggetti autorizzati verificano periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi. Al fine di assicurare che i dati siano strettamente pertinenti e non eccedenti rispetto alle finalità medesime, i soggetti autorizzati valutano specificamente il rapporto tra i dati e i singoli obblighi, compiti e prestazioni. I dati che, anche a seguito delle verifiche, risultino eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'essenzialità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente gli obblighi, i compiti e le prestazioni.

4) Comunicazione e diffusione.

I dati possono essere comunicati e, ove previsto dalla legge, diffusi, a soggetti pubblici o privati, nei limiti strettamente necessari per le finalità perseguite e nel rispetto, in ogni caso, del segreto professionale e delle altre prescrizioni sopraindicate.

5) Richieste di autorizzazione.

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione al Garante, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante si riserva l'adozione di ogni altro provvedimento per i trattamenti non considerati nella presente autorizzazione.

Per quanto riguarda invece i trattamenti disciplinati nel presente provvedimento, il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle relative prescrizioni, salvo che il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute nell'art. 8 della legge 20 maggio 1970, n. 300, 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.

6) Efficacia temporale e disciplina transitoria.

La presente autorizzazione ha efficacia a decorrere dal 1° ottobre 2000, fino al 31 dicembre 2001.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 20 settembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

113

PROVVEDIMENTO DEL 7 MARZO 2001 IN MATERIA ELETTORALE UN "DECALOGO" PER L'UTILIZZAZIONE DI DATI DA PARTE DI PARTITI E MOVIMENTI POLITICI NELLA PROPAGANDA ELETTORALE

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, con la partecipazione del prof. Giuseppe Santaniello, che presiede la riunione, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTE le numerose note pervenute in merito alla conformità alle disposizioni della legge 31 dicembre 1996, n. 675 di alcune iniziative di propaganda politica ed elettorale;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

RELATORE il prof. Giuseppe Santaniello;

PREMESSO

In relazione allo svolgimento di consultazioni elettorali e referendarie sono pervenute a questa Autorità, sia da parte di formazioni politiche, sia di singoli cittadini, numerose segnalazioni e richieste di parere in ordine alle modalità di trattamento dei dati personali utilizzati per la propaganda elettorale o per la presentazione di liste e candidature o per la sottoscrizione di richieste di referendum.

Su alcune questioni il Garante si è già pronunciato fin dal primo periodo della propria attività con alcune decisioni (consultabili sul sito internet dell'Autorità www.garanteprivacy.it e sul bollettino "Cittadini e società dell'informazione"), riassunte nelle relazioni annuali presentate al Parlamento e al Governo.

Con il presente provvedimento, al fine di tracciare linee-guida per i titolari del trattamento e per tutti gli interessati sono richiamati in un quadro organico i principi che regolano la protezione dei dati personali nella materia elettorale, quali risultano dalla legge n. 675/1996 e dai successivi decreti legislativi che hanno integrato quest'ultima.

1) Possibilità di utilizzare i dati personali ricavati da registri o elenchi "pubblici". In base agli artt. 12, comma 1, lettera c), e 20, comma 1, lettera b), della legge n. 675 è possibile trattare e divulgare, anche senza il consenso degli interessati, dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque. Tale particolare categoria comprende registri, elenchi, atti o documenti "pubblici" (in quanto formati o tenuti da uno o più soggetti pubblici) e da tutti accessibili, nonché analoghi registri, elenchi, atti o documenti eventualmente formati da privati, ma sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque (come l'elenco degli abbonati al servizio di telefonia vocale per la rete fissa).

Fra le predette categorie vi rientrano gli elenchi degli iscritti a vari albi e collegi professionali (vedi sul punto i provvedimenti del Garante del 30 giugno 1997 e del 20 aprile 1998), i dati contenuti in taluni registri detenuti dalle camere di commercio e, soprattutto, le liste elettorali (che chiunque, come precisato dall'art. 51 del d.P.R. 20 marzo 1967 n. 223, può visionare ed ottenere in copia presso

i competenti uffici comunali), queste ultime più comunemente usate per attività di propaganda elettorale, unitamente ai dati ricavati dagli elenchi telefonici.

L'insieme dei nominativi presenti nelle liste elettorali può anzi integrare una base di dati ampia riferita alla popolazione adulta, da cui è possibile ricavare un insieme di informazioni (quale cognome e nome, luogo e data di nascita, residenza, professione e titolo di studio). La lecita acquisizione dei dati contenuti in tali liste spiega pertanto come molti cittadini il cui nominativo non compare, ad esempio, nell'elenco telefonico per la rete fissa abbiano potuto ricevere messaggi e sollecitazioni elettorali presso l'indirizzo risultante dalle liste.

2) **Utilizzazione di altri tipi di dati personali.** Le categorie di dati prima richiamate riguardano un insieme di informazioni predeterminato per legge e quindi facilmente riscontrabile. Qualora pertanto un cittadino riceva messaggi pubblicitari e di propaganda da parte di un soggetto politico, in favore del quale non abbia manifestato uno specifico consenso al trattamento delle informazioni che lo riguardano, e queste ultime non corrispondano ai dati effettivamente presenti negli elenchi predetti, tale circostanza può essere significativa di una raccolta illecita o non corretta dei dati. In questi casi è possibile inviare una circostanziata segnalazione al Garante cui spetta il potere di svolgere accertamenti anche attraverso il proprio servizio ispettivo.

3) **L'informativa all'interessato: obblighi ed esoneri.** Il trattamento dei dati estratti dalle liste elettorali o da altri elenchi pubblici deve avvenire nel rispetto delle disposizioni della legge n. 675. Per quanto riguarda l'informativa agli interessati, il Garante ha disposto di recente un parziale esonero fino al 30 giugno 2001 in favore di partiti e movimenti politici, comitati promotori e sostenitori di liste e di candidati che utilizzino dati estratti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque senza però contattare gli interessati, o qualora inviino semplice materiale di propaganda diverso da lettere articolate o messaggi di posta elettronica che non permetta l'inserimento dell'informativa (provvedimento del 7 febbraio 2001, in Gazzetta Ufficiale n. 36 del 13 febbraio 2001, pag. 65).

Fuori di questi casi, ciascun partito politico, comitato elettorale, ecc. deve fornire la prevista informativa ai singoli cittadini interessati almeno in occasione dell'invio del primo messaggio pubblicitario o propagandistico. In tale informativa, che può essere redatta anche con formule sintetiche e con stile colloquiale, deve essere indicata, tra l'altro, con chiarezza, la denominazione e l'indirizzo del titolare o del responsabile del trattamento, onde permettere all'interessato di individuare il destinatario delle richieste ai sensi dell'art. 13 della legge n. 675 volte ad opporsi all'ulteriore invio di materiale o ad ottenere, a seconda dei casi, l'aggiornamento, la correzione, l'integrazione o la cancellazione dei dati.

Tali richieste comportano poi un dovere per i titolari del trattamento di darvi riscontro ed obbligano, nel caso di opposizione dell'interessato all'ulteriore invio di materiale, a non recapitare più a tale soggetto altri messaggi, anche in occasione di successive campagne elettorali. Infine, qualora un titolare di trattamento non fornisca un idoneo riscontro ad una richiesta di esercizio dei diritti di cui al predetto art. 13, l'interessato, in ordine a tale istanza, ha diritto di presentare ricorso ai sensi dell'art. 29 della legge n. 675 rivolgendosi al giudice ordinario o, in via alternativa, direttamente a questa Autorità.

4) **Casi nei quali è necessario acquisire il consenso dell'interessato.** L'utilizzazione di altri tipi di dati non estratti da atti, documenti, elenchi o registri pubblici (da intendersi nel senso sopra precisato) può essere effettuato solo in presenza del consenso espresso del soggetto interessato, manifestato (in forma scritta se si tratta di dati sensibili) in relazione ad una informativa nella quale la finalità dell'utilizzo a fini di comunicazione politica o di propaganda elettorale dei dati dell'interessato deve essere posta chiaramente in evidenza. La necessità del consenso si impone altresì nell'ipotesi in cui determinati dati personali siano stati conoscibili semplicemente su un piano di fatto, anche momentaneamente e da parte di una pluralità di soggetti, come nel caso di indirizzi di posta elettronica ricavati da pagine web o nell'ambito di forum o newsgroup in rete (come precisato dal Garante nel già citato provvedimento dell'11 gennaio 2001).

5) **Dati "sensibili".** La raccolta e l'utilizzazione da parte di partiti o associazioni politiche di dati relativi ad iscritti alle loro stesse organizzazioni, nonché di partecipanti ad iniziative politiche in occasione delle quali siano stati raccolti dati sui partecipanti, oppure di dati acquisiti in occasione della sottoscrizione di petizioni, proposte di legge, manifesti o richieste di referendum, comporta un trattamento di dati personali sensibili (ai sensi dell'art. 22, comma 1, della citata legge) e richiede l'espressione da parte dell'interessato di un consenso scritto. Per gli aderenti a partiti ed associazioni

politiche questo viene in genere espresso con l'atto di adesione al partito stesso (vedi in proposito il comunicato stampa del Garante del 16 ottobre 1997 in "Cittadini e società dell'informazione", n. 2, pag. 82). In assenza di questo consenso o per dati acquisiti in altre occasioni politiche, occorre che l'informativa evidenzi con chiarezza, oltre all'indicazione delle principali finalità ed ai trattamenti ad esse specificamente connessi, un utilizzo più ampio di tali dati (ad esempio comunicazione degli stessi ai comitati elettorali di candidati delle medesime formazioni politiche). Qualora si intenda ipotizzare la possibile comunicazione di tali dati anche ad altri soggetti (organizzazioni di simpatizzanti, enti, associazioni, società e persone fisiche non direttamente connesse all'attività del titolare del trattamento...) tale possibilità (indipendente ed ulteriore rispetto alle ragioni precipue della raccolta dei dati) deve essere associata all'espressione di un consenso, specifico e distinto da quello previsto per il trattamento principale.

6) Obblighi in caso di uso di dati di aderenti a organizzazioni diverse da quelle politiche. L'utilizzazione a fini di propaganda elettorale di dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politico-partitica, è possibile qualora venga espressamente prevista nell'informativa resa agli iscritti al momento dell'adesione o del rinnovo della stessa (e qualora gli organi dirigenti dell'associazione decidano, con loro autonoma determinazione, di prevedere una tale possibilità). È pertanto illegittima la prassi, riscontrata in alcuni casi segnalati a questa Autorità, di utilizzare gli indirizzari associativi per iniziative di propaganda elettorale a favore di dirigenti o ex dirigenti di associazioni o addirittura di soggetti estranei alle stesse, candidatisi successivamente ad elezioni politiche o amministrative. (v. provvedimenti del Garante del 5 ottobre 1999 e del 9 ottobre 2000).

7) Utilizzazione di dati personali acquisiti in ragione dell'esercizio di un mandato politico o amministrativo. I titolari di determinate cariche elettive, politiche o amministrative, nell'esercizio del loro mandato e sulla base di specifiche disposizioni volte a favorire il pieno esercizio del mandato elettorale medesimo (es. art. 31 legge n. 142 del 1990, ecc.), possono legittimamente venire a conoscenza di numerosi dati personali. I dati in tal modo acquisiti devono essere però utilizzati esclusivamente per le finalità pertinenti all'esercizio del mandato (presentazione di interrogazioni, svolgimento di attività di controllo e di denuncia nelle competenti sedi istituzionali, ecc.). Non è pertanto legittimo utilizzare gli stessi dati per finalità non pertinenti quale l'attività di propaganda elettorale (vedi parere del 20 maggio 1998 in Bollettino ufficiale del Garante "Cittadini e società dell'informazione", n. 4, pag. 7 ss.).

8) Dati personali trattati da scrutatori e rappresentanti di lista: limiti e doveri. In materia elettorale e in particolare in occasione di consultazioni elettorali, di referendum e di verifica della loro regolarità, è possibile, in conformità alla legge, la raccolta di alcuni dati sensibili. Ciò è considerato lecito anche dall'art. 8 del d.lg. 11 maggio 1999 n. 135, in materia di trattamento di dati sensibili da parte di soggetti pubblici, che espressamente colloca tale attività tra quelle di rilevante interesse pubblico che giustificano il trattamento. In questo quadro particolari cautele in tema di riservatezza devono essere osservate da scrutatori e rappresentanti di lista che, nell'esercizio delle funzioni e dei compiti loro affidati o riconosciuti dalla legge, vengano a conoscenza di dati personali anche di natura sensibile. La funzione svolta da tali soggetti è collegata al corretto svolgimento delle operazioni elettorali. I dati di cui i medesimi soggetti vengano a conoscenza per effetto delle funzioni svolte (quali quelli relativi alla partecipazione o meno al voto dei cittadini votanti presso una determinata sezione elettorale) devono essere trattati con ogni opportuna cautela anche a tutela del principio costituzionale della libertà e segretezza del voto. Ciò, tanto più, in quelle ipotesi (quali referendum abrogativi o votazioni di ballottaggio) nelle quali la partecipazione o la mancata partecipazione al voto può evidenziare di per sé anche una particolare opzione politica dell'elettore. È illegittima la compilazione da parte degli stessi soggetti, per un successivo utilizzo a fini politici da parte della stessa persona o della formazione politica di riferimento, di elenchi di persone astenutesi dalla partecipazione al voto (ad esempio, allo scopo di sollecitare le stesse rispetto a futuri appuntamenti elettorali). Tenendo presente anche che l'elenco degli elettori astenutisi nelle elezioni per la Camera dei Deputati a suo tempo previsto dall'art. 115 del d.P.R. 30 marzo 1957 n. 361 (in base al quale tale elenco formato dal sindaco era esposto per un mese nell'albo comunale) non è più previsto e che il citato art. 115 è stato abrogato dall'art. 3 del d.lg. 20 dicembre 1993 n. 534.

9) Adozione di misure di sicurezza ed altri adempimenti. Ciascun partito, movimento o comitato elettorale, anche se esonerato dall'obbligo della notificazione del trattamento di cui all'art. 7, comma 5 ter, lettera l), della legge n. 675, è tenuto, oltre che agli adempimenti di cui agli artt. 8 e 19 della medesima legge in ordine all'individuazione e alla nomina dei responsabili e degli incaricati del

trattamento, ad adottare le misure minime di sicurezza di cui al d.P.R. n. 318 del 1999 con riferimento ai trattamenti di dati cartacei e automatizzati.

TUTTO CIÒ PREMESSO IL GARANTE:

segnala a tutti i titolari del trattamento interessati, ai sensi dell'art. 31, comma 1, lettera c), della legge n. 675 del 1996 la necessità di conformare il trattamento dei dati ai principi della medesima legge n. 675 richiamati nel presente provvedimento.

Roma, 7 marzo 2001

IL PRESIDENTE
Santaniello

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

PROVVEDIMENTO DEL 10 FEBBRAIO 2000
CODICI DI DEONTOLOGIA E DI BUONA CONDOTTA RELATIVI AI DATI PERSONALI UTILIZZATI PER FINALITÀ STORICHE, STATISTICHE, DI RICERCA SCIENTIFICA, DI INVESTIGAZIONI DIFENSIVE, E AI DATI PERSONALI UTILIZZATI DA OPERATORI SANITARI E DA ISTITUZIONI BANCARIE E FINANZIARIE (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta del 10 febbraio 2000, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, 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'art. 31, comma 1, lett. h), della citata legge n. 675/1996, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Considerato che la legge n. 675/1996 prevede che il Garante promuova un codice di deontologia in materia di attività giornalistica (adottato il 29 luglio 1998 e pubblicato sulla G.U. n. 179 del 3 agosto 1998), nonché un codice di deontologia e di buona condotta in materia di investigazioni difensive e di dati utilizzati per far valere o difendere un diritto in sede giudiziaria (art. 22, comma 4, legge n. 675/1996);

Considerato che il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare l'art. 6, comma 1, prevede che entro sei mesi dalla data del 1° ottobre 1999, il Garante promuova la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per le finalità sopra indicate, tenendo conto della specificità dei trattamenti nei diversi ambiti;

Visti gli artt. 7, comma 5, e 10, comma 6, del medesimo decreto legislativo;

Considerato che l'art. 17, comma 3, del decreto legislativo 11 maggio 1999, n. 135, quale modificato dall'art. 3 del decreto legislativo 30 luglio 1999, n. 282, prevede che per quanto non previsto dal decreto di cui all'articolo 23, comma 1-bis, della legge n. 675/1996, il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale da parte di organismi sanitari e di esercenti le professioni sanitarie è fatto oggetto di appositi codici di deontologia e di buona condotta adottati ai sensi dell'articolo 31, comma 1, lettera h), della medesima legge;

Considerata la necessità di adempiere alle predette disposizioni di legge e di promuovere altresì un ulteriore codice relativo alle attività bancarie e finanziarie in ragione dei diversi profili applicativi emersi e del loro rilievo rispetto alla generalità dei cittadini;

Considerata la necessità di osservare il principio di rappresentatività nell'ambito delle categorie coinvolte e di acquisire maggiori elementi di valutazione dai diversi soggetti potenzialmente interessati alla sottoscrizione di codici di deontologia e di buona condotta per determinati settori;

(*) G.U. 25 febbraio 2000, n. 46, p. 35.

Ritenuta l'opportunità di conferire la massima pubblicità all'iniziativa del Garante e al procedimento per la sottoscrizione dei predetti codici di deontologia e di buona condotta anche attraverso la pubblicazione del presente provvedimento sulla Gazzetta Ufficiale;

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva, adottate dagli Stati membri;

Considerata la necessità che i codici su base nazionale siano adottati tenendo conto degli eventuali progetti di codici di condotta comunitari;

Riservata l'iniziativa di promuovere ulteriori codici di deontologia e di buona condotta in altri settori di rilevante interesse generale;

Visti gli atti d'ufficio e le richieste di soggetti pubblici e privati sinora pervenute;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 7, comma 2, lettera a) del decreto del Presidente della Repubblica 31 marzo 1998, n. 501;

Relatore il prof. Ugo De Siervo;

TUTTO CIÒ PREMESSO IL GARANTE:

1) promuove la sottoscrizione di uno o più codici di deontologia e di buona condotta nei settori di seguito indicati:

a) trattamenti di dati personali per scopi storici effettuati da archivisti e utenti;

b) trattamenti di dati personali per scopi statistici e di ricerca scientifica;

c) trattamenti di dati personali ai fini dello svolgimento delle investigazioni difensive o per far valere o difendere in sede giudiziaria un diritto di rango pari a quello dell'interessato;

d) trattamenti di dati personali effettuati da istituzioni bancarie e finanziarie;

e) trattamenti di dati personali effettuati da organismi sanitari ed esercenti le professioni sanitarie;

2) invita tutti i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività di cui all'art. 31, comma 1, lett. h), della legge n. 675/1996, a darne comunicazione a questa Autorità entro il 31 marzo 2000 al seguente indirizzo: Garante per la protezione dei dati personali, Largo del Teatro Valle, 6 – 00186 Roma - fax 06.6818649 [1] E-mail: codici@garanteprivacy.it;

3) riserva ad altri provvedimenti la verifica della conformità alle leggi e ai regolamenti dei progetti di codici, l'esame di eventuali osservazioni, nonché le iniziative necessarie ai sensi del citato art. 31, comma 1, lett. h) per garantirne la diffusione e il rispetto.

Roma, 10 febbraio 2000

IL PRESIDENTE
Rodotà

[1] *Nuovo indirizzo: "Garante per la protezione dei dati personali" 00186 Roma - Piazza di Monte Citorio, 121*

DELIBERAZIONE N. 8 DEL 29 FEBBRAIO 2000

115 *MISURE MINIME DI SICUREZZA*

MODIFICA AL MODELLO PER LA NOTIFICA DEL TRATTAMENTO

OGGETTO: applicazione delle misure minime di sicurezza di cui al d.P.R. n. 318/1999. Modifica da apportare al modello per la notificazione del trattamento dei dati personali.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, Presidente, del prof. Giuseppe Santaniello, vice-presidente, del prof. Ugo De Siervo, dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale:

PREMESSO CHE:

- l'art. 7 della legge 31 dicembre 1996, n. 675, prevede per i titolari che intendano procedere ad un trattamento di dati l'obbligo di darne notificazione al Garante e, in caso di successive modifiche apportate per i profili indicati nel medesimo articolo, di comunicarle attraverso una successiva notificazione;
- l'art. 12, commi 1 e 3, del d.P.R. 31 marzo 1998, n. 501, stabilisce che le notificazioni sono effettuate utilizzando modelli conformi allo schema predisposto dal Garante;
- detti modelli sono stati predisposti e resi disponibili al pubblico, in particolare attraverso convenzioni con Poste italiane S.p.A. ed altri soggetti ed organismi interessati;
- l'art. 15, commi 2 e 3, della l. 675/1996 stabilisce che con regolamento devono essere individuate le misure minime di sicurezza relative ai dati personali oggetto di trattamento;
- il regolamento è stato emanato con d.P.R. n. 318 del 28 luglio 1999;
- ai sensi dell'art. 41, comma 3, della legge n. 675/1996 il termine per l'adozione delle misure minime di sicurezza previste da tale d.P.R. è fissato al 29 marzo 2000;

CONSIDERATO CHE:

- il modello di notificazione sarà aggiornato e perfezionato nel suo complesso entro la fine del corrente anno, in base all'esperienza acquisita e tenendo conto delle novità intercorse;
- l'applicazione del d.P.R. n. 318/1999 potrebbe indurre numerosi titolari dei trattamenti a modificare la precedente notificazione ai sensi dell'art. 7, commi 2 e 4 della citata legge, relativamente al riquadro d) del modello adottato dal Garante ai sensi del richiamato art. 12 del d.P.R. 31 marzo 1998, n. 501;
- si potrebbe così determinare l'afflusso al Garante di un enorme numero di notificazioni non necessarie in quanto non è indispensabile annotare nel registro generale dei trattamenti, in questa fase transitoria, modifiche di notificazioni già effettuate derivanti dall'adempimento di un obbligo di legge;

VISTE le osservazioni in atti formulate dall'Ufficio ai sensi dell'art. 7, comma 2, lett. a), del d.P.R. n. 501/1998, con nota a firma del segretario generale;

RELATORE il prof. Ugo De Siervo;

DELIBERA:

a) di inserire nel riquadro d) ("descrizione generale delle misure adottate per la sicurezza dei dati") dei modelli di notificazione al Garante del trattamento dei dati personali l'avvertenza che figura in allegato alla presente deliberazione;

b) di dare atto che i soggetti che hanno notificato i trattamenti dei dati personali prima del 29 marzo 2000 non devono presentare una nuova notificazione di modifica in relazione al medesimo riquadro d) qualora abbiano adottato le misure previste dal d.P.R. n. 318 del 28 luglio 1999;

c) di consentire ai titolari dei trattamenti, in riferimento a nuove notificazioni, di continuare ad utilizzare i modelli precedentemente approvati dal Garante.

Roma, 29 febbraio 2000

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

Allegato A

d) descrizione generale delle misure adottate per la sicurezza dei dati
(barrare le caselle pertinenti)

I soggetti che hanno effettuato la notificazione del trattamento dei dati personali prima della data del 29 marzo 2000, non sono tenuti a notificarla - limitatamente al presente riquadro - qualora abbiano adottato ulteriori misure prescritte dal D.P.R. n. 318 del 28 luglio 1999 "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell' art. 15, comma 2, della legge 31 dicembre 1996, n. 675".

Nel caso in cui il trattamento è in parte automatizzato (effettuato con strumenti elettronici o comunque automatizzati) e in parte non automatizzato, barrare entrambe le caselle.
(la restante parte del modello non è variata)

CODICE DI DEONTOLOGIA

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI PER SCOPI STORICI

116

PROVVEDIMENTO N. 8/P/2001 DEL 14 MARZO 2001

REGISTRO DELLE DELIBERAZIONI N. 8 DEL 14 MARZO 2001 (*)

Nella seduta odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visto l' art. 31, comma 1, lettera h) della legge 31 dicembre 1996, n. 675, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare il relativo art. 6, comma 1, il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici;

Visto l'articolo 7, comma 5, del medesimo decreto legislativo n. 281/1999, relativo ad alcuni profili che devono essere individuati dal codice per i trattamenti di dati per scopi storici;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla Gazzetta Ufficiale n. 46 del 25 febbraio 2000, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi del trattamento di dati personali per scopi storici effettuati da archivisti e utenti ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione del medesimo codice in base al principio di rappresentatività a darne comunicazione al Garante entro il 31 marzo 2000;

Viste le comunicazioni pervenute al Garante in risposta al provvedimento del 10 febbraio 2000, con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare alla redazione del codice e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro composto da componenti della Commissione consultiva per le questioni inerenti la consultabilità degli atti d'archivio riservati, del Centro di Documentazione ebraica, del Ministero per i beni e le attività culturali, dell'Associazione delle istituzioni culturali italiane, dell'Associazione nazionale archivistica italiana, dell'Istituto nazionale per la storia del movimento di liberazione in Italia, della Società per lo studio della storia contemporanea, dell'Istituto storico italiano per l'età moderna e contemporanea, della Società per gli studi di storia delle istituzioni, della Società italiana delle storiche, dell'Istituto romano per la storia d'Italia dal fascismo alla resistenza;

Considerato che il testo del codice è stato oggetto di ampia diffusione, anche attraverso la sua pubblicazione su alcuni siti Internet, al fine di favorire il più ampio dibattito e di permettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

(*) *Gazzetta Ufficiale n. 80 del 5 aprile 2001.*

Vista la nota del 28 febbraio 2001 con cui il gruppo di lavoro ha trasmesso il testo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici approvato e sottoscritto in pari data;

Rilevato che il rispetto delle disposizioni contenute nel codice costituisce condizione essenziale per la liceità del trattamento dei dati personali;

Constatata la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, ed in particolare all'art. 31, comma 1, lettera h) della legge n. 675/1996, nonché agli artt. 6 e 7 del decreto legislativo n. 281/1999;

Considerato che, ai sensi dell'art. 6, comma 1, del decreto legislativo n. 281/1999, il codice deve essere pubblicato nella Gazzetta Ufficiale della Repubblica Italiana a cura del Garante;

Rilevato che anche dopo tale pubblicazione il codice potrà essere eventualmente sottoscritto da altri soggetti pubblici e privati, società scientifiche ed associazioni professionali interessati;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000, adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il prof. Ugo De Siervo;

Dispone:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici che figura in allegato all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana.

Roma, 14 marzo 2001

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

Preambolo

I sottoindicati soggetti pubblici e privati sottoscrivono il presente codice sulla base delle seguenti premesse:

1) Chiunque accede ad informazioni e documenti per scopi storici utilizza frequentemente dati di carattere personale per i quali la legge prevede alcune garanzie a tutela degli interessati. In considerazione dell'interesse pubblico allo svolgimento di tali trattamenti, il legislatore - con specifico riguardo agli archivi pubblici e a quelli privati dichiarati di notevole interesse storico ai sensi dell'art. 36 del d.P.R. 30 settembre 1963 n. 1409- ha esentato i soggetti che utilizzano dati personali per le suddette finalità dall'obbligo di richiedere il consenso degli interessati ai sensi degli artt. 12, 20 e 28 della legge (l. 31 dicembre 1996, n. 675, in particolare art. 27; dd.lg. 11 maggio 1999, n. 135 e 30 luglio 1999, n. 281, in particolare art. 7, comma 4; d.P.R. 30 settembre 1963, n. 1409, e successive modificazioni e integrazioni).

2) L'utilizzazione di tali dati da parte di utenti ed archivisti deve pertanto rispettare le previsioni di legge e quelle del presente codice di deontologia e di buona condotta, l'osservanza del quale, oltre a rappresentare un obbligo deontologico, costituisce condizione essenziale per la liceità del trattamento dei dati (art. 31, comma 1, lettera h), l. 31 dicembre 1996, n.675; art. 6, d. lg. 30 luglio 1999, n. 281).

3) L'osservanza di tali regole non deve pregiudicare l'indagine, la ricerca, la documentazione e lo studio ovunque svolti, in relazione a figure, fatti e circostanze del passato.

4) I trattamenti di dati personali concernenti la conservazione, l'ordinamento e la comunicazione dei documenti conservati negli Archivi di Stato e negli archivi storici degli enti pubblici sono considerati di rilevante interesse pubblico (art. 23 d.lg. 11 maggio 1999, n. 135).

5) La sottoscrizione del presente codice è promossa per legge dal Garante, nel rispetto del principio di rappresentatività dei soggetti pubblici e privati interessati. Il codice è espressione delle associazioni professionali e delle categorie interessate, ivi comprese le società scientifiche, ed è volto ad assicurare l'equilibrio delle diverse esigenze connesse alla ricerca e alla rappresentazione di fatti storici con i diritti e le libertà fondamentali delle persone interessate (art. 1, l. 31 dicembre 1996, n. 675).

6) Il presente codice, sulla base delle prescrizioni di legge, individua in particolare: a) alcune regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, armonizzate con quelle che riguardano il diritto di cronaca e la manifestazione del pensiero; b) particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare; c) modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati per scopi storici (art. 7, comma 5, d.lg. 30 luglio 1999, n. 281) .

7) La sottoscrizione del presente codice è effettuata ispirandosi, oltre agli artt. 21 e 33 della Costituzione della Repubblica italiana, alle pertinenti fonti e documenti internazionali in materia di ricerca storica e di archivi e in particolare:

a) agli artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;

b) alla Raccomandazione N. R (2000) 13 del 13 luglio 2000 del Consiglio d'Europa;

c) agli artt. 1, 7, 8, 11 e 13 della Carta dei diritti fondamentali dell'Unione europea;

d) ai Principi direttivi per una legge sugli archivi storici e gli archivi correnti, individuati dal Consiglio internazionale degli archivi al congresso di Ottawa nel 1996, e al Codice internazionale di deontologia degli archivisti approvato nel congresso internazionale degli archivi, svoltosi a Pechino nel 1996.

Capo I – Principi generali

Art. 1 - Finalità e ambito di applicazione

1. Le presenti norme sono volte a garantire che l'utilizzazione di dati di carattere personale acquisiti nell'esercizio della libera ricerca storica e del diritto allo studio e all'informazione, nonché nell'accesso ad atti e documenti, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

2. Il presente codice detta disposizioni per i trattamenti di dati personali effettuati per scopi storici in relazione ai documenti conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico. Il codice si applica, senza necessità di sottoscrizione, all'insieme dei trattamenti di dati personali comunque effettuati dagli utenti per scopi storici.

3. Il presente codice reca, altresì, principi-guida di comportamento dei soggetti che trattano per scopi storici dati personali conservati presso archivi pubblici e archivi privati dichiarati di notevole interesse storico, e in particolare:

a) nei riguardi degli archivisti, individua regole di correttezza e di non discriminazione nei confronti degli utenti, indipendentemente dalla loro nazionalità, categoria di appartenenza, livello di istruzione;

b) nei confronti degli utenti, individua cautele per la raccolta, l'utilizzazione e la diffusione dei dati contenuti nei documenti.

4. La competente sovrintendenza archivistica riceve comunicazione da parte di proprietari, possessori e detentori di archivi privati non dichiarati di notevole interesse storico o di singoli documenti di interesse storico, i quali manifestano l'intenzione di applicare il presente codice nella misura per essi compatibile.

Art. 2. - Definizioni

1. Nell'applicazione del presente codice si tiene conto delle definizioni e delle indicazioni contenute nella disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni citate nel preambolo. Ai medesimi fini si intende, altresì:

a) per "archivista", chiunque, persona fisica o giuridica, ente o associazione, abbia responsabilità di controllare, acquisire, trattare, conservare, restaurare e gestire archivi storici, correnti o di deposito della pubblica amministrazione, archivi privati dichiarati di notevole interesse storico, nonché gli archivi privati di cui al precedente art. 1, comma 4;

b) per "utente", chiunque chieda di accedere o acceda per scopi storici a documenti contenenti dati personali, anche per finalità giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero;

c) per "documento", qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali.

Capo II - Regole di condotta per gli archivisti e liceità dei relativi trattamenti

Art. 3 - Regole generali di condotta

1. Nel trattare i dati di carattere personale e i documenti che li contengono, gli archivisti adottano, in armonia con la legge e i regolamenti, le modalità più opportune per favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati.

2. Gli archivisti di enti o istituzioni pubbliche si adoperano per il pieno rispetto, anche da parte dei terzi con cui entrano in contatto per ragioni del proprio ufficio o servizio, delle disposizioni di legge e di regolamento in materia archivistica e, in particolare, di quanto previsto negli artt. 21 e 21-bis del d.P.R. 30 settembre 1963, n. 1409, come modificati dal d.lg. 30 luglio 1999, n. 281, dall'art. 7 del medesimo d.lg. n. 281, e successive modificazioni ed integrazioni.

3. I soggetti che operano presso enti pubblici svolgendo funzioni archivistiche, nel trattare dati di carattere personale si attengono ai doveri di lealtà, correttezza, imparzialità, onestà e diligenza propri dell'esercizio della professione e della qualifica o livello ricoperti. Essi conformano il proprio operato al principio di trasparenza della attività amministrativa.

4. I dati personali trattati per scopi storici possono essere ulteriormente utilizzati per tali scopi, e sono soggetti in linea di principio alla medesima disciplina indipendentemente dal documento in cui

sono contenuti e dal luogo di conservazione, ferme restando le cautele e le garanzie previste per particolari categorie di dati o di trattamenti.

Art. 4 - Conservazione e tutela

1. Gli archivisti si impegnano a:

a) favorire il recupero, l'acquisizione e la tutela dei documenti. A tal fine, operano in conformità con i principi, i criteri metodologici e le pratiche della professione generalmente condivisi ed accettati, curando anche l'aggiornamento sistematico e continuo delle proprie conoscenze storiche, amministrative e tecnologiche;

b) tutelare l'integrità degli archivi e l'autenticità dei documenti, anche elettronici e multimediali, di cui promuovono la conservazione permanente, in particolare di quelli esposti a rischi di cancellazione, dispersione ed alterazione dei dati;

c) salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;

d) assicurare il rispetto delle misure di sicurezza previste dall'art. 15 della legge 31 dicembre 1996, n. 675 e dal d.P.R. 28 luglio 1999, n. 318 e successive integrazioni e modificazioni, sviluppando misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, e adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati.

Art. 5 - Comunicazione e fruizione

1. Gli archivi sono organizzati secondo criteri tali da assicurare il principio della libera fruibilità delle fonti.

2. L'archivista promuove il più largo accesso agli archivi e, attenendosi al quadro della normativa vigente, favorisce l'attività di ricerca e di informazione nonché il reperimento delle fonti.

3. L'archivista informa il ricercatore sui documenti estratti temporaneamente da un fascicolo perché esclusi dalla consultazione.

4. In caso di rilevazione sistematica dei dati realizzata da un archivio in collaborazione con altri soggetti pubblici o privati, per costituire banche dati di intere serie archivistiche, la struttura interessata sottoscrive una apposita convenzione per concordare le modalità di fruizione e le forme di tutela dei soggetti interessati, attenendosi alle disposizioni della legge, in particolare per quanto riguarda il rapporto tra il titolare, il responsabile e gli incaricati del trattamento, nonché i rapporti con i soggetti esterni interessati ad accedere ai dati.

Art. 6 - Impegno di riservatezza

1. Gli archivisti si impegnano a:

a) non fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attività anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati. Nel caso in cui l'archivista svolga ricerche per fini personali o comunque estranei alla propria attività professionale, è soggetto alle stesse regole e ai medesimi limiti previsti per gli utenti;

b) mantenere riservate le notizie e le informazioni concernenti i dati personali apprese nell'esercizio delle proprie attività.

2. L'archivista osserva tali doveri di riserbo anche dopo la cessazione dalla propria attività.

Art. 7 - Aggiornamento dei dati

1. L'archivista favorisce l'esercizio del diritto degli interessati all'aggiornamento, alla rettifica o all'integrazione dei dati, garantendone la conservazione secondo modalità che assicurino la distinzione delle fonti originarie dalla documentazione successivamente acquisita.

2. Ai fini dell'applicazione dell'art. 13 della legge n. 675/1996, in presenza di eventuali richieste generalizzate di accesso ad un'ampia serie di dati o documenti, l'archivista pone a disposizione gli strumenti di ricerca e le fonti pertinenti fornendo al richiedente idonee indicazioni per una loro agevole consultazione.

3. In caso di esercizio di un diritto, ai sensi dell'art. 13, comma 3, della legge n. 675/1996, da parte di chi vi abbia interesse in relazione a dati personali che riguardano persone decedute e documenti assai risalenti nel tempo, la sussistenza dell'interesse è valutata anche in riferimento al tempo trascorso.

Art. 8 - Fonti orali

1. In caso di trattamento di fonti orali, è necessario che gli intervistati abbiano espresso il proprio consenso in modo esplicito, eventualmente in forma verbale, anche sulla base di una informativa semplificata che renda nota almeno l'identità e l'attività svolta dall'intervistatore nonché le finalità della raccolta dei dati.

2. Gli archivi che acquisiscono fonti orali richiedono all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti nell'intervista stessa e del relativo consenso manifestato dagli intervistati.

Capo III – Regole di condotta per gli archivisti e liceità dei relativi trattamenti

Art. 9 - Regole generali di condotta

1. Nell'accedere alle fonti e nell'esercitare l'attività di studio, ricerca e manifestazione del pensiero, gli utenti, quando trattino i dati di carattere personale, secondo quanto previsto dalla legge e dai regolamenti, adottano le modalità più opportune per favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate.

2. In applicazione del principio di cui al comma 1, gli utenti utilizzano i documenti sotto la propria responsabilità e conformandosi agli scopi perseguiti e delineati nel progetto di ricerca, nel rispetto dei principi di pertinenza ed indispensabilità di cui all'art. 7, del d.lg. 30 luglio 1999, n. 281.

Art. 10 - Accesso agli archivi pubblici

1. L'accesso agli archivi pubblici è libero. Tutti gli utenti hanno diritto ad accedere agli archivi con eguali diritti e doveri.

2. Fanno eccezione, ai sensi delle leggi vigenti, i documenti di carattere riservato relativi alla politica interna ed estera dello Stato che divengono consultabili cinquanta anni dopo la loro data e quelli contenenti i dati di cui agli artt. 22 e 24 della legge n. 675/1996, che divengono liberamente consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute o la vita sessuale oppure rapporti riservati di tipo familiare.

3. L'autorizzazione alla consultazione dei documenti di cui al comma 2 può essere rilasciata prima della scadenza dei termini dal Ministro dell'Interno, previo parere del direttore dell'Archivio di Stato o del sovrintendente archivistico competenti e udita la Commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati istituita presso il Ministero dell'Interno, secondo la procedura dettata dagli artt. 8 e 9 del decreto legislativo n. 281/1999.

4. In caso di richiesta di autorizzazione a consultare i documenti di cui al comma 2 prima della scadenza dei termini, l'utente presenta all'ente che li conserva un progetto di ricerca che, in relazione alle fonti riservate per le quali chiede l'autorizzazione, illustri le finalità della ricerca e le modalità di diffusione dei dati. Il richiedente ha facoltà di presentare ogni altra documentazione utile.

5. L'autorizzazione di cui al comma 3 alla consultazione è rilasciata a parità di condizioni ad ogni altro richiedente. La valutazione della parità di condizioni avviene sulla base del progetto di ricerca di cui al comma 4.

6. L'autorizzazione alla consultazione dei documenti, di cui al comma 3, prima dello scadere dei termini, può contenere cautele volte a consentire la comunicazione dei dati senza ledere i diritti, le libertà e la dignità delle persone interessate.

7. Le cautele possono consistere anche, a seconda degli obiettivi della ricerca desumibili dal progetto, nell'obbligo di non diffondere i nomi delle persone, nell'uso delle sole iniziali dei nominativi degli interessati, nell'oscuramento dei nomi in una banca dati, nella sottrazione temporanea di singoli documenti dai fascicoli o nel divieto di riproduzione dei documenti. Particolare attenzione è prestata al principio della pertinenza e all'indicazione di fatti o circostanze che possono rendere facilmente individuabili gli interessati.

8. L'autorizzazione di cui al comma 3 è personale e il titolare dell'autorizzazione non può delegare altri al conseguente trattamento dei dati. I documenti mantengono il loro carattere riservato e non possono essere ulteriormente utilizzati da altri soggetti senza la relativa autorizzazione.

Art. 11 - Diffusione

1. L'interpretazione dell'utente, nel rispetto del diritto alla riservatezza, del diritto all'identità personale e della dignità degli interessati, rientra nella sfera della libertà di parola e di manifestazione del pensiero costituzionalmente garantite.

2. Nel far riferimento allo stato di salute delle persone l'utente si astiene dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad una determinata persona identificata o identificabile.

3. La sfera privata delle persone note o che abbiano esercitato funzioni pubbliche deve essere rispettata nel caso in cui le notizie o i dati non abbiano alcun rilievo sul loro ruolo o sulla loro vita pubblica.

4. In applicazione di quanto previsto dall'art. 7, comma 2, del d.lg. n. 281/1999, al momento della diffusione dei dati il principio della pertinenza è valutato dall'utente con particolare riguardo ai singoli dati personali contenuti nei documenti, anziché ai documenti nel loro complesso. L'utente può diffondere i dati personali se pertinenti e indispensabili alla ricerca e se gli stessi non ledono la dignità e la riservatezza delle persone.

5. L'utente non è tenuto a fornire l'informativa di cui all'art. 10, comma 3, della legge n. 675/1996 nei casi in cui tale adempimento comporti l'impiego di mezzi manifestamente sproporzionati.

6. L'utente può utilizzare i dati elaborati o le copie dei documenti contenenti dati personali, accessibili su autorizzazione, solo ai fini della propria ricerca, e ne cura la riservatezza anche rispetto ai terzi.

Art. 12 - Applicazione del codice

1. I soggetti pubblici e privati, comprese le società scientifiche e le associazioni professionali, che siano tenuti ad applicare il presente codice si impegnano, con i modi e nelle forme previste dai propri ordinamenti, a promuoverne la massima diffusione e la conoscenza, nonché ad assicurarne il rispetto.

2. Nel caso degli archivi degli enti pubblici e degli archivi privati dichiarati di notevole interesse storico, le sovrintendenze archivistiche promuovono la diffusione e l'applicazione del codice.

Art. 13 - Violazione delle regole di condotta

1. Nell'ambito degli archivi pubblici le amministrazioni competenti applicano le sanzioni previste dai rispettivi ordinamenti.

2. Le società e le associazioni tenute ad applicare il presente codice adottano, sulla base dei propri ordinamenti e regolamenti, le opportune misure in caso di violazione del codice stesso, ferme restando le sanzioni di legge.

3. La violazione delle prescrizioni del presente codice da parte degli utenti è comunicata agli organi competenti per il rilascio delle autorizzazioni a consultare documenti riservati prima del decorso dei termini di legge, ed è considerata ai fini del rilascio dell'autorizzazione medesima. L'Amministrazione competente, secondo il proprio ordinamento, può altresì escludere temporaneamente dalle sale di studio i soggetti responsabili della violazione delle regole del presente codice. Gli stessi possono essere esclusi da ulteriori autorizzazioni alla consultazione di documenti riservati.

4. Oltre a quanto previsto dalla legge per la denuncia di reato cui sono tenuti i pubblici ufficiali, i soggetti di cui ai commi 1 e 2 possono segnalare al Garante le violazioni delle regole di condotta per l'eventuale adozione dei provvedimenti e delle sanzioni di competenza.

Art. 14 - Entrata in vigore

1. Il presente codice si applica a decorrere dal quindicesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

DOCUMENTAZIONE INTERNAZIONALE E COMUNITARIA

UNIONE EUROPA

117 CARTA DI VENEZIA

(30 settembre 2000) (*)

"I commissari per la protezione dei dati dei diversi Paesi riuniti a Venezia in occasione della 22ª Conferenza internazionale sulla privacy e la protezione dei dati personali convengono sulla necessità di ribadire principi e criteri comuni per la protezione dei dati in una situazione in cui si fanno sempre più pervasive le tecnologie di trattamento dei dati, aumenta il numero dei soggetti che possono utilizzarle e si intensifica ogni giorno di più la circolazione delle informazioni su scala mondiale.

Esistono già molti documenti internazionali in materia, dalle Linee-guida dell'OCSE alla Convenzione del Consiglio d'Europa n. 108, alle direttive dell'Unione europea, alle risoluzioni e raccomandazioni di organismi internazionali.

Questi documenti costituiscono già un significativo nucleo di riferimento di principi assistito da largo consenso e rappresentano un punto di partenza per un lavoro comune, al fine di giungere alla loro applicazione a livello mondiale tenendo conto dei numerosi mutamenti tecnologici e sociali.

Alla luce del riconoscimento della privacy come diritto fondamentale della persona e quale elemento costitutivo della libertà del cittadino, il nostro obiettivo dovrebbe essere il riconoscimento a livello globale di linee-guida per il trattamento dei dati personali:

- ribadendo il carattere vincolante di tali principi, relativi in particolare alle finalità della raccolta, alla lealtà e trasparenza del trattamento (con particolare riferimento ai c.d. trattamenti invisibili), alla proporzionalità, alla qualità dei dati, alla durata della conservazione, all'accesso e agli altri diritti degli interessati;
- rendendo ancora più effettiva la tutela degli interessati attraverso un controllo indipendente dei trattamenti e la disponibilità di mezzi di ricorso facilmente utilizzabili;
- rafforzando le garanzie per particolari trattamenti di dati come quelli genetici o legati alle diverse forme di sorveglianza elettronica.

Ai cittadini verrebbe così assicurato universalmente un livello di garanzie adeguato e maggiormente condiviso, indipendentemente dal luogo in cui i dati sono trattati e dagli strumenti con i quali tali garanzie sono attuate a livello nazionale e internazionale.

I commissari per la protezione dei dati e la *privacy* opereranno con altri soggetti al fine di meglio definire ed attuare i principi riconosciuti a livello globale".

(*) Dichiarazione sottoscritta dai rappresentanti di 27 Paesi nei quali esiste un'Autorità garante per la protezione dei dati personali, in occasione della Conferenza di Venezia del 28-30 settembre 2000, organizzata dal Garante italiano.

118 CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA DEL 18 DICEMBRE 2000 (*)

Preambolo

I popoli europei nel creare tra loro un'unione sempre più stretta hanno deciso di condividere un futuro di pace fondato su valori comuni.

Consapevole del suo patrimonio spirituale e morale, l'Unione si fonda sui valori indivisibili e universali di dignità umana, di libertà, di uguaglianza e di solidarietà; l'Unione si basa sui principi di democrazia e dello stato di diritto. Essa pone la persona al centro della sua azione istituendo la cittadinanza del l'Unione e creando uno spazio di libertà, sicurezza e giustizia.

L'Unione contribuisce al mantenimento e allo sviluppo di questi valori comuni, nel rispetto della diversità delle culture e delle tradizioni dei popoli europei, dell'identità nazionale degli Stati membri e dell'ordinamento dei loro pubblici poteri a livello nazionale, regionale e locale; essa cerca di promuovere uno sviluppo equilibrato e sostenibile e assicura la libera circolazione delle persone, dei beni, dei servizi e dei capitali nonché la libertà di stabilimento.

A tal fine è necessario, rendendoli più visibili in una Carta, rafforzare la tutela dei diritti fondamentali alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici.

La presente Carta riafferma, nel rispetto delle competenze e dei compiti della Comunità e dell'Unione e del principio di sussidiarietà, i diritti derivanti in particolare dalle tradizioni costituzionali e dagli obblighi internazionali comuni agli Stati membri, dal trattato sull'Unione europea e dai trattati comu nitari, dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dalle carte sociali adottate dalla Comunità e dal Consiglio d'Europa, nonché i diritti riconosciuti dalla giurisprudenza della Corte di giustizia delle Comunità europee e da quella della Corte europea dei diritti dell'uomo.

Il godimento di questi diritti fa sorgere responsabilità e doveri nei confronti degli altri come pure della comunità umana e delle generazioni future.

Pertanto, l'Unione riconosce i diritti, le libertà ed i principi enunciati qui di seguito.

Capo I - Dignità

Articolo 1 - Dignità umana

La dignità umana è inviolabile. Essa deve essere rispettata e tutelata.

Articolo 2 - Diritto alla vita

1. Ogni individuo ha diritto alla vita.
2. Nessuno può essere condannato alla pena di morte, né giustiziato.

Articolo 3 - Diritto all'integrità della persona

1. Ogni individuo ha diritto alla propria integrità fisica e psichica.
2. Nell'ambito della medicina e della biologia devono essere in particolare rispettati:
- il consenso libero e informato della persona interessata, secondo le modalità definite dalla legge,
- il divieto delle pratiche eugenetiche, in particolare di quelle aventi come scopo la selezione delle persone,
- il divieto di fare del corpo umano e delle sue parti in quanto tali una fonte di lucro,
- il divieto della clonazione riproduttiva degli esseri umani.

Articolo 4 - Proibizione della tortura e delle pene o trattamenti inumani o degradanti

Nessuno può essere sottoposto a tortura, né a pene o trattamenti inumani o degradanti.

Articolo 5 - Proibizione della schiavitù e del lavoro forzato

1. Nessuno può essere tenuto in condizioni di schiavitù o di servitù.
2. Nessuno può essere costretto a compiere un lavoro forzato o obbligatorio.
3. È proibita la tratta degli esseri umani.

(*) *Gazzetta ufficiale delle Comunità europee - 2000/C - 364/01.*

Capo II - Libertà

Articolo 6 - Diritto alla libertà e alla sicurezza

Ogni individuo ha diritto alla libertà e alla sicurezza.

Articolo 7 - Rispetto della vita privata e della vita familiare

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8 - Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Articolo 9 - Diritto di sposarsi e di costituire una famiglia

Il diritto di sposarsi e il diritto di costituire una famiglia sono garantiti secondo le leggi nazionali che ne disciplinano l'esercizio.

Articolo 10 - Libertà di pensiero, di coscienza e di religione

1. Ogni individuo ha diritto alla libertà di pensiero, di coscienza e di religione. Tale diritto include la libertà di cambiare religione o convinzione, così come la libertà di manifestare la propria religione o la propria convinzione individualmente o collettivamente, in pubblico o in privato, mediante il culto, l'insegnamento, le pratiche e l'osservanza dei riti.

2. Il diritto all'obiezione di coscienza è riconosciuto secondo le leggi nazionali che ne disciplinano l'esercizio.

Articolo 11 - Libertà di espressione e d'informazione

1. Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.

2. La libertà dei media e il loro pluralismo sono rispettati.

Articolo 12 - Libertà di riunione e di associazione

1. Ogni individuo ha diritto alla libertà di riunione pacifica e alla libertà di associazione a tutti i livelli, segnatamente in campo politico, sindacale e civico, il che implica il diritto di ogni individuo di fondare sindacati insieme con altri e di aderirvi per la difesa dei propri interessi.

2. I partiti politici a livello dell'Unione contribuiscono a esprimere la volontà politica dei cittadini dell'Unione.

Articolo 13 - Libertà delle arti e delle scienze

Le arti e la ricerca scientifica sono libere. La libertà accademica è rispettata.

Articolo 14 - Diritto all'istruzione

1. Ogni individuo ha diritto all'istruzione e all'accesso alla formazione professionale e continua.

2. Questo diritto comporta la facoltà di accedere gratuitamente all'istruzione obbligatoria.

3. La libertà di creare istituti di insegnamento nel rispetto dei principi democratici, così come il diritto dei genitori di provvedere all'educazione e all'istruzione dei loro figli secondo le loro convinzioni religiose, filosofiche e pedagogiche, sono rispettati secondo le leggi nazionali che ne disciplinano l'esercizio.

Articolo 15 - Libertà professionale e diritto di lavorare

1. Ogni individuo ha il diritto di lavorare e di esercitare una professione liberamente scelta o accettata.

2. Ogni cittadino dell'Unione ha la libertà di cercare un lavoro, di lavorare, di stabilirsi o di prestare servizi in qualunque Stato membro.

3. I cittadini dei paesi terzi che sono autorizzati a lavorare nel territorio degli Stati membri hanno diritto a condizioni di lavoro equivalenti a quelle di cui godono i cittadini dell'Unione.

Articolo 16 - Libertà d'impresa

È riconosciuta la libertà d'impresa, conformemente al diritto comunitario e alle legislazioni e prassi nazionali.

Articolo 17 - Diritto di proprietà

1. Ogni individuo ha il diritto di godere della proprietà dei beni che ha acquistato legalmente, di usarli, di disporne e di lasciarli in eredità. Nessuno può essere privato della proprietà se non per causa di pubblico interesse, nei casi e nei modi previsti dalla legge e contro il pagamento in tempo utile di una giusta indennità per la perdita della stessa. L'uso dei beni può essere regolato dalla legge nei limiti imposti dall'interesse generale.

2. La proprietà intellettuale è protetta.

Articolo 18 - Diritto di asilo

Il diritto di asilo è garantito nel rispetto delle norme stabilite dalla convenzione di Ginevra del 28 luglio 1951 e dal protocollo del 31 gennaio 1967, relativi allo status dei rifugiati, e a norma del trattato che istituisce la Comunità europea.

Articolo 19 - Protezione in caso di allontanamento, di espulsione e di estradizione

1. Le espulsioni collettive sono vietate.

2. Nessuno può essere allontanato, espulso o estradato verso uno Stato in cui esiste un rischio serio di essere sottoposto alla pena di morte, alla tortura o ad altre pene o trattamenti inumani o degradanti.

Capo III - Uguaglianza

Articolo 20 - Uguaglianza davanti alla legge

Tutte le persone sono uguali davanti alla legge.

Articolo 21 - Non discriminazione

1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età o le tendenze sessuali.

2. Nell'ambito d'applicazione del trattato che istituisce la Comunità europea e del trattato sull'Unione europea è vietata qualsiasi discriminazione fondata sulla cittadinanza, fatte salve le disposizioni parti colari contenute nei trattati stessi.

Articolo 22 - Diversità culturale, religiosa e linguistica

L'Unione rispetta la diversità culturale, religiosa e linguistica.

Articolo 23 - Parità tra uomini e donne

La parità tra uomini e donne deve essere assicurata in tutti i campi, compreso in materia di occupazione, di lavoro e di retribuzione. Il principio della parità non osta al mantenimento o all'adozione di misure che prevedano vantaggi specifici a favore del sesso sottorappresentato.

Articolo 24 - Diritti del bambino

1. I bambini hanno diritto alla protezione e alle cure necessarie per il loro benessere. Essi possono esprimere liberamente la propria opinione; questa viene presa in considerazione sulle questioni che li riguardano in funzione della loro età e della loro maturità.

2. In tutti gli atti relativi ai bambini, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del bambino deve essere considerato preminente.

3. Ogni bambino ha diritto di intrattenere regolarmente relazioni personali e contatti diretti con i due genitori, salvo qualora ciò sia contrario al suo interesse.

Articolo 25 - Diritti degli anziani

L'Unione riconosce e rispetta il diritto degli anziani di condurre una vita dignitosa e indipendente e di partecipare alla vita sociale e culturale.

Articolo 26 - Inserimento dei disabili

L'Unione riconosce e rispetta il diritto dei disabili di beneficiare di misure intese a garantirne l'autonomia, l'inserimento sociale e professionale e la partecipazione alla vita della comunità.

Capo IV - Solidarietà

Articolo 27 - Diritto dei lavoratori all'informazione e alla consultazione nell'ambito dell'impresa

Ai lavoratori o ai loro rappresentanti devono essere garantite, ai livelli appropriati, l'informazione e la consultazione in tempo utile nei casi e alle condizioni previsti dal diritto comunitario e dalle legislazioni e prassi nazionali.

Articolo 28 - Diritto di negoziazione e di azioni collettive

I lavoratori e i datori di lavoro, o le rispettive organizzazioni, hanno, conformemente al diritto comunitario e alle legislazioni e prassi nazionali, il diritto di negoziare e di concludere contratti collettivi, ai livelli appropriati, e di ricorrere, in caso di conflitti di interessi, ad azioni collettive per la difesa dei loro interessi, compreso lo sciopero.

Articolo 29 - Diritto di accesso ai servizi di collocamento

Ogni individuo ha il diritto di accedere a un servizio di collocamento gratuito.

Articolo 30 - Tutela in caso di licenziamento ingiustificato

Ogni lavoratore ha il diritto alla tutela contro ogni licenziamento ingiustificato, conformemente al diritto comunitario e alle legislazioni e prassi nazionali.

Articolo 31 - Condizioni di lavoro giuste ed eque

1. Ogni lavoratore ha diritto a condizioni di lavoro sane, sicure e dignitose.

2. Ogni lavoratore ha diritto a una limitazione della durata massima del lavoro e a periodi di riposo giornalieri e settimanali e a ferie annuali retribuite.

Articolo 32 - Divieto del lavoro minorile e protezione dei giovani sul luogo di lavoro

Il lavoro minorile è vietato. L'età minima per l'ammissione al lavoro non può essere inferiore all'età in cui termina la scuola dell'obbligo, fatte salve le norme più favorevoli ai giovani ed eccettuate deroghe limitate.

I giovani ammessi al lavoro devono beneficiare di condizioni di lavoro appropriate alla loro età ed essere protetti contro lo sfruttamento economico o contro ogni lavoro che possa minarne la sicurezza, la salute, lo sviluppo fisico, mentale, morale o sociale o che possa mettere a rischio la loro istruzione.

Articolo 33 - Vita familiare e vita professionale

1. È garantita la protezione della famiglia sul piano giuridico, economico e sociale.

2. Al fine di poter conciliare vita familiare e vita professionale, ogni individuo ha il diritto di essere tutelato contro il licenziamento per un motivo legato alla maternità e il diritto a un congedo di maternità retribuito e a un congedo parentale dopo la nascita o l'adozione di un figlio.

Articolo 34 - Sicurezza sociale e assistenza sociale

1. L'Unione riconosce e rispetta il diritto di accesso alle prestazioni di sicurezza sociale e ai servizi sociali che assicurano protezione in casi quali la maternità, la malattia, gli infortuni sul lavoro, la dipendenza o la vecchiaia, oltre che in caso di perdita del posto di lavoro, secondo le modalità stabilite dal diritto comunitario e le legislazioni e prassi nazionali.

2. Ogni individuo che risieda o si sposti legalmente all'interno dell'Unione ha diritto alle prestazioni di sicurezza sociale e ai benefici sociali conformemente al diritto comunitario e alle legislazioni e prassi nazionali.

3. Al fine di lottare contro l'esclusione sociale e la povertà, l'Unione riconosce e rispetta il diritto all'assistenza sociale e all'assistenza abitativa volte a garantire un'esistenza dignitosa a tutti coloro che non dispongano di risorse sufficienti, secondo le modalità stabilite dal diritto comunitario e le legi slazioni e prassi nazionali.

Articolo 35 - Protezione della salute

Ogni individuo ha il diritto di accedere alla prevenzione sanitaria e di ottenere cure mediche alle condizioni stabilite dalle legislazioni e prassi nazionali. Nella definizione e nell'attuazione di tutte le politiche ed attività dell'Unione è garantito un livello elevato di protezione della salute umana.

Articolo 36 - Accesso ai servizi d'interesse economico generale

Al fine di promuovere la coesione sociale e territoriale dell'Unione, questa riconosce e rispetta l'accesso ai servizi d'interesse economico generale quale previsto dalle legislazioni e prassi nazionali, conforme mente al trattato che istituisce la Comunità europea.

Articolo 37 - Tutela dell'ambiente

Un livello elevato di tutela dell'ambiente e il miglioramento della sua qualità devono essere integrati nelle politiche dell'Unione e garantiti conformemente al principio dello sviluppo sostenibile.

Articolo 38 - Protezione dei consumatori

Nelle politiche dell'Unione è garantito un livello elevato di protezione dei consumatori.

Capo V - Cittadinanza

Articolo 39 - Diritto di voto e di eleggibilità alle elezioni del Parlamento europeo

1. Ogni cittadino dell'Unione ha il diritto di voto e di eleggibilità alle elezioni del Parlamento europeo nello Stato membro in cui risiede, alle stesse condizioni dei cittadini di detto Stato.
2. I membri del Parlamento europeo sono eletti a suffragio universale diretto, libero e segreto.

Articolo 40 - Diritto di voto e di eleggibilità alle elezioni comunali

Ogni cittadino dell'Unione ha il diritto di voto e di eleggibilità alle elezioni comunali nello Stato membro in cui risiede, alle stesse condizioni dei cittadini di detto Stato.

Articolo 41 - Diritto ad una buona amministrazione

1. Ogni individuo ha diritto a che le questioni che lo riguardano siano trattate in modo imparziale, equo ed entro un termine ragionevole dalle istituzioni e dagli organi dell'Unione.
2. Tale diritto comprende in particolare:
- il diritto di ogni individuo di essere ascoltato prima che nei suoi confronti venga adottato un provvedimento individuale che gli rechi pregiudizio,
- il diritto di ogni individuo di accedere al fascicolo che lo riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale,
- l'obbligo per l'amministrazione di motivare le proprie decisioni.
3. Ogni individuo ha diritto al risarcimento da parte della Comunità dei danni cagionati dalle sue istituzioni o dai suoi agenti nell'esercizio delle loro funzioni conformemente ai principi generali comuni agli ordinamenti degli Stati membri.
4. Ogni individuo può rivolgersi alle istituzioni dell'Unione in una delle lingue del trattato e deve ricevere una risposta nella stessa lingua.

Articolo 42 - Diritto d'accesso ai documenti

Qualsiasi cittadino dell'Unione o qualsiasi persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro ha il diritto di accedere ai documenti del Parlamento europeo, del Consiglio e della Commissione.

Articolo 43 - Mediatore

Qualsiasi cittadino dell'Unione o qualsiasi persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro ha il diritto di sottoporre al mediatore dell'Unione casi di cattiva amministrazione nell'azione delle istituzioni o degli organi comunitari, salvo la Corte di giustizia e il Tribunale di primo grado nell'esercizio delle loro funzioni giurisdizionali.

Articolo 44 - Diritto di petizione

Qualsiasi cittadino dell'Unione o qualsiasi persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro ha il diritto di presentare una petizione al Parlamento europeo.

Articolo 45 - Libertà di circolazione e di soggiorno

1. Ogni cittadino dell'Unione ha il diritto di circolare e di soggiornare liberamente nel territorio degli Stati membri.

2. La libertà di circolazione e di soggiorno può essere accordata, conformemente al trattato che istituisce la Comunità europea, ai cittadini dei paesi terzi che risiedono legalmente nel territorio di uno Stato membro.

Articolo 46 - Tutela diplomatica e consolare

Ogni cittadino dell'Unione gode, nel territorio di un paese terzo nel quale lo Stato membro di cui ha la cittadinanza non è rappresentato, della tutela delle autorità diplomatiche e consolari di qualsiasi Stato membro, alle stesse condizioni dei cittadini di detto Stato.

Capo VI - Giustizia

Articolo 47 - Diritto a un ricorso effettivo e a un giudice imparziale

Ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni individuo ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni individuo ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia.

Articolo 48 - Presunzione di innocenza e diritti della difesa

1. Ogni imputato è considerato innocente fino a quando la sua colpevolezza non sia stata legalmente provata.
2. Il rispetto dei diritti della difesa è garantito ad ogni imputato.

Articolo 49 - Principi della legalità e della proporzionalità dei reati e delle pene

1. Nessuno può essere condannato per un'azione o un'omissione che, al momento in cui è stata commessa, non costituiva reato secondo il diritto interno o il diritto internazionale. Parimenti, non può essere inflitta una pena più grave di quella applicabile al momento in cui il reato è stato commesso. Se, successivamente alla commissione del reato, la legge prevede l'applicazione di una pena più lieve, occorre applicare quest'ultima.
2. Il presente articolo non osta al giudizio e alla condanna di una persona colpevole di un'azione o di un'omissione che, al momento in cui è stata commessa, costituiva un crimine secondo i principi generali riconosciuti da tutte le nazioni.
3. Le pene inflitte non devono essere sproporzionate rispetto al reato.

Articolo 50 - Diritto di non essere giudicato o punito due volte per lo stesso reato

Nessuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge.

Capo VII - Disposizioni generali

Articolo 51 - Ambito di applicazione

1. Le disposizioni della presente Carta si applicano alle istituzioni e agli organi dell'Unione nel rispetto del principio di sussidiarietà come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Pertanto, i suddetti soggetti rispettano i diritti, osservano i principi e ne promuovono l'applicazione secondo le rispettive competenze.
2. La presente Carta non introduce competenze nuove o compiti nuovi per la Comunità e per l'Unione, né modifica le competenze e i compiti definiti dai trattati.

Articolo 52 - Portata dei diritti garantiti

1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.
2. I diritti riconosciuti dalla presente Carta che trovano fondamento nei trattati comunitari o nel trattato sull'Unione europea si esercitano alle condizioni e nei limiti definiti dai trattati stessi.

3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa.

Articolo 53 - Livello di protezione

Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti, nel rispettivo ambito di applicazione, dal diritto dell'Unione, dal diritto internazionale, dalle convenzioni internazionali delle quali l'Unione, la Comunità o tutti gli Stati membri sono parti contraenti, in particolare la convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, e dalle costituzioni degli Stati membri.

Articolo 54 - Divieto dell'abuso di diritto

Nessuna disposizione della presente Carta deve essere interpretata nel senso di comportare il diritto di esercitare un'attività o compiere un atto che miri alla distruzione dei diritti o delle libertà riconosciuti nella presente Carta o di imporre a tali diritti e libertà limitazioni più ampie di quelle previste dalla presente Carta.

COMMISSIONE EUROPEA

119 CLAUSOLE CONTRATTUALI PER IL TRASFERIMENTO DI DATI IN PAESI TERZI

C(2001) 1539 definitivo - IT

Decisione della Commissione del 15 giugno 2001
relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE

(Testo rilevante ai fini del SEE)

La Commissione delle comunità europee,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1) e in particolare l'articolo 26, paragrafo 4,

considerando quanto segue:

1) A norma della direttiva 95/46/CE gli Stati membri devono assicurarsi che un trasferimento di dati a carattere personale verso un paese terzo possa avere luogo soltanto se il paese terzo in questione garantisce un livello adeguato di protezione dei dati e se la legislazione degli Stati membri attuativa delle altre disposizioni della direttiva viene rispettata prima del trasferimento.

2) L'articolo 26, paragrafo 2 della direttiva 95/46/CE prevede tuttavia che gli Stati membri possano autorizzare, nel rispetto di determinate garanzie, un trasferimento o una serie di trasferimenti di dati personali verso paesi terzi che non assicurino un livello adeguato di protezione dei dati. Dette garanzie possono in particolare essere fornite dalla previsione di appropriate clausole contrattuali.

3) A norma della direttiva 95/46/CE, il livello di protezione dei dati deve essere valutato alla luce di tutte le circostanze relative all'operazione o serie di operazioni di trasferimento di dati. Il gruppo di lavoro sulla protezione degli individui per quanto riguarda il trattamento dei dati personali costituito ai sensi della direttiva (2) ha elaborato una serie di linee direttrici per l'effettuazione di questa valutazione (3).

4) L'articolo 26, paragrafo 2 della direttiva 95/46/CE, che consente una certa flessibilità nei riguardi di organizzazioni che debbano trasferire dati personali in paesi terzi, nonché l'articolo 26, paragrafo 4,

(1) GU L 281 del 23.11.1995, pag. 31.
(2) Indirizzo Internet del gruppo di lavoro:
http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm
(3) **WP4 (5020/97)** "Primi orientamenti sui trasferimenti di dati personali verso paesi terzi - Possibili modalità di verifica dell'adeguatezza", documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997;
WP 7 (5057/97) Documento di lavoro: "Valutazione dell'autoregolamentazione dell'industria: quando reca un contributo significativo al livello di protezione dei dati in un paese terzo?", approvato dal gruppo di lavoro il 14 gennaio 1998;
WP 9 (5005/98) Documento di lavoro: "Pareri preliminari sull'impiego delle clausole contrattuali nel contesto dei trasferimenti di dati personali a paesi terzi", approvato dal gruppo di lavoro il 22 aprile 1998;
WP12: Trasferimenti di dati personali a paesi terzi: Applicazione degli articoli 25 e 26 della direttiva UE per la protezione dei dati, approvato dal gruppo di lavoro il 24 luglio 1998, disponibile sul sito Internet:
europa.eu.int/comm/internal_markt/en/media.dataprot/wpdocs/wp12/en della Commissione europea.

che prevede clausole contrattuali tipo, costituiscono elementi essenziali per il mantenimento del necessario flusso di dati personali fra la Comunità europea e i paesi terzi, senza creare inutili oneri per gli operatori economici. Tali disposizioni rivestono particolare importanza in quanto è probabile che la Commissione, a breve o anche a medio termine, constati l'adeguatezza del livello di protezione ai sensi dell'articolo 25, paragrafo 6 soltanto per un numero limitato di paesi.

5) Le clausole contrattuali tipo costituiscono soltanto una delle possibilità previste dalla direttiva 95/46/CE per la liceità dei trasferimenti di dati personali in paesi terzi, oltre a quanto previsto agli articoli 25 e 26, paragrafi 1 e 2. Sarà più agevole per le organizzazioni trasferire i dati in paesi terzi incorporando tali clausole nei contratti. Le clausole contrattuali tipo riguardano soltanto la protezione dei dati. Gli esportatori e importatori dei dati sono liberi di inserire altre clausole a carattere commerciale ritenute pertinenti ai fini del contratto, ad esempio in materia di assistenza reciproca in caso di controversie con le persone interessate dai dati o con un'autorità di controllo, purché esse non siano incompatibili con le clausole tipo.

6) La presente decisione deve applicarsi fatte salve le eventuali autorizzazioni concesse dagli Stati membri ai sensi delle disposizioni nazionali di attuazione dell'articolo 26, paragrafo 2. La presente decisione ha esclusivamente l'effetto di vietare che gli Stati membri rifiutino di riconoscere come adeguate garanzie le clausole contrattuali in essa contenute, e non produce alcun effetto su clausole contrattuali diverse.

7) La presente decisione si limita a prevedere che le clausole di cui all'allegato possono essere utilizzate da un responsabile del trattamento con sede nella Comunità europea come garanzie sufficienti ai sensi dell'articolo 26, paragrafo 2 della direttiva 95/46/CE. Il trasferimento di dati personali in paesi terzi costituisce un'operazione di trattamento in uno Stato membro la cui legittimità è soggetta alla legislazione nazionale. Le autorità di controllo in materia di protezione dei dati degli Stati membri, nell'esercizio di funzioni e poteri loro attribuiti ai sensi dell'articolo 28 della direttiva 95/46/CE, restano competenti per determinare se l'esportatore dei dati ha rispettato la legislazione nazionale che recepisce le disposizioni della direttiva 95/46/CE, ed in particolare eventuali norme specifiche per quanto riguarda l'obbligo di fornire informazioni a norma della direttiva.

8) L'ambito di applicazione della presente decisione non si estende al trasferimento di dati personali, operato da responsabili del trattamento aventi sede nella Comunità a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici. Detti trasferimenti non richiedono le stesse garanzie in quanto l'incaricato del trattamento agisce esclusivamente per conto del responsabile del trattamento. La Commissione intende provvedere in ordine a questo genere di trattamenti con una successiva decisione.

9) È opportuno stabilire le informazioni minime che le parti devono specificare nel contratto relativo al trasferimento. Gli Stati membri devono mantenere il potere di specificare le informazioni che le parti sono tenute a fornire. L'applicazione della presente decisione sarà rivista alla luce dell'esperienza acquisita.

10) La Commissione potrà inoltre considerare in futuro se altre clausole tipo presentate da organizzazioni commerciali o altre parti interessate offrano garanzie adeguate ai sensi della direttiva 95/46/CE.

11) Le parti devono essere libere di convenire le prescrizioni alle quali deve conformarsi l'importatore dei dati ai fini dell'effettiva protezione degli stessi, ma determinati principi di protezione devono essere applicati in qualunque circostanza.

12) I dati devono essere trattati e successivamente utilizzati o comunicati ulteriormente soltanto per scopi determinati e non devono essere trattenuti che per il tempo strettamente necessario.

13) Ai sensi dell'articolo 12 della direttiva 95/46/CE le persone interessate dai dati devono avere accesso a tutti i dati che le riguardano e se del caso diritto di rettifica, di cancellazione o di congelamento di determinati dati.

14) L'ulteriore trasferimento di dati personali ad altro responsabile del trattamento, avente sede in un paese terzo, deve essere consentito soltanto subordinatamente al rispetto di determinate condizioni, tendenti in particolare a garantire che le persone interessate dai dati siano adeguatamente informate ed abbiano la possibilità di formulare osservazioni e, in casi determinati, di negare il proprio consenso al trasferimento.

15) Oltre a verificare se i trasferimenti in paesi terzi sono conformi alla legislazione nazionale, le autorità di controllo devono inoltre svolgere un ruolo fondamentale nel meccanismo contrattuale, al fine di garantire che i dati personali siano adeguatamente protetti dopo il trasferimento. In determinate fattispecie le autorità degli Stati membri devono avere la possibilità di proibire o sospendere un trasferimento o serie di trasferimenti di dati basati sulle clausole contrattuali tipo, in relazione a casi eccezionali in cui si accerti che un trasferimento su base contrattuale avrebbe la probabile conseguenza di recare sostanziale pregiudizio alle garanzie di adeguata tutela delle persone interessate dai dati.

16) Deve potersi esigere l'esecuzione delle clausole contrattuali tipo non soltanto su istanza delle parti che stipulano il contratto, ma anche delle persone interessate dai dati, in particolare qualora le stesse subiscano pregiudizio in conseguenza di violazioni del contratto.

17) Il contratto deve essere retto dalla legge dello Stato membro in cui ha sede l'esportatore dei dati, che abiliti il terzo beneficiario di un contratto a ottenerne l'esecuzione. Le persone interessate dai dati devono poter essere rappresentate da associazioni o altre organizzazioni se lo desiderano e ciò sia autorizzato dalla legislazione nazionale.

18) Per ridurre le difficoltà pratiche che le persone interessate dai dati potrebbero incontrare all'atto dell'esercizio dei loro diritti in base alle clausole contrattuali tipo, l'esportatore e l'importatore dei dati devono essere tenuti responsabili separatamente e in solido per danni derivanti da qualsiasi violazione di disposizioni soggette alla clausola del terzo beneficiario.

19) Le persone interessate dai dati hanno diritto di azione nonché diritto al risarcimento del danno a carico dell'esportatore e dell'importatore dei dati stessi, o di entrambi, per i danni derivanti da qualsiasi atto incompatibile con gli obblighi di cui alle clausole contrattuali tipo. Entrambe le parti possono essere esonerate da tale responsabilità se dimostrano di non essere responsabili del danno.

20) La responsabilità separatamente e in solido non si estende alle disposizioni escluse dalla clausola del terzo beneficiario, e non espone necessariamente una delle parti a responsabilità per illecito trattamento ad opera dell'altra. Benché tale reciproco indennizzo fra le parti non costituisca un requisito per l'adeguatezza della tutela delle persone interessate dai dati e le parti possano quindi eliminarlo dal contratto, esso deve essere incluso nelle clausole contrattuali tipo a fini di chiarezza e per evitare che le parti siano obbligate a concordare di volta in volta le clausole in materia di indennizzo.

21) Qualora una disputa fra le parti e le persone interessate dai dati non possa essere risolta amichevolmente e le persone interessate invochino la clausola del terzo beneficiario, le parti convengono di riconoscere alle persone interessate dai dati la possibilità di scegliere fra la mediazione, l'arbitrato e l'azione in giudizio. La misura in cui le persone interessate dai dati potranno effettivamente esercitare tale scelta dipenderà dalla disponibilità di sistemi attendibili e riconosciuti di mediazione e di arbitrato. La mediazione ad opera delle autorità di controllo degli Stati membri deve costituire un'alternativa nel caso in cui esse la forniscano.

22) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito in virtù dell'articolo 29 della direttiva 95/46/CE, ha emesso un parere sul livello di protezione raggiunto in base alle clausole contrattuali tipo allegate alla presente decisione che è stato preso in considerazione per la stesura della stessa (4).

23) Le disposizioni di cui alla presente decisione sono conformi al parere del comitato istituito in virtù dell'articolo 31 della direttiva 95/46/CE,

ha adottato la presente decisione:

Articolo 1

Le clausole contrattuali tipo di cui all'allegato della presente decisione costituiscono garanzie sufficienti ai fini della tutela della riservatezza, dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi a norma dell'articolo 26, paragrafo 2 della direttiva 95/46/CE.

(4) Parere n. 1/2001 adottato dal gruppo di lavoro in data 26.1.2001 (DG MARKT 5102/00 WP 38), disponibile sul sito "Europa" della Commissione europea.

Articolo 2

La presente decisione concerne esclusivamente l'adeguatezza della tutela assicurata dalle clausole contrattuali tipo per il trasferimento di dati personali di cui all'allegato. Essa si applica fatte salve le disposizioni nazionali di attuazione di altre disposizioni della direttiva 95/46/CE relative al trattamento dei dati personali negli Stati membri.

La presente decisione non si applica al trasferimento di dati personali operato da responsabili del trattamento, aventi sede nella Comunità, a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici.

Articolo 3

Ai fini della presente decisione:

a) si applicano le definizioni della direttiva 95/46/CE;
b) per "categorie particolari di dati" si intendono i dati di cui all'articolo 8 di detta direttiva;
c) per "autorità di controllo" si intende l'autorità di cui all'articolo 28 di detta direttiva;
d) per "esportatore di dati" si intende il responsabile del trattamento che trasferisce dati personali;
e) per "importatore di dati" si intende il responsabile del trattamento che conviene di ricevere dati personali dall'esportatore di dati, a fini di ulteriore trattamento ai sensi della presente decisione.

Articolo 4

1. Fatta salva la possibilità delle competenti autorità degli Stati membri di adottare provvedimenti, al fine di garantire il rispetto delle disposizioni nazionali di attuazione delle disposizioni di cui ai capi II, III, V e VI della direttiva 95/46/CE, dette autorità possono avvalersi dei poteri loro attribuiti per proibire o sospendere flussi di dati verso paesi terzi, a fini di tutela delle persone per quanto riguarda il trattamento dei rispettivi dati personali, qualora:

(a) sia accertato che la legislazione cui è sottoposto l'importatore dei dati lo obbliga a deroghe dai pertinenti principi di protezione dei dati che eccedano quelle ritenute necessarie in una società democratica ai sensi dell'articolo 13 della direttiva 95/46/CE, e che tali deroghe siano probabilmente destinate a recare sostanziale pregiudizio alle garanzie di cui alle clausole contrattuali tipo, oppure
(b) un'autorità competente abbia accertato che l'importatore dei dati non ha rispettato le clausole contrattuali, oppure
(c) sia sostanzialmente probabile che le clausole contrattuali tipo di cui all'allegato non siano o non saranno rispettate, e che la prosecuzione del trasferimento comporterebbe un rischio imminente di grave pregiudizio alle persone interessate dai dati.

2. Il divieto o la sospensione cessano non appena vengono meno le ragioni che li hanno imposti.

3. Quando uno Stato membro prende provvedimenti di cui ai paragrafi 1 e 2 ne informa la Commissione, che trasmette le informazioni agli altri Stati membri.

Articolo 5

La Commissione valuta il funzionamento della presente decisione sulla base delle informazioni disponibili tre anni dopo la notifica della stessa agli Stati membri, e riferisce in merito alle eventuali risultanze al comitato istituito ai sensi dell'articolo 31 della direttiva 95/46/CE, ivi compreso qualsiasi elemento suscettibile di interessare la valutazione di cui all'articolo 1 della presente decisione nonché qualsiasi elemento tale da indicare che la presente decisione viene applicata in maniera discriminatoria.

Articolo 6

La presente decisione si applica dal 3 settembre 2001.

Articolo 7

La presente decisione è indirizzata agli Stati membri.

Fatto a Bruxelles, il 15 giugno 2001

ALLEGATO

Clausole contrattuali tipo, a norma dell'articolo 26, paragrafo 2 della direttiva 95/46/CE per il trasferimento di dati personali a paesi terzi che non garantiscono un livello adeguato di protezione

Nome dell'organizzazione che esporta dati:
.....
indirizzo .....
.....
tel.: .....; fax: .....; e-mail: .....

Altre informazioni identificative: .....

("l'esportatore dei dati")
e

Nome dell'organizzazione che importa dati:
.....
indirizzo .....
.....
tel.: .....; fax: .....; e-mail: .....

Altre informazioni identificative: .....

("l'importatore dei dati")

HANNO CONVENUTO le seguenti clausole contrattuali ("le clausole") al fine di addurre salvaguardie adeguate per quanto riguarda la protezione della riservatezza nonché delle libertà e dei diritti fondamentali degli individui per il trasferimento dall'esportatore all'importatore dei dati personali specificati nell'appendice 1.

Clausola 1

Definizioni

Ai fini delle clausole:

(a) "dati personali", "categorie particolari di dati", "trattamento", "responsabile del trattamento", "incaricato del trattamento"," persona interessata" e "autorità di controllo" hanno la stessa accezione di cui alla direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("la direttiva");

(b) "l'esportatore dei dati" è il responsabile del trattamento che trasferisce i dati personali;

(c) "l'importatore dei dati" è il responsabile del trattamento che accetta di ricevere dati personali dall'esportatore per ulteriore trattamento in conformità alle presenti clausole, e che non è soggetto ad un sistema vigente in un paese terzo per assicurare un'adeguata protezione.

Clausola 2

Particolari del trasferimento

I particolari del trasferimento, e in particolare le categorie di dati personali ed i fini a cui vengono trasferite, sono specificati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

Clausola 3

Clausola del terzo beneficiario

Le persone interessate dai dati possono chiedere l'esecuzione della presente clausola nonché della clausola 4, lettere b), c) e d), della clausola 5, lettere a), b), c), ed e), della clausola 6, paragrafi 1 e 2, nonché delle clausole 7, 9 e 11 in qualità di terzi beneficiari. Le parti non si oppongono a che le persone inte-

ressate dai dati siano rappresentate da un'associazione o da altre organizzazioni se lo desiderano, e se ciò è autorizzato dalla legislazione nazionale.

Clausola 4

Obblighi dell'esportatore dei dati

L'esportatore dei dati s'impegna e garantisce quanto segue:

(a) il trattamento dei dati personali, compreso il loro trasferimento, viene effettuato, e continua ad essere effettuato fino al momento del trasferimento stesso, in conformità a tutte le pertinenti disposizioni (e viene notificato, se del caso, alle autorità competenti) dello Stato membro in cui ha sede l'esportatore, nel pieno rispetto delle leggi vigenti in tale Stato;

(b) qualora il trasferimento riguardi speciali categorie di dati, le persone interessate vengono informate che i dati che li riguardano potrebbero essere trasmessi ad un paese terzo che non fornisce una protezione adeguata, al più tardi all'atto del trasferimento;

(c) mette a disposizione, a richiesta delle persone interessate, copia delle presenti clausole;

(d) risponde entro un termine ragionevole e nella misura del possibile ad eventuali richieste delle autorità di controllo per quanto riguarda il trattamento dei dati personali in questione da parte dell'importatore dei dati, nonché a qualsiasi richiesta delle persone interessate per quanto riguarda il trattamento dei relativi dati da parte dell'importatore degli stessi.

Clausola 5

Obblighi dell'importatore dei dati

L'importatore dei dati s'impegna e garantisce quanto segue:

(a) di non aver ragione di ritenere che la legge applicabile nel suo caso gli impedisca di adempiere agli obblighi di cui al contratto. Qualora la suddetta legge venisse modificata in termini tali da essere probabilmente destinata ad esercitare un sostanziale effetto avverso alle garanzie di cui alle clausole, l'importatore dei dati notifica la variazione all'esportatore dei dati e all'autorità di controllo del paese in cui ha sede l'esportatore. In tal caso l'esportatore dei dati ha diritto di sospendere il trasferimento e/o di rescindere il contratto;

(b) a trattare i dati personali conformemente ai principi obbligatori di tutela dei dati di cui all'appendice 2,

oppure, su esplicito consenso delle parti espresso barrando le caselle che seguono e fatto salvo il rispetto dei principi obbligatori di protezione dei dati di cui all'appendice 3, a trattare i dati sotto ogni punto di vista rispettando:

- le pertinenti disposizioni di diritto nazionale per la protezione dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare il diritto alla riservatezza per quanto riguarda il trattamento dei dati personali, applicabili a un responsabile del trattamento nel paese in cui ha sede l'esportatore dei dati, oppure,
- le pertinenti disposizioni di cui a decisioni della Commissione a norma dell'articolo 25, paragrafo 6 della direttiva 95/46/CE, accertanti che un paese terzo fornisce adeguata protezione soltanto in taluni settori d'attività, purché l'importatore dei dati avente sede in tale paese terzo non sia assoggettabile a dette disposizioni, nella misura in cui le disposizioni stesse siano applicabili nel settore del trasferimento;

(c) a rispondere prontamente e adeguatamente a tutte le ragionevoli richieste dell'esportatore dei dati o delle persone interessate dai dati, per quanto riguarda il trattamento dei dati personali soggetti a trasferimento, a collaborare con la competente autorità di controllo nel corso di tutte le indagini e a rispettare il parere di tale autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

(d) a sottoporre a controllo, su richiesta dell'esportatore dei dati, i propri servizi di trattamento. Il controllo viene effettuato dall'esportatore dei dati o da un ente ispettivo indipendente e in possesso delle necessarie qualifiche professionali, selezionato dall'esportatore dei dati e, ove necessario, di concerto con le autorità di controllo;

(e) a fornire su richiesta copia delle clausole stipulate alle persone interessate dai dati, e ad indicare la sede competente per eventuali reclami.

Clausola 6

Responsabilità

1. Le parti convengono che le persone interessate dai dati che abbiano subito pregiudizio per qualsiasi violazione delle disposizioni di cui alla clausola 3 hanno diritto di essere indennizzate dalle parti per il danno sofferto. Le parti convengono che non sussista responsabilità soltanto se dimostrino che nessuna di esse si è resa responsabile di violazioni delle dette disposizioni.

2. L'esportatore e l'importatore dei dati convengono di assumersi separatamente e in solido la responsabilità dei danni causati alle persone interessate dai dati a seguito di violazioni di cui al paragrafo 1. In caso di violazione di dette disposizioni le persone interessate dai dati possono citare in giudizio sia l'esportatore sia l'importatore dei dati, sia entrambi.

3. Le parti concordano che se una di esse viene riconosciuta responsabile di una violazione commessa dall'altra di qualsiasi disposizione di cui al paragrafo 1, la seconda delle parti indennizza la prima per ogni costo, onere, danno, spesa o perdita sostenuta dalla prima, nei limiti che gli sono imputabili (*).

Clausola 7

Mediazione e giurisdizione

1. In caso di controversie che non possano essere risolte in via amichevole fra le persone interessate dai dati e una delle parti, e qualora le persone interessate dai dati invochino la disposizione relativa al terzo beneficiario di cui alla clausola 3, le parti convengono di accettare la decisione delle persone interessate dai dati di:

(a) ricorrere alla mediazione ad opera di un terzo indipendente o, se del caso, dell'autorità di controllo;

(b) deferire la controversia ai tribunali dello Stato membro in cui ha sede l'esportatore dei dati.

2. Le parti convengono che, di comune accordo fra le persone interessate dai dati e la relativa controparte, la risoluzione di una specifica controversia possa essere deferita ad un organo arbitrale, purché tale parte abbia sede in un paese che ha ratificato la convenzione di New York sull'applicazione dei lodi arbitrali.

3. Le parti convengono che i paragrafi 1 e 2 si applicano fatti salvi i diritti soggettivi o di azione di cui le persone interessate dai dati possono avvalersi al fine del risarcimento dei danni, in forza di altre disposizioni di diritto nazionale o internazionale.

Clausola 8

Collaborazione con l'autorità di controllo

1. Le parti convengono di depositare copia del presente contratto presso l'autorità di controllo su richiesta di tale autorità o se tale deposito è previsto dalla legge nazionale.

Clausola 9

Scadenza delle clausole

1. Le parti convengono che la scadenza delle presenti clausole, in qualsiasi circostanza e per qualsiasi motivo, non esonera le parti stesse dagli obblighi e/o condizioni di cui alle clausole stesse per quanto riguarda il trattamento dei dati trasferiti.

Clausola 10

Legislazione applicabile

1. Alle presenti clausole si applica la legge dello Stato membro in cui ha sede l'esportatore dei dati.

(*) Il paragrafo 3 è facoltativo.

Clausola 11

Modifica del contratto

1. Le parti si impegnano a non alterare o modificare i termini qui convenuti delle presenti clausole.

Per conto dell'esportatore dei dati:

Cognome e nome: .....
Qualifica: .....
Indirizzo: .....

Altre eventuali informazioni necessarie per convalidare il contratto:
.....
Firma .....

(Sigillo dell'organizzazione)

Per conto dell'importatore dei dati

Nome (per esteso): .....
Qualifica: .....
Indirizzo: .....

Altre eventuali informazioni necessarie per convalidare il contratto:
.....
Firma .....

(Sigillo dell'organizzazione)

APPENDICE 1
alle clausole contrattuali tipo

La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti (*).

Esportatore dei dati

(specificare brevemente le attività pertinenti al trasferimento):
.....
.....
.....

Importatore dei dati

(specificare brevemente le attività pertinenti al trasferimento):
.....
.....
.....

Persone interessate dai dati

I dati personali trasferiti interessano le seguenti categorie di persone (specificare):
.....
.....
.....

Fini del trasferimento

Il trasferimento è necessario ai fini seguenti (specificare):
.....
.....
.....

Categorie di dati oggetto di trasferimento

I dati trasferiti interessano le seguenti categorie di dati (specificare):
.....
.....
.....

Dati delicati (se del caso)

Il trasferimento interessa le seguenti categorie di dati a carattere delicato (specificare):
.....
.....
.....

Destinatari

I dati personali trasferiti possono essere comunicati esclusivamente ai seguenti destinatari o categorie di destinatari (specificare):
.....
.....
.....

(*) Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, in conformità alle rispettive procedure nazionali, qualsiasi altra informazione che debba fare parte della presente appendice).

Limite di durata

I dati personali trasferiti possono essere conservati soltanto per (specificare): ..... (mesi/anni)

L'ESPORTATORE DEI DATI

Nome:.....

Firma del rappresentante autorizzato

.....

L'IMPORTATORE DEI DATI

.....

.....

APPENDICE 2
alle clausole contrattuali tipo

Principi obbligatori di protezione di cui alla clausola 5, lettera b), primo capoverso

Questi principi di tutela dei dati devono essere letti ed interpretati alla luce delle disposizioni della direttiva 95/46/CE (1).

Essi si applicano fatte salve le norme imperative di diritto nazionale, cui sia soggetto l'importatore dei dati, che non eccedano quanto necessario, in una società democratica, per i motivi elencati all'articolo 13, paragrafo 1 della direttiva 95/46/CE, cioè se esse costituiscono misure necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato o della protezione della persona interessata o dei diritti e delle libertà altrui.

1) Limitazione del fine - I dati devono essere elaborati e successivamente utilizzati ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presenti clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2) Qualità e proporzionalità dei dati - i dati devono essere corretti e, ove necessario, aggiornati. I dati devono essere adeguati, pertinenti e non esuberanti in relazioni ai fini per cui vengono trasferiti e ulteriormente trattati.

3) Trasparenza - gli individui interessati dai dati devono essere informati sui fini del trattamento e sull'identità del responsabile dello stesso nel paese terzo, e su qualsiasi altro aspetto necessario per garantire la correttezza del trattamento, salvo che queste informazioni siano già state fornite dall'esportatore dei dati.

4) Sicurezza e riservatezza - il responsabile del trattamento è tenuto a prendere provvedimenti tecnici ed organizzativi di sicurezza appropriati ai rischi presentati dal trattamento, come accesso non autorizzato. Qualsiasi persona che agisca in virtù dell'autorità del responsabile del trattamento non deve effettuare operazioni di trattamento dei dati se non per disposizione del responsabile del trattamento stesso.

5) Diritti di accesso, rettifica, cancellazione e congelamento dei dati - come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi. Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

6) Restrizioni sui trasferimenti successivi - ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6 della direttiva 96/45/CE (trasferimenti successivi) possono essere effettuati soltanto:

a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

- gli scopi del successivo trasferimento,
- l'identità dell'esportatore di dati con sede nella Comunità,

(1) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

- le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e
- l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui, oppure,

ovvero

b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

7) Speciali categorie di dati - nel caso che il trattamento riguardi dati che possano rivelare l'origine razziale o etnica, ovvero le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione a sindacati, dati relativi allo stato di salute o alla vita sessuale, nonché dati relativi a reati, condanne penali o provvedimenti di sicurezza, devono essere previste ulteriori salvaguardie ai sensi della direttiva 95/46/CE, ed in particolare idonee misure di sicurezza come trasmissione cifrata o registrazione di ogni accesso ai dati.

8) Marketing diretto - quando i dati vengono trattati a fini di marketing diretto, devono essere previste procedure tali da consentire ai soggetti dei dati di negare in qualsiasi momento il proprio consenso all'utilizzazione a tali fini dei dati che li riguardano.

9) Decisioni individuali automatizzate - le persone interessate dai dati hanno il diritto di non essere assoggettati a decisioni basate unicamente sul trattamento automatizzato di dati, a meno che non vengano presi altri provvedimenti per salvaguardare i loro legittimi interessi ai sensi dell'articolo 15 della direttiva 95/46/CE. Qualora l'obiettivo del trasferimento sia una decisione automatizzata ai sensi del citato articolo 15 la persona interessata deve avere il diritto di conoscere le motivazioni su cui si basa detta decisione.

APPENDICE 3
alle clausole contrattuali tipo

Principi obbligatori di protezione di cui alla clausola 5, lettera b), secondo capoverso

1) Limitazione del fine - I dati devono essere elaborati e successivamente utilizzati ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presenti clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2) Diritti di accesso, rettifica, cancellazione e congelamento dei dati - come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi. Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

3) Restrizioni sui trasferimenti successivi ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6 della direttiva 96/45/CE (trasferimenti successivi) possono essere effettuati soltanto:

a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

- gli scopi del successivo trasferimento,
- l'identità dell'esportatore di dati con sede nella Comunità,
- le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione,
- l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui,

ovvero

b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO ALLA TUTELA DEI DATI PERSONALI (ART. 29)

120 RACCOMANDAZIONE 1/2000 SULL'ATTUAZIONE DELLA DIRETTIVA 95/46/CE (*)

Adottata il 3 febbraio 2000

Il gruppo per la tutela delle persone con riguardo al trattamento dati personali

istituito a seguito della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 (1),

visti gli articoli 29 e 30, paragrafi 1, lettera a) e 3, della direttiva,

visto il suo regolamento interno, in particolare gli articoli 12 e 14,

considerando che gli obiettivi della Comunità, enunciati nel trattato, come è stato modificato dal trattato di Amsterdam, consistono nel realizzare un'unione sempre più stretta tra i popoli europei, nell'assicurare, mediante un'azione comune, il progresso economico e sociale eliminando le barriere che dividono l'Europa, nel promuovere il miglioramento costante delle condizioni di vita delle sue popolazioni, nel preservare e rafforzare la pace e la libertà e nel promuovere la democrazia basandosi sui diritti fondamentali sanciti dal trattato, dalle costituzioni e dalle leggi degli Stati membri nonché dalla convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali;

considerando che la direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati richiede agli Stati membri di proteggere i diritti e le libertà fondamentali delle persone, in particolare il loro diritto alla vita privata con riguardo al trattamento dei dati personali;

considerando che la direttiva forma parte delle misure comunitarie indispensabili per eliminare gli ostacoli ai flussi di dati personali nelle varie sfere dell'attività economica, amministrativa e sociale in seno al mercato interno e che a tal fine essa mira ad armonizzare le norme relative al trattamento dei dati personali offrendo un elevato livello di protezione nella Comunità;

considerando che il Consiglio e il Parlamento europeo hanno approvato all'unanimità il recepimento della direttiva nelle legislazioni nazionali entro il 24 ottobre 1998,

ha adottato la presente raccomandazione:

Il gruppo rileva che, finora, gran parte degli Stati membri non ha ancora promulgato la legge per il recepimento della direttiva 95/46/CE nella loro legislazione nazionale (2).

(*) 5139/99/IT/DEF WP 30.

1 Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile sul sito: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

2 Cfr. tabella di attuazione della DG Mercato interno, disponibile sul sito indicato alla nota 1.

Il gruppo, istituito dalla direttiva 95/46/CE, è un organo indipendente di consulenza dell'UE per la protezione dei dati e della vita privata (3). Esso ha in particolare il compito di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della direttiva per contribuire alla loro applicazione omogenea (4).

Il gruppo deplora il fatto che non tutti gli Stati membri abbiano attuato la direttiva entro i termini prescritti. Tale ritardo fa sì che continuino ad esistere regimi diversi che comportano un'insicurezza giuridica per quanto riguarda gli obblighi dei responsabili del trattamento dei dati personali, quali imprese e amministrazioni, nonché i diritti delle persone.

Nei suoi lavori svolti finora (5) il gruppo si è basato sulla direttiva e, nei limiti del possibile, sulle legislazioni nazionali che la recepiscono. Peraltro, il gruppo non può svolgere interamente il suo mandato e contribuire in tal modo all'applicazione uniforme delle misure nazionali miranti a garantire la libera circolazione dei dati personali nell'Unione e al di fuori di essa senza poter disporre di un quadro completo delle legislazioni nazionali.

Il gruppo gradirebbe inoltre attirare l'attenzione sugli sforzi intrapresi da taluni paesi terzi per proteggere il diritto fondamentale alla vita privata sul territorio di loro giurisdizione e per garantire un livello di protezione adeguato per i trasferimenti di dati personali dall'Unione europea (6) come previsto dalla direttiva.

Il gruppo teme che trasferimenti di dati personali verso paesi che non hanno intrapreso tali sforzi e non hanno recepito la direttiva rischiano di causare una violazione dei diritti e delle libertà fondamentali delle persone garantiti dalla direttiva.

Tenuto conto di quanto detto in precedenza, il gruppo rammenta agli Stati membri l'importanza del loro obbligo di ottemperare alla direttiva al fine della protezione dei diritti e delle libertà fondamentali. Il gruppo è a conoscenza dell'azione intrapresa dalla Commissione europea per avviare le procedure di infrazione contro gli Stati membri che non osservano l'obbligo di segnalare le misure di attuazione (7) e approva appieno tutti gli sforzi volti a garantire una rapida attuazione della direttiva.

Il gruppo raccomanda quindi agli Stati membri, Governi e Parlamenti inclusi, di adottare tempestivamente le misure necessarie per attuare la direttiva il più rapidamente possibile.

Fatto a Bruxelles, il 3 febbraio 2000

Per il gruppo

Il Presidente

Peter J. HUSTINX

3 Cfr. articolo 29, paragrafo 1, seconda frase, della direttiva 95/46/CE.

4 Cfr. articolo 30, paragrafo 1, lettera a), della direttiva 95/46/CE.

5 Cfr. pareri, raccomandazioni e documenti di lavoro adottati dal gruppo sul sito indicato alla nota 1.

6 Cfr. il principio di protezione adeguata di cui all'articolo 25, paragrafo 1, della direttiva 95/46/CE. Cfr. altresì il parere 5/99 riguardo al livello di protezione in Svizzera e il parere 6/99 riguardante il livello di protezione in Ungheria, come pure i pareri 1/99, 2/99 e 4/99 e altri documenti riguardanti il dialogo sull'"Approdo sicuro" con gli Stati Uniti disponibili sul sito di cui alla nota 1. Attualmente vari paesi stanno consolidando o sviluppando le loro politiche in materia di protezione dei dati e di vita privata.

7 Cfr. articolo 32, paragrafo 4, della direttiva 95/46/CE. La Commissione ha trasmesso pareri motivati agli Stati membri inadempienti e sta attualmente preparando un'ulteriore azione (cfr. comunicato stampa del 29 luglio, disponibile sul sito indicato alla nota 1).

GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI (*)

PARERE 1/2000

SU ALCUNI ASPETTI DEL COMMERCIO ELETTRONICO RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI (APPROVATO IL 3 FEBBRAIO 2000)

1. Introduzione

L'UE sta attualmente preparando una proposta di direttiva su alcuni aspetti del commercio elettronico (1). Come già in passato, il Gruppo di lavoro per la protezione dei dati personali di cui all'articolo 29 (2) intende recare un contributo costruttivo al rafforzamento del quadro giuridico del commercio elettronico. Mediante il presente parere, il Gruppo di lavoro desidera richiamare l'attenzione su un problema di protezione dei dati sollevato dal commercio elettronico, e illustrare in quale modo tale problema viene trattato nella legislazione europea. Il quadro giuridico per la protezione del diritto fondamentale alla riservatezza ed alla protezione dei dati personali è già stato realizzato mediante la direttiva 95/46/CE, che fissa i principi generali per la protezione dei dati, nonché la direttiva 97/66/CE, che integra tali principi per il settore delle telecomunicazioni.

Il Gruppo di lavoro esprime la propria soddisfazione per il fatto che il testo attualmente in corso di approvazione contiene un esplicito chiarimento, mediante un nuovo considerando e un nuovo articolo 1(4)(b), sulla corretta e integrale applicazione della legislazione per la protezione dei dati (3) ai servizi internet. Ciò significa che l'applicazione della direttiva sul commercio elettronico deve essere integralmente conforme ai principi della protezione dei dati.

Il Gruppo di lavoro ha già prestato notevole attenzione ai problemi di tutela dei dati su internet, in modo particolare con una serie di pareri nel 1999 su tre importanti problemi relativi alle caratteristiche specifiche delle nuove tecnologie dell'informazione.

Il Gruppo ha così formulato un parere sull'informazione del settore pubblico (4), e due raccomandazioni rispettivamente sull'elaborazione automatica ed invisibile dei dati personali su internet (5) e sulla conservazione dei dati sul traffico da parte dei fornitori di servizi internet a fini giudiziari (6). Nel contesto del commercio elettronico, si pone anche un quarto problema. Il Gruppo di lavoro desidera pertanto formulare un'interpretazione della maniera in cui le norme europee per la protezione dei dati si applicano all'elaborazione di dati a fini di spedizioni elettroniche (mailing) di massa.

2. Il problema dei mailing elettronici

Per lanciare una campagna pubblicitaria o effettuare un mailing commerciale, un'impresa deve acquistare un elenco esteso e appropriato di indirizzi di clienti potenziali. Vi sono tre modi in cui una socie-

---

(*) 5007/00/IT/def. WP28

1 Proposta modificata di direttiva del Parlamento europeo e del Consiglio relativa a taluni aspetti giuridici del commercio elettronico nel mercato interno, COM (1999) 427 def. L'accordo politico sul testo è stato raggiunto in sede di Consiglio dei Ministri il 7 dicembre 1999; fra breve sarà formalmente approvata una posizione comune in vista di una seconda lettura da parte del Parlamento europeo. Vedi comunicato stampa IP/99/952 pag. 1 e 4.

2 Istituito in virtù dell'articolo 29 della direttiva 95/46/CE, vedi nota 3 infra.

3 Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281/31 del 23 novembre 1995, e direttiva 97/66 del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, GU L 24/1 del 30 gennaio 1998, disponibili presso:
http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm

4 Parere 3/99 sulle informazioni del settore pubblico e sulla protezione dei dati personali, approvato il 3 maggio 1999: WP 20 (5055/99). Tutti i documenti approvati dal Gruppo di lavoro sono disponibili all'indirizzo seguente: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm

5 Raccomandazione 1/99 sull'elaborazione automatica ed invisibile dei dati personali su Internet mediante Software e Hardware, approvata il 23 febbraio 1999: WP 17 (5093/98).

6 Raccomandazione 3/99 sulla conservazione dei dati di traffico da parte di fornitori di servizi internet a fini giudiziari, approvata il 7 settembre 1999: WP 25 (5085/99).

tà può acquisire indirizzi e-mail su Internet: raccolta diretta di clienti o visitatori di siti web; elenchi preparati da terzi (7); e raccolta su spazi internet pubblici, come guide, newsgroup o chat-room.

Un aspetto particolare delle spedizioni postali *elettroniche* è che mentre per il mittente il costo è estremamente basso rispetto ai metodi di direct marketing tradizionali, vi è un costo per il destinatario in termini di tempo di collegamento. Questo stato di cose costituisce pertanto un chiaro incentivo all'impiego su vasta scala di questo strumento di marketing, ignorando i problemi di protezione dei dati e quelli causati dalla spedizione elettronica.

Dal punto di vista dei cittadini, il problema ha tre aspetti: primo, la raccolta dell'indirizzo e-mail senza il consenso o la conoscenza dell'interessato; secondo, l'arrivo di notevoli quantitativi di pubblicità indesiderata; terzo, il costo del tempo di collegamento. A questo proposito, l'aspetto più cospicuo è costituito dal cosiddetto "spam" (8) ("robaccia" o "spazzatura"). Lo spamming è l'invio di posta elettronica non richiesta, solitamente a carattere commerciale, in grossi quantitativi e in diverse riprese, a individui con i quali il mittente non ha alcun precedente contatto. Il fenomeno di solito si verifica successivamente alla raccolta di un indirizzo elettronico in uno spazio pubblico Internet. Dal punto di vista del mercato interno, il problema che ne deriva è la possibilità che regolamenti nazionali divergenti in materia di comunicazioni elettroniche commerciali possano costituire barriere al commercio. Ambedue gli aspetti hanno influito sullo sviluppo della legislazione comunitaria.

3. La legislazione comunitaria e la sua applicazione alle spedizioni elettroniche

È già stato osservato che, in generale, il commercio elettronico è soggetto alla legislazione sulla protezione dei dati (9). Le spedizioni elettroniche di massa costituiscono un esempio specifico di come i problemi di protezione dei dati sollevati dal commercio elettronico possono essere risolti con l'applicazione dei principi giuridici delle due direttive. La direttiva a carattere generale stabilisce che i dati personali devono essere raccolti lecitamente a fini espliciti, legittimi e specificati, e che devono essere trattati in maniera equa e legittima conformemente a tali espliciti principi (10) . Anche il trattamento dei dati deve essere effettuato su base legittima, come consenso, contratto, obbligo di legge o legittimo interesse (11). Inoltre, l'interessato deve essere informato del previsto trattamento (12), e deve avere la possibilità di opporsi al trattamento dei propri dati personali a fini di marketing diretto (13). La direttiva sulla riservatezza delle telecomunicazioni lascia agli Stati membri la facoltà di decidere se applicare norme che offrono la possibilità di scelta in positivo o in negativo ("opt-in" e "opt-out") in fatto di comunicazioni commerciali non richieste (14). Alle norme sulla protezione dei dati si aggiungono alcuni requisiti legati alla tutela dei consumatori. La direttiva sulle vendite a distanza richiede ad esempio che i consumatori abbiano come minimo il diritto di opporsi all'invio su posta elettronica di comunicazioni a distanza (15).

La direttiva sul commercio elettronico, una volta approvata, potrà stabilire espressamente, all'articolo 7, due elementi a carattere *tecnico*: l'obbligo di identificare come tale la posta elettronica a carattere commerciale, e l'obbligo di consultare e rispettare i registri di esclusione ove stabiliti dalle normative nazionali. Ma il considerando e l'articolo 1(4)(b) chiariscono che la direttiva non intende modificare in alcun modo i principi e i requisiti *giuridici* stabiliti dall'esistente quadro legislativo illustrato sopra. Dato che la legislazione sulla protezione dei dati si applica integralmente al commercio elettronico, il recepimento della direttiva sul commercio elettronico deve essere integralmente coerente con i principi per la protezione dei dati. Ciò significa, in primo luogo, che per quanto riguarda la protezione dei dati la legge nazionale applicabile ad una società responsabile del trattamento di dati personali continuerà ad essere quella del paese dell'UE in cui la società risiede (16). Ciò significa anche che la direttiva sul commercio

7 Gli elenchi preparati da terzi possono essere compilati sulla base di dati raccolti direttamente dalla clientela o sulla base di dati raccolti in siti pubblici.
8 L'argomento è stato trattato nella relazione sulle spedizioni elettroniche e la protezione dei dati personali approvata dal CNIL il 14 ottobre 1999, disponibile su www.cnil.fr Le sezioni 2 e 3 del presente parere si basano in parte su tale relazione.
9 Documento di lavoro: Elaborazione dei dati personali su Internet. Approvato il 3.2.1999: WP 16 (5013/99).
10 Direttiva 95/46/CE, articolo 6.
11 Direttiva 95/46/CE, articolo 7.
12 Direttiva 95/46/CE, articolo 10.
13 Direttiva 95/46/CE, articolo 14.
14 Direttiva 97/66, articolo 12. Si può anche sostenere che l'impiego della posta elettronica a fini di marketing diretto debba essere considerato equivalente a quello di sistemi automatizzati di chiamata, che richiedono il consenso degli interessati.
15 Direttiva 97/7/CE del Parlamento europeo e del Consiglio del 20 maggio 1997 riguardante la protezione dei consumatori in materia di contratti a distanza, GU L 144/19 del 4 giugno 1997, articolo 10 (la posta elettronica è espressamente compresa in virtù dell'articolo 2(4) ed allegato 1): disponibile su: http://www.europa.eu.int/eur-lex/en/lef/dat/1997/en_397L0007.html

elettronico non può impedire agli Stati membri di obbligare le imprese ad ottenere in anticipo il consenso degli interessati prima di effettuare comunicazioni commerciali (17), né può impedire l'utilizzazione anonima di internet (18).

Il Gruppo di lavoro ritiene che queste norme costituiscano una chiara risposta ai problemi di riservatezza sollevati nella sezione 2 supra, e che esse definiscano chiaramente i diritti e i doveri di tutti gli interessati. È necessario distinguere due situazioni:

• Se un indirizzo e-mail viene raccolto da una società *direttamente presso l'interessato* in vista dell'effettuazione di mailing elettronici da parte della società stessa, o di terzi a cui l'indirizzo possa essere successivamente ceduto, la società in questione deve informare l'interessato al momento in cui ne trascrive l'indirizzo (19). L'interessato, inoltre, come minimo, deve avere la possibilità, al momento della raccolta e successivamente in qualsiasi momento, di opporsi all'utilizzazione dell'indirizzo, e ciò in maniera facile ed elettronica, come ad esempio cliccando su un'apposita casella, sia per quanto riguarda le utilizzazioni effettuate dalla società originale che per quelle effettuate successivamente da altre imprese che abbiano ricevuto i dati da quella originale (20). Alcune norme nazionali di recepimento delle direttive interessate prevedono persino l'obbligo di richiedere il consenso preventivamente. I requisiti dell'articolo del progetto di direttiva sul commercio elettronico in materia di comunicazioni commerciali non richieste permetterebbero di integrare a livello tecnico tali norme stabilendo l'obbligo di consultare un registro presso il fornitore di servizi Internet, senza peraltro sminuire in alcun modo gli obblighi generali applicabili ai responsabili del controllo dei dati.

• Se un indirizzo e-mail viene raccolto in uno *spazio pubblico di Internet*, il suo impiego per mailing elettronici sarebbe contrario alla pertinente legislazione comunitaria, e ciò per tre ragioni. Primo, il fatto potrebbe essere considerato come un trattamento "sleale" dei dati personali ai sensi dell'articolo 6(1)(a) della direttiva generale. Secondo, sarebbe contrario al principio della finalità di cui all'articolo 6(1)(b) di tale direttiva, in quanto l'interessato aveva reso noto il suo indirizzo e-mail per motivi del tutto diversi, ad esempio la partecipazione ad un newsgroup. Terzo, dato il citato squilibrio dei costi e il fastidio recato al destinatario, tali spedizioni non possono essere considerate giustificate in termini dell'equilibrio di interessi di cui all'articolo 7(f) (21).

4. Conclusioni

Questo parere non costituisce la posizione finale del Gruppo di lavoro sull'interazione fra il commercio elettronico e la protezione dei dati. L'obiettivo è di richiamare l'attenzione sui problemi sollevati da un tipo particolare di elaborazione dei dati che attualmente costituisce oggetto di dibattito in molte sedi, e di contribuire ad una migliore comprensione del quadro giuridico applicabile al commercio elettronico. Può darsi che vi siano altri aspetti del commercio elettronico, oltre quelli già trattati dal Gruppo di lavoro, che richiedano una guida interpretativa o un approccio comune. Pertanto, il Gruppo di lavoro ritiene necessario sviluppare una politica comune su aspetti che vanno dal cyber-marketing ai pagamenti elettronici ed alle tecnologie per il potenziamento (enhancing) della privacy. Il gruppo ha incaricato l'"Internet Task Force" di proseguire i lavori in tal senso. Sono previsti diversi risultati, fra cui raccomandazioni su misure a carattere tecnico relative allo spam, o l'omologazione dei siti web in conformità ad un elenco comune di principi europei basati sulle direttive per la protezione dei dati.

Bruxelles, 3 febbraio 2000

Per il Gruppo di lavoro

Il Presidente

Peter J. HUSTINX

16 Direttiva 95/46/CE, articolo 4.
17 Vedi articolo 12 della direttiva 97/66/CE.
18 Vedi considerando 6a della proposta modificata, nota 1 supra.
19 Direttiva 95/46/CE, articolo 10.
20 Direttiva 95/46/CE, articolo 14.
21 Ove si stabilisce (oltre a diversi altri casi che possono giustificare il legittimo trattamento dei dati) che il trattamento dei dati personali sia "necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento . . . a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

PARERE 2/2000
CONCERNENTE LA REVISIONE DEL QUADRO GIURIDICO DELLE TELECOMUNICAZIONI (APPROVATO IL 3 FEBBRAIO 2000)

Introduzione

Il Gruppo di lavoro per il trattamento dei dati personali (1) ha preso nota della Comunicazione della Commissione europea (2) concernente la revisione generale dell'esistente quadro giuridico delle telecomunicazioni a livello europeo.

Nel contesto della pubblica consultazione indetta dalla Commissione europea fino al 15 febbraio 2000, il Gruppo di lavoro desidera sottolineare l'importanza delle questioni di protezione dei dati sollevate in tale contesto.

Inoltre, Il Gruppo di lavoro auspica la possibilità di partecipare costruttivamente alla revisione del quadro giuridico delle telecomunicazioni.

Principali problemi relativi alla protezione dei dati nel contesto della revisione del quadro giuridico

Nel contesto della prevista revisione generale del quadro giuridico delle telecomunicazioni, verrà anche rivista e aggiornata l'esistente direttiva concernente il trattamento dei dati personali e la protezione della riservatezza nel settore delle telecomunicazioni 3.

L'art. 14, paragrafo (3), di questa direttiva incarica il Gruppo di lavoro istituito dalla Direttiva 95/46/CE di svolgere i compiti previsti da tale direttiva anche per quanto concerne la tutela dei diritti e delle libertà fondamentali nonché dei legittimi interessi nel settore delle telecomunicazioni, che sono oggetto della Direttiva 97/66/CE.

L'art. 30 della direttiva generale sulla protezione dei dati specifica i compiti del Gruppo di lavoro. Uno di essi è di consigliare la Commissione europea in merito a ogni progetto di modifica della direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà.

Nei precedenti pareri, il Gruppo di lavoro ha già sottolineato la necessità di tenere conto di nuovi sviluppi tecnologici (4) che potrebbero chiamare in causa la protezione dei dati personali e il diritto alla riservatezza.

Per questo motivo, il Gruppo di lavoro è favorevole all'aggiornamento della direttiva in quanto ciò possa consentire di affrontare in maniera più specifica i problemi di protezione dei dati nel settore delle telecomunicazioni, mantenendo o anche rafforzando l'esistente livello di protezione.

Non bisogna però dimenticare che la direttiva specifica 97/66/CE ha funzioni puramente complementari nei riguardi della direttiva generale 95/46/CE dal punto di vista della definizione di specifiche norme giuridiche e tecniche (5). Per la revisione della direttiva specifica, sarà necessario tenere conto in maniera coerente dei disposti della direttiva generale 95/46/CE per la protezione dei dati, che si appli-

---

(*) 5009/00/IT/def. WP29

1 Istituito in virtù dell'art. 29 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, GU L 281. 23 novembre 1995, pag. 31. Disponibile presso: http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm

2 Documento COM (1999) 539.

3 Direttiva 97/66/CE del 15 dicembre 1997, Gazzetta ufficiale L 24, Volume 41del 30 gennaio 1998.

4 Tra l'altro, nel Documento di lavoro "Trattamento dei dati personali su Internet", approvato il 23 febbraio 1999, documento 5013/99/IT/def. WP 16. Tutti i documenti approvati dal Gruppo di lavoro sono disponibili presso:
http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm

5 In tutti i casi non specificatamente coperti dalla Direttiva 97/66/CE, come gli obblighi del controllore, i diritti degli individui e i servizi di telecomunicazione non disponibili pubblicamente, si applica la Direttiva 95/46/CE (vedi considerando 11 della Direttiva 97/66/CE).

cano a qualsiasi trattamento dei dati personali che rientri nella portata della direttiva stessa indipendentemente dai mezzi tecnici utilizzati.

La direttiva specifica deve evidentemente non solo proteggere i diritti fondamentali degli individui ma anche tenere conto di altri legittimi interessi, come quelli della confidenzialità e integrità delle pubbliche telecomunicazioni.

Il testo della Comunicazione della Commissione europea sottolinea che la prevista revisione presterà particolare attenzione alla terminologia utilizzata dalla direttiva 97/66/CE al fine di chiarire esplicitamente che tali direttiva copre anche i nuovi servizi e le nuove tecnologie, evitando in tal modo possibili ambiguità e facilitando un'applicazione coerente dei principi per la protezione dei dati.

Il Gruppo di lavoro è favorevole ad una tale revisione della terminologia ai fini citati.

Come correttamente enunciato dalla Comunicazione della Commissione, il quadro giuridico delle telecomunicazioni deve applicarsi ai servizi Internet allo stesso modo in cui si applica alle altre forme di comunicazione.

Il Gruppo di lavoro ha già sollevato la questione nei precedenti pareri, dichiarando chiaramente che il trattamento dei dati personali su Internet deve rispettare i principi di protezione dei dati esattamente come nel caso delle comunicazioni *off-line* (6). Il trattamento dei dati personali su Internet deve essere pertanto considerato alla luce di ambedue le direttive sulla protezione dei dati.

Il Gruppo di lavoro, ed in particolare l'"*Internet Task Force*" creata nell'ambito del gruppo stesso, desidera offrire alla Commissione le proprie competenze specifiche in materia di protezione dei dati in vista dell'esame dei problemi relativi a Internet che dovranno essere trattati nel quadro della revisione generale della legislazione sulle telecomunicazioni.

Un altro interessante problema sollevato dalla Comunicazione della Commissione è l'impatto crescente del software e delle configurazioni tecnologiche software.

Il Gruppo di lavoro ha già dedicato una certa attenzione a questo problema, in particolare nella raccomandazione 1/99 sul trattamento invisibile e automatico dei dati personali su Internet mediante software e hardware (7). In tale raccomandazione il Gruppo di lavoro ha incoraggiato l'industria del software e dell'hardware a creare prodotti Internet rispettosi dei principi della riservatezza e tali da fornire gli strumenti necessari per l'ottemperanza alle norme europee sulla protezione dei dati.

Il Gruppo di lavoro ritiene che il ruolo sempre più importante del software nel campo delle telecomunicazioni debba essere preso in considerazione nell'ambito della revisione della direttiva, particolarmente dal punto di vista della responsabilità di tutti gli operatori coinvolti nel trattamento dei dati personali.

La revisione della direttiva potrebbe costituire inoltre una buona occasione per un riesame delle diverse responsabilità che gli operatori di reti e i fornitori di servizi dovrebbero avere a questo proposito.

Uno degli obiettivi della revisione del quadro legislativo delle telecomunicazioni è lo sviluppo della legislazione europea in direzione neutrale sotto il profilo delle tecnologie.

Il Gruppo di lavoro è d'accordo con questo obiettivo. Questa intenzione, peraltro, non deve impedire al legislatore europeo di elaborare un nuovo quadro giuridico che consideri adeguatamente i problemi specifici sollevati dai nuovi sviluppi tecnologici del settore.

Il Gruppo desidera inoltre sottolineare che la nuova direttiva dovrebbe stabilire il principio che tutte le tecnologie, indipendentemente dalle caratteristiche tecniche, devono rispettare, e possibilmente proteggere, la riservatezza.

Conclusione

In termini generali, il Gruppo di lavoro è favorevole all'aggiornamento della direttiva 97/66/CE allo scopo di affrontare in maniera specifica i problemi di protezione dei dati del settore delle telecomunicazioni nel mantenimento o, se necessario, nel miglioramento del livello esistente di protezione. Il Gruppo di lavoro annette la massima importanza ad un elevato livello di protezione dei dati nel settore delle telecomunicazioni e, in particolare, alla garanzia della confidenzialità e integrità delle comunicazioni.

6 Vedi anche la Dichiarazione ministeriale alla Conferenza di Bonn sulle Reti globali, giugno 1997, disponibile presso: http://www2.echo.lu/bonn/conference.html.

7 Raccomandazione 1/99 approvata dal Gruppo di lavoro il 23 febbraio 1999, documento 5093/98/IT/def. WP 17.

Pur essendo favorevole all'aggiornamento e miglioramento del quadro giuridico delle telecomunicazioni, il Gruppo di lavoro desidera sottolineare l'importanza di un tempestivo recepimento a livello nazionale dell'attuale direttiva nel settore delle telecomunicazioni. Il Gruppo invita pertanto la Commissione a dichiarare esplicitamente che il nuovo quadro giuridico entrerà in vigore soltanto fra alcuni anni, e che nel frattempo gli Stati membri devono proseguire l'elaborazione delle rispettive legislazioni nazionali sulla base dell'esistente quadro giuridico.

Il Gruppo di lavoro desidera incoraggiare la Commissione a tenere conto delle raccomandazioni, pareri e documenti redatti dal presente Gruppo di lavoro in merito ai problemi a cui si riferisce la comunicazione sul processo di revisione.

Il presente parere non costituisce in alcun modo la posizione definitiva del Gruppo di lavoro sull'argomento. Il Gruppo di lavoro desidera contribuire alle ulteriori discussioni nonché alla formulazione di proposte specifiche, se desiderato, in vista delle fasi successive della procedura di revisione.

Bruxelles, 3 febbraio 2000

Per il Gruppo di lavoro

Il Presidente

Peter J. HUSTINX

123

PARERE 5/2000 SULL'USO DEGLI ELENCHI PUBBLICI PER I SERVIZI DI RICERCA DERIVATA O A CRITERI MULTIPLI (ELENCHI DERIVATI) (APPROVATO IL 13 LUGLIO 2000)

1. Introduzione

Nel quadro del processo di liberalizzazione del settore europeo delle telecomunicazioni, nuove società offrono servizi in precedenza forniti solo dai tradizionali operatori delle telecomunicazioni. Per tale motivo, sempre più di frequente, vengono resi disponibili nuovi prodotti, tra i quali elenchi telefonici in formato elettronico. Tali elenchi, contenenti nome, indirizzo e numero telefonico di milioni di cittadini europei dei vari Stati membri, vengono commercializzati in numerosi paesi europei e riportano informazioni sui cittadini del paese nel quale ha sede il servizio o la società e su quelli di altri paesi dell'UE. I supporti più utilizzati per la distribuzione di tali prodotti sono i CD ROM e i siti *web* su Internet.

Una delle principali innovazioni introdotte dalla pubblicazione elettronica è la possibilità di offrire in modo semplice ed economico funzioni avanzate per il trattamento delle informazioni presenti negli elenchi telefonici. Tali funzioni si riferiscono principalmente alla possibilità di utilizzare criteri di ricerca avanzati per rivelare informazioni presenti nell'elenco stesso.

In effetti, tali prodotti offrono in genere servizi di ricerca derivata o a criteri multipli. Oltre ai tradizionali metodi di ricerca che consentono di trovare il numero telefonico di un dato abbonato a partire dal suo nome, i nuovi servizi permettono di accedere, mediante metodi di ricerca multipla, ai dati personali di un determinato abbonato o addirittura di un gruppo di abbonati i cui dati personali corrispondono ai criteri di ricerca.

Quale esempio delle funzioni di questi nuovi tipi di ricerca, vanno ricordate la possibilità di risalire al nome e all'indirizzo di un abbonato telefonico indicandone il numero di telefono e quella di effettuare una ricerca basata sull'indirizzo, tramite la quale è possibile reperire il nome e il numero telefonico degli

abbonati partendo dal loro indirizzo. Sarebbe tecnicamente possibile ottenere persino il nome e il numero telefonico di tutti gli abbonati che abitano in una data zona (ad esempio, una strada).

Questa nuova funzione potrebbe comportare un radicale cambiamento nelle prospettive di *privacy* dei cittadini in relazione ai dati personali conservati negli elenchi pubblici. In realtà, prima dell'esistenza di questi nuovi prodotti, quando una persona comunicava il proprio numero di telefono a un terzo, ciò non implicava, in circostanze normali, la possibilità di ottenere ulteriori informazioni da quel dato; ora, tuttavia, grazie alla presenza sul mercato di tali prodotti, la situazione è mutata radicalmente: la semplice rivelazione, intenzionale o casuale, di un numero telefonico potrebbe costituire la chiave per accedere ad un numero di informazioni pari in genere a quello che compare su un biglietto da visita, compreso il nome, l'indirizzo e, in taluni casi, la professione e l'impiego. Inoltre, la semplice conoscenza della bolletta telefonica dettagliata di un cittadino, nella quale sono riportati i soli numeri chiamati, consentirebbe di ottenere un elenco dei nomi e degli indirizzi delle persone da lui chiamate durante un determinato lasso di tempo.

È necessario altresì tenere in considerazione un'altra categoria di prodotti contenenti informazioni geografiche, quali piante di città, e banche dati che comprendono le fotografie di tutte le abitazioni di una città. Tali informazioni possono essere collegate con semplicità all'indirizzo che compare in un elenco telefonico che consente le ricerche a criteri multipli. Enormi possibilità si aprono poi combinando tali informazioni con quelle provenienti da altre fonti, quali i registri di dominio pubblico. La quantità di informazioni ottenibili per il semplice fatto di disporre di un numero telefonico va, pertanto, ben oltre quanto un cittadino medio può ragionevolmente aspettarsi (1).

2. Analisi giuridica

La direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (2) recita al considerando 21 che *"(...) gli elenchi sono ampiamente distribuiti e disponibili al pubblico; che il diritto al rispetto della vita privata delle persone fisiche e i legittimi interessi delle persone giuridiche richiedono che gli abbonati possano determinare in quale misura i loro dati personali debbano essere pubblicati nei medesimi elenchi; che gli Stati membri possono riconoscere questa possibilità ai soli abbonati che sono persone fisiche"*. D'altronde, l'articolo 11 sancisce il principio che i dati personali raccolti negli elenchi telefonici debbano limitarsi *"(...) agli elementi necessari per identificare un abbonato, salvo nel caso in cui l'abbonato abbia inequivocabilmente consentito alla pubblicazione di dati personali supplementari"*.

A parte quanto esposto in precedenza, l'articolo 11 sancisce inoltre che l'abbonato *"(...) ha il diritto, gratuitamente, di non essere incluso in un elenco stampato o elettronico, di indicare che i suoi dati personali non possono essere utilizzati a fini di invio di materiale pubblicitario, di ottenere che il suo indirizzo sia in parte omesso e, se ciò è fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso"*.

Inoltre, la direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali (3), all'articolo 6, paragrafo 1, lettera b), sancisce che i dati personali devono essere *"rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità"*. In tal senso, lo scopo degli elenchi telefonici convenzionali è quello di rivelare il numero telefonico di un abbonato a partire dalla conoscenza del nome dell'abbonato (l'indirizzo è necessario solo in caso di omonimia) e l'uso di tali dati personali è circoscritto a quello scopo specifico. Pertanto, l'utilizzo di questi elenchi per reperire dati personali relativi a una persona fisica a partire da un determinato numero telefonico del quale si ignora l'abbonato oppure i nomi e i numeri telefonici delle persone che abitano in una determinata zona rappresenta un uso completamente diverso da quel-

1 I rappresentanti delle autorità per la tutela dei dati personali di Austria, Danimarca e Portogallo hanno espresso il parere che nei loro paesi le pratiche di ricerche derivate non abbiano comportato, a tutt'oggi, l'insorgere di problemi specifici. Il rappresentante danese si è astenuto dal voto.

2 Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni:
GU L 24 del 30 gennaio 1998, p. 1. Disponibile all'indirizzo:
http://158.169.50.95:10080/legal/en/dataprot/protection.html

3 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati:
GU L 281 del 23 novembre 1995, p. 31. Disponibile all'indirizzo:
http://www.europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm

lo che un consumatore può ragionevolmente attendersi per il fatto di essere stato inserito nell'elenco. Si tratta, pertanto, di una nuova finalità che non è compatibile con quella iniziale (cfr. l'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE) (4).

Le ricerche derivate possono, tuttavia, rivelarsi di grande utilità e non dovrebbero essere proibite in quanto tali. Allo scopo di rendere tale elaborazione equa e legale è necessario rispettare le condizioni della direttiva.

Poiché l'utilizzo dei dati personali inseriti negli elenchi pubblici per servizi di ricerca derivata o a criteri multipli è una finalità di recente introduzione, i responsabili del trattamento dei dati sono tenuti ad informarne le persone interessate (articoli 10 e 11 della direttiva 95/46/CE).

Inoltre, per essere legittimo tale trattamento deve rispettare anche uno dei criteri previsti all'articolo 7 della direttiva 95/46/CE. In base all'articolo 7, lettera f), il trattamento può essere legittimo se è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure dei terzi e a condizione che non prevalgano gli interessi della persona alla tutela dei propri diritti fondamentali.

Al fine di garantire l'equilibrio tra gli interessi, sono stati individuati e valutati gli interessi ed i rischi per la *privacy* in gioco. In tal senso, la direttiva 97/66/CE offre indicazioni utili: è possibile inserire in elenchi pubblici convenzionali le informazioni minime necessarie per identificare un abbonato, a meno che l'abbonato non si opponga alla pubblicazione di tali informazioni. Tuttavia, è richiesto il consenso dell'abbonato quando si tratta di informazioni aggiuntive o di funzioni complementari dell'elenco pubblico. Per quanto riguarda l'utilizzo degli elenchi pubblici per ricerche derivate o a criteri multipli, la situazione è analoga e, anzi, tale trattamento potrebbe configurare anche un'indebita violazione della *privacy*. È necessario considerare che gli interessi alla tutela dell'abbonato prevalgono sugli interessi del responsabile del trattamento o dei terzi.

Di conseguenza, tale trattamento è legittimo solo se l'interessato ha dato il proprio consenso informato prima dell'inserimento dei suoi dati personali in elenchi pubblici con funzioni di ricerca derivata o a criteri multipli (articolo 7, lettera a) e articolo 2, lettera h) della direttiva 95/46/CE).

In pratica, ciò significa che:

• è necessario ottenere il *consenso specifico e informato* dell'abbonato prima dell'inserimento dei dati personali che lo riguardano in elenchi pubblici di ogni tipo (telefonia tradizionale e mobile, posta elettronica, firme elettroniche, ecc.) utilizzati per ricerche derivate o a criteri multipli;

• *in particolare*, il responsabile del trattamento deve informare l'abbonato
– circa l'utilizzo dei dati personali negli elenchi alfabetici,
– se, e in quale misura, si intende utilizzare i dati personali dell'abbonato in servizi di ricerca derivata o a criteri multipli (quale tipo di ricerca a criteri multipli è consentito),
– del suo diritto di modificare, in qualsiasi momento e senza alcun onere, la sua decisione di consentire ciascun tipo specifico di trattamento dei dati.

• Il responsabile del trattamento deve inoltre attuare *misure tecniche ed organizzative* appropriate ai rischi che il trattamento comporta e alla natura dei dati tutelati (cfr. articolo 17 della direttiva 95/46/CE). Ciò significa, ad esempio, che il *database* dovrà essere progettato al fine di impedirne, per quanto possibile, usi fraudolenti, quali modifiche illecite dei criteri di ricerca oppure la copia o l'accesso all'intero *database* per ulteriori elaborazioni. I criteri di ricerca, ad esempio, dovranno essere abbastanza precisi da consentire solo la visualizzazione di un numero limitato di risultati per

---

4 Seguendo la stessa linea, il gruppo di lavoro internazionale sulla tutela dei dati nel settore delle telecomunicazioni (Gruppo di Berlino) ha approvato, nel corso della sua ventitreesima riunione, una posizione comune sugli elenchi derivati 4 che recita che "l'esistenza degli elenchi derivati, senza regole specifiche per la tutela, può minacciare gravemente la privacy". La posizione comune sottolinea, inoltre, che la finalità di un elenco derivato "(...) non è identica a quella di un elenco telefonico: un elenco telefonico consente di ottenere il numero telefonico di una persona nota, a partire dal suo nome e da un criterio geografico, mentre la finalità di un elenco derivato è quella di ricercare l'identità e l'indirizzo di abbonati dei quali si conosce esclusivamente il numero telefonico". Analogamente, il gruppo di Berlino afferma che l'attuazione di una ricerca derivata in un elenco telefonico senza il consenso della persona interessata "(...) costituisce una raccolta di informazioni illegittima".
Un parere ancora più dettagliato in questo senso è stato approvato dalla commissione belga per la tutela dei dati nel giugno 1999 (Commission de la protection de la vie privée, recommandation n. 01/1999 du 23 juin 1999, disponibile all'indirizzo:
http://www.privacy.fgov.be

pagina. Il risultato dovrà essere quello di garantire, anche con mezzi tecnici, le finalità di ricerca alle quali l'abbonato ha dato il proprio consenso.

Tali condizioni non si applicano solo agli operatori delle telecomunicazioni, ma anche ad altre parti, quali i redattori, e pertanto a *tutti* coloro che desiderano utilizzare dati personali al fine di offrire elenchi o servizi di ricerca a criteri multipli (5).

Conclusioni

Viste le considerazioni esposte in precedenza e considerato il quadro giuridico creato dalla direttiva 97/66/CE e dalla direttiva 95/46/CE, il gruppo di lavoro sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali è del parere che il trattamento dei dati personali all'interno di elenchi derivati o nell'ambito di servizi di ricerca a criteri multipli senza il consenso informato ed inequivocabile dell'abbonato sia iniquo ed illegittimo. Per rendere legittimo tale trattamento è necessario rispettare le condizioni esposte in precedenza.

Il gruppo di lavoro accoglie con favore ed appoggia pienamente la proposta della Commissione europea per un progetto di direttiva riguardante il trattamento dei dati personali e la tutela della *privacy* nel settore delle comunicazioni elettroniche (6) che prende in considerazione le varie possibilità di utilizzo, in particolare, degli elenchi elettronici pubblici (quali le funzioni di ricerca derivata). Il progetto di direttiva prevede che l'abbonato dia il proprio consenso informato all'inserimento dei suoi dati personali in un elenco pubblico, per finalità ed entro limiti determinati. La proposta della Commissione adatta pertanto le norme alla realtà considerando il fatto che per i nuovi servizi elettronici di comunicazione, quali GSM e posta elettronica, la maggioranza degli abbonati non desidera rendere pubblico il proprio numero di cellulare e il proprio indirizzo di posta elettronica e la maggior parte dei fornitori del servizio ha in pratica rispettato i desideri dei propri abbonati per evidenti ragioni commerciali.

Il gruppo di lavoro apporterà ulteriori contributi alla discussione su tutte le questioni riguardanti tale progetto di direttiva.

Fatto a Bruxelles il 13 luglio 2000

Per il gruppo di lavoro

Il presidente

Stefano RODOTÀ

5 Vedere la definizione di "responsabile del trattamento" all'articolo 2, lettera d) della direttiva 95/46/CE. 6 Cfr. COM xxx (adottata il 12 luglio 2000). 6 Cfr. il parere xxx sul riesame della direttiva 97/66/CE, approvato il xxx).

124 PARERE 6/2000 SUL PROBLEMA DEL GENOMA (APPROVATO IL 13 LUGLIO 2000)

Il gruppo di lavoro sulla protezione degli individui per il trattamento dei dati personali

istituito in virtù della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 (1),

considerando gli articoli 29 e 30, paragrafi 1 (a) e 3, della direttiva citata,

considerando il proprio regolamento ed in particolare gli articoli 12 e 14,

ha approvato il parere seguente:
Parere 6/2000 sul genoma umano e la riservatezza

Il completamento di una prima versione della mappa del DNA è stato annunciato di recente dai partecipanti al progetto sul genoma umano.

Il gruppo di lavoro riconosce che questo risultato, di grande significato, può permettere la diagnosi e la terapia delle malattie in maniere precedentemente inimmaginabili.

In occasione della presentazione pubblica il 26 giugno, è stato riconosciuto che i rischi di abuso delle conoscenze genetiche sollevano legittime preoccupazioni per la riservatezza degli individui. Il gruppo di lavoro condivide queste preoccupazioni. La decodificazione della mappa del DNA costituisce la premessa di nuove scoperte e applicazioni nel settore degli esami genetici. D'altra parte, le relative informazioni possono permettere di identificare gli individui, collegarli ad altri, e rivelare complessi elementi d'informazione sul futuro sviluppo e sulle future condizioni sanitarie delle persone e di coloro ai quali sono collegate geneticamente.

Il gruppo di lavoro desidera sottolineare l'importanza della riservatezza in quanto diritto fondamentale, e la conseguente necessità di applicare le nuove tecnologie genetiche con salvaguardie adeguate alla protezione di tale diritto.

Fatto a Bruxelles, 13 luglio 2000

Per il gruppo di lavoro

Il Presidente

Stefano RODOTÁ

1 Gazzetta Ufficiale n. L 281 del 23/11/1995, pag. 31, disponibile all'indirizzo seguente: http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm

125 RACCOMANDAZIONE RELATIVA AI REQUISITI MINIMI PER LA RACCOLTA DI DATI ON-LINE NELL'UNIONE EUROPEA (ADOTTATA IL 17 MAGGIO 200)1

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 1, lettera a), e paragrafo 3 di detta direttiva,

visto il regolamento interno, in particolare gli articoli 12 e 14,

ha adottato la presente raccomandazione:

1. Introduzione

1. Nel documento di lavoro intitolato "Tutela della vita privata su Internet–Un approccio integrato dell'EU alla protezione dei dati *on-line*", del 21 novembre 2001 (2), il Gruppo di lavoro ha evidenziato come sia importante garantire la messa in atto di strumenti adeguati per assicurare che l'utente Internet riceva tutte le informazioni necessarie affinché possa riporre la propria fiducia, con cognizione di causa, sui siti visitati e, se necessario, esercitare determinate scelte conformemente ai propri diritti come previsto dalla normativa europea. Tale fattore risulta particolarmente importante in considerazione del fatto che l'uso di Internet moltiplica le possibilità di raccolta di dati personali e, conseguentemente, i pericoli per i diritti fondamentali e le libertà degli individui, soprattutto per quel che riguarda la loro vita privata. Nel suo Parere n. 4/2000 del 16 maggio 2000 sul livello di tutela dei dati offerto dai principi dell'"approdo sicuro" (*Safe Harbor*), il Gruppo di lavoro ha invitato la Commissione a valutare con urgenza l'opportunità di creare un marchio di qualità per i siti Internet, che si basi su criteri comuni che potrebbero essere stabiliti a livello comunitario.

Questa raccomandazione fa seguito ai due documenti sopracitati. Essa intende contribuire all'effettiva ed omogenea applicazione delle disposizioni nazionali adottate in conformità alle direttive (3) sulla tutela dei dati personali fornendo indicazioni concrete sull'attuazione delle norme contenute in tali direttive relativamente alle pratiche più comuni esercitate attraverso Internet. Tali pratiche si verificano soprattutto al momento del "contatto iniziale" tra l'utente Internet ed un sito *web* sia nel caso di esclusiva ricerca di informazioni, sia nel caso di esecuzione di operazioni commerciali su base graduale.

Le indicazioni fornite di seguito riguardano in particolar modo la raccolta di dati personali su Internet e si prefiggono di identificare le misure che dovranno essere attuate nei confronti delle persone interessate per garantire la lealtà e la liceità di tali pratiche (applicazione degli articoli 6, 7, 10 e 11 della direttiva 95/46/CE). Tali indicazioni focalizzano in particolare sul come, quando e quali informazioni occorre fornire all'utente individuale, con l'aggiunta di dettagli pratici relativi a diritti ed obblighi risultanti da dette direttive.

Il principale obiettivo di questa raccomandazione consiste dunque nel fornire un concreto valore aggiunto all'attuazione dei principi generali della direttiva. Il Gruppo di lavoro considera la presente raccomandazione come la prima iniziativa per la presentazione a livello europeo dell'insieme "minimo" di obblighi ai quali i responsabili del trattamento (le persone fisiche o giuridiche responsabili del trattamento dati nell'ambito di un sito *web*) (4) che si occupano di siti Internet in cui vengono richieste infor-

---

1 Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile su:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 WP 37 (5063/00): documento di lavoro - Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line. Adottato il 21 novembre 2000. Disponibile su:
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.htm

3 Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e direttiva 97/66/CE del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. Disponibili su:
http://europa.eu.int/comm/inernal_market/en/media/dataprot/law.htm

4 A titolo di riferimento, l'articolo 2 della direttiva 95/46/CE definisce il responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario".

mazioni particolareggiate o la specificazione del campo d'azione (5) possano facilmente conformarsi. Certamente questa raccomandazione non esonera i responsabili del trattamento dall'obbligo attualmente vigente di verificare la conformità di tali trattamenti all'intera serie di requisiti e condizioni precisati nel diritto nazionale applicabile per renderlo legittimo, verifica senza la quale tale trattamento non risulta idoneo.

Tale raccomandazione si applica nel caso in cui il responsabile del trattamento abbia sede in uno degli Stati membri dell'Unione europea. In questa circostanza sarà applicato il diritto nazionale dello Stato membro in oggetto al trattamento dei dati personali che avvenga nel contesto delle attività di tale stabilimento. Tale raccomandazione si applica altresì quando il responsabile del trattamento non ha sede nel territorio della Comunità ma ricorre, ai fini del trattamento di dati personali, a strumenti automatizzati o non automatizzati situati nel territorio di uno degli Stati membri dell'UE. Tale trattamento è contemplato dalla legislazione nazionale dello Stato membro in cui si trovano i supporti tecnici o le risorse (6).

2. La raccomandazione, per poter conseguire tale obiettivo, è rivolta particolarmente:

– ai responsabili del trattamento che raccolgono dati *on-line*, dotandoli di una guida pratica che elenchi l'insieme minimo delle misure concrete da attuare;

– ai singoli utenti Internet affinché siano informati a riguardo e affinché possano esercitare i propri diritti;

– alle istituzioni desiderose di assegnare un'etichetta certificante la conformità delle procedure di trattamento impiegate alle direttive europee sulla protezione dei dati, dotandole di criteri di riferimento per l'assegnazione di tale etichetta riguardo alle informazioni da apporre e alla raccolta di dati personali. È ovvio che, al momento dell'assegnazione dell'etichetta, occorrerà tener conto di separati criteri concernenti altri obblighi e diritti oltre ai suddetti criteri di riferimento. Il Gruppo di lavoro pubblicherà successivamente un esauriente documento relativo a detta problematica;

alle autorità europee responsabili della protezione dei dati per poterle dotare di un quadro di riferimento comune per il loro compito di verifica della conformità alle disposizioni nazionali adottate dagli Stati membri, conformemente alle direttive sopracitate;

3. Il Gruppo di lavoro è inoltre del parere che tale raccomandazione dovrebbe servire da riferimento per la definizione dei criteri per *software* e *hardware* preposti alla raccolta e al trattamento di dati personali su Internet.

II. Raccomandazioni sulle informazioni da fornire in caso di raccolta di dati nel territorio degli Stati membri dell'Unione europea.

2.1. Informazioni da fornire alla persona interessata e tempi da rispettare

4. Qualsiasi raccolta di dati personali individuali ottenuta attraverso un sito *web* richiede l'anticipata fornitura di determinate informazioni. In termini di contenuto la conformità a tale obbligo rende necessario:

5. menzionare l'identità, l'indirizzo fisico e quello elettronico del responsabile del trattamento e, ove possibile, quello dell'eventuale rappresentante in forza all'articolo 4.2 della direttiva;

---

5 Le raccomandazioni concrete della presente raccomandazione costituiscono i requisiti minimi nel senso che non sono le uniche. In futuro tali raccomandazioni dovrebbero essere integrate da altre relative al trattamento di dati personali ancor più sensibili, come il trattamento riguardante siti sanitari e siti rivolti a bambini o i servizi offerti dai portali. In quanto ad altre specifiche modalità di trattamento, come la divulgazione di dati personali in un sito o la conservazione dei dati sul traffico da parte dei fornitori di servizi Internet e dei fornitori di contenuti e servizi Internet, si rimanda alle raccomandazioni del Gruppo di lavoro contenute nel documento citato nella nota n. 1 e alle altre posizioni del caso assunte dal Gruppo di lavoro, come il WP 25 (5085/99): Raccomandazione 3/99 relativa alla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari. Approvata il 7 settembre 1999. WP 18 (5005/99): Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni. Approvata il 3 maggio 1999. WP 17 (5093/98): Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software ed hardware. Approvata il 23 febbraio 1999. Tutto disponibile su: cfr. nota n. 1.

6 Cfr. articolo 4, paragrafo 1, punti a) e c) della direttiva 95/46/CE. È necessario mantenere nettamente distinto tale aspetto dalla questione del trasferimento legale di dati personali dall'UE ad un paese terzo. Tale problematica è trattata dagli articoli 25 e 26 della direttiva 95/46/CE e dalle connesse decisioni della Commissione europea relative all'adeguatezza della tutela nei paesi terzi. Ad esempio, se un sito web americano fa uso di strumenti situati all'interno dell'UE per la raccolta ed il trattamento di dati personali sarà applicata alle operazioni di raccolta e di trattamento la legislazione dello stato europeo in questione, a prescindere dall'adeguatezza del livello di protezione fornito da tale compagnia e conformemente alla decisione della Commissione europea relativa all'approdo sicuro. Tale problematica relativa all'adesione o meno dello Stato destinatario di dati all'approdo sicuro sarà pertinente esclusivamente in merito alla liceità delle successive cessioni di dati personali dalla compagnia con sede all'interno dell'UE a quell'altra

6. menzionare chiaramente la/le finalità del trattamento con il quale il responsabile raccoglie dati attraverso un sito *web*. Ad esempio, nel caso in cui tali dati vengano raccolti per stipulare un contratto (abbonamento ad Internet, ordine di prodotti, ecc.) ed anche per la commercializzazione diretta, occorre che il responsabile specifichi chiaramente le due finalità in questione;

7. menzionare chiaramente il carattere obbligatorio o facoltativo delle informazioni richieste. Le informazioni obbligatorie sono quelle indispensabili all'espletamento del servizio richiesto. Ad esempio, è possibile evidenziare il carattere obbligatorio o facoltativo apponendo un asterisco all'informazione di carattere obbligatorio oppure, in alternativa, è possibile scrivere "facoltativo" accanto all'informazione non obbligatoria. Il fatto che la persona interessata non fornisca informazioni facoltative non deve tornarle a svantaggio in nessun modo;

8. menzionare l'esistenza di diritti, e delle condizioni per il loro esercizio, in base ai quali l'interessato possa esprimere il proprio consenso o, eventualmente, opporsi al trattamento di dati personali (7). È necessario parimenti fornire indicazioni sulle modalità di accesso, di rettifica o di cancellazione di tali dati o informazioni, sia riguardo la persona o il servizio al quale occorre rivolgersi per l'esercizio di tali diritti, che relativamente alla possibilità di esercitarli on-line e all'indirizzo fisico del responsabile;

9. elencare i destinatari o le categorie di destinatari delle informazioni raccolte. Al momento della raccolta di dati i siti Internet dovrebbero specificare se i dati raccolti saranno comunicati o resi disponibili a terzi – tra cui, in particolare, partner commerciali, imprese figlie, ecc. – e le relative motivazioni (con finalità diverse dalla fornitura del servizio richiesto e per la commercializzazione diretta (8). In questi casi è fondamentale che gli utenti Internet dispongano di un'effettiva possibilità di opporsi *on-line* a detta comunicazione cliccando su di una casella di spunta ed esprimendo così il proprio favore alla comunicazione dei dati con finalità diverse dalla fornitura del servizio richiesto. Dal momento che il diritto di opporsi può essere esercitato in qualunque momento, occorre menzionare anche nelle informazioni fornite alla persona interessata la possibilità di esercitare tale diritto *on-line*. Il Gruppo di lavoro, consapevole degli svantaggi recati dal sovraccarico di informazioni negli schermi, è del parere che, se non appaiono nomi di destinatari, il responsabile del trattamento si impegna a non comunicare le informazioni raccolte a terzi i cui nomi ed indirizzi non siano stati forniti (a meno che la loro identità sia ovvia), garantisce che la comunicazione dei dati sia necessaria all'espletamento del servizio richiesto dall'utente Internet e che tale comunicazione sia effettuata esclusivamente con quella finalità.

10. Nel caso in cui sia previsto che il responsabile del trattamento trasmetta i dati a paesi esterni all'Unione europea, specificare se tali paesi garantiscono una protezione adeguata degli individui riguardo al trattamento dei loro dati personali, in forza dell'articolo 25 della direttiva 95/46/CE. In questo caso è necessario fornire informazioni specifiche a proposito dell'identità e dell'indirizzo dei destinatari (indirizzo fisico e/o elettronico) (9) ;

11. fornire nome ed indirizzo (indirizzo fisico e/o elettronico) del servizio o della persona incaricata di rispondere ad eventuali quesiti riguardanti la protezione di dati personali;

12. menzionare chiaramente l'esistenza di procedure di raccolta automatica di dati prima di utilizzare simili metodi per detta raccolta (10) . Nel caso di un ricorso a tali procedure è necessario che la persona interessata riceva le informazioni contenute in questo documento. Detta persona dovrà inoltre essere

---

7 Il trattamento a finalità specifiche è consentito solo se motivato da una delle considerazioni elencate nell'articolo 7 della direttiva 95/46/CE (tra l'altro nei casi in cui la persona interessata abbia fornito esplicitamente il proprio consenso, in cui il trattamento risulti indispensabile per l'esecuzione del contratto con la persona interessata, in cui il trattamento risulti indispensabile per adempiere ad un obbligo legale del responsabile del trattamento e in cui tale trattamento risulti indispensabile per il perseguimento dell'interesse legittimo del responsabile oppure di quello di terzi che hanno fatto uso di tali dati, a meno che l'interesse della persona in oggetto non risulti prevalente).

Il diritto ad opporsi (cfr. articolo 14) è fissato dagli Stati membri in almeno due situazioni di cui all'articolo 7, inclusa l'ultima menzionata sopracitata. L'individuo ha il diritto, salvo disposizione contraria prevista dalla normativa nazionale, di opporsi in qualsiasi momento per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che lo riguardano. Il diritto di opporsi su richiesta e gratuitamente sussiste in ogni caso quando il trattamento in oggetto è finalizzato alla commercializzazione diretta. La persona interessata può inoltre opporsi gratuitamente (una volta informata ed a partire dalla prima comunicazione) alla comunicazione di dati personali a terzi o al loro utilizzo per conto di terzi per la commercializzazione diretta.

8 La comunicazione a terzi è consentita solo nel caso in cui la finalità prevista non sia incompatibile con quella per la quale i dati sono stati raccolti e se motivata da una delle considerazioni elencate nell'articolo 7, condizioni che rendono legittimo il trattamento.

9 Informazioni riguardo l'adeguatezza delle decisioni sono disponibili sul sito Web della Commissione al seguente indirizzo:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

10 Il trattamento "invisibile" ed automatico dei dati personali è soggetto alle medesime modalità, condizioni e garanzie delle altre tipologie di trattamento di dati personali. Cfr. Raccomandazione 1/99 del Gruppo di lavoro sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware (23 febbraio 1999), disponibile sul sito web citato nella nota n. 1.

informata circa il nome del dominio dal quale il server del sito trasmette le procedure di raccolta automatica, le finalità di dette procedure, il loro periodo di validità, l'eventualità in cui l'accettazione di tali procedure sia necessaria per visitare il sito e le possibili conseguenze di una loro disattivazione. Se vi sono altri responsabili del trattamento coinvolti nella raccolta dei dati personali occorre che la persona interessata riceva tutte le informazioni riguardanti l'identità del responsabile e le finalità del trattamento relativamente a ciascun responsabile di detto trattamento. È necessario comunicare la possibilità di opporsi alla raccolta prima di ricorrere a qualsiasi procedura automatica che provochi la connessione di un utente PC ad un altro sito *web*. Es. allo scopo di evitare che un secondo sito possa raccogliere dati ad insaputa di in utente Internet nel caso in cui questo venga automaticamente connesso da un sito *web* ad un altro per visualizzare pubblicità sotto forma di *banner*. Ad esempio, se un cookie viene collocato dal server del responsabile del trattamento è necessario comunicare detta informazione prima che venga spedito all'*hard disk* dell'utente Internet, in aggiunta alle informazioni fornite grazie alla tecnologia esistente che si limita a specificare il nome del sito di trasmissione ed il periodo di validità di detto cookie (11).

13. Indicare le misure di sicurezza a garanzia dell'autenticità del sito, del grado di completezza e riservatezza delle informazioni trasmesse nella detta rete in applicazione della legislazione nazionale applicabile. (12)

14. Fornire le informazioni in tutte le lingue usate nel sito *web* e, specialmente, in quei passaggi ove avviene la raccolta dei dati personali.

15. Che i responsabili del trattamento verifichino la coerenza delle informazioni contenute nei vari documenti destinati al sito (le sezioni "dati personali e protezione della vita privata", i moduli elettronici, testi relativi alle condizioni generali di vendita e ad altre comunicazioni commerciali).

2.2. Modalità di presentazione delle informazioni

16. Il Gruppo di lavoro ritiene che le seguenti informazioni debbano apparire direttamente sullo schermo prima che avvenga la raccolta, così da assicurare un giusto trattamento dei dati.

Dette informazioni riguardano:
l'identità del responsabile del trattamento;
la/le finalità;
la natura obbligatoria o facoltativa delle informazioni richieste;
i destinatari o le categorie di destinatari dei dati raccolti;
l'esistenza del diritto di accesso e di rettifica;
l'esistenza del diritto di opporsi a qualsiasi comunicazione dei dati a terzi con finalità diverse dalla fornitura del servizio richiesto e le modalità per esercitare tale diritto (ad esempio fornendo la possibilità di cliccare su una casella di spunta);
le informazioni da fornire in caso di utilizzo di procedure di raccolta automatica;
il livello di sicurezza nel corso di tutte le fasi del trattamento compresa la trasmissione, ad esempio sulle reti.

In tali situazioni le informazioni devono essere fornite interattivamente e devono apparire sullo schermo. Così, nel caso di metodi automatici di raccolta dati, dette informazioni possono essere fornite, se necessarie, tramite la tecnica delle finestre *pop-up*.

A proposito del livello di sicurezza nel corso della trasmissione dei dati dall'apparecchiatura occorre visualizzare un'intestazione del tipo "Stai accedendo ad una connessione protetta" oppure le procedure di informazione automatica presenti nei *browser*, come la comparsa di icone specifiche sotto forma di chiave o di lucchetto.

17. Il Gruppo di lavoro ritiene inoltre che sia necessario poter accedere ad informazioni esaustive riguardo alla politica di tutela della sfera privata (comprese le modalità per l'esercizio del diritto d'accesso) direttamente dalla pagina d'entrata del sito e ovunque vengano raccolti dati personali on-line. Il

11 Se il cookie è collocato da un'organizzazione attraverso il proprio sito web e soltanto questa è in grado di accedere al contenuto di detto cookie non occorre fornire informazioni aggiuntive riguardo l'organizzazione responsabile del collocamento del cookie, purché l'organizzazione che ospita tale sito web sia già stata adeguatamente identificata.

12 Cfr. le norme specifiche dell'articolo 17, paragrafi 1 e 3 secondo trattino della direttiva 95/46/CE.

titolo dell'intestazione su cui cliccare deve essere sufficientemente messo in risalto, chiaro e preciso in modo da consentire all'utente Internet di crearsi un'idea chiara del contenuto al quale sta per accedere. Ad esempio, l'intestazione potrebbe asserire "Stiamo raccogliendo e trattando dati personali che La riguardano. Per ulteriori informazioni clicchi qui" oppure "Dati personali o tutela della sfera privata". Il contenuto delle informazioni alle quali l'utente Internet è indirizzato deve altresì essere sufficientemente preciso.

III. Raccomandazioni per il perfezionamento degli altri diritti e doveri

Il Gruppo di lavoro desidera inoltre attirare l'attenzione dei destinatari della presente Raccomandazione su altri diritti dell'individuo ed obblighi dei responsabili del trattamento basati su direttive di particolare attinenza nell'ambito della raccolta di dati personali su siti *web*. Il Gruppo di lavoro ritiene che le raccomandazioni seguenti, così come le indicazioni sulle informazioni, abbiano un'utilità pratica immediata sia per i responsabili del trattamento che per gli utenti Internet.

18. Raccogliere esclusivamente i dati necessari per il conseguimento dello scopo prefisso;

19. garantire che i dati siano trattati esclusivamente nelle suddette legittime modalità, conformemente ad uno dei criteri elencati nell'articolo 7 della direttiva 95/46/CE;

20. garantire l'effettivo esercizio del diritto di accesso e di rettifica; l'esercizio di tali diritti dovrebbe essere possibile sia all'indirizzo fisico del responsabile del trattamento che *on-line*. È necessario predisporre particolari misure di sicurezza affinché esclusivamente la persona interessata abbia accesso *on-line* alle informazioni che la riguardano;

21. conformarsi al principio della "finalità" o "scopo" in base al quale occorre far uso di dati personali solo se necessario e per finalità determinate. In altri termini, in assenza di un motivo legittimo, non è possibile fare uso di dati personali ed è necessario mantenere l'anonimato degli individui (articolo 6, paragrafo 1, punto b) della direttiva 95/46/CE). Detto principio è altresì denominato "principio di minimizzazione".

22. Fornire ed incoraggiare la consultazione in modalità anonima di siti commerciali, nello stesso ambito descritto nel punto 21, senza richieste di identificazione degli utenti per cognome, nome, indirizzo di posta elettronica o altri dati identificativi. Qualora sia necessario un collegamento ad una persona senza completa identificazione della stessa è bene suggerire ed accogliere l'uso di pseudonimi di qualsivoglia natura. Ove non sussistano necessità di identificazione legale occorre incoraggiare ed accogliere l'uso di pseudonimi, anche nel caso di determinate operazioni. Un esempio è dato dall'uso di certificati pseudonimi per le firme elettroniche (cfr. articolo 8 della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche).

23. Stabilire un periodo di conservazione per i dati raccolti. È possibile conservare detti dati esclusivamente per il tempo necessario allo scopo del trattamento indicato e perseguito (articolo 6 della direttiva 95/46/CE e articolo 6 della direttiva 97/66/CE).

24. Adottare gli accorgimenti necessari per garantire la sicurezza dei dati nel corso del loro trattamento e della loro trasmissione (ad esempio limitare e determinare il numero delle persone che hanno accesso ai dati, far uso di trasmissioni cifrate, ecc.; articolo 17 della direttiva 95/46/CE).

25. Se è coinvolto un responsabile per l'elaborazione, ad esempio per ospitare un sito web, stipulare un contratto che gli imponga di attuare appropriate misure di sicurezza in conformità anche della normativa dello Stato membro in cui si trova il responsabile per l'elaborazione, nonché effettuare il trattamento dei dati personali attenendosi esclusivamente alle indicazioni del responsabile di detto trattamento.

26. A seconda dei casi e in forza della legge nazionale, procedere alla notificazione dell'autorità di controllo (se il responsabile dell'elaborazione del sito si trova nell'Unione europea o se lo stesso dispone di un rappresentante nell'Unione europea). Il numero di registrazione di detta notifica può essere indicato all'interno del sito, in modo vantaggioso, al di sotto dell'intestazione destinata alla protezione dei dati.

27. Se vengono trasferite informazioni ad un paese terzo in cui non è garantito un adeguato livello di protezione è necessario assicurare che il trasferimento dei dati avvenga esclusivamente se lo stesso è in linea con le deroghe all'articolo 26 della direttiva 95/46/CE. In questi casi occorre informare le persone delle adeguate garanzie fornite affinché il trasferimento risulti lecito.

IV. Raccolta di indirizzi per la commercializzazione diretta tramite posta elettronica e per la spedizione di newsletter

28. Per ciò che concerne la commercializzazione diretta per posta elettronica:

il Gruppo di lavoro ripropone il proprio parere secondo il quale gli indirizzi di posta elettronica reperiti nelle aree pubbliche di Internet all'insaputa delle persone interessate, ad esempio nei gruppi di discussione, non sono stati raccolti lecitamente. Tali indirizzi non possono perciò essere utilizzati con finalità diverse da quelle per le quali sono stati originariamente resi pubblici; in particolar modo non possono essere utilizzati per la commercializzazione diretta (13);

fare uso di indirizzi di posta elettronica per la commercializzazione diretta a condizione che questi siano stati raccolti lealmente e legalmente. Affinché la raccolta sia leale e legale è necessario che le persone interessate siano state informate della possibilità dell'uso di tali dati per la commercializzazione diretta e che dette persone abbiano potuto acconsentire a tale uso direttamente al momento della raccolta (cliccando su una casella di spunta) (14) . L'invio di posta elettronica a scopo promozionale deve altresì prevedere la possibilità di esercitare il recesso *on-line* dall'elenco di indirizzi impiegato (15).

29. Per ciò che concerne la spedizione di *newsletter*:

Procurarsi il previo consenso delle persone interessate e garantire la possibilità di un loro recesso da tali spedizioni in qualsiasi momento; occorrerà pertanto informare dette persone riguardo a questa possibilità ogniqualvolta viene spedita una *newsletter*.

Il gruppo di lavoro invita il Consiglio d'Europa, la Commissione europea, il Parlamento europeo e gli Stati membri a tener conto della presente raccomandazione.

Il gruppo si riserva la facoltà di formulare ulteriori osservazioni.

Fatto a Bruxelles, 21 maggio 2001

Per il gruppo

Il Presidente

Stefano RODOTÀ

13 Cfr. WP 28 (5007/00): "Parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali", approvato il 3.2.2000, WP 29 (5009/00);"Parere 2/2000 concernente la revisione generale del quadro giuridico delle telecomunicazioni", approvato il 3.2.2000, e, specialmente, riguardo l'applicazione degli articoli 6 e 7 della direttiva 95/46/CE. WP 36 (5042/00): "Parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 (COM(2000)385)", approvato il 2.11.2000 e WP 37 (5063/00); "Documento di lavoro: Tutela della vita privata su Internet. un approccio integrato dell'UE alla protezione dei dati on-line", approvato il 21.11.2000.

14 All'interno dell'Unione europea cinque Stati membri (Germania, Austria, Italia, Finlandia e Danimarca) hanno adottato misure intese a vietare le comunicazioni commerciali non sollecitate. In altri Stati membri esiste un sistema di possibilità di recesso oppure permane una situazione poco chiara. È bene notare che la proposta di direttiva della Commissione relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM(2000) 385) del 12 luglio 2000 è in favore di una soluzione armonizzata basata sulla possibilità di adesione; tale approccio è stato unanimemente sostenuto dal Gruppo di lavoro nel Parere 7/2000 (WP 36 sopracitato). Si veda inoltre lo studio di S. Gauthronet e di E. Drouard (ARETE) per la Commissione. "Messaggi pubblicitari indesiderati e protezione dei dati personali", gennaio 2001. http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamsumit.pdf

15 La direttiva sul commercio elettronico stabilisce ulteriori requisiti relativi alle comunicazioni commerciali non sollecitate in quei casi in cui è consentita la possibilità di recesso conformemente alla direttiva 97/66/EC.

126 RACCOMANDAZIONE N. 1/2001 SULLE VALUTAZIONI RELATIVE A LAVORATORI

5008/01/EN final WP 42
Adopted on 22.3.2001

Draft Recommendation on Employee Evaluation Data

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT RECOMMENDATION:

Directive 95/46/EC on the protection of individuals with regard to the processing of their personal data and the free movement of such data calls upon Member States to protect the fundamental rights and freedoms of individuals, and in particular their right to privacy with respect to the processing of personal data.

The Directive is part of the Community measures necessary to remove obstacles to flows of personal data in the various spheres of economic, administrative and social activity within the internal market, and that to this end it aims at harmonising the rules on processing of personal data by affording a high level of protection in the Community.

Based on the definition included in Article 2(a) of Directive 95/46/EC, personal data means any information relating to an identifiable or identified person, such as for instance data relating to his/her physical, physiological, mental, economic, cultural or social identity.

The scope of this definition implies that personal data includes not only population registry data or information resulting from objective factors which can be verified or rectified, but also any other element, information or circumstance having an information content such as to add to the knowledge of an identified or identifiable person.

Personal data can be therefore found in subjective judgments and evaluations which can actually include elements specific to the physical, physiological, psychical, economic, cultural or social identity of data subjects. This is equally true if a judgment or a evaluation is summarised by a score or rank or is expressed by means of other evaluation criteria.

The fact that under national law a few of these subjective data cannot be always accessed and rectified directly, or that they can be rectified by the inclusion of statements or notes made by data subjects, does not prevent them from being personal data, with a view to transparency of processing and the exercise of right of access.

Similar considerations apply in respect of the fact that direct access to the data included in subjective judgments or evaluations can be deferred or limited under national law.

AUTORITÀ DI CONTROLLO COMUNE SCHENGEN

127 QUARTA RELAZIONE DI ATTIVITÀ DELL'AUTORITÀ DI CONTROLLO COMUNE: MARZO 1999 - FEBBRAIO 2000

SOMMARIO:

NOTA DI SINTESI

Il presente documento riporta la quarta relazione annuale di attività dell'Autorità di controllo comune Schengen (ACC). In uno spirito di trasparenza e di apertura democratica, ACC ritiene opportuno rendere conto ad un pubblico quanto più vasto possibile dei suoi sforzi costanti intesi a difendere gli interessi dell'individuo nella tutela della vita privata. Le attività svolte dall'ACC nel periodo compreso tra marzo 1999 e febbraio 2000 dimostrano una volta di più che l'autorità di controllo è parte integrante della struttura di Schengen.

L'ACC, basandosi su relazioni, ha formulato anche questa volta raccomandazioni o pareri, proposte e suggerimenti riguardanti sia il controllo della sicurezza del SIS che la tutela degli interessi dei singoli individui segnalati, o ancora l'adempimento dell'obbligo d'informazione nei confronti del cittadino.

Questa volontà di contribuire in modo costruttivo al corretto funzionamento del meccanismo Schengen che anima tutti i colleghi delegati delle autorità di controllo nazionali e gli osservatori dei paesi candidati all'adesione, contrasta talvolta fortemente con il trattamento ingeneroso riservato all'ACC, soprattutto per quanto concerne il debito rispetto della sua autonomia e rigorosa indipendenza e l'assegnazione delle risorse finanziarie necessarie per garantirle.

La chiara volontà manifestata dall'attuale Presidenza dell'UE di pervenire a un segretariato comune di tutte le autorità di controllo nel settore di polizia europeo (Schengen, Europol, Sistema d'informazione doganale, ecc.) può rappresentare un passo nella buona direzione e l'ACC non può che compiacersene. Soltanto con risorse proprie - e la correlata responsabilizzazione - l'autonomia potrà essere reale ed efficace.

Il 1° gennaio 2000 vi è stato un cambiamento della Presidenza dell'ACC. A nome di tutti i colleghi mi pregio di trasmettere al sig. Joào Labescat i nostri vivi ringraziamenti e tutta la nostra riconoscenza per lo straordinario impegno e la perseveranza con cui ha curato gli interessi dell'ACC - e dunque di tutti i cittadini - nel difficile periodo della sua integrazione nell'ambito dell'Unione europea.

Bruxelles, 9 maggio 2000

Il Presidente
Bart De Schutter

PRIMA PARTE: INTRODUZIONE

Sono trascorsi 15 anni da quel giorno del 1985 in cui, in un villaggio della Mosella lussemburghese da cui avrebbe tratto il nome, fu firmato l'accordo di Schengen.

Precursore dello spazio di libertà, sicurezza e giustizia che avrebbe poi creato il trattato di Amsterdam, l'accordo ha indubbiamente avuto successo, come dimostra il numero crescente di paesi che hanno aderito all'accordo stesso e alla relativa convenzione di applicazione firmata nel 1990. Ai cinque paesi firmatari del 1985 se ne sono infatti nel frattempo aggiunti altri dieci e, se nel 1995 erano sette i paesi che soddisfavano le condizioni necessarie all'attuazione della convenzione, saranno presto 15 i paesi che applicheranno l'acquis di Schengen[1] all'inizio del 2001[2].

Si ricorda che lo scopo dell'accordo di Schengen e della relativa convenzione di applicazione è l'abolizione dei controlli alle frontiere interne degli Stati membri e, quindi, la creazione di un grande spazio di libera circolazione delle persone. Per conseguire questo obiettivo garantendo nel contempo, all'interno di tale spazio, un livello di sicurezza almeno pari a quello esistente in precedenza, la convenzione di applicazione dell'accordo di Schengen prevede misure compensative, principalmente: armonizzazione della politica dei visti, definizione di una politica comune in materia di determinazione dello Stato responsabile dell'esame di una domanda di asilo, miglioramento della cooperazione di polizia e giudiziaria, intensificazione della lotta al traffico illecito di stupefacenti, armonizzazione del livello dei controlli alle frontiere esterne dello spazio Schengen e creazione di un sistema d'informazione Schengen (SIS).
Il SIS è un sistema comune che collega tutti i paesi che applicano la convenzione di Schengen e consente ai suoi utenti (uffici con compiti di polizia, ambasciate e consolati, uffici stranieri, ecc.) di disporre in tempo reale delle informazioni necessarie all'esercizio dei loro compiti rispettivi inserite da uno degli Stati membri che applicano la convenzione.

Tali informazioni riguardano le persone (ricercate per arresto estradizionale, non ammissibili nel territorio, scomparse o oggetto di una sorveglianza discreta) e gli oggetti (veicoli, armi, documenti, banconote rubate, sottratte o smarrite).

Alla creazione del SIS si è affiancata quella di un'Autorità di controllo comune per la protezione dei dati personali, incaricata segnatamente di vigilare sul rispetto delle disposizioni della convenzione relative all'unità di supporto tecnico del SIS (articolo 115). A quest'organo, composto di due rappresentanti di ogni autorità di controllo nazionale della Parti contraenti, è inoltre attribuito un compito di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

Sin dal giugno 1992, una decisione ministeriale ha istituito un'autorità di controllo comune provvisoria, organo che ha compiuto i primi passi nella preparazione dell'applicazione dei principi della protezione dei dati.

Il 26 marzo 1995, contestualmente alla messa in applicazione della convenzione nei sette paesi membri che soddisfacevano le condizioni preliminari, l'autorità di controllo provvisoria si è trasformata in definitiva, ossia nell'Autorità di controllo comune Schengen (ACC) prevista all'articolo 115 della convenzione.

Fin dalla messa in applicazione della convenzione, il 26 marzo 1995, l'ACC ha dovuto faticare molto perché ne fossero riconosciute le competenze e l'indipendenza rispetto agli organi esecutivi di Schengen. Prova ne è la prima relazione di attività, che sottolinea in particolare le difficoltà incontrate per ottenere un bilancio autonomo o quelle sperimentate dal gruppo di esperti cui l'ACC aveva affidato il controllo dell'unità centrale del SIS (C.SIS) installata a Strasburgo. A oltre un anno di distanza l'ACC non aveva ancora ottenuto dagli organi esecutivi di Schengen una risposta alle raccomandazioni formulate in base al controllo del C.SIS, cui aveva replicato soltanto il ministero dell'interno francese. Soltanto dal febbraio 1998 l'ACC può disporre delle informazioni inerenti al SIS che le sono necessarie per svolgere i propri compiti, perché le autorità responsabili del sistema esaminavano le richieste d'informazioni caso per caso.

---

[1] *A seguito dell'integrazione di Schengen nell'ambito dell'Unione europea gli Stati membri non applicano più la convenzione di applicazione dell'accordo di Schengen, bensì "l'acquis di Schengen integrato nell'Unione europea".*

[2] *Danimarca, Finlandia, Islanda, Norvegia e Svezia dovrebbero applicare pienamente l'acquis di Schengen dall'inizio del 2001.*

Nonostante i progressi compiuti il cammino è ancora lungo. Nelle visite di controllo che l'ACC ha effettuato nel 1996 e 1999 presso il sistema centrale di Strasburgo si è sì constatato il buon funzionamento complessivo del sistema, ma si sono anche rilevati diversi problemi, tra cui alcuni che pongono reali difficoltà in termini d'integrità.
I problemi rilevati dall'ACC hanno acquisito un'importanza vieppiù significativa quando, alla fine del 1997, il numero di Stati Schengen che applicano la convenzione è passato da 7 a 10 e, in prospettiva, con il passaggio a 15 all'inizio del 2001. Il numero dei dati inseriti nel SIS aumenta infatti di conseguenza.

Al pari di tutti i sistemi d'informazione nel settore della polizia, anche quello di Schengen registra un'evoluzione, cui deve affiancarsi un potenziamento del ruolo delle pertinenti autorità di controllo indipendenti. L'integrazione di Schengen nell'Unione europea risultante dal trattato di Amsterdam[1] deve migliorare la trasparenza e offrire maggiori garanzie per i diritti fondamentali del cittadino. I parlamenti nazionali e gli organi europei possono ora intervenire più attivamente per la realizzazione di questi obiettivi.

SECONDA PARTE: UN ANNO DI ATTIVITA' DELL'ACC

CAPITOLO I: PARERI E RACCOMANDAZIONI

I.1. Sicurezza degli uffici SIRENE

Nel dicembre 1997, a seguito di una fuga di documenti e di informazioni prodottasi presso un ufficio SIRENE qualche settimana prima, l'ACC ha incaricato le autorità nazionali di controllo di verificare la sicurezza dei rispettivi uffici SIRENE.

Avvalendosi delle relazioni nazionali l'ACC ha elaborato un documento di sintesi relativo alla sicurezza degli uffici SIRENE, nel quale ricordava i requisiti di sicurezza, previsti all'articolo 118 della convenzione di Schengen, cui devono conformarsi tutti gli uffici SIRENE e formulava dieci raccomandazioni. L'8 gennaio 1999 il documento di sintesi è stato trasmesso ai competenti organi di Schengen (Comitato esecutivo, Gruppo centrale, Gruppo di lavoro "SIRENE").

Una risposta è giunta il 19 novembre 1999, vale a dire dopo l'integrazione di Schengen nell'ambito dell'Unione europea (SCHAC 2512/99). In essa il Presidente del Comitato dell'articolo 36 –che può essere considerato il consesso cui fanno ora capo, segnatamente, le competenze del Gruppo centrale di Schengen- afferma: "*In generale gli Stati membri ritengono che buona parte delle raccomandazioni dell'Autorità di controllo comune siano già attuate negli uffici SIRENE.*
Gli Stati membri desiderano altresì richiamare l'attenzione sul fatto che alcune raccomandazioni sono piuttosto onerose sotto il profilo tecnico ed organizzativo rispetto all'obiettivo perseguito. Essi ritengono che, poiché il SIS, per contenuto e qualità dei dati, costituisce una base di dati di polizia utilizzata quotidianamente, le misure intese a garantire la sicurezza dei dati non possano avere l'effetto di limitare eccessivamente l'utilizzazione degli stessi."
Nella risposta specifica acclusa alla lettera del Presidente del Comitato dell'articolo 36, il Gruppo SIRENE sostiene inoltre, riguardo alla tracciatura e alla verifica dei motivi delle interrogazioni: "*Considerato che gli agenti di polizia di tutti gli Stati devono consultare quanto più possibile il SIS, l'utilizzazione del SIS costituisce parte della regolare attività di servizio. In alcuni Stati non è fattibile, sotto il profilo tecnico ed organizzativo, fornire una motivazione per ogni singola interrogazione del SIS, per via del numero elevato delle interrogazioni (in Germania, ad esempio, 5,4 milioni al mese)*".
"*La verifica regolare dei motivi di una interrogazione del SIS è effettuata soltanto in alcuni paesi (...). Si considera che, in principio, gli agenti di polizia agiscano in modo legittimo nell'assolvimento dei loro compiti. Al posto di una verifica regolare del motivo di una interrogazione SIS, sono pertanto ipotizzabili soltanto controlli per sondaggio*".

L'ACC, nel prendere atto della risposta, ha deciso di perseverare affinché la sicurezza degli uffici SIRENE fosse migliorata e uniformata. Ha in particolare convenuto di stendere un questionario uniforme che permetta alle autorità nazionali di controllo per la protezione dei dati di effettuare le verifiche in modo armonizzato.

[1] *V. articolo 7 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea, allegato al trattato di Amsterdam.*

I.2 Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

Fin dal 1997 uno dei membri dell'ACC aveva chiesto all'Autorità come andasse interpretato l'articolo 102, paragrafo 1 della convenzione, relativo alla conservazione dei documenti ad avvenuta cancellazione di una segnalazione. Gli Stati membri davano infatti interpretazioni diverse alla disposizione: alcuni di essi conservano i documenti relativi alle segnalazioni dopo che queste sono state cancellate e li utilizzano per completare gli schedari di polizia.

L'articolo 102, paragrafo 1 vieta però alle Parti contraenti di utilizzare i dati di cui agli articoli da 95 a 100 per fini diversi da quelli enunciati per ciascuna delle segnalazioni di cui ai detti articoli.
Nel parere 98/1 del 3 febbraio 1998 l'ACC ha ricordato i principi della convenzione e i diritti fondamentali in materia di protezione dei dati, chiedendo poi che ciascuna Parte contraente distrugga immediatamente tutta la documentazione relativa a una segnalazione cancellata, conformemente all'articolo 112 della convenzione e che il manuale SIRENE sia riveduto per eliminare le disposizioni che violano la convenzione di Schengen.

Nel gennaio 1999 il Gruppo centrale ha replicato al parere dell'ACC senza tener conto né dell'esigenza di rispettare il principio di finalità né della necessità di armonizzare le prassi. L'ACC ha allora redatto una nota complementare in cui insisteva sull'obbligo di rispettare il principio di finalità, in base al quale il dossier può essere utilizzato soltanto per i fini che hanno motivato l'inserimento della segnalazione, e sottolineava che i requisiti di finalità e di conservazione limitata alla finalità per la quale la segnalazione è stata effettuata sono altresì enunciati nell'articolo 5 della convenzione n. 108 del Consiglio d'Europa, del 28 gennaio 1981, che tutti gli Stati sono tenuti a osservare (articolo 126, paragrafo 1 della convenzione di Schengen).

Questa raccomandazione complementare al parere n. 98/1 dell'ACC è stata approvata dall'ACC il 22 ottobre 1999 (SCHAC 2505/99) ed esaminata dal Comitato dell'articolo 36 il 15 dicembre 1999.

Al riguardo, i risultati dei lavori di tale riunione del Comitato dell'articolo 36 affermano:
Al Comitato è stato sottoposto il parere dell'Autorità di controllo circa l'uso dei documenti relativi a una segnalazione dopo che i dati sono stati distrutti nel SIS. Il Servizio giuridico ritiene che il parere dell'ACC si riferisca alla prassi seguita in alcuni Stati membri e non alle regole del Consiglio.

Il Comitato decide di consultare il Gruppo SIS per verificare se occorra modificare il manuale SIRENE alla luce delle osservazioni dell'ACC.

Da allora l'ACC non ha più ricevuto notizie.

I.3 Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata

In caso di usurpazione d'identità alcuni Stati membri introducono nel SIS il nome del titolare legittimo dell'identità usurpata, mentre il bersaglio è piuttosto l'usurpatore.

In altre parole, l'identità segnalata nel sistema non corrisponde, né di fatto né di diritto, all'identità del ricercato, bensì a quella della vittima dell'usurpazione. Tuttavia, il titolare legittimo non è assolutamente informato del fatto che la sua identità sia stata introdotta nel SIS.

Alcuni Stati sono favorevoli ad una procedura secondo la quale i dati di carattere personale relativi alle persone la cui identità è stata usurpata dovrebbero essere immediatamente cancellati, mentre altri sostengono che la segnalazione contenente l'identità usurpata dovrebbe essere mantenuta anche se il titolare legittimo dell'identità inserita nel SIS ne richiedesse la cancellazione: l'argomento da essi addotto a sostegno della loro tesi è la necessità di trovare il responsabile.

Nel parere 98/2 del febbraio 1998 l'ACC ha ricordato i diritti fondamentali e i principi della convenzione in materia di protezione dei dati, sottolineando soprattutto il principio di proporzionalità, che impone di raggiungere un equilibrio fra i diritti della persona la cui identità è stata usurpata e la necessità di individuare gli usurpatori.

L'Autorità proposto che, fino all'avvio del SIS II, si cerchi di definire una soluzione comune e, se possibile, si indichi che la segnalazione riguarda un'identità usurpata.

In risposta a tale parere il Comitato dell'articolo 36 ha comunicato all'ACC le soluzioni ipotizzate (nel prossimo futuro, misure temporanee per il SIS I +, a fine 2000, e soluzione definitiva a più lungo termine per il SIS II).
L'ACC ha esaminato queste proposte nel dicembre 1999 e nel febbraio 2000. Un altro parere, complementare al primo reso dall'ACC al riguardo, è stato approvato con procedura scritta nel marzo 2000. In esso l'ACC ribadisce il principio di proporzionalità, in virtù del quale non tutti i casi di usurpazione d'identità giustificano la segnalazione del nome del titolare legittimo e sottolinea che l'elaborazione dei dati relativi alle persone la cui identità è stata usurpata potrà essere consentita solo previo libero ed esplicito accordo delle stesse o dietro loro richiesta. Devono inoltre essere previste altre misure, quali la possibilità di rilasciare al titolare legittimo dell'identità usurpata un documento supplementare, ad esempio integrativo al passaporto, che attesti che il titolare non è la persona che usurpa l'identità.

CAPITOLO II: ATTIVITÀ DI CONTROLLO

II.1. Controllo del C.SIS

Nel corso del 1998 l'ACC ha messo a punto, in collaborazione con il Ministero dell'interno francese, un documento contenente i principi applicabili alle visite e ai controlli del C.SIS. Il tempo trascorso dall'ultimo controllo effettuato e l'adesione al sistema di tre nuovi paesi (Austria, Grecia e Italia) giustificavano l'organizzazione di un nuovo controllo. L'ACC ha creato un gruppo tecnico costituito di esperti delle autorità di controllo nazionali, coordinato dal rappresentante lussemburghese. Tale gruppo di esperti si è riunito tre riprese, principalmente alla vigilia delle riunioni plenarie dell'ACC, per preparare la missione d'ispezione. Al termine del controllo effettuato nell'aprile 1999, gli esperti hanno completato per iscritto il loro progetto di relazione redatto Strasburgo. Si sono quindi riuniti a Bruxelles il 9 settembre 1999 per metterlo a punto. Il 17 settembre 1999 tale progetto è stato trasmesso al Ministero dell'interno francese, invitato a presentare le sue osservazioni entro un termine di un mese. Il gruppo di esperti ha esaminato queste ultime il 1° dicembre 1999 e ha apportato su tale base varie correzioni alla sua relazione. Le osservazioni del Ministero dell'interno francese sono quindi state allegate alla relazione dell'ACC, quali parte integrante della medesima.
La visita di controllo è stata effettuata nell'aprile 1999. Ne è emersa la possibilità di migliorare la sicurezza del sistema, giudicata globalmente soddisfacente. Una sintesi delle raccomandazioni figura in appresso.

Potrebbero essere apportati miglioramenti relativamente alla sicurezza fisica, in particolare per quanto concerne la separazione fisica tra le zone riservate rispettivamente al personale del C.SIS e al Ministero dell'interno francese o un controllo più severo dell'accesso alla sala operativa del C.SIS, grazie ad un elenco delle persone autorizzate o ad un lettore di tessere magnetiche. Le stesse osservazioni valgono per la cassaforte che custodisce i nastri contenenti i dati, per i quali dovrebbe essere messa a punto una procedura formale di distruzione.

Le funzioni fondamentali che consentono l'audit trail non sono attivate, in quanto ostacolano il corretto funzionamento del sistema. Benché il C.SIS abbia compiuto sensibili progressi per compensare tale mancanza di traccia, è possibile utilizzare le potenziali risorse non sfruttate del sistema SINIX in modo da aggiungere meccanismi di controllo nelle aree più sensibili.

Le procedure di autorizzazione e di verifica periodica dei diritti degli utenti dovrebbero essere formalizzate, l'elenco degli utenti dovrebbe essere aggiornato periodicamente e il loro accesso dovrebbe essere controllato.

Dovrebbero essere studiate varie misure tecniche in grado di migliorare la protezione contro i tentativi di intrusione.

In materia di telecomunicazioni, alcuni elementi delle apparecchiature di cifratura sono stati giudicati problematici e potrebbero provocare lacune gravi nella sicurezza delle trasmissioni.

La procedura di raffronto delle basi di dati è ancora troppo lunga e occorre pertanto prendere opportune disposizioni in modo da assicurare che le discrepanze vengano tempestivamente individuate e corrette. D'altra parte, tutte le divergenze o discrepanze, per quanto minime, devono essere debitamente rilevate e corrette in modo da rendere tutti gli archivi nazionali identici l'uno all'altro.

I dati relativi a segnalazioni che sono stati cancellati sono conservati per più di un anno presso il C.SIS, contravvenendo in tal modo alle disposizioni dell'articolo 113, paragrafo 2.
Alcune Parti contraenti hanno inserito per errore segnalazioni su persone ai sensi dell'articolo 96 della convenzione per cittadini dell'Unione europea. Il C.SIS dovrebbe inserire delle procedure di monitoraggio che rilevino l'inserimento nel SIS di segnalazioni ai sensi dell'articolo 96 (persone non ammissibili) per cittadini dell'Unione europea.

L'articolo 112, paragrafi 1 e 2, stabilisce che i dati personali inseriti nel C.SIS ai fini della ricerca di persone sono conservati soltanto per il periodo necessario ai fini per i quali sono stati forniti. Al massimo tre anni dopo il loro inserimento, la Parte contraente che ha fornito l'informazione deve esaminare la necessità di conservarli. Dalla verifica degli esperti è emerso che la procedura attualmente seguita permette di garantire la soppressione dei dati al termine in cui spira ciascuna segnalazione inserita nella base di dati del C.SIS. Ciononostante, numerose date di inserimento nelle tabelle relative alle persone segnalate sono inesatte, il che significa che le procedure di verifica delle date registrate nel C.SIS sono inadeguate. Risulta quindi necessario introdurre misure che consentano di controllare l'esattezza delle date di inserimento delle segnalazioni.

La relazione riservata sulla visita di controllo è stata approvata nel febbraio 2000 ed è stata trasmessa, corredata di una sintesi, al Comitato dell'articolo 36. Il passo che segue è tratto dai risultati dei lavori della riunione del Comitato dell'articolo 36 del 28/29 febbraio 2000, durante la quale la relazione dell'ACC è stata esaminata:

"I gruppi "SIS" hanno ricevuto il mandato per preparare entro la fine del mese di maggio un progetto di risposta sulla relazione dell'ACC in merito alla visita di controllo al C.SIS; il Coreper sarà informato dei lavori effettuati dall'ACC e delle raccomandazioni formulate".

II.2. Gruppi tecnici ed esperti

In seguito alla riunione informativa tenutasi il 20 novembre 1998, nella quale esperti dell'ACC hanno ricevuto informazioni sulla futura rete SIS II dai rappresentanti dell'IBM e dagli esperti dei gruppi di lavoro Schengen interessati, l'ACC aveva deplorato che l'IBM non avesse ancora potuto esaminare in modo approfondito, in particolare, gli aspetti legati alla sicurezza. Essa aveva allora ottenuto informazioni tecniche supplementari e l'assicurazione di poter prendere conoscenza del capitolato d'oneri per conoscere i criteri che avevano portato alla scelta delle architetture prese in considerazione e i criteri di sicurezza. Gli Stati membri non hanno ancora stabilito i requisiti funzionali della futura rete.

II.3. Criptazione dei collegamenti SIS

Durante un controllo dell'ufficio nazionale SIRENE, uno dei membri dell'ACC non ha potuto ottenere informazioni relative all'algoritmo di cifratura utilizzato nei collegamenti SIS, in quanto esso era stato messo a punto dall'Ufficio federale tedesco per la sicurezza in materia di tecnologie dell'informazione[1] e dalla società Bosch Telecom. L'ACC ha quindi chiesto al Comitato dell'articolo 36 di fornirle tali informazioni per accertarsi che i collegamenti SIS siano sufficientemente sicuri. Il Comitato dell'articolo 36 ha annunciato, nella riunione del 28/29 febbraio 2000, che la Germania avrebbe comunicato all'ACC tali informazioni entro la fine del mese di maggio del 2000.

II.4. Elenco delle autorità autorizzate a consultare direttamente il SIS

Per verificare se i requisiti ai quali la convenzione subordina l'accesso al SIS siano rispettati da tutti gli Stati membri e applicati in modo uniforme, l'ACC ha chiesto al Comitato dell'articolo 36 di trasmet-

[1] *Il BSI, ossia il "Bundesamt für die Sicherheit in der Informationstechnik".*

terle l'elenco delle autorità autorizzate a consultare direttamente il SIS, di cui all'articolo 101, paragrafo 4, della convenzione. Il Comitato dell'articolo 36 si è dichiarato d'accordo affinché l'ultimo aggiornamento di tale elenco sia trasmesso all'ACC dopo essere stato sottoposto al Consiglio GAI del 27 marzo 2000. Nel frattempo tale elenco è stato esaminato dall'ACC, che ha incaricato il suo Presidente di ricordare ai presidenti delle autorità di controllo nazionali e al Presidente del Comitato dell'articolo 36 il ruolo delle autorità nazionali nell'esame del rispetto delle condizioni di accesso al SIS.

CAPITOLO III: CAMPAGNA D'INFORMAZIONE

III.1. Campagna d'informazione sui diritti dei cittadini nei confronti del SIS

Nel 1997, l'ACC aveva deciso di varare in tutti paesi una campagna d'informazione destinata ai cittadini dal titolo "Il sistema di informazione Schengen vi riguarda". L'ACC aveva infatti constatato un insufficiente esercizio dei diritti del cittadino e soprattutto del diritto di accesso e di verifica dei dati. Uno dei motivi di questo deficit è la mancanza di informazione diretta al pubblico. Essa ha dunque deciso di informare i cittadini dei loro diritti nei confronti del SIS mediante opuscoli.

L'ACC ha ottenuto dagli organi Schengen che sostenessero la campagna di informazione, incaricandosi della stampa degli opuscoli informativi e della loro diffusione alle frontiere esterne di Schengen.

L'ACC ha proceduto a varie riprese alla valutazione di tale campagna. A tre anni dal suo avvio, gli opuscoli dell'ACC sono diffusi nella maggior parte degli Stati membri. Il numero di domande di accesso presentate da cittadini ai quali è stato rifiutato l'ingresso nel territorio Schengen è notevolmente aumentato in seguito a tale campagna, dimostrandone l'efficacia. Gli Stati membri hanno ricevuto numerose domande di accesso relative a segnalazioni di cui i cittadini erano oggetto. (In Francia, la CNIL ha ricevuto 367 domande di accesso fra il 1° marzo 1999 e 29 febbraio 2000). Va rilevato che una ventina di persone si sono inizialmente rivolte al Segretariato dell'ACC per ottenere orientamenti quanto ai passi da compiere. Per migliorare il trattamento delle domande per le quali è necessaria l'applicazione della procedura di cooperazione definita dall'ACC in base all'articolo 114, paragrafo 2, della convenzione, il gruppo di esperti che ha ideato l'opuscolo informativo si è riunito nel dicembre 1999 e ha individuato vari problemi in merito ai quali le autorità di controllo sono state invitate a pronunciarsi attraverso due questionari.

L'ACC deplora tuttavia che finora le autorità competenti francese e olandese non abbiano ancora fornito gli strumenti necessari al lancio di tale campagna di informazione dei cittadini.

III.2. Pagina Internet dell'ACC

Mossa dalla stessa volontà di informare il cittadino sui suoi diritti, nel 1998 l'ACC ha deciso di creare una pagina Internet. Il cittadino ritroverà informazioni sui suoi diritti e sull'attività dell'ACC. Prevista nel corso del 1999, la disponibilità di tale strumento per il pubblico è stata ritardata: l'integrazione di Schengen nell'ambito dell'Unione Europea – sarà il sito del Consiglio ad ospitare la pagina dell'ACC - impone modifiche tecniche al progetto in corso. L'ACC dovrebbe poter aprire il proprio sito nel corso di quest'anno.

III.3. Presentazione della relazione annuale alla sessione annuale e alla conferenza stampa di Firenze

L'ACC ha presentato la relazione sulle sue attività per il 1998/1999 nella conferenza stampa organizzata a margine della sessione annuale svoltasi nel maggio 1999 a Firenze. La stampa internazionale si è mostrata particolarmente interessata al ruolo e alle competenze dell'ACC nel sistema Schengen, al funzionamento del SIS, al tipo di dati in esso contenuti e gli strumenti di accesso di cui dispone il cittadino, così come al futuro dell'ACC.

Le relazioni sono state diffuse dalle autorità di controllo nazionali utilizzando gli stessi canali di cui si avvalgono per le loro relazioni nazionali e, in taluni casi, Internet. Sono state altresì trasmesse al Parlamento europeo dal Presidente dell'ACC. In alcuni paesi si sono tenute conferenza stampa per presentare il documento e per sensibilizzare il pubblico.

CAPITOLO IV: INTEGRAZIONE DELL'UNIONE EUROPEA E ACQUIS DELL'ACC

Ai sensi del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea allegato al trattato di Amsterdam, le decisioni e dichiarazioni del Comitato esecutivo e gli atti adottati ai fini dell'applicazione della convenzione da parte di autorità alle quali il Comitato esecutivo ha conferito potere decisionale costituiscono acquis comunitario. Diverse di queste decisioni riguardano l'ACC, in particolare quelle che riconoscono la sua indipendenza, l'autonomia della sua linea di bilancio, i bilanci annuali e l'accesso alla documentazione e alle informazioni Schengen ecc.

Su richiesta del Gruppo centrale Schengen, l'ACC ha redatto l'elenco del suo acquis, nella prospettiva dell'integrazione dell'acquis di Schengen nell'Unione Europea (allegato 7), nel quale erano enumerati i pareri adottati dall'ACC e le decisioni adottate dagli organi esecutivi di Schengen in merito al funzionamento dell'ACC e alla sua indipendenza.

Tale elenco è stato trasmesso al Consiglio dell'Unione Europea e al Presidente del Gruppo centrale il 18 maggio 1998.

L'11 dicembre 1998, l'ACC ha approvato una nota supplementare relativa al suo acquis istituzionale e funzionale e l'ha trasmessa al Gruppo centrale e al Comitato esecutivo Schengen, oltre che al Consiglio dell'Unione Europea, affinché fosse sottoposta all'esame del Gruppo "Acquis di Schengen" dell'UE all'inizio del 1999. L'ACC ha inoltre conferito al Presidente il mandato di illustrare la portata di tale nota dinanzi il Comitato esecutivo. Il presidente dell'ACC ha presentato il documento al Comitato esecutivo a Berlino, il 16 dicembre 1998, e ha motivato una richiesta di bilancio supplementare per l'ACC, che chiedeva un segretario a tempo pieno per il proprio segretariato. I Ministri hanno respinto tale domanda supplementare e hanno convenuto di affidare l'esame dell'acquis organizzativo dell'ACC al Gruppo centrale.
Tale punto non è stato trattato dal Gruppo centrale né nella riunione del 19 febbraio 1999 né successivamente, nonostante un sollecito rivolto dall'ACC al Presidente di tale gruppo.

Nessuno dei pareri dell'ACC o delle decisioni che la riguardano è stato incorporato nell'acquis di Schengen integrato nell'ambito dell'Unione Europea. Il Consiglio dei Ministri ha adottato, il 20 maggio 1999, una decisione del Consiglio concernente l'Autorità di controllo comune istituita dall'articolo 115 della convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmata il 19 giugno 1990[1]. Con tale decisione il Consiglio si impegna a provvedere al segretariato dell'ACC e a fornirle i mezzi logistici necessari all'organizzazione delle sue riunioni a Bruxelles, oltre che a rimborsare le spese di viaggio dei suoi membri per le riunioni dell'ACC a Bruxelles o dei suoi esperti per i controlli a Strasburgo. Nella decisione si constata inoltre che l'ACC dovrà adattare il suo regolamento interno alla nuova situazione.

L'ACC deplora che, in seguito ad un'interpretazione restrittiva del Protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione Europea allegato al trattato di Amsterdam, l'acquis dell'ACC ottenga come base giuridica unicamente quella dell'ACC stessa.

L'ACC rileva quindi che i suoi pareri e le sue raccomandazioni costituiscono un insieme la cui base giuridica è fondata su quella dell'ACC stessa, che deve essere presa in considerazione dagli Stati che applicano attualmente l'acquis di Schengen e da ogni nuovo Stato che si unirà ad essi.

CAPITOLO V : FUNZIONAMENTO DELL'ACC

V.1. Riunioni

Dal marzo 1999 l'ACC ha tenuto sette riunioni plenarie, alle quali si aggiungono 2 riunioni degli esperti incaricati del controllo del C.SIS, una riunione del gruppo sul diritto di accesso e la sessione annuale svoltasi a Firenze.

[1] *Decisione approvata dal Consiglio il 20.05.1999 e pubblicata nella Gazzetta ufficiale GU L 176 del 10.07.1999, pag. 34.*

V.2. Elezioni del Presidente e del Vicepresidente

Nel dicembre 1999, i Sigg. B. De Schutter (delegazione belga) e G. Buttarelli (delegazione italiana) sono stati eletti rispettivamente Presidente e Vicepresidente.

V.3. Bilancio dell'ACC e sostegno del Segretariato

Non essendo state integrate nell'acquis di Schengen le decisioni degli organi esecutivi di Schengen relative alla linea di bilancio dell'ACC, garanzia della sua indipendenza, l'ACC non dispone più di una propria linea di bilancio né dispone di personale a tempo pieno per provvedere al segretariato.

Il bilancio dell'ACC e il sostegno da parte del Segretariato sono aspetti fondamentali per l'efficacia delle sue attività e per l'esercizio delle sue competenze. Gli organi esecutivi di Schengen hanno per molto tempo rifiutato di dotare l'ACC dei mezzi indispensabili al suo funzionamento indipendente prima di assegnarle un bilancio simbolico che le offra un minimo di garanzie[1].
Nella sua decisione, il Consiglio non ha tenuto conto delle competenze dell'ACC attribuitele dalla Convenzione. Va rilevato che il bilancio di funzionamento di Schengen era, fino al 1° maggio 1999, approvato dal Comitato esecutivo di Schengen. Mentre i bilanci relativi al funzionamento del SIS sono stati ripresi nell'acquis, la linea di bilancio autonoma assegnata all'ACC, che rientra tuttavia nella definizione dell'acquis di Schengen ai sensi del protocollo allegato al Trattato di Amsterdam, è stata esclusa. L'ACC non ha potuto neppure disporre del saldo del suo bilancio.

Si ricorda che questo bilancio comprendeva spese connesse con le competenze dell'ACC attribuitele dalla Convenzione e per le quali le autorità nazionali non dispongono di stanziamenti : spese di viaggio e di soggiorno degli esperti dell'ACC per il controllo del C.SIS, spese per l'elaborazione degli opuscoli per informare i cittadini sui diritti nei confronti del SIS, l'organizzazione della sessione annuale dell'ACC, la presentazione della relazione annuale, la traduzione e la stampa di quest'ultima.

Il Consiglio dell'UE si è impegnato naturalmente a sostenere l'ACC segnatamente per quanto riguarda la traduzione dei documenti o la riproduzione della relazione annuale, ma l'ACC non avrà più un sostegno per quanto riguarda il suo compito d'informare i cittadini mediante conferenze stampa e campagne d'informazione. I bilanci delle autorità nazionali di controllo non sono sempre in grado di coprire spese supplementari.

Preoccupata per tale assenza palese di sostegno degli organi esecutivi dell'Unione europea, l'ACC continua a sostenere di dover disporre delle risorse umane, tecniche e finanziarie necessarie alle sue competenze. Essa si augura che sia istituito tra breve un segretariato comune alle autorità di controllo comuni esistenti nel Terzo Pilastro del TUE, che preceda un ravvicinamento delle autorità di controllo comuni stesse. Questa fase potrà essere superata solo svolgendo una riflessione approfondita sul ruolo delle autorità di controllo istituite a livello europeo e sui mezzi da assegnare loro affinché non costituiscano soltanto un pretesto per autorizzare il funzionamento di strumenti di polizia.

V.4. Regolamento interno

La decisione del Consiglio del 20 maggio 1999 sull'ACC contiene il seguente considerando :

"considerando che il 2 febbraio 1996 l'autorità di controllo comune ha approvato il suo regolamento interno, modificato da ultimo il 27 aprile 1998, al quale occorre che essa apporti gli adattamenti necessari a seguito dell'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea;"

---

[1] *Nel 1997, il bilancio dell'ACC (70.400,52 EURO) corrispondeva allo 0,011% del bilancio globale del Segretariato Schengen (6.258.493,45 EURO).*
Nel 1998, il bilancio del Segretariato ha registrato un aumento (6.753.336,77 EURO) e quello dell'ACC vi contribuiva a concorrenza dello 0,012%. Per i primi 6 mesi il bilancio dell'ACC ammontava a 43.381,37 EURO.
Nel 1999, la proposta dell'ACC (137.580,91 EURO) corrispondeva allo 0,021 del bilancio globale del Segretariato Schengen.
Il bilancio dell'ACC approvato corrisponde al primo semestre 1999 e ammonta a 43.381,37 EURO. La chiave di ripartizione è la seguente: Gruppo 1 (Germania, Grecia, Spagna, Francia, Italia, Austria e Portogallo): 4.333,80 EURO; Gruppo 2 (Belgio e Paesi Bassi): 2.101,84 EURO + Lussemburgo 130,12 EURO; Gruppo 3 (Danimarca, Norvegia, Finlandia e Svezia): 2;166,91 EURO + Islanda 43,38 EURO.

L'ACC non ha adattato il suo regolamento interno. Essa ritiene che le incompatibilità tra il regolamento interno dell'ACC e la decisione del Consiglio riguardino solo aspetti pratici e organizzativi, considerato che l'ACC dipende ora de facto dal Consiglio, che ospita le sue riunioni. Nessuna modifica è apportata alle sue competenze. L'ACC continua inoltre a rivendicare un'indipendenza compatibile con le sue competenze, non consentita dall'attuale situazione. Essa considera pertanto che questa situazione sia provvisoria e che non possa allineare il suo regolamento interno alla medesima.

TERZA PARTE: RELAZIONI DELL'ACC ALL'INTERNO E AL DI FUORI DELLA STRUTTURA SCHENGEN E DEL CONSIGLIO

I.1. Relazioni con la Commissione delle libertà pubbliche del Parlamento europeo

Dal 1997 l'ACC ha proposto alla Presidenza della Commissione delle libertà pubbliche del Parlamento europeo di presentarle la sua relazione annuale. Una serie di esemplari della stessa sono stati inviati ogni anno a questa Commissione del Parlamento europeo. Il Presidente dell'ACC è stato invitato ad un'audizione dedicata all'"Unione europea e alla protezione dei dati" svoltasi il 22 e 23 febbraio 2000. Ha così potuto illustrare il ruolo dell'ACC e i suoi principali risultati. L'ACC si compiace per tale iniziativa del Parlamento europeo che risponde al suo desiderio di trasparenza e d'informazione.

I.2. Relazioni con il Gruppo centrale e il Comitato esecutivo

Prima dell'integrazione di Schengen nell'Unione europea, il Gruppo centrale aveva accettato di associare l'ACC alle attività sullo studio preliminare della rete SIRENE fase II e sul SIS I+. L'ACC doveva in tal modo accertarsi che il sistema futuro comprendesse specifiche tecniche che consentissero di esercitare i controlli previsti dalla Convenzione. Dal marzo 1999, l'ACC non è stata più informata sullo stato dei lavori di integrazione dei cinque paesi nordici nel SIS né sugli sviluppi tecnici in preparazione (SIS 1 + e SIS II).

Dall'integrazione di Schengen nell'ambito dell'Unione europea, ciascuno dei Presidenti successivi dell'ACC ha avuto l'occasione di incontrare in modo informale un rappresentante della Presidenza di turno. Il primo incontro ha avuto luogo sotto Presidenza finlandese e verteva su un progetto di segretariato comune alle autorità di controllo comuni del Terzo Pilastro mentre il secondo si è svolto sotto Presidenza portoghese e riguardava la valutazione del livello di protezione dei dati di carattere personale nei paesi nordici.

I.3. Commissione permanente di applicazione della Convenzione

Il Comitato esecutivo ha istituito nel 1998 una commissione di visita incaricata di verificare la corretta applicazione della Convenzione da parte degli Stati Schengen. La Germania è stata il primo paese a ricevere le visite di detta Commissione. Uno dei gruppi di visita appositamente istituiti ha proceduto ad una serie di verifiche presso il SIRENE Germania e sui terminali SIS. Tali verifiche hanno riguardato aspetti connessi con gli articoli 126 e seguenti della Convenzione di applicazione dell'Accordo di Schengen, materie per le quali è competente l'autorità di controllo nazionale.

Non essendo stati associati a tale visita né l'ACC né i rappresentanti del garante tedesco per la protezione dei dati, l'ACC ha insistito presso la Presidenza del Gruppo centrale affinché rappresentanti dell'autorità di controllo tedesca potessero accompagnare detta commissione di visita durante tutta la sua missione. Il Gruppo centrale ha respinto questa richiesta nella riunione del 19 febbraio 1999. Ha tuttavia rilevato che il Presidente dell'ACC poteva assistere al colloquio previsto tra l'autorità di controllo tedesca e il gruppo di visita.

Si pone attualmente un problema analogo per quanto riguarda la visita dei paesi nordici, destinata a verificare se questi soddisfino le condizioni preliminari stabilite dalla Convenzione per consentirne l'applicazione nel loro territorio. Questa potrebbe infatti aver luogo alla fine del 2000.

Il Presidente dell'ACC ha inviato una lettera il 21 marzo 2000 al Presidente del Comitato dell'articolo 36 nella quale ha constatato che uno dei gruppi di visita ha affrontato aspetti relativi alla protezione dei

dati. Ha rammentato le competenze dell'ACC e ha chiesto, per evitare doppioni, che i risultati dei lavori di questo Gruppo siano trasmessi all'ACC. Questa deve infatti adottare una decisione sul rispetto delle condizioni preliminari in materia di protezione dei dati da parte dei paesi nordici, prima dell'applicazione dell'acquis di Schengen nel loro territorio. Il Presidente del Comitato dell'articolo 36 ha incontrato il 10 aprile il Presidente dell'ACC e ha espresso il suo accordo a che la relazione del gruppo di visita sulla sicurezza dei dati e il SIS nei paesi nordici sia trasmessa all'ACC non appena approvata dal gruppo di lavoro del Consiglio da cui il gruppo di visita dipende.

I.4. Posizione del Regno Unito e dell'Irlanda

Questi due paesi sono gli unici due dell'Unione europea che non applicano a tutt'oggi l'acquis di Schengen.

L'articolo 4 del protocollo Schengen offre la possibilità al Regno Unito e all'Irlanda, i quali non sono vincolati dall'acquis di Schengen, di chiedere di partecipare, in tutto o in parte, alle disposizioni di detto acquis.

Benché l'ACC non sia stata associata ai lavori in corso sulla partecipazione di questi paesi all'acquis di Schengen, essa rileva che il Regno Unito si è avvalso di tale disposizione nel 1999 e, su tale base, applicherà in parte l'acquis di Schengen, in particolare il SIS. Il progetto di decisione prevede che il regime in materia di protezione dei dati della Convenzione Schengen sarà applicabile al Regno Unito nella misura in cui questo paese applicherà l'acquis di Schengen. Allo stato attuale del fascicolo, solo l'articolo 96 della Convenzione dovrebbe essere escluso dal campo di applicazione.

QUARTA PARTE : REAZIONI DELLE AUTORITÁ SCHENGEN ALLA RELAZIONE ANNUALE DELL'ACC

A parte le risposte del Gruppo centrale sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione e del Comitato dell'articolo 36 sul parere relativo all'usurpazione di identità e sulla sicurezza degli uffici SIRENE, l'ACC non ha più ricevuto risposte complementari a quella contenuta nella relazione del Gruppo centrale del 1998. Questa relazione indica lo stato delle riflessioni dei gruppi di lavoro sui pareri dell'ACC o, per alcuni di essi, il seguito riservato.
Nella relazione si nega che l'ACC abbia una competenza in materia di armonizzazione delle prassi nazionali, quando una tale competenza è riconosciuta dall'articolo 115, paragrafo 3 della Convenzione e si indica che non esiste l'obbligo di dare esecuzione alle raccomandazioni dell'ACC.
Dallo stato dei lavori riportato in allegato emerge che numerosi pareri dell'ACC sollevano problemi tecnici che non possono essere risolti o potranno essere risolti solo mediante un rinnovo del SIS.

QUINTA PARTE: IL FUTURO DELL'ACC NEL NUOVO QUADRO ISTITUZIONALE

I sistemi d'informazione in Europa sono in continua evoluzione. Il sistema d'informazione Schengen sarà tra breve applicato nei 15 paesi, la Convenzione Europol è entrata in vigore e la sua autorità di controllo funziona, anche il Sistema d'informazione doganale e il sistema Eurodac saranno tra breve operativi. Il nuovo interesse del Parlamento europeo e la consapevolezza da parte dei cittadini dell'importanza dei garanti del corretto funzionamento di tali organi dovrebbero consentire di raggiungere rapidamente una soluzione globale, che permetta loro di funzionare armoniosamente.

SESTA PARTE: ALLEGATI

1. I COMPITI DELL'ACC PREVISTI DALLA CONVENZIONE

Gli Stati che hanno ratificato la Convenzione hanno attribuito all'ACC il compito principale di controllare l'unità di supporto tecnico del SIS, compito che solo questa può realizzare (articolo 115, comma 2). Spetta inoltre all'ACC formulare pareri e vigilare sull'armonizzazione delle prassi o delle dottrine nazionali.

Alla luce della sua composizione e delle sue attribuzioni, l'ACC è un'entità indipendente dalla struttura Schengen che gode di veri poteri di autorità come quelli risultanti dal controllo del C.SIS (accesso, verifica di legalità, elaborazione di relazioni).

La Convenzione di applicazione dell'Accordo di Schengen precisa i compiti dell'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 106, comma 3);

analizza le difficoltà di applicazione o di interpretazione che possono sorgere nell'utilizzo del SIS;
esamina i problemi che possono sorgere durante il controllo indipendente effettuato dalle autorità di controllo nazionali delle Parti contraenti;
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, comma 3);
elabora relazioni che vengono trasmesse alle autorità alle quali pervengono le relazioni delle autorità di controllo nazionali (articolo 115, comma 4);.
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 (articolo 118, comma 2).
Per quanto riguarda gli scambi di informazioni non riguardanti il SIS:
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 (articolo 126, comma 3, lettera f);
può, alle condizioni e secondo le modalità previste all'articolo 126, formulare un parere in caso di trasmissione di dati provenienti da un archivio non automatizzato e di inserimento di dati in un tale archivio (articolo 127, comma 1).

2. PARERI E RACCOMANDAZIONI DELL'ACC NEL PERIODO 1999-2000

Parere supplementare sull'usurpazione di identità

UNIONE EUROPEA
AUTORITÀ DI CONTROLLO COMUNE SCHENGEN

Bruxelles, 15 febbraio 2000 (24.02)
(OR. en)

SCHAC 2505/1/00
REV 1

LIMITE

PARERE dell':Autorità di controllo comune
al: Comitato dell'articolo 36
n. doc. prec.: SCHAC 2513/99

Oggetto: Proposta del Comitato dell'articolo 36 per una soluzione del problema dell'usurpazione di identità nel Sistema d'informazione Schengen

ANTEFATTI

Nei casi di sostituzione di persone, in alcuni paesi le segnalazioni relative alle persone che hanno usurpato l'identità altrui vengono inserite nel SIS sotto il nome della persona la cui identità é stata sostituita.

In altre parole, il sistema contiene segnalazioni in cui l'identità non corrisponde, né de facto né de jure, alla vera identità della persona ricercata e l'identità della persona che è stata sostituita è inserita nel SIS senza che ciò le sia stato preventivamente notificato.

Alcuni Stati sono favorevoli ad una procedura secondo la quale i dati di carattere personale relativi alle persone la cui identità é stata sostituita dovrebbero essere immediatamente cancellati, mentre altri sostengono che la segnalazione contenente l'identità usurpata dovrebbe essere mantenuta anche se la persona la cui identità è stata erroneamente inserita nel SIS ne richiedesse la cancellazione: l'argomento da essi addotto a sostegno della loro tesi è la necessità di trovare il responsabile.

L'ACC ha esaminato i problemi derivanti dall'usurpazione di alias da parte di persone oggetto di una segnalazione nel SIS, tenendo conto dei principi che regolano la protezione dei dati di cui alla convenzione di applicazione dell'accordo di Schengen. Nel parere n. 98/2 sull'introduzione nel Sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata (SCH/Aut-cont(97) 42 REV 2), l'ACC ha ribadito i diritti e i principi fondamentali in materia di protezione dei dati. Il parere, trasmesso all'ex "Gruppo centrale" e al Comitato esecutivo Schengen nel febbraio 1998, è stato inoltre integrato nella relazione annuale dell'ACC per il 1997-1998.

L'ex "Gruppo centrale" Schengen ha inviato una risposta provvisoria all'ACC nel marzo 1999 (SCH/C(99) 21), mentre il Comitato dell'articolo 36 ha risposto, formulando proposte, nel novembre 1999 (SCHAC 2513/99).

PROPOSTA DEL COMITATO DELL'ARTICOLO 36

La proposta del Comitato dell'articolo 36 prevede una soluzione provvisoria per il SIS I + e una soluzione definitiva per il SIS II.
Entrambe le soluzioni prevedono l'inserimento nel SIS di dati supplementari.
Nella soluzione SIS I + viene introdotto un nuovo codice "3" nei record dei ricercati ("Wanted Persons Records"). Oltre alle soluzioni tecniche, vengono proposte misure supplementari. I SIRENE nazionali elaboreranno i dati relativi alle persone la cui identità è usurpata. Se una persona viene controllata tramite il SIS e si verifica un "hit", questo dato consentirà all'autorità di controllo della polizia e alla persona controllata di chiarire che non si tratta della persona ricercata. Secondo questa proposta i dati di una persona la cui identità è usurpata possono essere elaborati dai SIRENE solo previo accordo esplicito della persona in questione.

Nella soluzione SIS II i dati della persona la cui identità è usurpata sono inseriti nel SIS.

OSSERVAZIONI DELL'ACC

In linea generale, l'ACC desidera esprimere il proprio convincimento che una soluzione favorevole alle persone interessate sarà infine raggiunta.
Quanto all'applicazione delle soluzioni, essa pone l'accento sul principio della proporzionalità applicato al problema dell'usurpazione di identità: non tutte le segnalazioni giustificano l'inserimento di alias di terze persone la cui identità è stata usurpata.

Soluzione SIS I +

Le proposte misure supplementari a livello di SIRENE sono possibili solo se il diritto nazionale consente ad un ufficio SIRENE di elaborare i dati. Inoltre, tale elaborazione da parte degli uffici SIRENE dovrebbe essere consentita soltanto con l'accordo libero ed esplicito della persona la cui identità è usurpata o su specifica richiesta della persona coinvolta.

Soluzione SIS II

È stato chiesto un parere all'ACC sulla legittimità dell'inserimento nel SIS dei dati di una persona la cui identità è usurpata. A questo proposito l'ACC ha dichiarato quanto segue: l'articolo 94 contiene un elenco dei dati che possono essere elaborati nel SIS. L'articolo 94, paragrafo 3, lettera a) elenca dati quali cognome, nome e alias eventualmente registrati separatamente. I dati relativi ad un alias possono includere anche le informazioni necessarie per stabilire chi sia il legittimo titolare dell'identità (ad esempio il nuovo numero di passaporto di tale persona).
Tenuto conto del fatto che i dati possono essere registrati solo se sono necessari ai fini previsti negli articoli da 95 a 100, l'elaborazione dei dati relativi al legittimo titolare di un'identità che sia stata usurpata è consentita solo nella misura in cui ciò sia necessario per determinare se la persona sottoposta al controllo è la persona segnalata.

PARERE DELL'ACC SULLE SOLUZIONI SIS I + E SIS II

A complemento del suo precedente parere (Parere 98/2, SCH/Aut-cont(97) 42 REV 2), sottolinea quanto segue:

Entrambe le soluzioni dovrebbero consentire l'elaborazione dei dati relativi alle persone la cui identità é stata usurpata solo previo libero ed esplicito accordo delle stesse o dietro specifica richiesta della persona coinvolta.
Devono inoltre essere previste altre misure, quali ad esempio la possibilità di integrare il passaporto con un ulteriore documento che attesti che il titolare non è la persona che usurpa l'identità. Solo in questo modo le persone coinvolte e il paese responsabile avranno la possibilità di scegliere liberamente le soluzioni a loro più adatte.
La scelta delle misure supplementari sarà necessaria anche quando il diritto nazionale non consente di applicare la soluzione proposta per il SIS I+.

Parere supplementare sull'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

UNIONE EUROPEA
Autorità di controllo comune
SCHENGEN

Bruxelles, 11 ottobre 1999
(OR. F) SCHAC 2505/99

LIMITE

RACCOMANDAZIONE

dell'Autorità di controllo comune Schengen
n. doc. prec.: SCH/Aut-cont (99) 17 (SN 3243/99)
Oggetto: Conservazione dei dossier ad avvenuta cancellazione di una segnalazione

L'Autorità di controllo comune ha approvato e trasmesso agli organi esecutivi di Schengen il parere relativo alla conservazione dei dossier ad avvenuta cancellazione di una segnalazione (parere n. 98/1 del 3 febbraio 1998, SCH/Aut-cont (97) 55, 2a rev.).

Il parere, approvato in dicembre sulla base della nota del Comitato di orientamento (SCH/OR.SIS (98) 130) previo esame del Gruppo di lavoro Sirene, è stato comunicato all'ACC il 13 gennaio 1999.

Nel parere n. 98/1 del 3 febbraio 1998 l'ACC ha sottolineato quanto segue:
"...
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. 102, 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 principi 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 ha ritenuto pertanto che si dovessero 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)."

Nel parere del Comitato di orientamento "SIS" si afferma, in sintesi, che non è possobile accettare la posizione dell'ACC per le seguenti ragioni:

– la rapida distruzione di tutta la documentazione relativa ad una segnalazione è incompatibile con il corretto sviluppo e follow-up del dossier;

– la distruzione di tutte le informazioni relative ad un hit renderebbe praticamente impossibile proseguire il follow-up dell'hit e stabilire nessi con il dossier. Ciò si verificherebbe, in particolare, in caso di estradizione in quanto il trasferimento della persona interessata può richiedere settimane, o addirittura mesi;

– i dossier devono essere conservati al fine di regolare eventuali successivi contenziosi;

– i dossier conservati dai SIRENE non devono sottostare alla stessa procedura di quella prevista dall'articolo 112 CSCH;

– le segnalazioni cancellate devono essere conservate per un anno ai fini della protezione dei dati personali (articolo 113 CSCH). Senza documentazione relativa a tali segnalazioni non è possibile verificare i dati cancellati.

Non essendo prevista alcuna disposizione legale espressa per la conservazione della documentazione stessa, in materia si applica il diritto nazionale che varia da Stato a Stato.

L'ACC mantiene la posizione adottata nel parere n. 98/1 e rileva quanto segue:

1. l'eventuale utilizzazione di dati contenuti nei dossier conservati presso gli uffici SIRENE ai fini di controllo o di supporto tecnico o ai fini della costituzione di nuovi dossier di natura penale o di altra natura potrebbe costituire uno sviamento di finalità. Ciò appare possibile alla luce della nota del Comitato di orientamento che ammette l'utilizzazione dei dossier per altri fini, violando il principio di finalità.

2. I principi di trattamento dell'informazione da parte degli uffici SIRENE - compreso il periodo di conservazione dei dati personali - devono rispettare il disposto dell'art. 112 della Convenzione di Schengen ed applicarsi in conformità dei principi sanciti dalla Convenzione n. 108 del Consiglio d'Europa del 28 gennaio 1981, che tutti gli Stati sono tenuti ad osservare (art. 126, 1° comma della Convenzione di Schengen). Non solo l'art. 112 CSCH si applica agli uffici Sirene, ma anche la Convenzione obbliga tutti gli Stati partner a soddisfare i requisiti di finalità e di conservazione limitata alla finalità per la quale la segnalazione è stata effettuata (art. 5 della Convenzione del Consiglio d'Europa).

3. L'esistenza di un sistema di controllo ad avvenuta cancellazione di una segnalazione (i cui tempi sono definiti dalla CSCH) non giustifica la conservazione del corrispondente dossier senza un limite temporale.

4. Parimenti, non devono essere conservati dossier relativi a segnalazioni cancellate per assicurare un ipotetico procedimento amministrativo o giudiziario. Tale criterio renderebbe possibile la conservazione pressoché illimitata dei dossier.

Il parere dell'ACC mirava essenzialmente ad armonizzare le diverse situazioni esistenti in ciascuno Stato.

L'ACC riafferma la necessità che gli uffici Sirene applichino il principio di finalità nel quadro del trattamento delle informazioni complementari. Tali informazioni complementari confluiscono nel sistema comune e sono soggette alle regole e ai principi della Convenzione (p.es. sicurezza, finalità, conservazione).

L'ACC è del parere che sia necessario ricercare una soluzione armonizzata.

L'ACC insisterà presso le autorità di controllo nazionali affinché tali regole siano applicate in base a criteri comuni ed uniformi.

3. QUADRO DEI PARERI DELL'ACC E REAZIONI DEGLI ORGANI ESECUTIVI E TECNICI

	Contenuto	Attività	Osservazioni
Controllo del C.SIS (marzo 1994) e parere del 18 maggio 1994	- Vigilare sul trasporto e sulla conservazione del back-up dei dati. - Migliorare l'affidabilità dei collegamenti tra il C.SIS e gli N.SIS. - Garantire una separazione fisica tra le apparecchiature del C.SIS e quelle del Ministero dell'Interno francese situate nello stesso edificio.	- La Francia ha adottato le misure ritenute più adeguate. - Il 4 marzo 1998, in occasione di una visita al C.SIS da parte del Gruppo centrale e del presidente dell'ACC, sono stati presentati alcuni lavori di adattamento del sito.	Stando alle informazioni in possesso dell'ACC questi lavori non sono stati realizzati.
Parere del 22 febbraio 1995 sul fondamento giuridico degli uffici SIRENE	Poiché la Convenzione non prevede una base giuridica per l'esistenza degli uffici SIRENE, tale base va creata modificando la Convenzione o modificando in modo armonizzato le legislazioni nazionali.	Il 27 giugno 1996, il Gruppo centrale ha ritenuto che la base giuridica esiste, che i metodi di lavoro, la struttura e lo statuto formale degli uffici SIRENE sono disciplinati dal diritto interno degli Stati Schengen e che le autorità di controllo nazionali garantiscono il controllo del funzionamento del SIS e degli uffici SIRENE e provvedono all'informazione dell'ACC.	Quindici mesi dopo essere stato adito, il Gruppo centrale respinge l'argomentazione dell'ACC.
Visita di controllo al C.SIS del mese di ottobre 1996: Raccomandazione n. 1	Vigilare sull'identità degli archivi delle Parti contraenti.	Definizione di una nuova procedura di raffronto dei dati che non evidenzia più le differenze riscontrate dall'ACC	**Le differenze continuano ad esistere, ma non sono più evidenziate**
Raccomandazione n. 2	Procedere ad una certificazione ITSEM/ITSEC del sistema informatico ed applicare le misure di sicurezza raccomandate o garantire almeno il livello di sicurezza previsto.	- Impossibilità di realizzare a posteriori la certificazione del sistema attuale. Impossibilità di attivare le funzioni di tracciatura.	Il Gruppo centrale dichiara che non è possibile procedere alla certificazione del sistema attuale.

	Contenuto	Attività	Osservazioni
segue: Raccomandazione n. 2		- Le specifiche tecniche definite nell'ambito della procedura di appalto per il rinnovo del C.SIS prevederanno che ogni componente del nuovo sistema debba obbligatoriamente essere conforme ai criteri ITSEC e alla norma 4-C2/E2. I sistemi saranno certificati o potranno esserlo su richiesta degli Stati Schengen.	Il futuro sistema potrà essere certificato.
Raccomandazione n. 3	Ridurre il numero di "super utenti" del C.SIS che usufruiscono di un accesso privilegiato al sistema che consente loro di accedere a qualsiasi archivio registrato nel sistema informatico, di modificarne il contenuto e di cancellare qualsiasi traccia del loro intervento.	- Il personale del C.SIS è oggetto di severissime procedure di assunzione e di controllo di sicurezza. - Nelle specifiche dei nuovi sistemi sarà prevista una ripartizione precisa dei compiti di gestione affinché le funzioni possano essere attribuite sulla base di tali compiti. - Questa misura dovrebbe permettere di ridurre il numero di "super utenti" necessari.	**L'ACC ha constatato, nel 1999, che il numero di "super utenti" è stato ridotto.**
Raccomandazione n. 4	Attivare le funzioni di tracciatura che consentono di verificare a posteriori le azioni effettuate dai vari utenti, a prescindere dal loro profilo. Gestione e trasporto dei supporti magnetici Ricorrere sistematicamente alla cifratura in caso di registrazione dei dati su supporto magnetico per fini di trasporto o stoccaggio. L'ACC ha in effetti constatato che le misure di sicurezza adottate dagli Stati Schengen nella gestione e nel trasporto dei supporti magnetici sui quali sono registrati i dati SIS sono insufficienti. Rifiutare l'accesso al SIS da parte degli Stati Schengen che non applicano ancora la Convenzione.	Le specifiche tecniche definite nell'ambito della procedura di appalto per il rinnovo del C.SIS prevederanno che le ditte offerenti dovranno indicare le risorse supplementari necessarie perché i criteri di prestazione del sistema siano rispettati in caso di attivazione delle funzioni di tracciatura. Le specifiche prevedono inoltre che siano realizzati test con le funzioni di tracciatura attivate, allo scopo di verificare che il sistema operativo sia in grado di funzionare anche con le funzioni di tracciatura attivate. Le specifiche tecniche e l'offerta selezionata saranno trasmesse all'ACC perché questa possa prendere posizione.	

	Contenuto	Attività	Osservazioni
Raccomandazione n. 5	Gestione e trasporto dei supporti magnetici Ricorrere sistematicamente alla cifratura in caso di registrazione dei dati su supporto magnetico per fini di trasporto o stoccaggio. L'ACC ha in effetti constatato che le misure di sicurezza adottate dagli Stati Schengen nella gestione e nel trasporto dei supporti magnetici sui quali sono registrati i dati SIS sono insufficienti.	Gli esperti del PWP hanno esaminato nel 1998 una soluzione che consiste nel trasmettere dati cifrati on-line. Questa soluzione consentirebbe una protezione equivalente a quella delle trasmissioni tra C.SIS e N.SIS ed eviterebbe i rischi di smarrimento, furto o sostituzione.	
Parere del 7 marzo 1997 sul progetto pilota relativo ai veicoli rubati, formulato su invito del Gruppo centrale del 10 febbraio 1997	Rifiutare l'accesso al SIS da parte degli Stati Schengen che non applicano ancora la Convenzione. L'ACC ha ricordato che le disposizioni della Convenzione autorizzano l'accesso al SIS dei soli Stati che applicano la Convenzione stessa. Ha tuttavia indicato che tali paesi potevano essere associati al progetto mediante meccanismi di cooperazione bilaterale o multilaterale disciplinati dalle legislazioni nazionali in materia di protezione dei dati e assoggettati al controllo delle autorità di controllo nazionali. Alla data di realizzazione del progetto, l'Austria, l'Italia e la Grecia non applicavano ancora la Convenzione.	Il progetto pilota è stato portato avanti evitando che gli Stati che non applicavano la Convenzione avessero accesso ai dati. I meccanismi di cooperazione bilaterale o multilaterale proposti dall'ACC hanno consentito di associare questi paesi al progetto pilota.	
Parere del 7 marzo 1997 sul progetto di accordo sulle infrazioni stradali	Richiamare nel testo dell'accordo le disposizioni relative alla protezione dei dati personali.	Il gruppo di lavoro competente ha adattato il progetto come richiesto dall'ACC.	

	Contenuto	Attività	Osservazioni
Parere 97/1 del 22 maggio 1997 sulla duplicazione di una parte delle segnalazioni SIS (per consentire il trasporto delle copie verso le rappresentanze diplomatiche e consolari, articolo 118, 2° comma della Convenzione)	Vigilare sulla sicurezza durante il trasporto delle copie. Provvedere alla registrazione di almeno il 10% delle consultazioni di questi supporti per consentire alle autorità di controllo di verificare se tali consultazioni erano autorizzate. Poiché l'uso di copie non aggiornate può recare pregiudizio ai diritti del cittadino, in attesa della creazione di un sistema di consultazione diretta, gli Stati membri debbono procedere a verifiche supplementari in tempo reale per garantire l'attualità di una segnalazione che figura su una copia ed accettare la propria responsabilità in caso di rilascio di un visto ad una persona segnalata nel SIS dopo duplicazione dei dati.	Nel 1998 la questione era ancora allo studio del Comitato di orientamento SIS.	
Parere 98/1 sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione **Parere supplementare dell'11 ottobre 1999**	Procedere alla distruzione fisica dei dossier relativi ad una segnalazione dopo cancellazione della stessa. Modificare in questo senso il Manuale SIRENE.	Il 13 gennaio 1999, il Gruppo centrale ha trasmesso all'ACC la risposta del gruppo di lavoro competente, stando al quale la conservazione dei dossier è disciplinata dal diritto nazionale. **Il Comitato dell'articolo 36 ha confermato l'analisi del Gruppo centrale e invita il Gruppo "SIRENE" ad adeguare, se necessario, il manuale SIRENE.**	

	Contenuto	Attività	Osservazioni
Parere 98/2 sulla segnalazione nel SIS di persone vittime di un'usurpazione di identità **Parere supplementare del 15 febbraio 2000**	Adottare una soluzione che consenta di indicare che si tratta di un'identità usurpata al fine di tutelare i diritti della vittima di tale usurpazione di identità.	Al momento non è ancora stata trovata una soluzione al problema. Il SIS II dovrebbe consentire di risolvere il problema. Nel mese di marzo 1998, il Gruppo centrale ha annunciato che esisteva una decisione in materia.	Il problema dovrebbe essere risolto entro il 2000.
Parere 98/3 sulle eventuali relazioni tra il SIS e il progetto di sistema "ASF – veicoli rubati" (Automated Search Facility) di Interpol Parere 98/4 sulla registrazione delle consultazioni ai sensi dell'articolo 103 della Convenzione Parere 98/5 sull'accesso al SIS da parte degli uffici della motorizzazione	Non autorizzare la trasmissione di dati personali dal SIS verso Stati non Schengen Rispettare le regole comuni per garantire che sia registrato il 10% delle consultazioni del SIS.	Il Gruppo centrale ha seguito il parere dell'ACC. Il Gruppo centrale non ha seguito il parere dell'ACC ritenendo che la questione è di competenza degli Stati membri.	
	Rifiutare l'accesso al Sistema d'informazione Schengen da parte degli uffici della motorizzazione. L'ACC considera tuttavia che l'accesso è ammissibile nei casi in cui l'ufficio della motorizzazione soddisfa le condizioni di competenza e di finalità previste dalla Convenzione ed è in grado di applicare le misure di sicurezza di cui all'articolo 118 della Convenzione stessa.		

4. PER MEMORIA

ORGANI COMPETENTI PER L'APPLICAZIONE DELLA CONVENZIONE

Oltre all'ACC, mantenuta dopo l'integrazione di Schengen nell'ambito dell'Unione europea, gli organi e gruppi di Schengen sono stati sciolti e le loro competenze ripartite fra i gruppi del Consiglio. L'acquis di Schengen è ora trattato e sviluppato nell'ambito della Direzione generale H del Consiglio, responsabile per il settore della giustizia e degli affari interni.

Il Comitato esecutivo era, con l'ACC, l'unico organo istituito dalla convenzione. Aveva il compito generale di vigilare alla corretta applicazione della Convenzione e disponeva di una serie di competenze specifiche (articolo 131), esercitate ora dal Consiglio dei Ministri.

Il Gruppo centrale Schengen non aveva esistenza legale, ma aveva assunto una grande importanza sul piano pratico quale interlocutore dei gruppi e effettuava la preparazione dei fascicoli prima che fossero sottoposti al Comitato esecutivo. Tale ruolo è ora esercitato dal Comitato dell'articolo 36 e dal Comitato dei Rappresentanti Permanenti.

Il SIS costituisce uno strumento totalmente nuovo nell'Unione europea, in quanto il Consiglio non disponeva di alcun gruppo di lavoro in tale settore. È stato quindi creato nell'ambito della Direzione generale H un nuovo settore "SIS" per accogliere i gruppi Schengen competenti in materia.

L'organigramma figura in allegato.

Obiettivi 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.

È 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 (articolo 95);
- ricerca in caso di scomparsa, ricerca di minori o di persone che devono essere internate per decisone 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° comma):

- 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 sicu-

rezza 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 identico il contenuto di 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).

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, l'ufficio SIRENE è stato incaricato di procedere, sulla base del SIS, allo scambio di informazioni supplementari e funge da intermediario 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.

Le autorità di controllo nazionali sono competenti a verificare il livello di sicurezza dei rispettivi uffici

SIRENE nazionali, che non deve essere inferiore a quello del SIS. Nel quadro delle sue competenze in materia di armonizzazione delle prassi, l'ACC ha peraltro ritenuto necessario coordinare le attività di verifica svolte dai suoi membri e formulare proposte per migliorare il livello di sicurezza degli uffici SIRENE. In tale ambito ha elaborato una relazione corredata di raccomandazioni, e provvede ora ad armonizzare i controlli stessi mediante un questionario uniforme.

PROTEZIONE DEI DATI PERSONALI

1. UNA LEGGE ED UN'AUTORITÀ DI CONTROLLO NAZIONALE: CONDIZIONI PRELIMINARI PER L'APPLICAZIONE DELLA CONVENZIONE

Gli Stati parte 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 principi 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 principi 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 principi 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 principi 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. 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 membri.

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 membro.

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.

b. Diritto di rettifica (articolo 110)

Chiunque può far rettificare dati contenenti errori di fatto o far cancellare dati contenenti errori di diritto che lo 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)

Chiunque deve poter adire, nel territorio di ciascuna Parte contraente, la giurisdizione o l'autorità competente relativamente ad una segnalazione che lo 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)

Chiunque ha il diritto di chiedere alle autorità di controllo nazionali di verificare i dati inseriti nel Sistema d'Informazione Schengen che lo 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.

Nonostante non sia ancora stato elaborato l'elenco delle domande presentate negli Stati Schengen relative all'esercizio dei diritti summenzionati, 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 principi 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

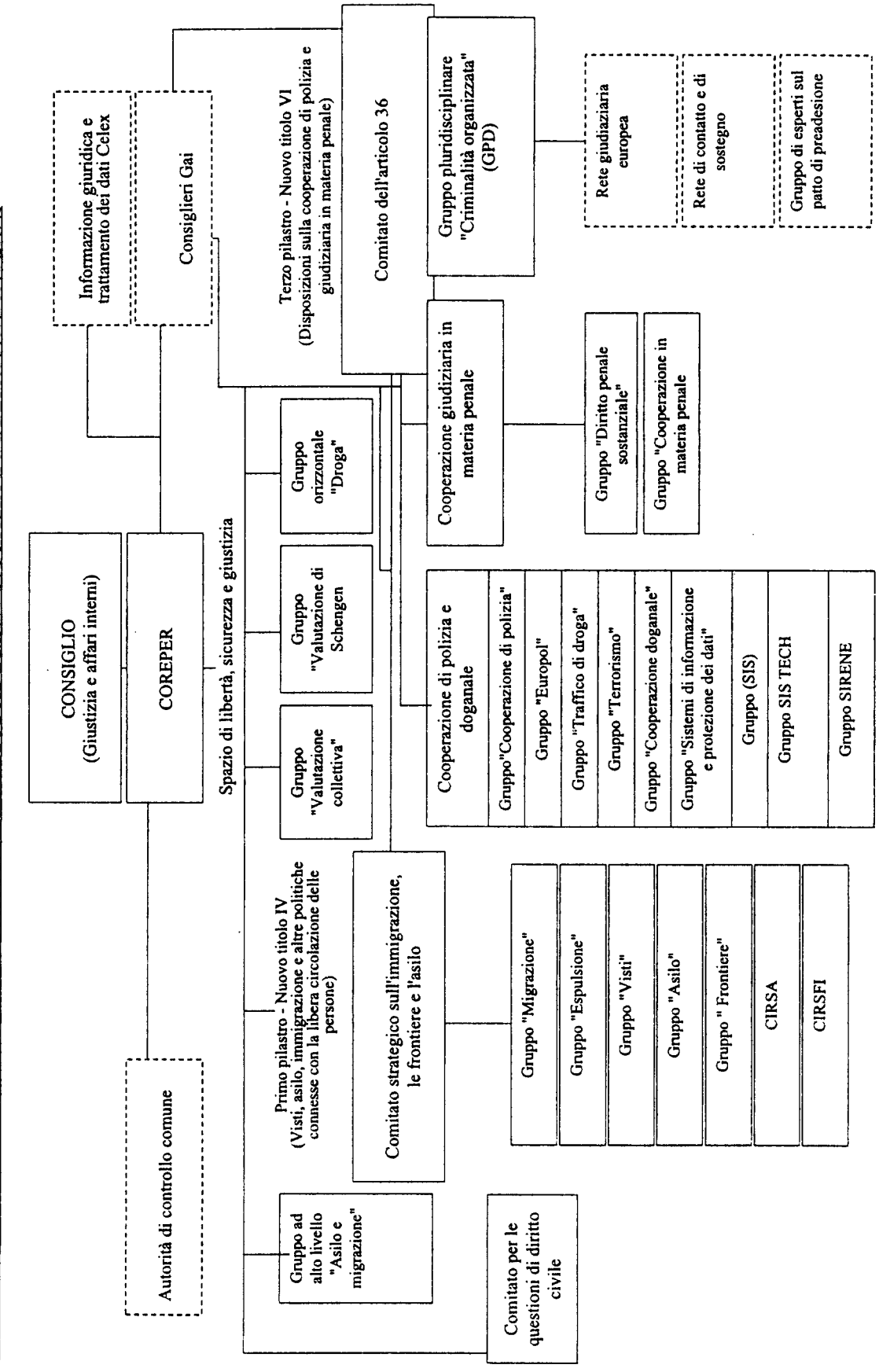
Il Titolo VI della Convenzione (articolo 126 e successivi), intitolato "Protezione dei dati di natura personale" è dedicato alle regole applicabili agli scambi di informazioni che non danno luogo ad una segnalazione nel SIS ma avvengono nel quadro dell'applicazione della Convenzione (v. punti 2.1.b e 2.1.c).

I principi 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.

5. ORGANIGRAMMA DEI GRUPPI DEL CONSIGLIO NEL SETTORE DELLA GIUSTIZIA E DEGLI AFFARI INTERNI



6. DECISIONE DEL CONSIGLIO CONCERNENTE L'AUTORITÁ DI CONTROLLO COMUNE ISTITUITA DALL'ARTICOLO 115 DELLA CONVENZIONE DI APPLICAZIONE DELL'ACCORDO DI SCHENGEN DEL 14 GIUGNO 1985 RELATIVO ALL'ELIMINAZIONE GRADUALE DEI CONTROLLI ALLE FRONTIERE COMUNI, FIRMATA IL 19 GIUGNO 1990

CONSIGLIO
DELL'UNIONE EUROPEA

Bruxelles, 12 maggio 1999
(OR. en)
8060/99

LIMITE

SCHENGEN 45

DECISIONE DEL CONSIGLIO
del
concernente l'Autorità di controllo comune
istituita dall'articolo 115 della convenzione di applicazione
dell'accordo di Schengen del 14 giugno 1985
relativo all'eliminazione graduale dei controlli alle
frontiere comuni, firmata il 19 giugno 1990

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea, e in particolare l'articolo 2,

(1) considerando che l'articolo 115 della convenzione di applicazione dell'accordo di Schengen del 14 giugno 1985 relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmata il 19 giugno 1990, ha istituito un'Autorità di controllo comune incaricata di controllare l'unità di supporto tecnico del Sistema di Informazione Schengen (SIS) e di esaminare altre questioni concernenti l'applicazione delle disposizioni relative al SIS e la protezione dei dati di natura personale;

(2) considerando che si tratta di un'Autorità indipendente che non può essere assimilata a un comitato o a un gruppo di lavoro del Consiglio ai sensi dell'articolo 19 del regolamento interno del Consiglio;

(3) considerando che il 2 febbraio 1996 l'Autorità di controllo comune ha approvato il suo regolamento interno, modificato da ultimo il 27 aprile 1998, al quale occorre che essa apporti gli adattamenti necessari a seguito dell'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea;

(4) considerando che occorre inoltre riconoscere che il regolamento interno dell'Autorità di controllo comune costituisce un elemento dell'acquis di Schengen in senso ampio, il cui funzionamento nell'ambito dell'Unione europea deve continuare ad essere garantito sul piano logistico e finanziario;

(5)considerando che la presente decisione è destinata a garantire il corretto funzionamento dell'Autorità di controllo comune nell'ambito dell'entrata in vigore del Trattato di Amsterdam;

(6) tenendo conto dello statuto del tutto specifico dell'Autorità di controllo comune;

(7) avendo dato la possibilità all'Autorità di controllo comune di esprimere la sua posizione,

DECIDE :

1. Il Segretariato generale del Consiglio dell'Unione europea ospiterà riunioni dell'Autorità di controllo comune e le agevolerà come lo fa per i gruppi di lavoro del Consiglio.

2. Il Segretariato generale del Consiglio provvederà al Segretariato dell'Autorità di controllo comune e si tiene a disposizione del Presidente dell'Autorità di controllo comune.

3. La Presidenza dell'Autorità di controllo comune fisserà, previo accordo della Presidenza del Consiglio, il calendario per le riunioni dell'Autorità di controllo nella sede del Consiglio a Bruxelles.

4. Le spese di viaggio per le riunioni a Bruxelles e per realizzare i controlli presso il C.SIS sono imputate al bilancio del Consiglio e sono eseguite secondo la decisione del Segretario Generale del 21 maggio 1997.

5. I beneficiari del rimborso delle spese di viaggio sono :

• per ciascuno degli Stati membri di cui all'articolo 1 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea e per ciascuno degli altri Stati membri che partecipano alle disposizioni di tale acquis relative al SIS, per le riunioni dell'ACC: due rappresentanti dell'autorità nazionale, di cui all'articolo 2, paragrafo 1 del regolamento interno dell'autorità di controllo comune;
• gli esperti di cui all'articolo 2, paragrafo 5 del regolamento interno dell'Autorità di controllo comune.

6. Le spese contemplate dalla presente decisione sono imputate alla voce 2501 della sezione II (Consiglio) del bilancio generale.

Fatto a Bruxelles, addì

Consiglio
Il Presidente

7. ELENCO DELLE DECISIONI, DELLE RACCOMANDAZIONI, DEI PARERI E DELLE RELAZIONI DELL'AUTORITÀ DI CONTROLLO COMUNE SCHENGEN CHE COSTITUIRANNO L'ACQUIS SCHENGEN IN CONFORMITÀ DEL PROTOCOLLO RELATIVO ALL'INCORPORAZIONE DELL'ACQUIS SCHENGEN NELL'AMBITO DELL'UNIONE EUROPEA PREVISTO NEL TRATTATO DI AMSTERDAM

Documento	Argomento	Rif. documento Schengen
Regolamento interno	Il Regolamento garantisce l'indipendenza dell'ACC e ne definisce la composizione, le modalità di elezione della presidenza, le regole di funzionamento e i compiti da assolvere.	SCH/Aut-cont (95) 25, 6a rev.
Linea di bilancio autonoma	Garantisce nel quadro del bilancio generale di Schengen una linea autonoma dell'ACC, come proposto da quest'ultima.	SCH/Com-ex (97) PV 1 riv. (riunione del Comitato esecutivo del 25 aprile 1997); SCH/Com-ex (97) 1 (decisione del Comitato esecutivo del 25 aprile 1997); SCH/Com-ex (98) 9 (progetto di decisione del Comitato esecutivo del 21 aprile 1998)
Bilancio dell'ACC 1997 e 1998	Stabilisce fondi e criteri di ripartizione adeguati per l'assolvimento dei compiti.	SCH/Aut-cont (96) 4a rev. + SCH/Aut-cont (98) budget 1
Decisione dell'ACC relativa alle leggi sulla protezione dei dati della Grecia	Dichiarazione dell'ACC sull'entrata in vigore delle leggi sulla protezione dei dati della Grecia.	SCH/Aut-cont (97) PV 3 (riunione dell'ACC del 27 marzo 1997) e SCH/Aut-cont (97) L 5
Decisione dell'ACC relativa alle leggi sulla protezione dei dati dell'Italia	Dichiarazione dell'ACC sull'entrata in vigore delle leggi sulla protezione dei dati dell'Italia	SCH/Aut-cont (97) PV 7 (riunione dell'ACC del 4 luglio 1997) e SCH/Aut-cont (97) 35
Elenco delle autorità autorizzate a consultare direttamente i dati inseriti nel SIS	Articolo 101, 4° comma della Convenzione. Decisione dell'ACCP.	SCH/Aut-cont (95) PV 1 (riunione dell'ACCP del 22 febbraio 1995)
Raccomandazioni dell'ACCP sul C.SIS	Raccomandazioni relative alla sicurezza presso il C.SIS, all'affidabilità delle trasmissioni tra gli N.SIS e il sistema centrale.	SCH/Aut-cont (94) dec. 1 (18 maggio 1994)
Parere sull'esercizio del diritto di accesso e sui principi di cooperazione nella verifica dei dati	Definisce i principi di cooperazione tra le autorità di controllo nazionali, nel quadro dell'esercizio dei diritti di accesso e di verifica.	SCH/Aut-cont (96) 16, 2a rev.
Raccomandazioni dell'ACC sul funzionamento del sistema d'informazione	Raccomandazioni sulla sicurezza del SIS contenute nella Relazione a carattere riservato del 27 marzo 1997 e riprodotte in parte nella relazione di attività 1995-1997.	• SCH/Aut-cont (96) 40, 2a rev. (dicembre 1996, versione definitiva del 27 marzo 1997) – (RISERVATO) • SCH/Aut-cont (97) 27, 2a rev. (Relazione di attività 1995-1997 del 17 marzo 1997) – pagg. 24-28

Documento	Argomento	Rif. documento Schengen
Parere sul progetto pilota relativo ai veicoli rubati	Principi da rispettare in materia di scambio di informazioni provenienti dal SIS, nell'ambito di operazioni tra Stati Schengen, con paesi che non applicano ancora la Convenzione.	Parere del 7 marzo 1997 (SCH/Aut-cont (96) 22 riv.)
Parere sull'Accordo di cooperazione nella contestazione delle infrazioni stradali e nell'esecuzione delle relative sanzioni pecuniarie	Enumerazione delle menzioni relative alla protezione dei dati (diritti delle persone, principio di cooperazione tra autorità nazionali e competenze dell'ACC) che devono figurare nell'Accordo.	Parere del 7 marzo 1997 (SCH/Aut-cont (96) 19 riv.)
Relazione sulle attività dell'ACC - marzo 1995/marzo 1997	Attività dell'ACC da marzo 1995 a marzo 1997 (Approvata e distribuita ai sensi dell'articolo 115, 4° comma della Convenzione di applicazione).	SCH/Aut-cont (97) 27, 2a rev. del 17 marzo 1997
Relazione sulle attività dell'ACC – marzo 1997/marzo 1998	Attività dell'ACC da marzo 1997 a marzo 1998 (Approvata e distribuita ai sensi dell'articolo 115, 4° comma della Convenzione di applicazione)	SCH/Aut-cont (98) 5, 5a rev., pubblicato il 28 aprile 1998
Decisione sulla composizione dell'Autorità	Decisione sul riconoscimento dello status di osservatori ai rappresentanti della Danimarca, della Finlandia, della Norvegia, dell'Islanda e della Svezia.	SCH/Aut-cont (97) PV 1 (verbale della riunione del 10 e 11 febbraio 1997 a Strasburgo)
Decisioni sulla composizione dell'Autorità	Decisione sul riconoscimento della qualità di membri dell'ACC ai rappresentanti dell'Austria, della Grecia e dell'Italia.	SCH/Aut-cont (97) PV 11 (verbale della riunione dell'ACC del 12 dicembre 1997)
Parere sulla duplicazione di una parte delle segnalazioni SIS	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 e consolari di alcuni Stati Schengen all'estero.	Parere 97/1 del 22 maggio 1997 (SCH/Aut-cont (97) 38 riv.)
Parere sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione	Cancellazione dei dati ai sensi dell'articolo 112. Revisione del Manuale Sirene.	Parere 98/1 del 3 febbraio 1998 (SCH/Aut-cont (97) 55, 2a rev.)
Parere sulla segnalazione nel SIS di persone la cui identità è stata usurpata	Denuncia da parte dell'ACC della situazione attuale e proposta di collaborazione ai fini della ricerca di una soluzione che non rechi pregiudizio ai diritti del legittimo titolare dell'identità usurpata.	Parere 98/2 del 3 febbraio 1998 (SCH/Aut-cont (97) 42, 2a rev.)

Documento	Argomento	Rif. documento Schengen
Parere sulle eventuali relazioni tra il SIS e il progetto "ASF – Veicoli rubati" di Interpol.	Tipo di dati che possono essere trasmessi dal SIS verso la banca dati d'Interpol ASF.	Parere 98/3 del 3 febbraio 1998 (SCH/Aut-cont (97) 50, 2a rev.)
Parere sulla registrazione delle consultazioni prevista all'articolo 103	Enumerazione dei criteri da rispettare al momento della registrazione di cui all'articolo 103.	Parere 98/4 del 3 febbraio 1998 (SCH/Aut-cont (97) 70 riv.)
Comunicazione all'ACC dei documenti di altri gruppi Schengen	Messa a disposizione dell'ACC dei documenti relativi alle attività legate al SIS perché questa possa verificare se vengono prese in considerazione le sue raccomandazioni tecniche.	Lettera del Presidente del Gruppo centrale all'ACC del 12 gennaio 1998 (SCH/Aut-cont (98) 11)
Assistenza del Segretariato all'ACC	Rafforzamento del sostegno del Segretariato all'ACC affinché questa possa assolvere i propri compiti.	• Regolamento interno dell'ACC (art. 10) (SCH/Aut-cont (95) 25, 6a rev.) • SCH/Aut-cont (97) PV 6 (riunione del 16 giugno 1997 tra i rappresentanti dell'ACC, del Gruppo centrale e del Ministero dell'Interno francese) • SCH/Aut-cont (97) 2 (lettera del Presidente del Gruppo centrale del 14 gennaio 1997) • SCH/Aut-cont (97) PV 1 (riunione del Gruppo centrale del 23 febbraio 1998)

Nota: la relazione del 27 marzo 1997 sul controllo del C.SIS contiene raccomandazioni sulla sicurezza del SIS nonché la reazione del Ministero dell'Interno francese ad alcune di esse (SCH/Aut-cont (96) 40, 2a rev.).

Tale documento è considerato riservato dall'ACC e dal Gruppo centrale. E' stato pertanto trasmesso dall'ACC al presidente del Comitato esecutivo e ai membri del Gruppo centrale che l'hanno trasmesso a loro volta ai propri esperti interessati.

Estratti di tale relazione sono ripresi alle pagine 24-28 della relazione sulle attività 1995/1997 SCH/Aut-cont (97) 27, 2a rev.

8. REGOLAMENTO INTERNO DELL'AUTORITÀ DI CONTROLLO COMUNE

approvato dall'ACC il 2 febbraio 1996
modificato all'articolo 2 per decisione adottata dall'ACC nella riunione del 4.7.1997
modificato il 27 aprile 1998 con l'aggiunta di un nuovo articolo 11

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, in conformità dell'articolo 115 della Convenzione, di due rappresentanti dell'Autorità di controllo nazionale di cui all'articolo 114 della Convenzione di ogni Parte contraente in cui è entrata in vigore la Convenzione, in conformità dell'articolo 140. È considerata Parte contraente anche la Parte che ha concluso con le Parti dell'Accordo e della Convenzione di Schengen un accordo di cooperazione relativo alla soppressione dei controlli delle persone alle frontiere interne definite all'articolo 1 della Convenzione, a condizione che tale accordo di cooperazione sia entrato in vigore. 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 delle Autorità di controllo nazionali di cui all'articolo 114 della Convenzione o agli esperti indipendenti delle Parti contraenti che non soddisfano ancora il disposto dell'articolo 140, 2° comma, ultima frase. È considerata Parte contraente anche la Parte che ha concluso con le Parti dell'Accordo e della Convenzione di Schengen un accordo di cooperazione relativo alla soppressione dei controlli delle persone alle frontiere interne definite all'articolo 1 della Convenzione, a condizione che tale accordo di cooperazione sia stato ratificato, accettato o approvato da tutte le Parti, ma non ancora entrato 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 può 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 alme-

no 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 può 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 Segretariato 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 – Bilancio dell'Autorità di controllo comune

All'Autorità di controllo comune è assegnato un bilancio, iscritto come linea autonoma nel bilancio Schengen, che le consente di realizzare il suo programma di lavoro annuale nel quadro delle attribuzioni che le sono conferite dalla Convenzione.

Articolo 12 – Verbali

1. È 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 13 – 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 14 - 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.

9. PRINCIPI GENERALI APPLICABILI ALLE VISITE ED AI CONTROLLI DEL C.SIS

Scopo dei presenti principi è chiarire le modalità delle visite e dei controlli dell'Autorità di controllo comune (ACC) sul sito del C.SIS a Strasburgo.
Tali visite si collocano nel quadro dei compiti derivanti dall'articolo 115 della Convenzione di applicazione dell'Accordo di Schengen (Convenzione di Schengen).

1) Tipi di visite

Le visite possono essere raccolte in due categorie:

- la visita d'informazione che, in generale, comprende la visita degli edifici, la presentazione generale del SIS e l'attività del C.SIS senza vera e propria consultazione della base dati.
Può essere effettuata dall'ACC nella sua composizione plenaria;

- la visita di controllo che ha lo scopo di verificare la corretta esecuzione delle disposizioni della Convenzione di Schengen e che, in principio, viene effettuata da un gruppo ristretto di persone appositamente incaricato di tale compito dall'ACC;

- tale gruppo di controllo è incaricato di verificare l'integrità, la qualità, la continuità, l'esclusività e la riservatezza del C.SIS nel quadro della Convenzione.

2) Informazione del Ministero dell'Interno

L'ACC informa il Ministero dell'Interno (direzione generale della polizia nazionale, direzione delle libertà pubbliche e degli affari giuridici, direzione delle trasmissioni e dell'informatica) della sua visita al C.SIS a Strasburgo.
L'ACC precisa la natura della visita, lo scopo, la lingua di lavoro e le soluzioni previste per ovviare alle difficoltà di ordine linguistico, la data prevista e la composizione del gruppo che effettua la visita.

3) Composizione del gruppo che effettua la visita

L'ACC determina la composizione del gruppo che effettua la visita o il controllo che può essere composto delle seguenti tre categorie di persone:
- membri dell'ACC e del Segretariato generale,
- membri e agenti delle autorità di controllo nazionali preposte alla protezione dei dati,
- esperti esterni.
Un elenco nominativo, completo, viene trasmesso al Ministero dell'Interno. Alle visite di controllo possono partecipare solo i membri effettivi dell'ACC, il Segretariato generale e le persone abilitate e mandate dall'ACC.
In caso di ricorso ad esperti esterni che non figurano nell'elenco di cui all'articolo 9 del Regolamento interno dell'ACC, questa ne informa il Ministero dell'Interno con un mese d'anticipo.

4) Svolgimento della visita di controllo

All'inizio della visita di controllo il programma di lavoro preliminarmente stabilito dall'ACC viene comunicato ai responsabili del sito al fine di consentire loro di prendere le disposizioni del caso per rispondere alle domande poste dall'ACC.

5) Consultazione del sistema informatico

Il gestore del C.SIS impiega tutti i mezzi necessari per soddisfare in tempo reale le richieste di consultazione del sistema informatico formulate dall'Autorità di controllo comune. Provvede in particolare a mettere a sua disposizione un tecnico incaricato di procedere a operazioni manuali necessarie per soddisfare le summenzionate richieste.

6) Accesso ai documenti

L'ACC ha accesso a tutti i documenti riguardanti il C.SIS utili al suo compito.
Essa rispetta il carattere riservato dei documenti.
I documenti classificati "secret défense" debbono rimanere nella sede del C.SIS, ma sono accessibili all'ACC.
La consegna di copie di documenti è subordinata alla firma di una ricevuta.

7) Relazioni tecniche

Le relazioni tecniche sono e rimangono riservate nella misura in cui potrebbero rivelare aspetti operativi del sistema.

Prima di essere trasmesse alle autorità Schengen, esse vengono trasmesse ai responsabili del C.SIS perché formulino eventuali osservazioni.

10. RELAZIONE SULLA SICUREZZA DEGLI UFFICI SIRENE

SCHENGEN

Autorità di controllo comune

Bruxelles, 11 dicembre 1998
SCH/Aut-cont. (98) 47 rev. 2

RELAZIONE DELL'ACC SULLA SICUREZZA DEGLI UFFICI SIRENE

In occasione della riunione del 12 dicembre 1997, l'Autorità di controllo comune ha deciso di procedere alla verifica delle misure di sicurezza messe in atto dagli Uffici SIRENE. Tale decisione è stata adottata in seguito alla fuga di documenti avvenuta tempo addietro in un Ufficio SIRENE.

Tutti i membri dell'ACC dei paesi che applicano la Convenzione hanno quindi effettuato controlli nei rispettivi uffici SIRENE e hanno trasmesso la loro relazione al Segretariato dell'ACC.[1] Alcuni membri hanno annunciato che avrebbero presentato una relazione complementare.

Le relazioni delle autorità nazionali descrivono la situazione nei settori della sicurezza fisica e delle comunicazioni tra l'ufficio SIRENE e l'NSIS, descrivono inoltre le funzioni di tracciatura, che consentono, non solo, di rintracciare l'ufficio e il terminale, ma anche di identificare l'operatore che ha utilizzato un applicativo (ad esempio per un aggiornamento), nonché le condizioni di accesso ai dati del SIS e agli archivi manuali.

Alla luce delle precedenti constatazioni, l'ACC conclude che sono stati prodigati sforzi al fine di migliorare la sicurezza del sistema ma che questi devono proseguire.

L'ACC richiama infatti i seguenti principi:

- gli uffici SIRENE devono soddisfare tutte le condizioni contemplate all'articolo 118 della Convenzione di applicazione di Schengen;
- il livello di sicurezza degli uffici SIRENE nazionali non può essere inferiore a quello del SIS.

Premesso ciò, l'ACC propone che negli Stati dove tali principi non sono ancora applicati vadano prese le seguenti disposizioni:

1. mantenimento della sicurezza fisica al massimo livello aggiornando le tecniche impiegate. Negli Stati in cui sono state constatate lacune, vanno apportate le modifiche necessarie quanto prima e va informata l'autorità di controllo nazionale;

[1] *Relazione SCH/Aut-cont (98) 9 della Francia, 13 e 40 del Belgio, 15 dell'Italia, 21 della Germania, 28 della Grecia, 31 del Portogallo, 33 dei Paesi Bassi, 35 della Spagna, 36 dell'Austria. La relazione sulla sicurezza dell'Ufficio SIRENE lussemburghese è integrata nella relazione annuale dell'autorità di controllo di quel paese e sarà prossimamente completata da un'altra relazione. È possibile che anche i Paesi Bassi comunichino prossimamente un'altra relazione di controllo.*

2. cifratura delle comunicazioni tra il SIRENE e l'N.SIS e controllo della cifratura da parte dei membri delle autorità di controllo;

3. a) realizzazione di un sistema di tracciatura di tutte le operazioni possibili riguardanti la base di dati N.SIS e dell'ufficio SIRENE (numero di interrogazioni, orario, tipi di dati consultati, ecc.);

b) analisi regolare degli archivi di tracciatura al fine di individuare eventuali anomalie riguardo, in particolare, al numero di interrogazioni;

4. limitazione e controllo dell'accesso agli archivi manuali dei dossier;

5. cifratura delle informazioni contenute su supporto informatico;

6. a) intensificazione delle misure di sicurezza al fine di garantire che l'accesso sia effettivamente limitato ai dati per i quali gli operatori hanno un'autorizzazione, in particolare verificando regolarmente le loro autorizzazioni di accesso e modificando regolarmente i password;

b) verifica regolare dei motivi di una interrogazione del SIS;

7. designazione di un funzionario responsabile della sicurezza e definizione delle norme di sicurezza comuni ai vari uffici SIRENE, applicabili al loro personale;

8. organizzazione della gestione delle informazioni stampate in modo da limitare l'ottenimento di stampe dello schermo contenenti informazioni della base di dati SIRENE e di segnalazioni SIS;

9. incoraggiamento dell'organizzazione di corsi di formazione incentrati sulla sicurezza dei dati per gli utenti degli uffici SIRENE;

10. raccomandazione dell'elaborazione da parte degli N.SIS e degli uffici SIRENE di relazioni sulla sicurezza, a intervalli regolari, per esempio ogni anno.
L'evoluzione futura del sistema di comunicazione dei dati tra gli Stati, per quanto riguarda in particolare lo sviluppo del SIS, dovrà obbligatoriamente tenere conto delle condizioni di sicurezza, qualunque sia il modello, centralizzato o non centralizzato, prescelto.

Infine, l'ACC sottolinea la cooperazione di tutte le autorità nazionali interessate ed esprime la sua soddisfazione per il fatto che questa operazione di verifica condotta in modo coordinato in tutti gli Stati ha contribuito a migliorare sensibilmente la sicurezza delle informazioni. Ciò è fondamentale per la fiducia dei cittadini e delle istituzioni democratiche nel funzionamento del Sistema Schengen.

11. COMPOSIZIONE DELLE DELEGAZIONI DELL'AUTORITÀ DI CONTROLLO COMUNE

AUTORITÀ DI CONTROLLO COMUNE
SCHENGEN

Bruxelles, 30 giugno 2000

Presidente: Sig. Bart DE SCHUTTER
Vicepresidente: Sig. Giovanni BUTTARELLI

AUSTRIA
MEMBRI
Sig.a Waltraut KOTSCHY
Sig.a Eva SOUHRADA-KIRCHMAYER
SUPPLENTI
s.RA Birgit HROVAT-WESENER

BELGIO
MEMBRI
Sig. Bart DE SCHUTTER
Sig.a Bénédicte HAVELANGE

DANIMARCA (OSSERVATORE)

MEMBRI

Sig.a Lotte N. JØRGENSEN

Sig.a Cristina Angela GULISANO

FINLANDIA (OSSERVATORE)

MEMBRI

Sig.a Maija KLEEMOLA

Sig. Reijo AARNIO

FRANCIA

MEMBRI

Sig. Alex TÜRK

Sig.a Florence FOURETS

SUPPLENTI

Sig. Olivier COUTOR

GERMANIA

MEMBRI

Sig. Joachim JACOB

rappresentato dal Sig. Wolfgang von POMMER ESCHE

Sig. Friedrich VON ZEZSCHWITZ

rappresentato dalla Sig.a Angelika SCHRIEVER-STEINBERG

GRECIA

MEMBRI

Sig. Constantinos DAFERMOS

SUPPLENTI

Sig. Georgios DELYANNIS

Sig. Dimitrios GRITZALIS

ITALIA

MEMBRI

Sig. Sebastiano NERI

Sig. Giovanni BUTTARELLI

LUSSEMBURGO

MEMBRI

Sig. René FABER

SUPPLENTI

Sig. Jean WAGNER

Sig. Georges WIVENES

PAESI BASSI

MEMBRI

Sig. Peter HUSTINX

Sig. Peter MICHAEL

PORTOGALLO

MEMBRI

Sig. João LABESCAT da SILVA

Sig.a Catarina SARMENTO e CASTRO

SPAGNA
MEMBRI
Sig. Juan Manuel FERNANDEZ LOPEZ
Sig. Miguel Angel LOPEZ HERRERO

SVEZIA (OSSERVATORE)
MEMBRI
Sig. Ulf WIDEBÄCK
Sig.a Britt-Marie WESTER
SUPPLENTI
Sig. Leif LINDGREN
Sig.a Margareta ÅBERG

NORVEGIA (OSSERVATORE)
MEMBRI
Sig. Knut-Magnar AANESTAD
Sig. G. APENES

ISLANDA (OSSERVATORE)
MEMBRI
Sig.a S. JÖHANNESDOTTIR
Sig. Páll HREINSSON

12. SIGNALAMENT DANS LE SIS [Tabella non riportata]

13. INDICE CRONOLOGICO

1985

L'Accordo di Schengen è firmato il 14 giugno 1985 dai governi degli Stati dell'Unione economica del Benelux, della Repubblica federale di Germania e della Repubblica francese. E' provvisoriamente applicato il giorno successivo a quello della firma (articolo 32) ed entra in vigore il 2 marzo 1986.

1990

La Convenzione di applicazione dell'Accordo di Schengen, firmata dalle stesse Parti contraenti il 19 giugno 1990, sviluppa, per fini legati ai controlli alle frontiere esterne comuni, la cooperazione di polizia, doganale e giudiziaria.

Una delle misure fondamentali del dispositivo di cooperazione è la creazione di un sistema di informazione comune, il Sistema d'informazione Schengen (Titolo IV della Convenzione).

L'istituzione di questo sistema induce la creazione di un'autorità di controllo comune, sull'esempio di modelli nazionali di autorità di controllo indipendenti competenti in questo settore.

1992

E' istituita un'Autorità di controllo comune provvisoria (ACCP), presieduta dal sig. Faber (Lussemburgo) e composta di uno o due rappresentanti delle autorità di controllo nazionali dei cinque Stati fondatori e di uno o due esperti indipendenti designati dagli Stati aderenti sul cui territorio la Convenzione non è ancora stata messa in applicazione.

L'ACCP si riunisce dodici volte a Bruxelles tra il 29 giugno 1992 e il 22 febbraio 1995.

1993

Il Portogallo e la Spagna ratificano l'Accordo e la Convenzione di applicazione di Schengen.

1994

L'Autorità di controllo comune effettua la prima visita al sistema centrale di Strasburgo.

È elaborato un questionario sulle norme di protezione dei dati applicabili negli Stati Schengen.

Viene eletto alla presidenza il sig. Von Pommer Esche (Germania), Capo di dipartimento presso il garante federale per la protezione dei dati.

1995

Il 26 marzo la Convenzione viene messa in applicazione nel territorio di sette paesi: Germania, Belgio, Spagna, Francia, Lussemburgo, Paesi Bassi e Portogallo. Lo stesso giorno viene istituita l'Autorità di controllo comune. Il Sistema d'informazione Schengen entra in servizio.

Tra il 17 maggio e il 14 dicembre dello stesso anno, l'ACC si riunisce 5 volte sotto la presidenza del sig. Von Pommer Esche.

Il 14 dicembre, il sig. Turk (Francia), senatore e membro della Commissione nazionale dell'Informatica e delle Libertà (CNIL), e il sig. Labescat (Portogallo), avvocato e membro della Commissione nazionale per la protezione dei dati, sono eletti rispettivamente presidente e vicepresidente dell'ACC.

1996

Il 2 febbraio è approvato il Regolamento interno dell'Autorità di controllo comune.

Il 19 dicembre, Danimarca, Finlandia e Svezia firmano l'Accordo di adesione a Schengen. Islanda e Norvegia siglano un Accordo di cooperazione in forza al quale la Convenzione di Schengen può essere applicata nel loro territorio.

L'ACC si riunisce nove volte nel corso dell'anno. Partecipano ai lavori, con lo status di osservatori, rappresentanti indipendenti di Austria, Italia e Grecia.

L'ACC approva i principi di cooperazione tra le autorità nazionali di controllo in materia di esercizio del diritto di accesso.

1997

L'ACC si riunisce dieci volte tra il mese di marzo 1997 e il mese di marzo 1998. Fatta eccezione per la sessione annuale tenutasi a Lisbona in aprile 1997, tutte le riunioni si svolgono a Bruxelles. Oltre alle riunioni plenarie, l'ACC si riunisce cinque volte in cerchia ristretta. Si tengono inoltre incontri tra rappresentanti dell'ACC ed esponenti del Ministero dell'Interno francese.

L'ACC vede riconoscere l'importanza del suo ruolo da parte degli organi esecutivi di Schengen. Viene dotata di un bilancio mediante una linea di bilancio autonoma e riceve con maggiore regolarità le informazioni necessarie per l'esercizio delle sue funzioni.

L'11 febbraio ha luogo il controllo presso il sistema centrale di Strasburgo, a seguito del quale l'ACC elabora una relazione contenente una serie di raccomandazioni sul funzionamento del sistema.

L'ACC elabora pareri sul progetto pilota relativo ai veicoli rubati, sull'accordo di cooperazione in materia di contestazione delle infrazioni stradali e di esecuzione delle relative sanzioni pecuniarie e sulla duplicazione di una parte delle segnalazioni SIS.

L'ACC approva la sua prima relazione di attività (marzo 1995 - marzo 1997) e la presenta al pubblico in aprile, nel quadro di una conferenza stampa organizzata a Lisbona.

Alla fine del 1997, il numero dei paesi che applicano la Convenzione passa a dieci: Germania, Austria, Belgio, Spagna, Francia, Grecia, Italia, Lussemburgo, Paesi Bassi e Portogallo. I rappresentanti delle autorità di controllo nazionali degli Stati nordici (Danimarca, Finlandia, Islanda, Norvegia e Svezia) partecipano ai lavori dell'ACC nella qualità di osservatori.

Il Sig. J. Labescat e B. De Schutter sono eletti rispettivamente presidente e vicepresidente dell'ACC.

1998

L'ACC formula pareri sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione, sull'usurpazione di identità e le conseguenze, per quanto riguarda il SIS, per il legittimo titolare dell'identità usurpata, sulla trasmissione di dati relativi ai veicoli rubati (dal SIS alla banca dati di Interpol), sul controllo di ammissibilità delle consultazioni SIS e sull'accesso ai dati SIS da parte degli uffici della motorizzazione.

Per la prima volta viene realizzato un controllo globale presso tutti gli uffici SIRENE, seguito da una serie di raccomandazioni relative al rafforzamento della sicurezza.

L'ACC segue i lavori di sviluppo del SIS I+ e gli studi preliminari sul SIS II.

Definisce un acquis comunitario nella prospettiva dell'integrazione di Schengen nell'Unione europea.

Promuove il primo colloquio sui "Diritti dei cittadini nei confronti dei sistemi d'informazione di polizia" e una conferenza stampa a Lisbona.

Lancia la campagna "Il Sistema d'informazione Schengen vi riguarda" che prevede la distribuzione di poster e opuscoli informativi sui diritti dei cittadini nei punti di ingresso dello spazio Schengen (aeroporti, frontiere marittime, ecc.).

Il presidente dell'ACC partecipa per la prima volta ad una riunione del Comitato esecutivo ed assiste ad una riunione del Gruppo centrale a Strasburgo.

1999

Controllo del C.SIS.

Integrazione di Schengen nell'Unione europea.

Presentazione della relazione di attività nella sessione annuale di Firenze.

Parere complementare sull'usurpazione d'identità e sulla conservazione dei dossier ad avvenuta cancellazione di una segnalazione.

Esame delle condizioni preliminari all'applicazione dell'acquis di Schengen nei paesi nordici.

14. INFORMAZIONI SUI DIRITTI DEI CITTADINI RISPETTO AL SIS

SCHENGEN

IT
Autorità di controllo comune

Bruxelles, 16 febbraio 1998
SCH/Aut-cont (97) 61, Rev. 3

NOTA DELL'ACC

"I VOSTRI DIRITTI NEI CONFRONTI
DEL SISTEMA D'INFORMAZIONE SCHENGEN"

Il sistema d'informazione Schengen

L'Accordo e la Convenzione di applicazione di Schengen hanno creato uno spazio di libera circolazione delle persone abolendo i controlli alle frontiere interne degli Stati membri ed instaurando il principio di un controllo unico all'ingresso nel territorio Schengen. E' tuttavia emersa, per motivi di sicurezza, la necessità di attuare misure compensative, prima tra tutte il Sistema d'informazione Schengen (SIS).

Il SIS è un archivio comune a tutti gli Stati membri dello spazio Schengen, che centralizza due grandi categorie di informazioni: quelle relative alle persone ricercate o poste sotto sorveglianza e quelle relative ai veicoli o agli oggetti ricercati.

Ad esempio, nel Sistema d'informazione Schengen possono essere segnalate:

- persone ricercate o sorvegliate dai servizi di polizia;
- persone scomparse o che devono essere poste sotto protezione, in particolare i minori ;
- persone, non cittadini di uno Stato membro dello spazio Schengen, a cui è stato vietato l'ingresso nel territorio Schengen;
- persone la cui identità è stata fraudolentemente utilizzata come alias da altre persone.

Il controllo del SIS è effettuato da un'autorità indipendente, l'Autorità di controllo comune Schengen (ACC).

Tale autorità, composta di membri delle autorità per la protezione dei dati personali degli Stati membri dello spazio Schengen, oltre ad esercitare un controllo tecnico sull'archivio centrale del sistema situato a Strasburgo, ha il compito di verificare che gli Stati Schengen rispettino i diritti delle persone previsti dalla Convenzione di Schengen.

I vostri diritti nei confronti del SIS

Il SIS vi riguarda direttamente, a prescindere dal fatto che siate o non cittadini di uno Stato membro dello spazio Schengen. La Convenzione di Schengen vi riconosce determinati diritti specifici.

Avete, in particolare :

- il diritto di accesso alle informazioni che vi riguardano registrate nel SIS;
- il diritto di rettificare i dati quando questi sono stati registrati sulla base di errori di fatto o di diritto;
- il diritto di promuovere un'azione giudiziaria o dinanzi le autorità competenti per ottenere la rettifica o la cancellazione delle informazioni errate o un indennizzo;
- il diritto di chiedere una verifica dei dati registrati e dell'uso che ne viene fatto.

Se pensate che il vostro nominativo figuri nel SIS, non esitate ad esercitare i vostri diritti. Le autorità nazionali per la protezione dei dati degli Stati membri dello spazio Schengen sono a vostra disposizione e vi forniranno tutte le informazioni utili per le formalità necessarie.

Le verifiche sulla vostra segnalazione nel SIS (pertinenza dell'inserimento nell'archivio e registrazione dei dati che vi riguardano) saranno effettuate in conformità al diritto nazionale applicabile nel paese in cui sceglierete di esercitare i vostri diritti. Su semplice richiesta, l'autorità di controllo nazionale competente (v. estremi sull'ultima pagina) metterà a vostra disposizione la legge nazionale applicabile. Sarete in seguito informati dell'esito o del seguito dato alla vostra richiesta.

I testi di riferimento

- L'Accordo di Schengen del 14 giugno 1985
- La Convenzione di applicazione dell'Accordo di Schengen del 19 giugno 1990

Questi testi vi saranno comunicati, su semplice richiesta, dal Segretariato dell'Autorità di controllo comune (v. indirizzo sull'ultima pagina).

Indirizzi utili

Autorità nazionali per la protezione dei dati.

Paesi-Bassi
Registratiekamer - Prins Clauslaan 20
2595 AJ 's-Gravenhage
tel: 00 31 70 381 13 00
fax: 00 31 70 381 13 01
e-mail: phu@registratiekamer.nl

Germania
Der Bundesbeauftragte für den Datenschutz
Friedrich-Ebert-straße 1 -53173 Bonn
tel.: 00 49 228 8 19950
fax: 00 49 228 8 1995 50
e-mail:
wolfgang.dr-von-pommer-esche@bfd.bund400.de

Der Hessische Datenschutzbeauftragte
Uhlandstraße 4 - 65189 Wiesbaden
tel.: 00 49 611 14 08-0
fax: 00 49 611 37 85 79
e-mail: DSB-HESSEN@t-online.de

Belgio
Commission de la protection de la vie privée /
Commissie voor de bescherming van de persoonlijke levenssfeer
Av. de la Porte de Hal 5-8 - 1060 Bruxelles
tel.: 00 32 2 542 72 00
fax: 00 32 2 542 72 12
e-mail: benedicte.havelange@privacy.fgov.be

Austria
Datenschutzkommission
Ballhausplatz 1 - 1014 Wien
tel.: 00 43 1 531 15/2525
fax: 00 43 1 53 115/2690
e-mail: waltraut.kotschy@bka.gv.at

Lussemburgo
Autorité de contrôle " Police " - Parquet général
B.P. 15
L -2010 Luxembourg
tel.: 00 352 47 59 81-331
fax: 00 352 47 05 50
e-mail: parquet.general@mj.etat.lu

Francia
Commission Nationale de l'Informatique et des Libertés
21 rue Saint Guillaume
75340 Paris Cedex 07
tel.: 00 33 1 53 73 22 22
fax: 00 33 1 53 73 22 00
e-mail: ffourets@cnil.fr

Portogallo
Comissão Nacional de Protecçao de Dados Pessoais Informatizados
Rua de São Bento 148, 3°
1200 Lisboa
tel.: 00351 1 392 84 00
fax: 00 351 1 397 68 32
e-mail: geral@cnpd.pt

Spagna
Agencia de Protección de Datos
Paseo de la Castellana 41
28046 Madrid
tel.: 00 34 91 339 62 18/339 62 19
fax: 00 34 91 308 46 92
e-mail: inspeccion@agenciaprotecciondatos.org

Italia
Garante per la protezione dei dati personali
Piazza di Monte Citorio 121
00186 Roma
tel.: 00 39 06 69 67 77 13
fax: 00 39 06 69 67 77 15
e-mail: garante@garanteprivacy.it

Grecia
Autorité de protection des données à caractère personnel
Omirou 8
105 64 Athènes
tel.: 00 301 335 26 04-5
fax: 00 301 335 26 17
e-mail: kourouni@dpa.gr

Segretariato dell'ACC
175, rue de la Loi
(bureau 50 CG 07)
1048 Bruxelles
tel.: 00 32 2 285 53 93
fax: 00 32 2 285 81 54
e-mail: bernard.philippart@consilium.eu.int

15. PROTOCOLLO SULL'INTEGRAZIONE DELL'ACQUIS DI SCHENGEN NELL'AMBITO DELL'UNIONE EUROPEA, ALLEGATO AL TRATTATO DI AMSTERDAM

LE ALTE PARTI CONTRAENTI,

RILEVANDO che gli accordi relativi all'eliminazione graduale dei controlli alle frontiere comuni firmati da alcuni Stati membri dell'Unione europea a Schengen il 14 giugno 1985 e il 19 giugno 1990, nonché gli accordi connessi e le norme adottate sulla base dei suddetti accordi mirano a promuovere l'integrazione europea e, in particolare, a consentire all'Unione europea di trasformarsi più rapidamente in uno spazio di libertà, di sicurezza e di giustizia,

DESIDEROSI di incorporare gli accordi e le norme summenzionati nel quadro dell'Unione europea,

CONFERMANDO che le disposizioni dell'acquis di Schengen sono applicabili solo se e nella misura in cui essi sono compatibili con l'Unione e il diritto comunitario,

TENENDO CONTO della particolare posizione della Danimarca,

TENENDO CONTO del fatto che l'Irlanda e il Regno Unito di Gran Bretagna e Irlanda del Nord non sono parti dei suddetti accordi e non li hanno firmati; che dovrebbero tuttavia essere previste disposizioni per consentire a tali Stati di accettare, in tutto o in parte, le disposizioni di tali accordi,

RICONOSCENDO che, pertanto, è necessario avvalersi delle disposizioni del trattato sull'Unione europea e del trattato che istituisce la Comunità europea relative ad una cooperazione rafforzata tra alcuni Stati membri e che a tali disposizioni si dovrebbe fare ricorso solo in ultima istanza,

TENENDO CONTO della necessità di mantenere un rapporto speciale con la Repubblica d'Islanda e il Regno di Norvegia, Stati che hanno entrambi confermato la loro intenzione di essere vincolati dalle disposizioni summenzionate, in base all'accordo firmato a Lussemburgo il 19 dicembre 1996,

HANNO CONVENUTO le seguenti disposizioni, che sono allegate al trattato sull'Unione europea e al trattato che istituisce la Comunità europea,

ARTICOLO 1

Il Regno del Belgio, il Regno di Danimarca, la Repubblica federale di Germania, la Repubblica ellenica, il Regno di Spagna, la Repubblica francese, la Repubblica italiana, il Granducato di Lussemburgo, il Regno dei Paesi Bassi, la Repubblica d'Austria, la Repubblica portoghese, la Repubblica di Finlandia e il Regno di Svezia, firmatari degli accordi di Schengen, sono autorizzati a instaurare tra loro una cooperazione rafforzata nel campo di applicazione di tali accordi e delle disposizioni collegate, quali sono elencati nell'allegato del presente protocollo, in prosieguo denominato acquis di Schengen. Tale cooperazione è realizzata nell'ambito istituzionale e giuridico dell'Unione europea e nel rispetto delle pertinenti disposizioni del trattato sull'Unione europea e del trattato che istituisce la Comunità europea.

ARTICOLO 2

A decorrere dall'entrata in vigore del trattato di Amsterdam, l'acquis di Schengen, incluse le decisioni del Comitato esecutivo istituito dagli accordi di Schengen che sono state adottate anteriormente a tale data, si applica immediatamente ai tredici Stati membri di cui all'articolo 1, fatte salve le disposizioni del paragrafo 2 del presente articolo. A decorrere dalla medesima data, il Consiglio si sostituirà al suddetto Comitato esecutivo.

Il Consiglio, deliberando all'unanimità dei membri di cui all'articolo 1, adotta le disposizioni necessarie per l'attuazione del presente paragrafo. Il Consiglio, deliberando all'unanimità, determina, in base alle pertinenti disposizioni dei trattati, la base giuridica di ciascuna delle disposizioni o decisioni che costituiscono l'acquis di Schengen.

Relativamente a tali disposizioni e decisioni e in base a detta determinazione delle basi giuridiche, la Corte di giustizia delle Comunità europee esercita le competenze conferitele dalle pertinenti disposizioni applicabili dei trattati. La Corte di giustizia non è comunque competente per quanto concerne le misure e le decisioni relative al mantenimento dell'ordine pubblico e alla salvaguardia della sicurezza interna.

Fino all'adozione delle misure di cui sopra e fatto salvo l'articolo 5, paragrafo 2, le disposizioni o decisioni che costituiscono l'acquis di Schengen sono considerate atti fondati sul titolo VI del trattato sull'Unione europea.

Le disposizioni del paragrafo 1 si applicano agli Stati membri che hanno firmato protocolli di adesione agli accordi di Schengen a decorrere dalle date stabilite dal Consiglio, che delibera all'unanimità dei

Membri di cui all'articolo 1, a meno che le condizioni per l'adesione di uno di tali Stati all'acquis di Schengen siano soddisfatte prima dell'entrata in vigore del trattato di Amsterdam.

ARTICOLO 3

A seguito della determinazione di cui all'articolo 2, paragrafo 1, secondo comma, la Danimarca mantiene rispetto agli altri firmatari degli accordi di Schengen gli stessi diritti e gli stessi obblighi che aveva anteriormente a detta determinazione per quanto concerne le parti dell'acquis di Schengen la cui base giuridica è individuata nel titolo III bis del trattato che istituisce la Comunità europea.

Per quanto attiene alle parti dell'acquis di Schengen la cui base giuridica è individuata nel titolo VI del trattato sull'Unione europea, la Danimarca mantiene gli stessi diritti e gli stessi obblighi degli altri firmatari degli accordi di Schengen.

ARTICOLO 4

L'Irlanda e il Regno Unito di Gran Bretagna e Irlanda del Nord, i quali non sono vincolati dall'acquis di Schengen, possono, in qualsiasi momento, chiedere di partecipare, in tutto o in parte, alle disposizioni di detto acquis.

Il Consiglio decide in merito a tale richiesta all'unanimità dei suoi membri di cui all'articolo 1 e del rappresentante del governo dello Stato interessato.

ARTICOLO 5

1. Le proposte e le iniziative che si baseranno sull'acquis di Schengen sono soggette alle pertinenti disposizioni dei trattati.

In tale contesto, laddove l'Irlanda o il Regno Unito, o entrambi, non abbiano notificato per iscritto al Presidente del Consiglio, entro un congruo periodo di tempo, che desiderano partecipare, l'autorizzazione di cui all'articolo 5 A del trattato che istituisce la Comunità europea o all'articolo K.12 del trattato sull'Unione europea si considera concessa agli Stati membri di cui all'articolo 1 nonché all'Irlanda e al Regno Unito, laddove uno di essi desideri partecipare ai settori di cooperazione in questione.

Le pertinenti disposizioni dei trattati di cui al paragrafo 1, primo comma, si applicano anche nel caso in cui il Consiglio non abbia adottato le misure di cui all'articolo 2, paragrafo 1, secondo comma.

ARTICOLO 6

La Repubblica di Islanda e il Regno di Norvegia sono associati all'attuazione dell'acquis di Schengen e al suo ulteriore sviluppo, in base all'accordo firmato a Lussemburgo il 19 dicembre 1996. A tal fine vengono concordate procedure appropriate in un accordo che sarà concluso con tali Stati dal Consiglio, che delibera all'unanimità dei suoi membri di cui all'articolo 1. Tale accordo include disposizioni relative al contributo dell'Islanda e della Norvegia ad ogni conseguenza finanziaria derivante dall'attuazione del presente protocollo.

Il Consiglio, deliberando all'unanimità, conclude con l'Islanda e la Norvegia un accordo separato, al fine di stabilire i diritti e gli obblighi fra l'Irlanda e il Regno Unito di Gran Bretagna e Irlanda del Nord, da un lato, e l'Islanda e la Norvegia, dall'altro, nei settori dell'acquis di Schengen che riguardano tali Stati.

ARTICOLO 7

Il Consiglio, che delibera a maggioranza qualificata, adotta le modalità relative all'integrazione del Segretariato Schengen nel Segretariato Generale del Consiglio.

ARTICOLO 8

Ai fini dei negoziati relativi all'adesione di nuovi Stati membri all'Unione europea, l'acquis di Schengen e le ulteriori misure adottate dalle istituzioni nell'ambito del suo campo d'applicazione sono considerati un acquis che deve essere accettato integralmente da tutti gli Stati candidati all'adesione.

ALLEGATO

ACQUIS DI SCHENGEN

1. L'accordo, firmato a Schengen il 14 giugno 1985, tra i Governi degli Stati dell'Unione economica del Benelux, la Repubblica federale di Germania e la Repubblica francese, relativo all'eliminazione graduale dei controlli alle frontiere comuni.

2. La Convenzione, firmata a Schengen il 19 giugno 1990, tra il Regno del Belgio, la Repubblica federale di Germania, la Repubblica francese, il Granducato di Lussemburgo e il Regno dei Paesi Bassi, recante applicazione dell'accordo relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmato a Schengen il 14 giugno 1985, nonché l'atto finale e le dichiarazioni comuni relativi.

3. I protocolli e gli accordi di adesione all'accordo del 1985 e la Convenzione di applicazione del 1990 con l'Italia (firmata a Parigi il 27 novembre 1990), la Spagna e il Portogallo (entrambe firmate a Bonn il 25 giugno 1991), la Grecia (firmata a Madrid il 6 novembre 1992), l'Austria (firmata a Bruxelles il 28 aprile 1995) e la Danimarca, la Finlandia e la Svezia (tutte firmate a Lussemburgo il 19 dicembre 1996), con i relativi atti finali e dichiarazioni.

4. Le decisioni e le dichiarazioni adottate dal Comitato esecutivo istituito dalla Convenzione di applicazione del 1990, nonché gli atti per l'attuazione della Convenzione adottati dagli organi cui il Comitato esecutivo ha conferito poteri decisionali.

DECISIONE DEL CONSIGLIO DEL 17 OTTOBRE 2000 CHE ISTITUISCE UN SEGRETARIATO DELLE AUTORITÀ DI CONTROLLO COMUNI PREPOSTE ALLA PROTEZIONE DEI DATI ISTITUITE DALLA CONVENZIONE CHE ISTITUISCE UN UFFICIO EUROPEO DI POLIZIA (CONVENZIONE EUROPOL), DALLA CONVENZIONE SULL'USO DELL'INFORMATICA NEL SETTORE DOGANALE E DALLA CONVENZIONE DI APPLICAZIONE DELL'ACCORDO DI SCHENGEN RELATIVO ALL'ELIMINAZIONE GRADUALE DEI CONTROLLI ALLE FRONTIERE COMUNI (CONVENZIONE DI SCHENGEN) (*)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto l'articolo 30 e l'articolo 34,paragrafo 2, lettera c) del trattato sull'Unione europea,

visto l'articolo 2 del protocollo sull'integrazione dell'*acquis* di Schengen nell'ambito dell'Unione europea, vista l'iniziativa della Repubblica portoghese (1), tenuto conto del parere del Parlamento europeo (2), considerando quanto segue:

1) La convenzione che istituisce un ufficio europeo di polizia (convenzione Europol) (3), la convenzione sull'uso dell'informatica nel settore doganale (4) e la convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni (convenzione di Schengen) (5) hanno istituito autorità di controllo comuni al fine di vigilare sulla corretta applicazione delle disposizioni relative alla protezione dei dati contenute in detti strumenti.

2) Per funzionare efficacemente limitando i costi, le autorità di controllo comuni dovrebbero essere coadiuvate da un unico segretariato indipendente «Protezione dati» che, nell'esercizio delle sue funzioni, è tenuto a seguire unicamente le istruzioni di tali autorità.

3) Per motivi pratici la gestione amministrativa del segretariato «Protezione dati» dovrebbe essere strettamente collegata al Segretariato generale del Consiglio, pur salvaguardando la propria indipendenza nell'esercizio delle sue funzioni.

4) Allo scopo di garantire tale indipendenza, le decisioni relative alla nomina e alla sospensione dall'incarico del capo del segretariato «Protezione dati» dovrebbero essere adottate dal Segretario generale aggiunto del Consiglio, in base a una proposta delle autorità di controllo comuni, e gli altri funzionari assegnati al segretariato «Protezione dati» dovrebbero seguire esclusivamente le istruzioni del capo del segretariato «Protezione dati».

5) Le spese amministrative del segretariato «Protezione dati» dovrebbero essere a carico del bilancio generale dell'Unione europea. L'Europol dovrebbe contribuire al finanziamento di talune spese connesse a riunioni riguardanti questioni relative all'attuazione della convenzione Europol.

6) Poiché la decisione 1999/438/CE del Consiglio, del 20 maggio 1999, concernente l'autorità di controllo comune istituita dall'articolo 115 della convenzione di applicazione dell'accordo di Schengen, del 14 giugno 1985, relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmata il 19 giugno 1990 (6), è superata dalla presente decisione, essa andrebbe pertanto abrogata e sostituita a decorrere dalla data di applicazione della presente decisione.

(7) Le autorità di controllo comuni esistenti hanno dichiarato di approvare i principi enunciati nella presente decisione,

(*) (2000/641/GAI) Pubblicato in G.U.C.E. del 24 ottobre 2000 L 271/1.

(1) GU C 141 del 19 maggio 2000, pag. 20.
(2) Parere reso il 21 settembre 2000 (non ancora pubblicato nella Gazzetta ufficiale).
(3) GU C 316 del 27 novembre 1995, pag. 2.
(4) GU C 316 del 27novembre 1995, pag. 33.
(5) GU L 239 del 22 settembre 2000, pag. 19.

DECIDE:

Articolo 1

Istituzione e compiti del segretariato «Protezione dati»

1. È istituito un segretariato (in seguito denominato: segretariato «Protezione dati ») delle autorità di controllo comuni istituite dalla convenzione che istituisce un ufficio europeo di polizia (convenzione Europol), dalla convenzione sull'uso dell'informatica nel settore doganale e dalla convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni (convenzione di Schengen).

2. Il segretariato «Protezione dati» assolve i compiti previsti per i segretariati delle autorità di controllo comuni quali stabiliti nei regolamenti interni di tali autorità.

Articolo 2

Segretario «Protezione dati»

1.Il segretariato «Protezione dati» è posto sotto la direzione di un segretario «Protezione dati »a cui viene garantita l'indipendenza nello svolgimento delle sue funzioni, e che è tenuto a seguire esclusivamente le istruzioni delle autorità di controllo comuni e dei loro presidenti. Il Segretario generale aggiunto del Consiglio nomina per un periodo di tre anni, in base a una proposta delle autorità di controllo comuni, il segretario «Protezione dati». Il suo mandato è rinnovabile.

2. Il segretario «Protezione dati» è scelto tra persone che siano cittadini dell'Unione europea, in pieno possesso dei diritti civili e politici, che abbiano l'esperienza e la capacità necessarie per svolgere le funzioni in questione e che offrano piena garanzia di indipendenza. Egli si astiene da qualsiasi azione incompatibile con le sue funzioni e, durante il periodo del suo mandato, non svolge un'altra attività professionale retribuita o non retribuita. Dopo la cessazione delle sue funzioni, egli rispetta i doveri di onestà e riserbo per quanto riguarda l'accettazione di funzioni e vantaggi.

3. Il segretario «Protezione dati» è sospeso dall'incarico dal Segretario generale aggiunto del Consiglio, in base a una proposta delle autorità di controllo comuni, qualora egli non soddisfi più le condizioni necessarie per l'esercizio delle sue funzioni o abbia commesso una colpa grave.

4. Oltre che per la normale procedura di sostituzione alla scadenza del suo mandato, per decesso o per sospensione dall'incarico a norma del paragrafo 3, le funzioni del segretario «Protezione dati» cessano allorché le sue dimissioni prendono effetto. In caso di cessazione del mandato e i dimissioni, egli mantiene le proprie funzioni, a richiesta delle autorità di controllo comuni, finché non viene sostituito.

5. Sia durante che dopo la cessazione del suo mandato, il segretario «Protezione dati» è tenuto al segreto professionale in merito a informazioni riservate di cui è venuto a conoscenza nell'assolvere le sue funzioni.

6. Durante il periodo del suo mandato, il segretario «Protezione dati» è soggetto, salvo disposizione contraria della presente decisione, alle norme che si applicano alle persone aventi lo status di agente temporaneo ai sensi dell'articolo 2, lettera a) del regime applicabile agli altri agenti delle Comunità europee (7), compresi gli articoli da 12 a 15 e 18 del protocollo sui privilegi e sulle immunità delle Comunità europee. Il segretario «Protezione dati» è inquadrato nella categoria A e il grado e lo scatto ai quali egli è impiegato sono determinati in base ai criteri applicabili ai funzionari e altri agenti delle Comunità. Se la persona nominata è già un funzionario delle Comunità, essa è comandata per il periodo del suo mandato nell'interesse del servizio ai sensi dell'articolo 37, lettera a), primo trattino dello statuto dei funzionari delle Comunità europee (statuto)(7). La prima frase dell'ultimo paragrafo dell'articolo 37 dello statuto si applica fatto salvo il paragrafo 1 del presente articolo.

Articolo 3

Personale

1. Il segretariato «Protezione dati» è dotato del personale necessario all'espletamento dei suoi compiti. I membri del personale assegnati al segretariato «Protezione dati » occupano posti inclusi nell'elenco dei posti aggiunti alla sezione del bilancio generale dell'Unione europea relativa al Consiglio.

(6) GU L 176 del 10 luglio 1999, pag. 34.

(7) GU L 56 del 4 marzo 1968, pag.1. Regolamento modificato da ultimo dalla comunicazione della Commissione (GU C 60 del 2 marzo1999, pag.11).

2. Nell'esercizio delle loro funzioni, i membri del personale di cui al paragrafo 1 sono soggetti esclusivamente alle istruzioni del segretario «Protezione dati» e delle autorità di controllo comuni o dei loro presidenti. In tale contesto, essi non possono chiedere né accettare istruzioni da alcun governo, autorità, organizzazione o persona, ma solo dal segretario «Protezione dati» e dalle autorità di controllo comuni o dai loro presidenti.

3. Fatto salvo il paragrafo 2, il personale assegnato al segretariato «Protezione dati» è soggetto ai regolamenti e alle regolamentazioni applicabili ai funzionari e agli altri agenti delle Comunità europee. Per quanto riguarda l'esercizio dei poteri conferiti all'autorità che ha il potere di nomina dallo statuto dei funzionari delle Comunità europee e dal regime applicabile agli altri agenti delle Comunità europee, il personale è soggetto alle stesse norme applicabili ai funzionari e agli altri agenti delle Comunità europee.

Articolo 4

Supporto amministrativo

1. Il Segretariato generale del Consiglio fornisce gli uffici e il materiale necessari all'espletamento dei compiti del segretariato «Protezione dati», nonché le strutture e i servizi necessari allo svolgimento delle riunioni delle autorità di controllo comuni nei locali del Consiglio, incluso un servizio di interpretazione.

2. Per quanto concerne le riunioni che si terranno nei locali del Consiglio le presidenze delle autorità di controllo comuni ne stabiliscono il calendario, previo accordo della presidenza del Consiglio.

Articolo 5

Finanziamento

1. Le spese amministrative generali del segretariato «Protezione dati» (in particolare, spese di materiale, retribuzioni, indennità e altre spese riguardanti il personale) sono imputate alla sezione del bilancio generale dell'Unione europea relativa al Consiglio.

2. I costi direttamente connessi con le riunioni sono a carico:

— del Consiglio, nel caso di riunioni nei locali del Consiglio riguardanti questioni relative all'attuazione delle disposizioni della convenzione di Schengen, spese di viaggio connesse con missioni di controllo presso il C.SIS o riunioni riguardanti questioni relative all'attuazione della convenzione sull'uso dell'informatica nel settore doganale,

— dell'Europol, nel caso di riunioni riguardanti questioni relative all'attuazione della convenzione Europol.

Articolo 6

Disposizioni finali

1. La presente decisione entra in vigore il giorno successivo all'adozione da parte del Consiglio.
Essa si applica dal 1 settembre 2001.

2. A decorrere dalla data di entrata in vigore della presente decisione, possono essere adottate le decisioni e gli atti necessari alla sua attuazione. Essi non producono effetti prima della data di applicazione della presente decisione.

3. Alla data di applicazione della presente decisione risulta abrogata la decisione 1999/438/CE, che continua tuttavia ad applicarsi alle spese derivanti da eventi antecedenti alla suddetta data.

Fatto a Lussemburgo, addì 17 ottobre 2000.

RICHIAMI IPERTESTUALI

Per esigenze di spazio i documenti riportati in questa sezione sono indicati solo con il relativo frontespizio, accompagnato dall'indicazione del sito web dove sono interamente riportati

129. TUTELA DELLA VITA PRIVATA SU INTERNET (*)

ARTICOLO 29 - GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI

5063/00/IT/DEF.
WP 37

Documento di lavoro

Tutela della vita privata su Internet
- Un approccio integrato dell'EU alla protezione dei dati on-line- (*)

adottato il 21 novembre 2000

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37it.pdf

130.

PARERE 3/2000 SUL DIALOGO EU/USA CONCERNENTE L'ACCORDO SULL'APPRODO SICURO (*)

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI - ART. 29

5019/00/IT/DEF.
WP 31

GRUPPO DI LAVORO PER LA PROTEZIONE DEGLI INDIVIDUI PER QUANTO RIGUARDA IL TRATTAMENTO DEI DATI PERSONALI

Parere 3/2000
sul dialogo EU/USA concernente
l'accordo sull'Approdo sicuro (*)

Approvato il 16 marzo 2000

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp31it.pdf

131. PARERE 4/2000 SUL LIVELLO DI TUTELA DEI DATI OFFERTO DAI PRINCIPI DELL'"APPRODO SICURO" (*)

GRUPPO DI LAVORO ARTICOLO 29 SULLA PROTEZIONE DEI DATI

CA07/434/00/IT
WP 32

Gruppo di lavoro articolo 29 sulla protezione dei dati

Parere 4/2000
sul livello di tutela dei dati offerto dai principi dell'"approdo sicuro" (Safe Harbor) (*)

adottato il 16 maggio 2000

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp32it.pdf

OPINION 1/2001 ON THE DRAFT COMMISSION DECISION ON STANDARD CONTRACTUAL CLAUSES (*)

132.

ARTICLE 29 - DATA PROTECTION WORKING PARTY

5102/00/EN
WP 38

Opinion 1/2001 on

the Draft Commission Decision on Standard Contractual Clauses for the transfer of Personal Data to third countries under Article 26(4) of Directive 95/46

(draft distributed to the Working Party on 17 January, 2001) (*)

Adopted on 26th January 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp38en.pdf

133. PARERE 2/2001 SUL LIVELLO DI ADEGUATEZZA DEL PERSONAL INFORMATION AND ELECTRONIC DOCUMENTS ACT (*)

ARTICOLO 29 - GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI

5109/00/IT
WP 39

Parere 2/2001 sul
Livello di adeguatezza del
Personal Information and Electronic Documents Act
(Legge sui dati personali e i documenti elettronici) canadese (*)

Adottato il 26 gennaio 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp39it.pdf

PARERE 3/2001 SUL LIVELLO DI PROTEZIONE DELLA LEGGE 2000 DI MODIFICA DELLA LEGGE AUSTRALIANA SULLA TUTELA DELLA VITA PRIVATA (*)

134.

ARTICOLO 29 – GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

5095/00/IT/Rev. 1

WP 40

Articolo 29 – Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

Parere 3/2001
sul livello di protezione della legge 2000 di modifica della legge australiana sulla tutela della vita privata (settore privato) (*)

Adottato il 26 gennaio 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40it.pdf

135. PARERE 4/2001 SUL PROGETTO DI CONVENZIONE SULLA CIBERCRIMINALITÀ DEL CONSIGLIO D'EUROPA (*)

ARTICOLO 29 - GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

5001/01/IT/def.
WP 41

Parere 4/2001

sul progetto di convenzione sulla cibercriminalità del Consiglio d'Europa (*)

Adottato il 22 marzo 2001

(*) http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41it.pdf

REGOLAMENTO (CE) N. 45/2001

DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, DEL 18 DICEMBRE 2000, CONCERNENTE LA TUTELA DELLE PERSONE FISICHE IN RELAZIONE AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELLE ISTITUZIONI E DEGLI ORGANISMI COMUNITARI, NONCHÉ LA LIBERA CIRCOLAZIONE DI TALI DATI (*)

136.

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la proposta della Commissione(1),

visto il parere del Comitato economico e sociale(2),

deliberando secondo la procedura di cui all'articolo 251 del trattato(3), considerando quanto segue:

(1) L'articolo 286 del trattato stabilisce che gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi comunitari.

(2) Un sistema di protezione dei dati personali richiede, per esser completo, non solo che si istituiscano diritti per le persone cui tali dati si riferiscono e obblighi per chi li elabora, ma anche adeguate sanzioni per i trasgressori e un'autorità di controllo indipendente.

(3) L'articolo 286, paragrafo 2 del trattato prescrive l'istituzione di un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari.

(4) L'articolo 286, paragrafo 2 del trattato prescrive l'adozione, se del caso, di tutte le altre pertinenti disposizioni.

(5) È necessario un regolamento per accordare alle persone fisiche diritti giuridicamente tutelati e per chiarire gli obblighi dei responsabili del trattamento dei dati in seno alle istituzioni e agli organismi comunitari, nonché per istituire un'autorità di controllo indipendente incaricata di sorvegliare il trattamento dei dati personali effettuato dalle istituzioni e dagli organismi comunitari.

(6) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati(4), è stato consultato

(7) Le persone che possono essere oggetto di tutela sono quelle i cui dati personali sono trattati da istituzioni o organismi comunitari, in qualsiasi circostanza, ad esempio in quanto impiegate presso tali istituzioni o organismi.

(8) È necessario applicare i principi della protezione dei dati a tutte le informazioni relative ad una persona identificata o identificabile. Per stabilire se una persona è identificabile, occorre tener conto di tutti gli strumenti ragionevolmente impiegati dal responsabile del trattamento dei dati o da chiunque altro al fine d'identificare detta persona. Non occorre applicare detti principi di protezione ai dati resi anonimi in modo sufficiente ad impedire l'identificazione dell'interessato.

(9) La direttiva 95/46/CE fa obbligo agli Stati membri di garantire la tutela delle libertà e dei diritti fondamentali delle persone fisiche e particolarmente del diritto alla vita privata con riguardo al trattamento dei dati personali, al fine di assicurare la libera circolazione dei dati personali nella Comunità. [...]

(*) Gazzetta Ufficiale n. L 008 del 12/01/2001 pag. 0001 - 0022; http://europa.eu.int/eur-lex/it/lif/dat/2001/it_301R0045.html

EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)
COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE (PC-CY)
137. *FINAL ACTIVITY REPORT*

List of contact points in certain negotiating States

Strasbourg, 25 May 2001 Restricted
CDPC (2001) 2 rev

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

Committee of Experts on Crime in Cyber-Space
(PC-CY)

FINAL ACTIVITY REPORT

Prepared by: Committee of Experts on Crime in Cyber-Space (PC-CY)

Submitted to: European Committee on Crime Problems (CDPC) at its 50th plenary session (18 - 22 June 2001)

DRAFT CONVENTION ON CYBER-CRIME

AND

EXPLANATORY MEMORANDUM RELATED THERETO

Secretariat Memorandum
prepared by the
Directorate General of Legal Affairs

[...]

(*) http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm

138. *GUIDING PRINCIPLES FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE COLLECTION AND PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE (*)*

GUIDING PRINCIPLES FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE COLLECTION AND PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE

Document prepared by Mr. Giovanni BUTTARELLI
(Secretary General of the Supervisory Authority on Data Protection - il Garante - Italy)

and presented by

the Directorate General I
(Legal Affairs)

Notice

The importance of the phenomenon of surveillance and surveillance activities by technical means which are becoming increasingly sophisticated demands serious thought at both national and international level with regard to the advantages and risks for democratic societies and individuals.

Several states have undertaken work in this field, even considering it necessary to draft specific legislative provisions on data protection in the field of (video-)surveillance.

In this context, the Council of Europe wishes to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe asked a consultant, Dr Giovanni BUTTARELLI, to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context.

It was therefore wished to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account when preparing specific legislative provisions on data protection with relation to video surveillance. These principles could, where appropriate, be applied to other forms or technical means of surveillance after making any necessary adjustments to them.

At the present stage the Report and the Guiding Principles are to be the subject of public consultation. Any comments on these texts may be transmitted to the Secretariat General of the Council of Europe before 21st January 2001, at the following address : judith.ledoux@coe.int.

FOREWORD

Many public and private entities have been increasingly using surveillance systems for various purposes and in different sectors, by controlling, in particular, movement of persons and goods, access to property as well as events, situations and conversations ö whether by telephone, electronic networks or at a physical location.

Surveillance systems often result into the collection of personal data even though their collection and/or storage is sometimes not aimed at by the surveillance data controller.

A considerable portion of these activities are performed by means of video surveillance devices, which raises specific issues as regards data protection.

Indeed, the data collected during video surveillance activities consist mainly in images and sound which either identify or allow identifying data subjects, whether directly or not, in addition to monitoring their conduct.

[...]

(*) http://www.coe.fr/dataprotection/e%20principles%20surveillance.htm

PROTECTION OF PERSONAL DATA WITH REGARD TO SURVEILLANCE
Report by Mr. Giovanni BUTTARELLI,
139. Secretary General of the Italian Data Protection Authority (Italy)

Protection of personal data with regard to surveillance

Report by Mr. Giovanni BUTTARELLI,

Secretary General of the Italian Data Protection Authority (Italy)

Notice

The importance of the phenomenon of surveillance and surveillance activities by technical means which are becoming increasingly sophisticated demands serious thought at both national and international level with regard to the advantages and risks for democratic societies and individuals.

Several states have undertaken work in this field, even considering it necessary to draft specific legislative provisions on data protection in the field of (video-)surveillance.

In this context, the Council of Europe wishes to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe asked a consultant, Dr Giovanni BUTTARELLI, to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context.

It was therefore wished to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account when preparing specific legislative provisions on data protection with relation to video surveillance. These principles could, where appropriate, be applied to other forms or technical means of surveillance after making any necessary adjustments to them.

At the present stage the Report and the Guiding Principles are to be the subject of public consultation. Any comments on these texts may be transmitted to the Secretariat General of the Council of Europe before 21st January 2001, at the following address : judith.ledoux@coe.int.

1) FOREWORD

Any research and/or report on surveillance is related to the technological development of control systems and is therefore to be considered in connection with the relevant historical context.

[...]

(*) http://www.coe.fr/dataprotection/eReport%20Buttarelli.htm

DIRETTIVA 2000/31/CE

DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DELL'8 GIUGNO 2000 RELATIVA A TALUNI ASPETTI GIURIDICI DEI SERVIZI DELLA SOCIETÀ DELL'INFORMAZIONE, IN PARTICOLARE IL COMMERCIO ELETTRONICO, NEL MERCATO INTERNO ("DIRETTIVA SUL COMMERCIO ELETTRONICO") (*)

140.

Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico")

(Gazzetta ufficiale n. L 178 del 17/07/2000 PAG. 0001 – 0016)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 47, paragrafo 2, l'articolo 55 e l'articolo 95,

vista la proposta della Commissione(1)

visto il parere del Comitato economico e sociale(2)

deliberando in conformità della procedura di cui all'articolo 251 del trattato(3),

considerando quanto segue:

(1) L'Unione europea intende stabilire legami sempre più stretti tra gli Stati ed i popoli europei, garantire il progresso economico e sociale. Secondo l'articolo 14, paragrafo 2, del trattato, il mercato interno implica uno spazio senza frontiere interne, in cui sono garantiti la libera circolazione delle merci e dei servizi, nonché il diritto di stabilimento. Lo sviluppo dei servizi della società dell'informazione nello spazio senza frontiere interne è uno strumento essenziale per eliminare le barriere che dividono i popoli europei.

(2) Lo sviluppo del commercio elettronico nella società dell'informazione offre grandi opportunità per l'occupazione nella Comunità, in particolare nelle piccole e medie imprese. Esso faciliterà la crescita delle imprese europee, nonché gli investimenti nell'innovazione ed è tale da rafforzare la competitività dell'industria europea a condizione che Internet sia accessibile a tutti.

(3) Il diritto comunitario e le caratteristiche dell'ordinamento giuridico comunitario costituiscono una risorsa essenziale affinché i cittadini e gli operatori europei possano usufruire appieno e al di là delle frontiere delle opportunità offerte dal commercio elettronico. La presente direttiva si prefigge pertanto di garantire un elevato livello di integrazione giuridica comunitaria al fine di instaurare un vero e proprio spazio senza frontiere interne per i servizi della società dell'informazione.

(4) È importante assicurare che il commercio elettronico possa beneficiare pienamente del mercato interno e pertanto che venga raggiunto un alto livello di integrazione comunitaria, come con la direttiva 89/552/CEE del Consiglio,

[...]

(*) Gazzetta ufficiale n. L 178 del 17/07/2000 pp. 0001 – 0016; http://europa.eu.int/eur-lex/it/lif/2000/it_300L0031.html

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

CHE ISTITUISCE UN QUADRO NORMATIVO COMUNE PER LE RETI E I SERVIZI DI COMUNICAZIONE ELETTRONICA (*)

141.

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 12.7.2000
COM(2000) 393 definitivo

2000/0184 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (*)

(presentata dalla Commissione)

(*) http://europa.eu.int/eur-lex/it/com/pdf/2000/it_500PC0393.pdf

DEC. 2000/520/CE DEL 26 LUGLIO 2000

142. *DECISIONE DELLA COMMISSIONE A NORMA DELLA DIRETTIVA 95/46/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO SULL'ADEGUATEZZA DELLA PROTEZIONE OFFERTA DAI PRINCIPI DI APPRODO SICURO E DALLE RELATIVE "DOMANDE PIÙ FREQUENTI" (FAQ) IN MATERIA DI RISERVATEZZA PUBBLICATE DAL DIPARTIMENTO DEL COMMERCIO DEGLI STATI UNITI (*)*

Dec. 2000/520/CE del 26 luglio 2000

Decisione della Commissione a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "Domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti (*)

La Commissione delle Comunità europee,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) A norma della direttiva 95/46/CE, gli Stati membri sono tenuti a consentire il trasferimento verso un paese terzo di dati personali soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se vengono rispettate, prima del trasferimento stesso, norme di attuazione delle altre disposizioni della direttiva adottate dagli Stati membri.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(3) A norma della direttiva 95/46/CE, il livello di protezione dei dati personali deve essere valutato con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni; il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali (4) ha fornito indicazioni circa le modalità di effettuazione di tali valutazioni (5).

(4) Tenuto conto della diversità degli approcci in materia di tutela dei dati nei Paesi terzi, la valutazione dell'adeguatezza e le decisioni a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE devono essere eseguite in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti dei Paesi terzi o fra questi, qualora sussistano condizioni analoghe, e da non costituire ostacoli dissimulati agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

[...]

(*) G.U.C.E. 25 agosto 2000, n. L 215; http://europa.eu.int/eur-lex/it/lif/dat/2000/it_300D0520.html

DEC. 2000/518/CE DEL 26 LUGLIO 2000

DECISIONE DELLA COMMISSIONE RIGUARDANTE L'ADEGUATEZZA DELLA PROTEZIONE DEI DATI PERSONALI IN SVIZZERA A NORMA DELLA DIRETTIVA 95/46/CE (*)

143.

Dec. 2000/518/CE del 26 luglio 2000

Decisione della Commissione riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE (*)

La Commissione delle Comunità europee,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) La direttiva 95/46/CE prescrive agli Stati membri di assicurarsi che i trasferimenti di dati personali verso un determinato paese terzo abbiano luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se le leggi dello Stato membro che attuano le altre disposizioni della direttiva sono rispettate prima del trasferimento.

(2) La Commissione può constatare che un Paese terzo garantisce un livello di protezione adeguato. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(3) A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma della direttiva, ha fornito indicazioni sull'effettuazione di tali valutazioni (1).

(4) Tenuto conto dei distinti modi in cui vengono protetti i dati nei Paesi terzi, sia la verifica dell'adeguatezza di tale protezione, sia l'applicazione di ogni decisione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE, devono avvenire in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti di o tra Paesi terzi in cui sussistono condizioni analoghe e da non costituire ostacoli occulti agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

(5) Nella Confederazione svizzera vigono in materia di protezione dei dati personali norme di legge che producono effetti giuridici vincolanti a livello federale e cantonale.

[...]

(*) G.U.C.E. 25 agosto 2000, n. L 215; http://europa.eu.int/eur-lex/it/lif/2000/it_300D0518.html

144.

DEC. 2000/519/CE DEL 26 LUGLIO 2000

DECISIONE DELLA COMMISSIONE RIGUARDANTE L'ADEGUATEZZA DELLA PROTEZIONE DEI DATI PERSONALI IN UNGHERIA A NORMA DELLA DIRETTIVA 95/46/CE (*)

Dec. 2000/519/CE del 26 luglio 2000

Decisione della Commissione riguardante l'adeguatezza della protezione dei dati personali in Ungheria a norma della direttiva 95/46/CE (*)

La Commissione delle Comunità europee,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) La direttiva 95/46/CE prescrive agli Stati membri di assicurarsi che i trasferimenti di dati personali verso un determinato paese terzo abbiano luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se le leggi dello Stato membro che attuano le altre disposizioni della direttiva sono rispettate prima del trasferimento.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(3) A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma della direttiva, ha fornito indicazioni sull'effettuazione di tali valutazioni (1).

(4) Tenuto conto dei distinti modi in cui vengono protetti i dati nei Paesi terzi, sia la verifica dell'adeguatezza di tale protezione, sia l'applicazione di ogni decisione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE, devono avvenire in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti di o tra Paesi terzi in cui sussistono condizioni analoghe e da non costituire ostacoli occulti agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

(5) In Ungheria vigono in materia di protezione dei dati personali norme di legge che producono effetti giuridici vincolanti.

[...]

(*) G.U.C.E. 25 agosto 2000, n. L 215; http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp36it.pdf

PARERE 7/2000

SULLA PROPOSTA DELLA COMMISSIONE EUROPEA DI DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVA AL TRATTAMENTO DEI DATI PERSONALI E ALLA TUTELA DELLA VITA PRIVATA NEL SETTORE DELLE COMUNICAZIONI ELETTRONICHE DEL 12 LUGLIO 2000 COM (2000) 385 (*)

145.

5042/00/EN/FINAL
WP36

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

Parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 COM (2000) 385

adottato il 2 novembre 2000

Il gruppo di lavoro 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, paragrafi 1 a) e 3 della direttiva,

viste le relative norme di procedura e in particolare gli articoli 12, 13 e 14,

ha adottato il presente parere 7/2000:

1. Introduzione

Nell'ambito della revisione del 1999 del quadro normativo comunitario in materia di telecomunicazioni 2, il 12 luglio 2000 la Commissione ha adottato alcune proposte relative alle nuove direttive nel settore delle comunicazioni elettroniche intese a sostituire il quadro normativo esistente. Una delle cinque proposte previste riguarda una revisione della direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. In seguito al parere 2/2000 concernente la revisione generale del quadro giuridico delle telecomunicazioni 3, il gruppo di lavoro per la tutela della vita privata intende ora contribuire alle discussioni sul progetto di direttiva in seno al Parlamento europeo e al Consiglio.

2. Analisi del progetto di direttiva

Le preoccupazioni principali del gruppo riguardano il trattamento dei dati personali attraverso Internet, che deve essere affrontato in modo più specifico, nonché i nuovi problemi derivanti dalla liberalizzazione del mercato delle telecomunicazioni.

Articolo 1 - Finalità e ambito di applicazione
Articolo 3 – Servizi interessati

Il gruppo prende atto del fatto che non sono previsti cambiamenti per quanto attiene all'ambito di applicazione e ai servizi interessati. Le disposizioni specifiche della nuova direttiva riguarderebbero pertanto la fornitura di servizi di comunicazione elettronica accessibili al pubblico sulle reti pubbliche di comunicazioni nella

[...]

(*) http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp36it.pdf

REGOLAMENTO (CE) N. 2725/2000

146. *DEL CONSIGLIO, DELL'11 DICEMBRE 2000, CHE ISTITUISCE L'"EURODAC" PER IL CONFRONTO DELLE IMPRONTE DIGITALI PER L'EFFICACE APPLICAZIONE DELLA CONVENZIONE DI DUBLINO (*)*

Regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino (*)

IL CONSIGLIO DELL'UNIONE EUROPEA,
visto il trattato che istituisce la Comunità europea, in particolare l'articolo 63, punto 1, lettera a),
vista la proposta della Commissione,
visto il parere del Parlamento europeo(1),
considerando quanto segue:

(1) Gli Stati membri hanno ratificato la convenzione di Ginevra, del 28 luglio 1951, relativa allo status dei rifugiati, modificata dal protocollo di New York del 31 gennaio 1967.

(2) Gli Stati membri hanno concluso la convenzione sulla determinazione dello Stato competente per l'esame di una domanda di asilo presentata in uno degli Stati membri delle Comunità europee, firmata a Dublino il 15 giugno 1990 (in seguito denominata: "la convenzione di Dublino")(2).

(3) Ai fini dell'applicazione della convenzione di Dublino è necessario determinare l'identità dei richiedenti asilo e delle persone fermate in relazione all'attraversamento irregolare delle frontiere esterne della Comunità. È inoltre auspicabile, ai fini di un'efficace applicazione della convenzione di Dublino e, in particolare, dell'articolo 10, paragrafo 1, lettere c) ed e), consentire a ciascuno Stato membro di accertare se uno straniero trovato illegalmente nel suo territorio abbia presentato domanda di asilo in un altro Stato membro.

(4) Costituendo le impronte digitali un elemento importante per la determinazione dell'identità esatta di tali persone, occorre istituire un sistema per il confronto dei dati relativi alle loro impronte digitali.

(5) A tal fine, è necessario istituire un sistema denominato "Eurodac", comprendente un'unità centrale, che opererà presso la Commissione e che gestirà una banca dati centrale informatizzata di dati sulle impronte digitali, e i mezzi telematici necessari per le trasmissioni tra gli Stati membri e la banca dati centrale.

(6) È altresì necessario invitare gli Stati membri a rilevare tempestivamente le impronte digitali di tutti i richiedenti asilo e di tutti gli stranieri che vengano fermati in relazione all'attraversamento irregolare della frontiera esterna di uno Stato membro, qualora costoro abbiano almeno 14 anni di età.

(7) È necessario dettare disposizioni precise in ordine alla trasmissione all'unità centrale dei dati relativi a tali impronte digitali, alla registrazione, nella banca dati centrale, dei dati suddetti e di altri dati pertinenti, alla loro memorizzazione, al loro confronto con altri dati relativi a impronte digitali, nonché in ordine alla trasmissione dei risultati di tali confronti e al congelamento ed alla cancellazione dei dati registrati. Dette disposizioni possono differire ed essere specificamente adattate per quanto riguarda altre categorie di stranieri.

[...]

(*) G.U.C.E. n. L 316 del 15/12/2000; http://europa.eu.int/eur-lex/it/lif/dat/2000/it_300R2725.html